





Privacy, security and resilience in mobile healthcare applications

Wenjun Lin ^a, Ming Xu^a, Jingyi He^b and Wenjun Zhang ^a

^aDepartment of Mechanical Engineering, University of Saskatchewan, Saskatoon, SK, Canada; ^bFaculty of Nursing, University of Alberta, Edmonton, Alberta, Canada

ABSTRACT

With the advent of mobile applications in health service systems, concerns such as security, privacy, usability, and resilience have been raised. We developed a system view of the concepts of security, privacy, resilience along with their relationship, and proposed a set of principles for designing a mobile application linking the resilience and security in privacy protection. Such study was not found in literature before. This system's view of privacy, security, and resilience has laid a foundation to develop a more effective service system. A case study is presented to illustrate how the proposed principles work in a mobile healthcare application.

ARTICLE HISTORY

Received 12 January 2021
Accepted 3 June 2021

KEYWORDS

Privacy; security; resilience; cloud; mobile application design; healthcare; scheduling

1. Introduction

Healthcare burden is one of the major social and economic problems around the world, especially in an ageing society, where it entails tremendous health expenses and labour resources. Traditional hospital-centric healthcare suffers from excessive in-hospital waiting times. One of the most complaint issues recorded is the dissatisfaction in the length of waiting time in hospitals. Patients are dissatisfied by the inconveniences and unavailable time of appointment slots, especially for patients with urgent needs. In some cases like emergency departments, if not dealt with effectively, the waiting time problem could lead to a huge loss of human life. Therefore, it is emerging to pose up-and-coming healthcare solutions to reduce the waiting time and release the heavy burden of the existing healthcare system.

Mobile applications, also known as 'apps', have been seen rapid growth with the release of affordable smart devices (e.g., smartphones, tablet computers). There is a massive opportunity for health service systems to take advantage of mobile apps to enhance the efficiency of healthcare information management systems and to improve the patients' service quality (Aceto, Persico, and Pescapé 2020; Lancharoen, Suksawang, and Naenna 2020; Li et al. 2019). On the flip side of the coin, concerns, such as security, privacy, usability and resilience, and so on, have limited the adoption of the technology (Al-Muhtadi et al. 2019; Hathaliya and Tanwar 2020). Since health information (e.g., phenomena, health condition, and emergency) is relatively sensitive for users, any

inappropriate disclosure may violate user privacy (Liang et al. 2012; Rahmadika and Rhee 2018). Users may also worry about their critical health data being tampered with when their health data are stored in untrusted cloud servers (Zhou et al. 2013; Loft et al. 2021). In addition, the mobile device is usually operated in a wireless environment and different devices have various hardware and operating systems (OSs) which might create compatibility issues that might cause system unavailability like data loss and a single point of failure (Lo'ai et al. 2015).

To cope with the issues above, in this paper we treat mobile apps, operating systems, databases, and their related communication services as a whole system called mobile network system (MNS). The infrastructure-substance (I-S) framework (Zhang and Lin 2010; Zhang and Van Luttervelt 2011; Zhang, Wang, and Lin 2019) along with a general modelling methodology for a system ontology (Cai et al. 2017; Wang et al. 2014; Zhang and Wang 2016) are used to build the system, in which an individual's privacy is secured in a highly resilient system. The remaining part of this paper is organised as follows. Section 2 provides an overview of studies related to security and resilience for privacy protection. Section 3 presents the MNS and a list of system design principles to achieve a high degree of resilience in privacy protection. Section 4 demonstrates the principles' application by a mobile app for hospital appointment scheduling. Finally, Section 5 concludes this paper with discussions of benefits and future works.

2. Background and literature review

2.1. Security of privacy protection

The NCVHS (National Committee on Vital and Health Statistics) definition of privacy (in a healthcare setting) is the user's right to 'control the acquisition, uses, or disclosures of his or her identifiable health data' (Collins 2006). A threat to user privacy is the possibility that his right to control his privacy is weakened or eliminated due to erroneous or malicious actions. When these threats are realised, the consequences can be severe: exposure of identifiable patient health data leading to loss of money or reputation, time spent recovering from medical identity theft, harm to health, or even death (Avancha, Baxi, and Kotz 2012). In this study, we study security specific to the protection of privacy, in other words, privacy security.

Several studies have been investigated on privacy security in mobile cloud computing environment. Zhang et al. (2009) developing an elastic application framework with a new application model and elasticity infrastructure. In this study, the elastic application is referred to as application which is hosted on one or more independent cloud servers. The choice of servers is depends on the resource requirements at the application launches. Such elasticity infrastructure reduces the server-side risks instead of the client-side ones with goals to give minimum security considerations to users. However, this also makes their framework heavily relying on the cloud platform and software stack. Huang et al. (2010) proposed a mobile cloud computing environment with a set of privacy protection services. For example, enforcing user-centred inter-media authentication, and isolating patient information, data protection in storage and transmission on server-side. Alpár, Hoepman, and Siljee (2011) developed an identity management model. The model ensures the privacy of data stored at privacy data providers to be well protected with

Encryption and steganography. A third-party service was also introduced to handle privacy data between service providers and clients. The same issue is addressed by Chen, Beaudoin, and Hong (2017) in three different aspects: applying a parallel process model, with theories of self-control and routine activity. The theories suggested that understanding how Internet scams work will help internet users to resist the desire for immediate monetary benefits. And as a consequence, the risk of privacy infringe can be avoided. Similar to Alpár, Hoepman, and Siljee (2011), they also suggested that both service provider and client needs to be involved to achieve comprehensive privacy protection. In the healthcare-related mobile-app development area, Al-Muhtadi et al. (2019) discussed the architecture of a typical mobile healthcare app, in which customised privacy levels are defined for the individuals participating in the system. They claimed the architecture achieves a more secure and private communication with a multi-cloud environment, especially for healthcare apps. Most recently, Khan and Reyad (2020) proposed a security model based on multi-agents to maintain and support the security and privacy of healthcare systems. This system uses agents to maintain security and privacy while accessing the E-health data between the users. By generalising the idea with attention to the user side or client side, human factors matter in information processing and management (Ogbeyemi et al. 2020).

2.2. Resilience

The concept of resilience was originally referred to tissue recovery from damages. Later, the concept has been expanded into the field of the natural ecosystem and material science, and a human-centred system or a sociology system (Holling 1973). Zhang and Lin (2010) maybe among one of the earliest researchers who study the resilience of data system. In their work, derived data was described for a data system recovery. This mechanism is similar with the idea of the derived attribute in data management (Zhang 1994), and the idea of functional redundancy in mechanical systems (Zhang and Van Luttervelt 2011). It is noted that a general categorisation of different types of redundancy in the context of system and system design may be referred to (Fan et al. 2015; Sun et al. 2011). Woods (2015) considered resilience as a property that covers robustness. In this work, resilience is spanned by three attributes that are robustness, recoverability and adaptation. This understanding of resilience is a mixing of means (adaption) and end (resilience and recoverability and as well as mixing of the three distinct concepts (reliability, robustness, and resilience) according to (Zhang and Van Luttervelt 2011) and is not conducive to developing independent theory for resilience. Further, efforts have been taken to establish the resilient digital and information system; particularly a method called forward secrecy was developed to enhance untended wireless networks from intrusion (Di et al. 2012). In this study, a method was developed to enforce the resource or function redundancy and ensures the security feature for the entire system, which is similar to the derived information mechanism and redundancy as proposed by zhang2010principle. In Taleb, Ksentini, and Sericola (2016)'s work, an idea of relocating and restoring lost state data from existing resources is used on the next generation mobile system development. Techniques like visualised network and mobility management were used in place of redundancy physical equipment.

2.3. Knowledge gaps and limitations of the existing work

From literature review in the previous sections, we found some knowledge gaps in works related to privacy, security and resilience. In terms of the security of privacy, the state of knowledge appears to lack a system view of the problem. Without clarification of the data content, the data access restriction, the context semantics, and the access principle cannot be explored thoroughly. Indeed, as Solove (2002) pointed out that in characterising the privacy of a piece of data, the context is absent.

The understanding of resilience from most of the existing work is related to one or more system elements. A system view of elements is lacking, except the work from Zhang and Lin (2010). As such, only element-wise changes will happen, and a possible cascade effect of privacy violation is absent.

To overcome those gaps and limitations, the I-S framework (Zhang and Lin 2010) can be adopted. This framework describes a system with an infrastructure sub-system and their substance sub-systems. The substance sub-systems 'flows' over the infrastructure subsystem. Therefore, in the I-S system, a change can be made on different levels for example, at the infrastructure sub-system level, or the substance sub-system level, or a combination of levels. More discussions on the I-S system will be given in Section 3.1. Besides, there are several different versions of definitions of resilience in literature. In this paper, the definition of resilience from Zhang's group (Zhang and Lin 2010; WaWang et al. 2018, 2014) is taken. It describes a system's capability of recovering from failures on the system's own resource. The failures include partial damage of the infrastructure, disruption of normal supply of resources, and shortage of supplied goods or services with respect to demands. This definition emphasises on the difference between robustness and resilience to a general system, a supply system or a service system (Wang et al. 2014).

3. MNS design principles

3.1. I-S framework of MNS

Based on the I-S framework, a general service system includes an infrastructure layer and a substance layer. In the MNS, the infrastructure layer is terminal and back-end, and the substance layer is signal and data. User sensory organs (video, audio, etc.) are used to fulfil the system function and provide user data (both information and knowledge) (Zhang 1994). In other words, the infrastructure processes the substance and allocates the data (Figure 1). For example, a cellphone station and its related infrastructures transmit voice message flow between two mobile phones to fulfil the function as a real-time voice call.

Figure 2 illustrates the relationship of Privacy, Security, and Resilience (PSR) in the MNS from the I-S framework prospect. Privacy in MNS is related to the data which can be used to identify an individual entity, for example, a person, or a group, and the data owned by one entity should not be shared by another entity. Therefore, in the I-S framework, privacy is related to the substance system. Besides, security in this study is specific to the protection of privacy, data of which are stored in the substance system and processed by the infrastructure system. Therefore, security is one of the functions of a system (e.g., MNS). Further, the system resilience is regarding that once a system's security function is partially damaged, the system can recover it in an allowable time and with an allowable cost by itself. Finally, to make the MNS run, energy or power must be available, which is an

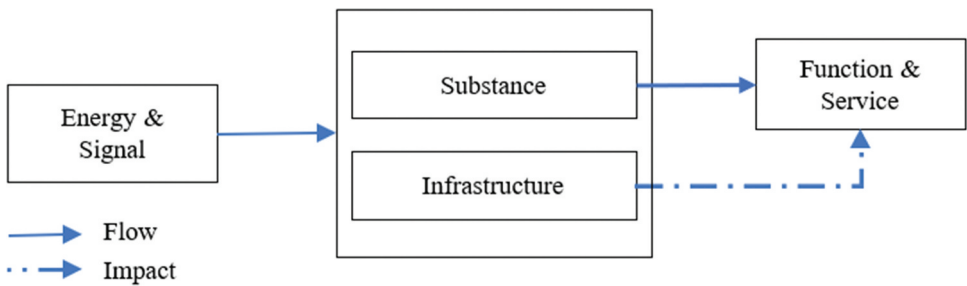


Figure 1. The I-S frameworks for MNS.

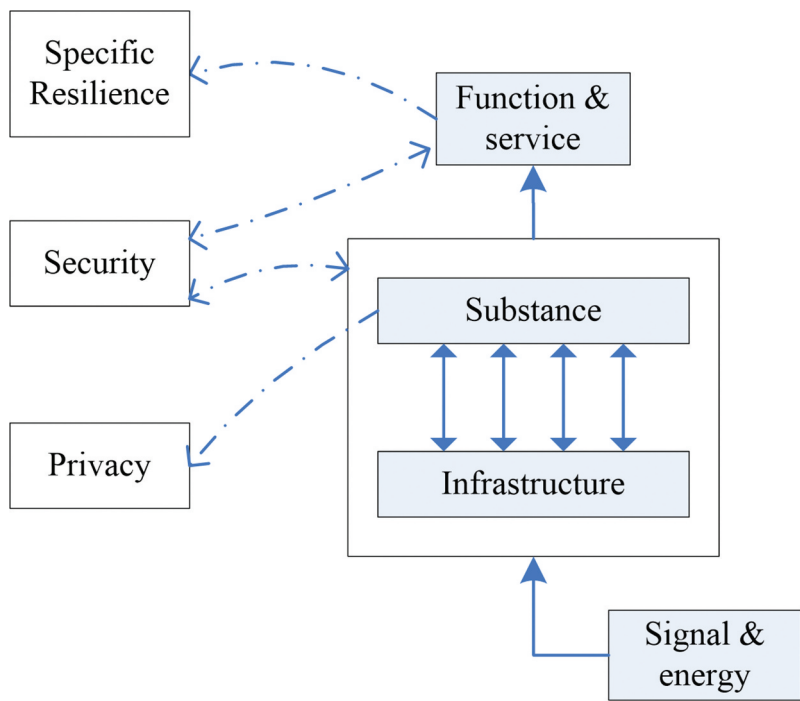


Figure 2. The I-S view of the relationship among PSR for MNS.

external resource to a service system (e.g., MNS), as well as external signals (or data), which represent the semantics of privacy.

3.2. Design principles for security in MNS

Based on Figure 2, we will discuss the design principles for security from three aspects: the infrastructure, substance and energy.

Infrastructure aspect

- Rule I-1: Fulfil the functional and constraint requirements with well evaluated, and widely accepted options;
- Rule I-2: Evaluate and test new algorithms before implementations;

- Rule I-3: Choose an adaptive app style based on the function and security requirements;
- Rule I-4: Evaluate a platform, at local servers or clouds, with both security and functional requirements. As both service and data storage of mobile apps are moving towards the clouds, the security obligation needs to be transferred as well due to different cloud platforms has different service requirements.

Substance aspect

- Rule S-1: Identify and classify privacy information into two categories: attribute and relationship. The attributes refer to those that define an entity. The relationship refers to information that links one entity to another entity or others;
- Rule S-2: Specify the responsibilities of users and systems to determine forms to enhance. There are two forms: legal binding and non-legal binding. Legal binding involves more steps to establish, which often makes the user shy away or has a poor understanding of terms and conditions. Therefore, non-legal binding could be chosen as a trade-off;
- Rule S-3: Minimise the information required from users. More information has a higher cost of losing privacy information;
- Rule S-4: Determine appropriate techniques and algorithms for the security of private information, for example, encryption and certificate verification;
- Rule S-5: Plan for both data storage and data processing security strategies. There is a trade-off between data storage security and processing efficiency. Local storage has a higher degree of security but may have insufficient data processing power. While cloud storage may have advantages of data processing efficiency, it might have a higher risk of a data breach.
- Rule S-6: Balance among encryption, authentication, authorisation, usability, storage strategy, encryption, and computational capability for an acceptable security expectation;
- Rule S-7: Develop a life-time management strategy against privacy abuse. Besides the techniques, human and cultural factors need to be taken into considerations.

Energy aspect

- Rule E-1: Check the energy (e.g., battery) level before running any critical process, like, heavy encryption, heavy algorithm calculation, or mass data transfer. The system should be designed to alert users of a low battery situation;
- Rule E-2: Monitor the status of the energy source closely considering environmental factors such as battery temperature to facilitate a pro-active energy plan.

3.3. Design principles for resilient security in MNS

In MNS, resilience refers to the system's ability to keep the functions of the system at an acceptable level subject to perturbations or mishaps. To provide resilience to the security functions designed based on rules in [Section 3.2](#), five axioms in design need to be followed.

Axiom 1: Redundant resources for critical security components. Resources for MNS include function, capacity and infrastructure.

- Rule R-1: Identify critical functions and design redundancy. For instance, data transportation is a crucial function for a mobile app. The tunnel for data transportation can be either 4G (4th Gen cellular network) or 2G (2nd Gen cellular network), and this forms a redundancy;

- Rule R-2: Arrange the redundant capacity regarding the critical functions. Capacity refers to the availability of electricity, computation, storage or bandwidth. Take data storage as an example. In complement to a remote database, redundancy of storage capacity would be having a local database as a duplicate safeguard to avoid a loss of data;
- Rule R-3: Design the redundant infrastructure for critical functions. Multiple back-end services are involved in a mobile apps based system. They include the clouds, web server, database server and cellular telephone network equipment. Their redundancy is to ensure a reliable and robust service;

Axiom 2: Effective management of redundancy. A resilient MNS needs to decide when and how to reconfigure a system for a lost function or replace a failed sector with redundant resources. In other words, a mechanism to manipulate the redundant resources is required.

- Rule R-4: List attributes, types, and availability status of redundant resources first;
- Rule R-5: Create clear instructions, like algorithm or management rules, about how and when to replace the resources as well as how to work with the re-configured system;

Axiom 3: Monitoring of system performance.

- Rule R-6: Keep sensing key system status concerning security functions. For example, Mozilla (n.d.) introduced a web Application Programme Interface, “navigator.battery”, to enquire system’s battery charge level and whether the device is charging. In this way, it is possible to decide whether or how to run a programme regarding battery status. Further, necessary status information is recorded for forecasting system errors;

Axiom 4: Error forecasting and handling mechanism. Mobile apps errors are a combined result from design, coding, operation, as well as resource utilisation. Suppose that an app has a low success rate to access a remote database due to uncontrollable factors. The remote database login operation should be treated as a separate procedure. By decoupling the login procedure, other functions can be operated with improved robustness.

- Rule R-7: Forecast and locate possible vulnerability from algorithms, logical procedure, and the relationship between different system components;
- Rule R-8: Predefine counter-measures for error situations;

Axiom 5: Software version control for system evolution.

- Rule R-9: Update software, like a mobile app, as a counter-measure against external attacks. By updating, the old violable programme is replaced by a new robust one. To effectively manage the updates, a version control mechanism needs to be implemented in an app.

4. Case study

To explain how the design principles may be applied to designing an MNS which processes healthcare information, a mobile app is demonstrated here. The app is developed for outpatients to make doctor appointments based on Dai (2016)’s previous work. Functions are added in this work to improve the system’s resilience and security. Note that although only a mobile app design is illustrated, the whole MNS system should actually include software, OS, hardware, and communication system, database, and so on.

The app is developed on a laptop with Windows 10 OS. The primary development platform is Eclipse which integrated with JDK (Java Development Kit) and Android SDK (Software Development Kit). The app is expected to operate in a wireless environment like 2 G/4 G or WiFi (Wireless Fidelity). On the same device, the Google Map android app is also required.

4.1. Conceptual design

The app is to help patients to make doctor appointments based on their symptoms and available hospital resources in the area. The goal is to set up an appointment with the minimum patient waiting time at the hospital chose by the patient. [Figure 3](#) is the app's operational procedure. A patient should first register in the app with the healthcare information. The information is then transferred via the wireless connection and authenticated by a remote server, which is owned by a corresponding healthcare database management authority. Once the input information matches an entry in the healthcare database, a brief description of the symptom needs to be provided by the patient. With that, the app lets the patient choose from several candidate hospitals. After receives the decision, the app will again access the healthcare database for authentication and record the appointment. At the same time, a navigation option is initiated by OS through the Google Map navigation service.

4.2. Application of the design principles

Infrastructure aspect

Application of Rule I-1 (choose matured options): AndroidManifest.xml is an entrance file to define the operational status and references for the app. First, set 'allowBackup' to 'false' to avoid an unauthorised copy of the application data by enabling the USB debugging option. Second, set 'Debuggable' to 'false' to reduce the likelihood of stealing users' login credentials or accessing data by bypassing an authentication process. [Figure 4](#) is a programme fragment intended to get the value of the 'Debuggable'.

Besides, the Native Development Kit (NDK) is chosen to implement app's codes in native C++ and C. Those languages have an excellent capability against decompilation. This reduces the risk of source code disclosure which may lead to a crack of the app. In our app, C++ was chosen with the NDK to realise crucial functions, like the login module in [Figure 5](#) and the user registration module.

Application of Rule I-2 (choose an adaptive application style): A soft keyboard provides safe inputs for sensitive data in the process of login and registration. Users are required to input the password during those processes. There may be a risk of password leakage using a third-party input method. As a result, the app chooses to develop a custom keyboard. As illustrated in [Figure 5](#), the randomly distributed keyboard ensures the security of password input.

Substance aspect

Application of Rule S-1 (identify privacy information): [Figure 6](#) shows an entity-relationship model for patients and hospitals in the context of appointment registration. Patients' attributes, such as the patient's telephone Number (Tel.), name, address (Addr.), personal health number (No.) and personal geographical location (PGL) are captured. The

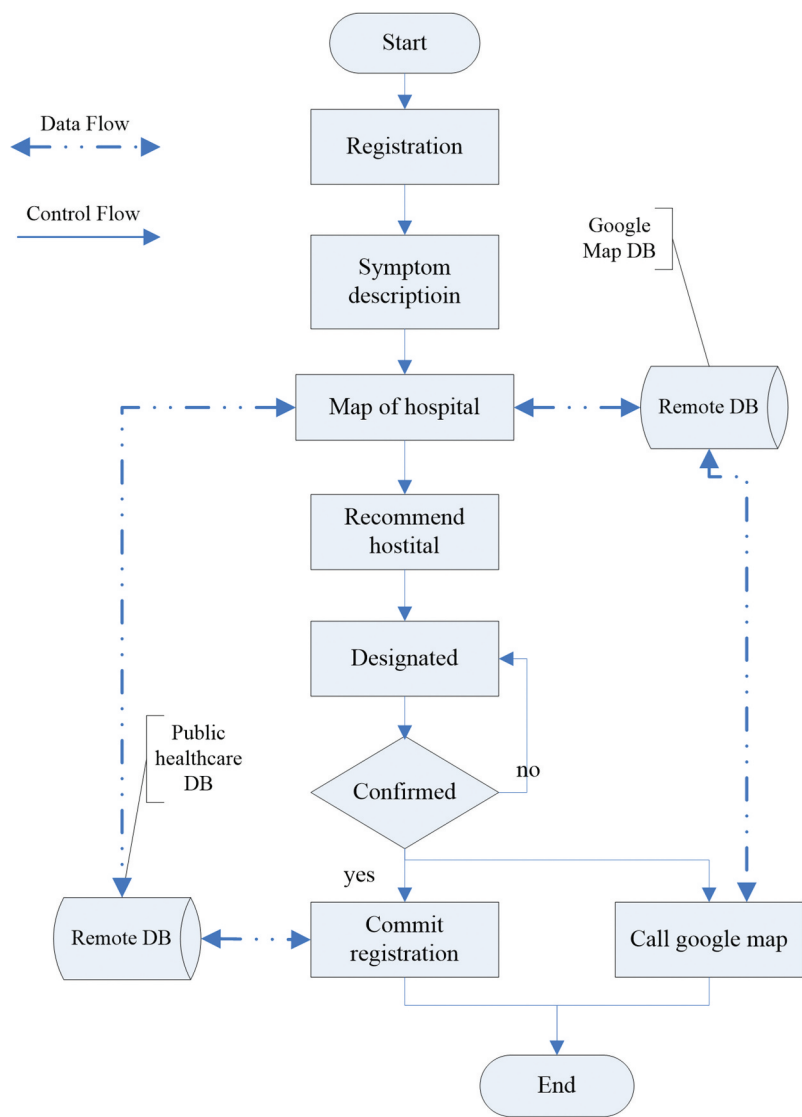


Figure 3. Programme flow of the mobile app.

attributes of the action (Register) include symptoms, time, and location that a patient requests an appointment. The last attribute is marked as registration geographical location (RGL). For hospitals, attributes such as hospital identity (ID), hospital geographical location (HGL) and address are identified.

Application of Rule S-3 (minimise information required): The PGL in Figure 6 is being monitored by the app when running. According to rule S-3, PGL should not be stored or transmitted because it is closely related to personal identity. In contrast, personal location information about registration (RGL in Figure 8) can be stored in local storage or transferred to remote servers and databases as evidence of registration. This helps to avoid

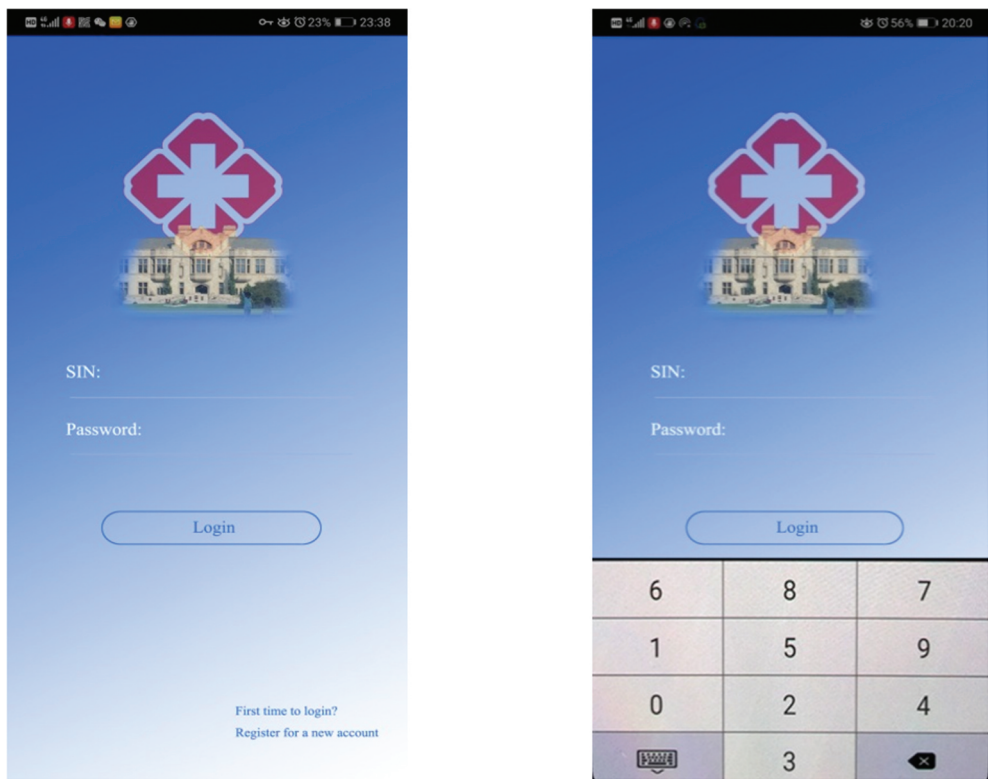


Figure 4. Code for the value of the ‘Debuggable’.

potential issues like data compromise from transferring privacy data like the patient location.

One of the most critical issues is what part of the location-related data should be transferred and stored to avoid compromise of personal privacy. According to Rule S-3, PGL should not be stored or transferred as it is closely related to personal identity. By contrast, the personal location information regarding registration, i.e., RGL in [Figure 6](#), can be stored either in the local storage or transferred to a remote server and database, as evidence of registration.

Application of Rule S-5 (management for data storage, use and transfer): A choice among local storage, remote server, and the clouds are made considering security, communication efficiency and cost. For instance, patients’ personal health No. and symptom descriptions are stored locally. This avoids the risk of patients’ private information leaked from a centralised database.

Further, two management rules are established. First, only the data owner or device owner has access to the data follows the authentication strategy and technique. Data access should not be permitted without the owner’s formal consent. Second, for the data stored remotely, tools such as the identity shielding technique are applied. This technique makes information breach through the data mining technique be difficult.

Application of Rule S-6 (Authentication and certification): Authentications are established with patients’ health No. and credentials like password and fingerprint. When the app

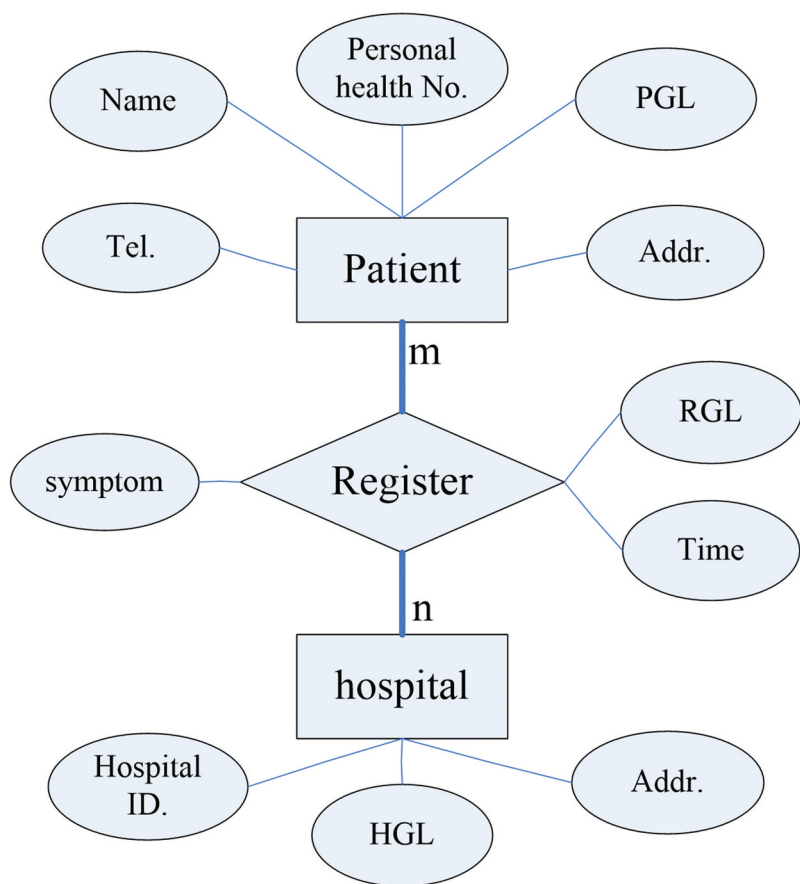


Figure 5. Screenshot of the app at login screen with (right) and without (left) a soft keyboard.

transfers the health No. and credentials to the server, the communication is secured by HTTPS (HyperText Transfer Protocol Secure) protocol. The protocol encrypted data with certifications. In the app, the public/private key pairs and certificates are managed by Keytool from JDK.

Energy aspect
Application of Rule E-1 and E-2 (Energy monitoring): The OS's attribute 'ACTION_BATTERY_CHANGED' is used to monitor the state of a system, in particular, the real-time battery charge level. In this way, users can decide whether to use a heavy energy consumption service, e.g., the Google Map navigation.

System resilience
Application of Rule R-1 (Identify critical functions and design redundancy): Critical information such as patients' current geographic data, symptom descriptions and designated hospital have dual-backup, i.e., one copy at a cloud database and one copy at a local database.
Application of Rule R-6 (Monitoring the state of the system function): The OS's 'enableNetwork' method to monitor whether the Internet is connected or not. The result triggers the app to choose which redundant resource to use. For example, to load critical information from the local database when the Internet is not available.

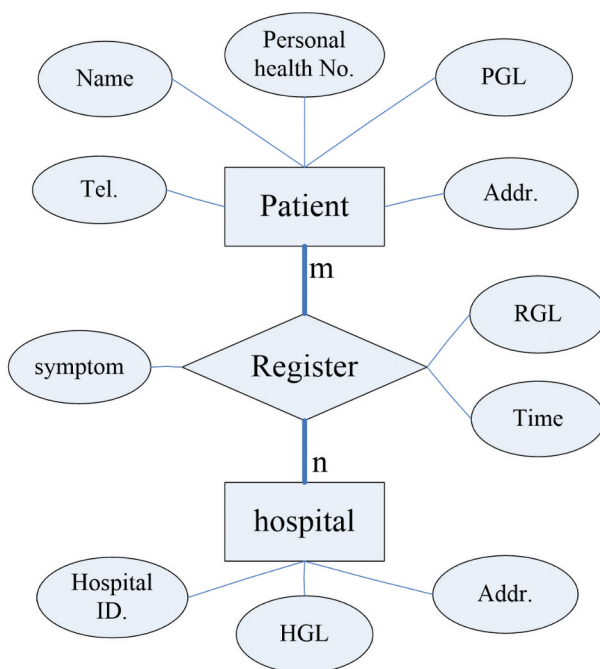


Figure 6. Entity relationship between patients and hospitals.

Application of Rule R-7 (Error forecasting): Potential errors are estimated, as: (1) error occurs while requesting a database connection; (2) users forget login credentials; (3) the app failed to launch; (4) insufficient power while performing a critical process.

5. Conclusion

The study is motivated by recent attention to the privacy issues in healthcare mobile apps (Al-Muhtadi et al. 2019; Hathaliya and Tanwar 2020). The private healthcare information will be compromised to a large extent if a system's security resilience is not adequate. In general, systematic consideration of the privacy issues is lacking in the development of a mobile app. The concept such as resilience privacy security is not clear in the literature. The main contribution of this study is advancing the understanding of privacy, privacy security, resilience in security, and their relationships. A set of mobile apps based system design principles are brought up for comprehensive privacy protections. Also, a mobile healthcare app is developed to demonstrate how to reduce patients waiting time and keep their privacy in protection using the design principles.

There are a few limitations of the present study. For one, it may be insufficient in literature coverage. In future, a systematic review process, which proves to be valuable in literature (Bokolo Anthony 2021; Ng et al. 2018; Tsang et al. 2021), will be applied to reviewing articles related to the security of privacy protection and its related resilience design. For another, proof of the effectiveness of the design principles is needed. We plan to work with our industry partners and use the MNS for their patient scheduling. Data

collected from case studies will be compared to those from their current system. From there, we will be able to demonstrate the effectiveness of our principles.

Several future endeavours could potentially be carried out. (1) An analysis could be performed on the relationship between PSR and other attributes like scalability, usability and system performance etc. Also, analysis strategies could be investigated for trading-off among those attributes towards different implementation contexts. (2) A detailed guide for testing and evaluating PSR in mobile app-based systems could be developed. Once a system is developed, an applicable and affordable way is needed to test and evaluate all its attributes. (3) Human factors to PSR need attention, especially how cultural factors may affect the performance of PSR.

Acknowledgments

Part of the work presented in this paper is based on a Master of Science thesis of Xu (2019), and herewith this is acknowledged.

Disclosure of statement

No potential conflict of interest was reported by the author(s).

ORCID

Wenjun Lin  <http://orcid.org/0000-0002-3907-1995>

Wenjun Zhang  <http://orcid.org/0000-0001-7973-8769>

References

- Aceto, G., V. Persico, and P. Antonio. 2020. "Industry 4.0 And Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0." *Journal of Industrial Information Integration* 18: 100129.
- Al-Muhtadi, J., B. Shahzad, K. Saleem, W. Jameel, and M. A. Orgun. 2019. "Cybersecurity and Privacy Issues for Socially Integrated Mobile Healthcare Applications Operating in a Multi-cloud Environment." *Health Informatics Journal* 25 (2): 315–329. doi:10.1177/1460458217706184.
- Alpár, G., J.-H. Hoepman, and J. Siljee. 2011. "The Identity Crisis. Security, Privacy and Usability Issues in Identity Management." *arXiv Preprint arXiv: 1101.0427*.
- Avancha, S., A. Baxi, and D. Kotz. 2012. "Privacy in Mobile Technology for Personal Healthcare." *ACM Computing Surveys (CSUR)* 45 (1): 1–54. doi:10.1145/2379776.2379779.
- Bokolo, Anthony Jnr. 2021. "Managing digital transformation of smart cities through enterprise architecture – a review and research agenda." *Enterprise Information Systems* 15 (3): 299–331. doi:10.1080/17517575.2020
- Cai, M. Y., Y. Lin, Z. Gao, C. W. Yuan, and W. J. Zhang. 2017. "Comparison of AH and MFM for Work Domain Analysis in Light of Interface Design." In *IEEE International Systems Engineering Symposium (ISSE)*, 1–6. Vienna, Austria: IEEE.
- Chen, H., C. E. Beaudoin, and T. Hong. 2017. "Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors." *Computers in Human Behavior* 70: 291–302. doi:10.1016/j.chb.2017.01.003.
- Collins, T. 2006. "NHS Trust Uncovers Password Sharing Risk to Patient Data." *ComputerWeekly.com*. ComputerWeekly.com, July 10, 2006. <https://www.computerweekly.com/news/2240077810/NHS-trust-uncovers-password-sharing-risk-to-patient-data>.

- Dai, F. 2016. "On Development of a Green Web-based System for Reducing Waiting Times of Outpatients." PhD diss., MSc Thesis, Division of Biomedical Engineering, University of Saskatchewan ...
- Di, P., G. O. Roberto, C. Soriente, and G. Tsudik. 2012. "United We Stand: Intrusion Resilience in Mobile Unattended WSNs." *IEEE Transactions on Mobile Computing* 12 (7): 1456–1468.
- Fan, L. X., M. Y. Cai, Y. Lin, and W. J. Zhang. 2015. "Axiomatic Design Theory: Further Notes and Its Guideline to Applications." *International Journal of Materials & Product Technology* 51 (4): 359–374. doi:10.1504/IJMPT.2015.072557.
- Hathaliya, J. J., and S. Tanwar. 2020. "An Exhaustive Survey on Security and Privacy Issues in Healthcare 4.0." *Computer Communications* 153: 311–335. doi:10.1016/j.comcom.2020.02.018.
- Holling, C. S. 1973. "Resilience and Stability of Ecological Systems." *Annual Review of Ecology and Systematics* 4 (1): 1–23. doi:10.1146/annurev.es.04.110173.000245.
- Huang, D., X. Zhang, M. Kang, and J. Luo. 2010. "MobiCloud: Building Secure Cloud Framework for Mobile Computing and Communication." In *fifth IEEE international symposium on service oriented system engineering*, 27–34. Nanjing, China: IEEE.
- Khan, F., and O. Reyad. 2020. "Application of Intelligent Multi Agent Based Systems for E-Healthcare Security." *arXiv Preprint arXiv: 2004.01256*.
- Lancharoen, S., P. Suksawang, and T. Naenna. 2020. "Readiness Assessment of Information Integration in a Hospital Using an Analytic Network Process Method for Decision-making in a Healthcare Network." *International Journal of Engineering Business Management* 12: 1847979019899318. doi:10.1177/1847979019899318.
- Li, Y., H. Wang, L. Yingying, and L. Li. 2019. "Patient Assignment Scheduling in a Cloud Healthcare System Based on Petri Net and Greedy-based Heuristic." *Enterprise Information Systems* 13 (4): 515–533. doi:10.1080/17517575.2018.1526323.
- Liang, X., M. Barua, C. Le, R. Lu, X. Shen, X. Li, and H. Y. Luo. 2012. "Enabling Pervasive Healthcare through Continuous Remote Health Monitoring." *IEEE Wireless Communications* 19 (6): 10–18. doi:10.1109/MWC.2012.6393513.
- Lo'ai, T., N. Alassaf, W. Bakheder, and A. Tawalbeh. 2015. "Resilience Mobile Cloud Computing: Features, Applications and Challenges." In *Fifth International Conference on e-Learning (econf)*, 280–284. Manama, Bahrain: IEEE.
- Loft, P., H. Ying, H. Janicke, and I. Wagner. 2021. "Dying of a Hundred Good Symptoms: Why Good Security Can Still Fail-a Literature Review and Analysis." *Enterprise Information Systems* 15 (4): 448–473. doi:10.1080/17517575.2019.1605000.
- Mozilla. "Web Technology for Developers". Last accessed 16 December 2020. <https://developer.mozilla.org/en-US/docs/DOM/window.navigator.battery>
- Ng, C. K., C. H. Wu, K. L. Yung, W. H. Ip, and T. Cheung. 2018. "A Semantic Similarity Analysis of Internet of Things." *Enterprise Information Systems* 12 (7): 820–855. doi:10.1080/17517575.2018.1464666.
- Ogbeyemi, A., W. Lin, F. Zhang, and W. Zhang. 2020. "Human Factors among Workers in a Small Manufacturing Enterprise: A Case Study."
- Rahmadika, S., and K.-H. Rhee. 2018. "Blockchain Technology for Providing an Architecture Model of Decentralized Personal Health Information." *International Journal of Engineering Business Management* 10: 1847979018790589. doi:10.1177/1847979018790589.
- Solove, D. J. 2002. "Conceptualizing Privacy." *Calif. L. Rev* 90 (4): 1087. doi:10.2307/3481326.
- Sun, Z., B. Zhang, L. Cheng, and W. J. Zhang. 2011. "Application of the Redundant Servomotor Approach to Design of Path Generator with Dynamic Performance Improvement." *Mechanism and Machine Theory* 46 (11): 1784–1795. doi:10.1016/j.mechmachtheory.2011.06.003.
- Taleb, T., A. Ksentini, and B. Sericola. 2016. "On Service Resilience in Cloudnative 5G Mobile Systems." *IEEE Journal on Selected Areas in Communications* 34 (3): 483–496. doi:10.1109/JSAC.2016.2525342.
- Tsang, Y. P., C. H. Wu, W. H. Ip, and W.-L. Shiau. 2021. "Exploring the Intellectual Cores of the blockchain-Internet of Things (Biot)." *Journal of Enterprise Information Management ahead-of-print (ahead-of-print)*. doi:10.1108/JEIM-10-2020-0395.

- Wang, J., R. Dou, R. R. Muddada, and W. Zhang. 2018. "Management of a Holistic Supply Chain Network for Proactive Resilience: Theory and Case Study." *Computers & Industrial Engineering* 125: 668–677. doi:[10.1016/j.cie.2017.12.021](https://doi.org/10.1016/j.cie.2017.12.021).
- Wang, J., R. R. Muddada, H. Wang, J. Ding, Y. Lin, C. Liu, and W. Zhang. 2014. "Toward a Resilient Holistic Supply Chain Network System: Concept, Review and Future Direction." *IEEE Systems Journal* 10 (2): 410–421. doi:[10.1109/JSYST.2014.2363161](https://doi.org/10.1109/JSYST.2014.2363161).
- Woods, D. D. 2015. "Four Concepts for Resilience and the Implications for the Future of Resilience Engineering." *Reliability Engineering & System Safety* 141: 5–9. doi:[10.1016/j.res.2015.03.018](https://doi.org/10.1016/j.res.2015.03.018).
- Xu, M. 2019. "A System Perspective to Privacy, Security and Resilience in Mobile Applications." Master's thesis, University of Saskatchewan.
- Zhang, W. 1994. "An Integrated Environment for CAD/CAM of Mechanical Systems." PhD diss., Delft University of Technology.
- Zhang, W. J., and C. A. Van Luttervelt. 2011. "Toward a Resilient Manufacturing System." *CIRP Annals* 60 (1): 469–472. doi:[10.1016/j.cirp.2011.03.041](https://doi.org/10.1016/j.cirp.2011.03.041).
- Zhang, W. J., and J. W. Wang. 2016. "Design Theory and Methodology for Enterprise Systems." *Enterprise Information Systems* 10 (3): 245–248. doi:[10.1080/17517575.2015.1080860](https://doi.org/10.1080/17517575.2015.1080860).
- Zhang, W. J., J. W. Wang, and Y. Lin. 2019. "Integrated Design and Operation Management for Enterprise Systems." *Enterprise Information Systems* 13 (4): 424–429. doi:[10.1080/17517575.2019.1597169](https://doi.org/10.1080/17517575.2019.1597169).
- Zhang, W.-J., and Y. Lin. 2010. "On the Principle of Design of Resilient Systems— Application to Enterprise Information Systems." *Enterprise Information Systems* 4 (2): 99–110. doi:[10.1080/17517571003763380](https://doi.org/10.1080/17517571003763380).
- Zhang, X., J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong. 2009. "Securing Elastic Applications on Mobile Devices for Cloud Computing." In *Proceedings of the 2009 ACM workshop on Cloud computing security*, 127–134. New York, NY, USA: Association for Computing Machinery.
- Zhou, J., Z. Cao, X. Dong, X. Lin, and A. V. Vasilakos. 2013. "Securing M-healthcare Social Networks: Challenges, Countermeasures and Future Directions." *IEEE Wireless Communications* 20 (4): 12–21. doi:[10.1109/MWC.2013.6590046](https://doi.org/10.1109/MWC.2013.6590046).