CHAPTER 8

Security and privacy solutions for smart healthcare systems

Yang Lu and Richard O. Sinnott

School of Computing and Information Systems, The University of Melbourne, Australia

8.1 Introduction

In the digital-rich era, online data management becomes increasingly essential. In the health domain, a seismic change is occurring from traditional, paper-based documents to electronic records stored in database systems (Nguyen, Bellucci, & Nguyen, 2014). This can cause many challenges. For instance, care providers may require the access to vital information in different locations; however, many safety issues arise in the handoff of patients among healthcare providers since necessary information cannot be shared. For clinical research, it is necessary to obtain approvals from cancer patients or their families before using their genomic data (Grossman et al., 2016). When it comes to distributed data analytics, the study goal can be balancing privacy and utility while attempting to share, integrate, and visualize health records (Grossman et al., 2016; Wang, Gui, Liu, Jin, & Chen, 2014; Takabi, Joshi, & Ahn, 2010). Due to the increasing use of Internet of Things (IoT) technology in the healthcare domain, certain e-health services are now equipped with more powerful communication and computing capabilities. As a result, connected objects can threaten system security and personal privacy by opening more interactive channels.

According to Solanas et al. (2014), the concept smart health (s-health) refers to "the provision of health services by using the context-aware network and sensing infrastructure of smart cities." Demirkan (2013) pointed that a smart healthcare system (SHS) should provide "opportunities for healthcare organizations to deploy solutions with fewer risks and increased context awareness, converging electronic medical records (EMRs), cloud platforms, social networks, advanced sensors, and data analysis techniques." The SHS technology can create values for taxpayers, care providers, and researchers by tracking, analyzing and processing healthcare information anytime, anywhere. For instance, elderly people can enjoy healthcare services at home (Amrutha, Haritha, Haritha Vasu, Jensy, & Charly, 2017). By building medical data centers for data collection and transmission, authorized individuals can access and decide whether to share their physiological data with

Innovation in Health Informatics.
DOI: https://doi.org/10.1016/B978-0-12-819043-2.00008-3

clinicians for disease diagnosis (Prakash & Balaji Ganesh, 2019). Due to the portable design, smart health services are especially helpful in emergency situations (Ambhati, Kota, Chaudhari, & Jain, 2017). For example, a diabetic patient suddenly faints in their workplace. In this medical scene, ambulance personnel often require his/her history records. With mobile applications tracking patients' diet, exercise, sleep, and blood sugar levels, it is now much easier to learn the basic health conditions immediately.

Policies are required to maintain system security and privacy so as to earn customers' and stakeholders' trust. In Australia, the National Statement on Ethical Conduct in Human Research (NHMRC) labels health data items as *individually identifiable*, *reidentifiable*, and *nonidentifiable*.[1] On this basis, security policies can be defined to constrain data collection and publishing, with the security categories and circumstantial information being considered. The Health Insurance Portability and Accountability Act 1996 (HIPPA)[2] suggests several privacy levels as the guidelines of anonymization. Specially, it identifies the "safe harbors" including 18 attribute types (name, address, date, biometric information, serial numbers of personal devices, etc.) to be removed from individual records before getting disclosed. Similar requirements can be found in the EU General Data Protection Regulation (GDPR).[3] In practice, researchers are required to use health data in an ethical and confidential manner. According to O'Keefe and Connolly (2010), the secured access to and use of health data can be guaranteed by following three procedures: (1) Obtaining consent from data owners (i.e., the patients) for using data; (2) gaining access by satisfying requirements defined for targeted resources, and (3) anonymizing personal data for secondary use, such as public health research activities (Lowrance, 2003). As wireless sensors such as wearable devices and environmental monitors intertwine into our daily lives, unprecedented challenges arise in maintaining security and minimizing privacy risks.

To help other researchers in the related fields, we identify security and privacy challenges by combining social (healthcare) and technical features of s-health applications. To see why such issues occured and how they might be tackled, the rest of this chapter is organized in the following sections: in Section 8.2, we clarify some key concepts related to SHSs (also known as s-health) and identify related technologies. Based on the functional characteristics, we determine the major focuses and review emerging strategies related to *Identification*, *Access Control*, and *Privacy Preservation* in Section 8.3. The key findings

[1] National Health and Medical Research Council (Australia). (2007). National statement on ethical conduct in human research. National Health and Medical Research Council.

[2] Centers for Medicare & Medicaid Services. (1996). The Health Insurance Portability and Accountability Act of 1996 (HIPAA). Online at: http://www.cms.hhs.gov/hipaa

[3] GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Off J European Union, vol. L119/59, May 2016.

are discussed in Section 8.4. Finally, we conclude the study with a summary of key contributions and several research directions in Section 8.5.

8.2 Smart healthcare framework and techniques

Smart city infrastructures have brought great convenience to people. In the process of monitoring and collecting data from diverse domains, wireless sensor networks become commonplace and have been widely used in the intelligent transportation systems, mobile networks for remote healthcare, and smart meters used for metering gas usage. Collectively, these can be used to deliver the Internet of Things (IoT) applications. The main idea of IoT is to connect all sorts of things (sensors and IoTs) that can shape the lives of citizens more efficiently and conveniently. Existing projects such as Smart Santander greatly relied on IoT technologies. Through deploying sensors in different cities, a test bed was developed to monitor the traffic status and help drivers to quickly locate available parking spaces (Domingue, Galis, & Gavras, 2011). Different types of data can be collected by an urban IoT system, and exploited to promote the activities of local governments and serve their citizens. For instance, the London Oyster Card system can generate 7 million data records per day and 160 million records per month.[4] With a wide spectrum of data sets being collected in such sizes, big data technologies can be adopted to support a variety of smart city applications, from collecting, processing to analyzing multivariate data sets.

As shown in Fig. 8.1, smart health (s-health) research can be seen as the result of projecting an e-health plane over a smart city plane (Solanas et al., 2014). Both smart health (s-health) and mobile health (m-health) can be presented as subsets of e-health; however, in the sense of underlying infrastructures, s-health might not consist of mobile devices/applications but fixed sensors. Due to the support of big data analytic techniques (e.g., pattern recognition, predictive modeling, and other machine learning algorithms), an s-health framework can be provisioned through automatic services (Provost & Fawcett, 2013).

Another s-health framework was designed to apply a variety of analytic techniques on health-related databases (Sakr & Elgammal, 2016). As shown in Fig. 8.2, a layered, scalable s-health framework was designed with four functional layers for data connection, data storage, data analytics, and result presentation. After collecting data items from diverse scenarios, the first challenge is integrating heterogeneous datasets (e.g., hospital information, laboratory records, radiology records, and prescriptions from pharmacies). This can rely on modeling related semantic ontologies at the connection layer. At the storage layer, synthetic data can be accessed and operated flexibly by using cloud-based relational databases and/or NoSQL storage services to process structured, semistructured, and unstructured data sources. Building on this, the analytic layer can provide various functions

[4] Batty, M. Smart cities and Big Data. http://www.spatialcomplexity.info/.

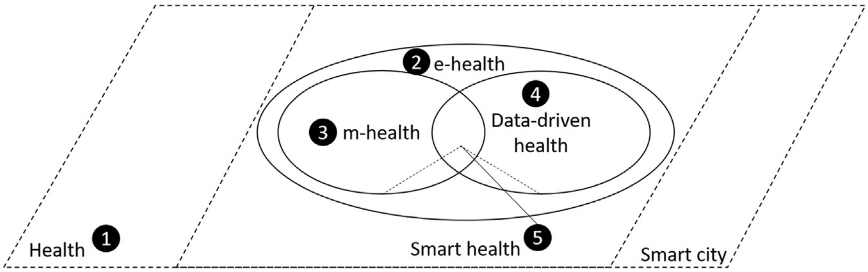

Figure 8.1
Diagram of smart health and related concepts[5].

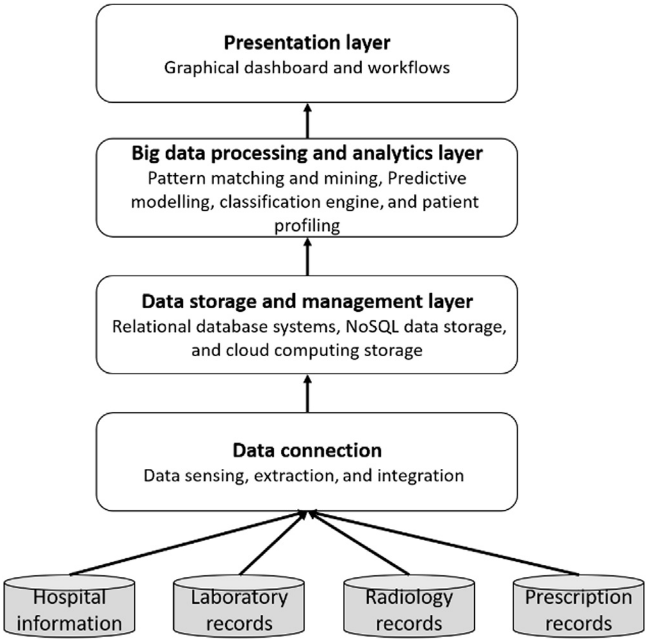

Figure 8.2
Architecture underlying smart healthcare systems (Sakr & Elgammal, 2016).

according to the data processing requirements. Finally, a user-friendly dashboard can be built to display the analytics results in the presentation layer. Throughout the treatment process, clinicians and researchers are able to make better, real-time decisions.

[5] (1) Health refers to health-related activities commonly occur in medical contexts; (2) e-health involves the use of the information communication technology, namely health-related activities relying on the access of electronic health records; (3) m-health practices are typically supported by the use of wireless infrastructures and mobile devices; (4) data-driven health business involves big data collecting, processing and analyzing; (5) smart health (s-health) is defined as the combination of (3) and (4), representing as m-health augmented with certain intelligence.

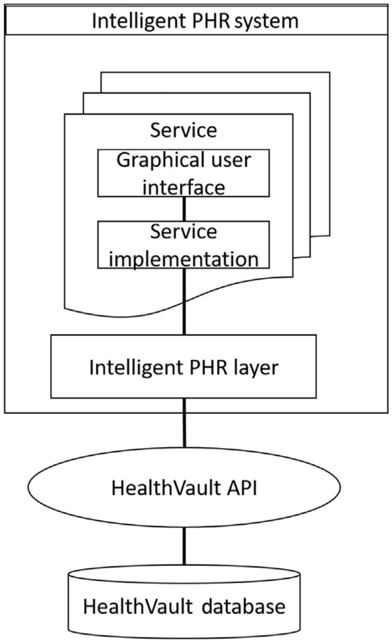

Figure 8.3
Intelligent PHR system built on Microsoft HealthVault (Kostadinovska et al., 2015).

Data-driven platforms such as HealthVault and Google health are widely adopted to provide s-health services. As shown in Fig. 8.3, a high-level architecture can be designed to underlie the intelligent personal health record (PHR) system (Kostadinovska, de Vries, Geleijnse, & Zdravkova, 2015). In this architecture, remote services can be delivered on the population-level data obtained through HealthVault APIs. Thus, a lightweight intelligent PHR system can be established without local storage. Another key principle of this approach is that patients are in control of their data, and thus they are encouraged to participate in their own treatment. In addition, the proposed PHR system can benefit care providers and researchers by supporting diverse analytical technologies. For instance, through monitoring health conditions, retrieving hospitalization and testing results, care providers can make better decisions at minimal cost, whilst public health researchers are able to predict and prevent adverse events from happening among a very large population through access to clinical and laboratory data in PHR records.

To make optimal use of wireless technologies, Catarinucci et al. (2015) designed an IoT-aware SHS by extending hospital services in an IoT network. Typically, the following three parts should be included in the architecture: (1) a sensing network built with wireless sensors for data acquisition; (2) an IoT smart gateway for authenticating local and remote users before they can access or use the sensitive information; and (3) a user interface allowing data management and real-time result display. An IoT-aware system should be able to collect and deliver patients' symptoms and environmental conditions to a operating center, such as processing data with intelligent algorithms and allowing alert messages to be sent in case of emergency.

Depending on the sensor types in use, Baig and Gholamhosseini (2013) further classified the s-health systems as wearable health monitoring system (WHMS), mobile health monitoring system (MHMS), and remote health monitoring system (RHMS). Specifically, a WHMS involves the use of wearable sensors while an MHMS is based on mobile devices. Through combining mobile communication and wearable monitoring technology, an RHMS can be established to transmit vital messages, such as from a health center to the patient's home. As shown in Fig. 8.4, wireless body area networks can provide patient symptom data such as blood pressure, ECG, and heartbeat through sensors placed on the human body. By using mobile devices, health-related data can be transmitted to the local network and e-health servers to support treatment and data analytics (Khan, Jilani, Khan, & Ahmed, 2017). Finally, the last layer provides services to patients living remotely. Data stored in the e-health server can be delivered to remote hospitals.

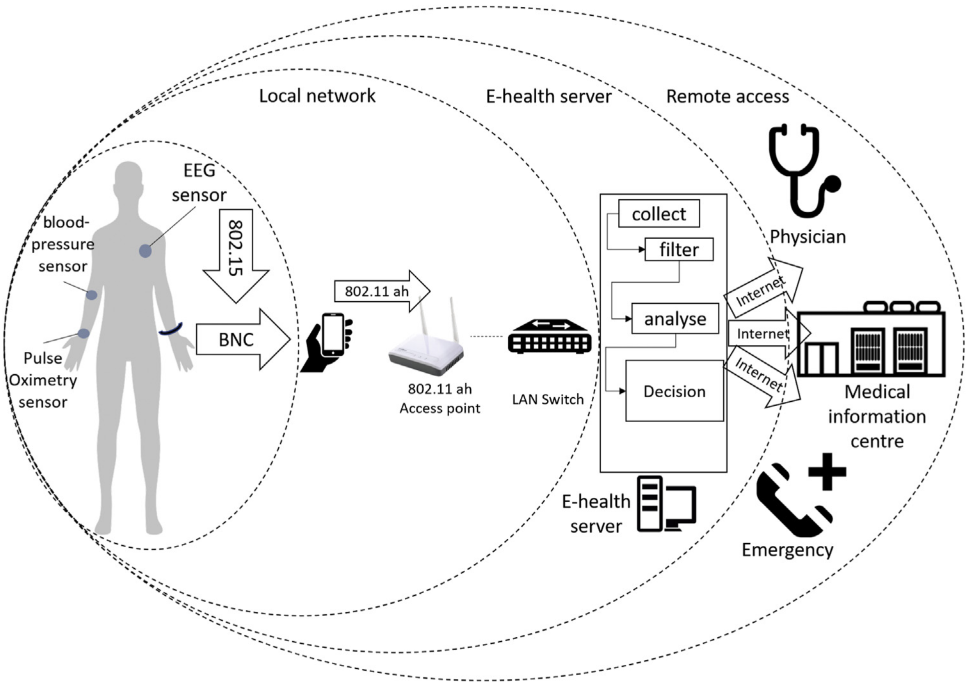

Figure 8.4
Smart health based in wireless body area networks (Ghamari et al., 2016).

In addition to healthcare, remote access to medical information also supports emergency services (Gope & Hwang, 2016). To generalize the use of such architecture, Sahi et al. (2018) designed a multitiered system to serve a larger group of users, including physicians, pharmacists, health insurance providers, etc. located at remote organizations. Through the adoption of communication technologies, multiple systems are connected to form a smart access solution. Smart health monitoring systems are often referred to as using advanced technologies to monitor patients' health conditions. Based on the behavioral models extracted from monitoring systems, Baig and Gholamhosseini (2013) proposed a generic s-health architecture and its communication within a smart city infrastructure. As shown in Fig. 8.5, it can be used in different contexts such as home, hospital and outdoors.

Due to the sensitive attributes included in PHRs, protection against unauthorized use/access is essential. Based on a systematic review of existing work, two main features are found in the s-health frameworks: the adoption of monitoring technologies (e.g., mobile, wearable sensors) in ubiquitous environments and complex data analytics (e.g., data integration and machine learning methods) on heterogenous datasets. Therefore, extra security measures are required in s-health infrastructures where diverse application functionalities need to be equipped with.

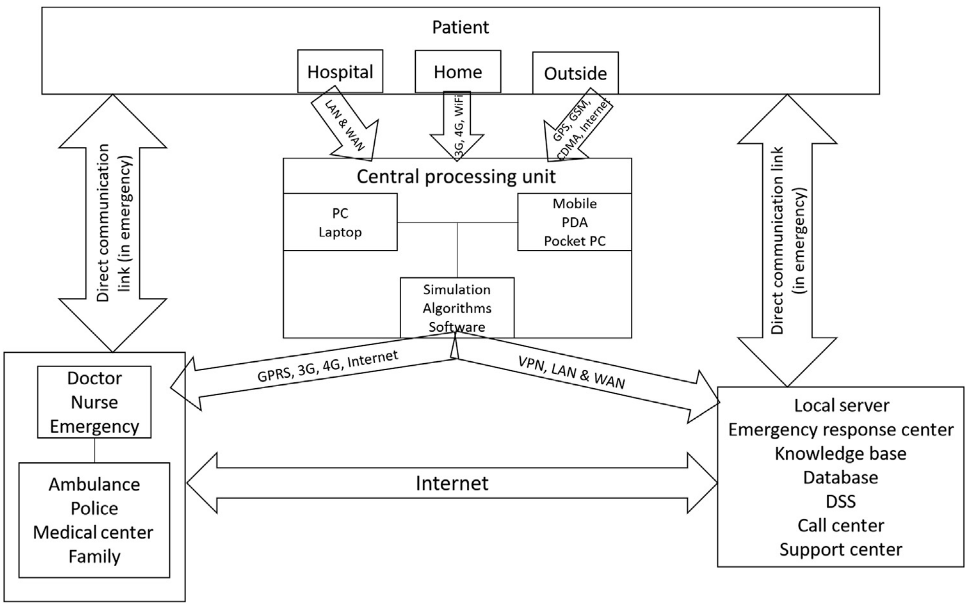

Figure 8.5
Health monitoring system (Baig & Gholamhosseini, 2013).

8.3 Identified issues and solutions

As a theoretical guideline for ICT, the *Confidentiality*, *Integrity*, and *Availability* (CIA) model has been widely used to safeguard online database systems (Cherdantseva & Hilton, 2013). As shown in Fig. 8.6, the CIA Security Principle addresses requirements in terms of *Confidentiality* through defining policies to prevent inappropriate data access; *Integrity* that protects data against unauthorized modification; and *Availability* that focuses on ensuring any reliable access/use of information (Samonas & Coss, 2014; Wang, Lee, & Wang, 1998; Zhao, You, Zhao, Chen, & Peng, 2010). Certain methods are designed by following appropriate guidelines. For instance, encryption algorithms can be applied to ensure confidentiality, whereby encrypted messages cannot be viewed by attackers who do not own the decryption keys (Kumar & Saxena, 2011). Authorization policies also restrict "editing" privileges to those who have the admin roles (Malik & Park, 2008).

In addition to CIA, Prasser, Kohlmayer, Spengler, and Kuhn (2018) suggested a general security framework for health information sharing. As shown in Fig. 8.7, it contains security principles related to *Trust, Controlled Data Access*, and *Deidentification* thereby offering a three-layer concept model. From the outermost layer, trust relations can be created (and strengthened) between organizations (Firth-Cozens, 2004) and thus provide the foundation for authentication (Cody-Allen & Kishore, 2006). The middle layer is tasked with protected data sources so as to satisfy requirements suggested in the CIA model. Finally, anonymizing strategies can help reduce (or eliminate) the chance of disclosing sensitive information (Fairchild et al., 2007; Shlomo, 2007). For instance, individual health records containing HIV test results must be kept anonymous before they are used for secondary purposes. Datasets containing such patient information may

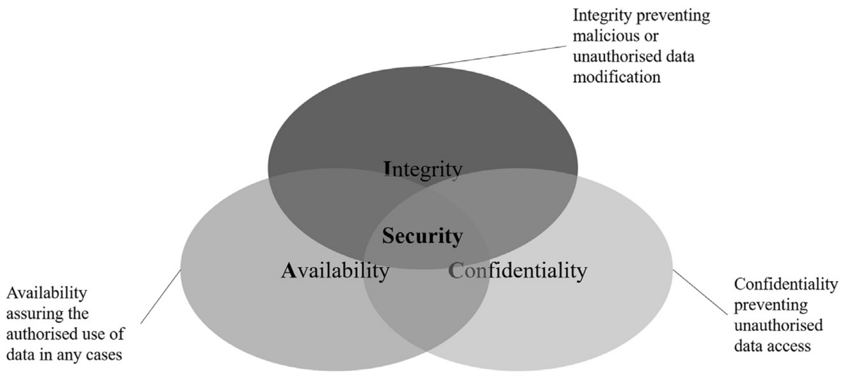

Figure 8.6
CIA: confidentiality, integrity, and availability model.

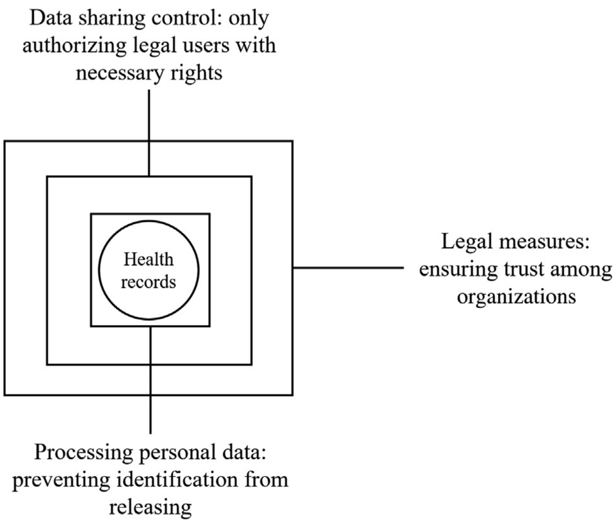

Figure 8.7
Principles guaranteeing security and privacy of health records.

be accessible to people who are identified as “specialists” in the e-health platform. When it comes to collaborative research activities, cross-domain authentication can also ensure the secured data sharing.

Both conceptual models present a range of security issues that need to be carefully dealt with in online data sharing. As a subfield of smart cities (shown in Fig. 8.1), smart health enjoys the same group of technologies while heavily relies on the access to health information. As a result, security and privacy preserving solutions should be developed by taking all features into consideration. This requires the involved entities are truly connected to intelligent healthcare services. For instance, Fig. 8.8 outlines a “mind map” of this study: (1) identifying the technical features of smart cities such as *Wireless, Mobile, and Ubiquitous Computing*; (2) identifying smart health applications by combining available functionalities of existing e-health systems; and (3) determining security and privacy requirements for s-health applications, given the wide range of smart city technologies (shown in Fig. 8.1).

In this chapter, we review the innovative work that has been done to mitigate security or privacy risks within smart healthcare applications. In this study, we consider several procedures in the following order: *Technical Enablers→s-Health Applications→Security and Privacy Solutions*. Based on the key issues outlined in the two models (Figs. 8.6 and 8.7), strategies can be categorized into *Authentication*, *Privacy-aware access control*, and *Anonymization*.

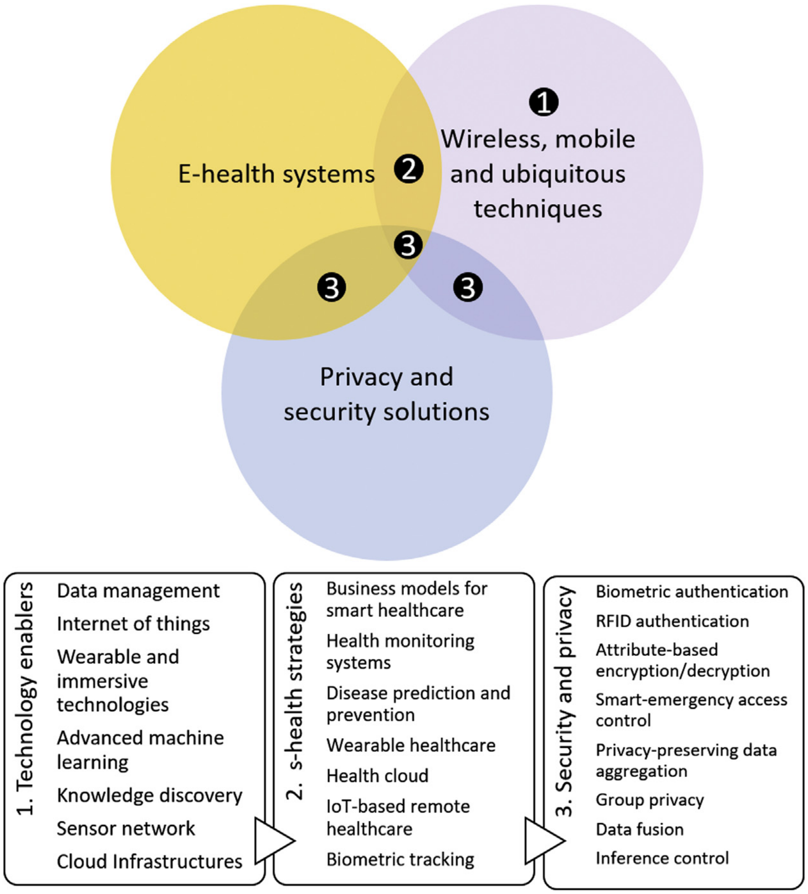

Figure 8.8
Mind map of this work.

8.3.1 Authentication

Identifying legitimate people and objects is paramount to s-health system design. Due to the functional characteristics, both subject and object authentication are required in using s-health applications. Technologies such as radio frequency identification (RFID) are widely used to identify physical objects and people in ubiquitous environments. Due to the system openness, authentication technologies can be further categorized as centralized and decentralized authentication, depending on how the processes are performed.

8.3.1.1 Internet of Things authentication

Thousands of connected things can be built within SHSs. As a result, authentication is an important security service, determining valid accessible objects in IoT networks. RFID is

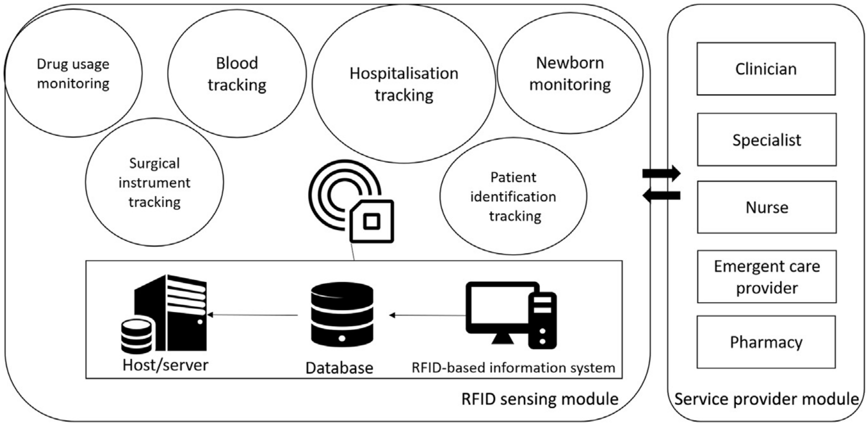

Figure 8.9
A generic RFID-enhanced hospital system (Rahman, Bhuiyan, & Ahamed, 2017).

widely used to identify IoT objects based on a serial number stored in a microchip (Amendola, Lodato, Manzari, Occhiuzzi, & Marrocco, 2014). It has the advantage of reading information without physical contact. As shown in Fig. 8.9, a generic hospital system consists of two modules: RFID Sensing Module including all RFID identifying and monitoring systems and Service Provider Module containing systems used for legitimate RFID identification data. For instance, with RFID sending patient information to a given monitoring system, the alarm can be activated in case of an emergency happening.

A major concern in RFID-based healthcare systems is how user privacy can be protected when using RFID identification data. In this regard, Rahman et al. (2017) suggested a healthcare service access control framework where unauthorized disclosures of health information need to be prevented by using access control techniques (Dafa-Alla, Kim, Ryu, & Heo, 2005). As shown in Fig. 8.10, through writing and managing privacy policies by an "Administrator," the use of and access to various data can be related to user-defined policies. A "Privacy Policy Manager" breaks down policies into unit policies and unit roles, which are respectively stored in "Privacy Policy Database" and "User Role Database" to deliver protection on real-time RFID tags that are read into the system.

8.3.1.2 User authentication

In IoT-based scenarios, there is a rise in the use of biometric authentication mechanism. Different from using traditional passwords, biometric data such as fingerprints, face scans can be used as an "unforgettable" means to authenticate individuals into various smart infrastructures. For instance, biometric systems such as Apple's Touch ID and Android's Face Unlock are designed for authenticating smartphone users (De Luca, Hang, Von Zezschwitz, & Hussmann, 2015). Based on the use of fingerprint information, a novel

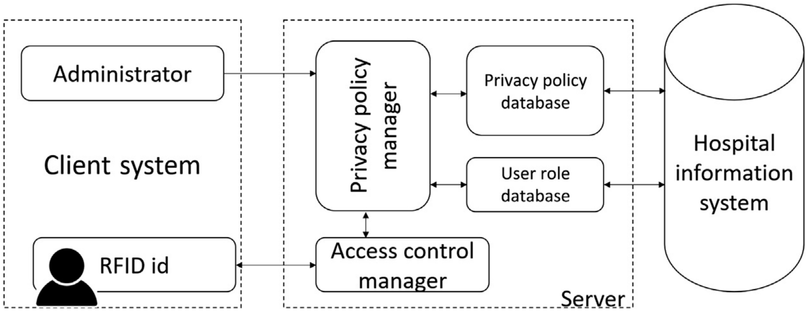

Figure 8.10
Architecture of healthcare service access control (Rahman et al., 2017).

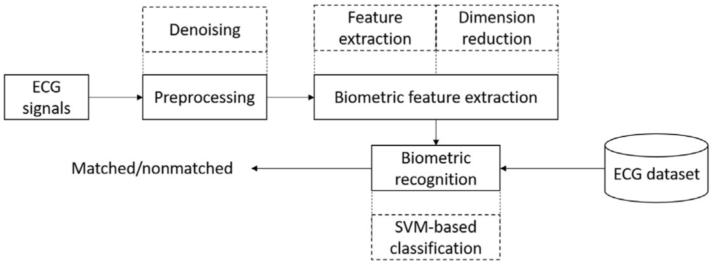

Figure 8.11
ECG authentication in smart healthcare systems (Hejazi et al., 2016).

authentication system is implemented for user registration and secured access control (Murillo-Escobar, Cruz-Hernández, Abundiz-Pérez, & López-Gutiérrez, 2015). Electrocardiogram (ECG) signals are monitored in nearly all healthcare systems, and thus, ECG-based authentication is considered in user authentication and medical information access (Zhang, Gravina, Lu, Villari, & Fortino, 2018).

The use of machine learning algorithms for processing patients' biometric data can support user authentication. For instance, Fig. 8.11 illustrates a generic framework describing how ECG signals can realize the user (patient) authentication (Hejazi, Al-Haddad, Singh, Hashim, & Aziz, 2016). Generally, it involves such procedures as data collection, preprocessing, feature extraction, and classification-based recognition. Based on the feature vectors extracted from cleaned ECG signals, a decision model can be learned by training feature vectors from the ECG dataset. Based on the evaluation, optimal testing results can be achieved by using SVM-based classification in the recognition phrase.

8.3.1.3 Distributed authentication

Due to the increasing complexity of smart healthcare business models, different types of attributes can be incorporated into the design of security measures. For instance, the attribute-based encryption (ABE) can be used as an effective cryptographic tool for secure communication in SHSs (Ambrosin et al., 2016). ABE variants such as ciphertext-policy attribute-based encryption (CP-ABE) and key-policy attribute-based encryption (KP-ABE) are explored to protect IoT devices (Bethencourt, Sahai, & Waters, 2007; Goyal, Pandey, Sahai, & Waters, 2006). According to Ambrosin et al. (2016), a secret key represents access policies in the KP-ABE mode. Therefore, users can decrypt the ciphertext whenever the access policy associated with the secret key (policy) can be satisfied by assigned attributes. In contrast, the CP-ABE method enforces access policies on data and associates a set of attributes to the secret key. As a result, a user can decrypt a ciphertext when the key (attributes) satisfies the access policies on the plaintext.

Based on trust relations among known certificate authorities (CAs), public key infrastructures (PKIs) can underpin a multitude of secure, collaborative platforms (Aberer, Datta, & Hauswirth, 2005). A typical PKI authentication scenario is depicted in Fig. 8.12. With a key certificate being created/issued at a CA, clients can securely communicate with each other by sharing public keys for encryption and limiting the access of encrypted contents to private key owners. In addition, a hierarchical trust model is implemented to allow more entities and CAs to participate (Perlman, 1999). Normally hierarchies reflect different security levels, each of which requires certain CAs to respond in a given interaction.

Single sign-on (SSO) has been widely applied to exempt legal users from repeated authentications to potentially remote services (Pashalidis & Mitchell, 2003). This scheme

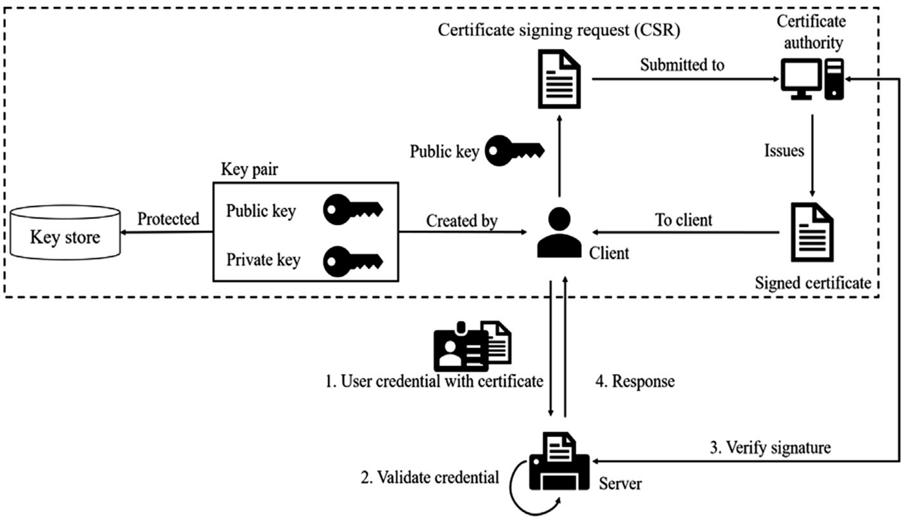

Figure 8.12
PKI certification and authentication.

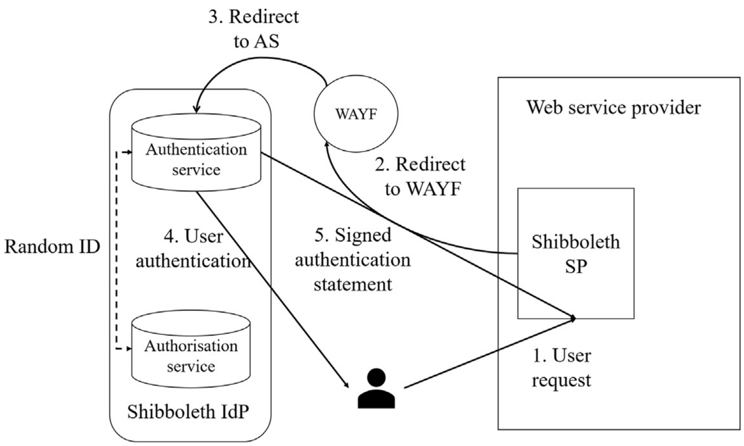

Figure 8.13
Shibboleth components and user authentication (Chadwick & Fatema, 2012).

can be implemented through configuring the Shibboleth system (Chadwick & Fatema, 2012; Watt & Sinnott, 2011). As shown in Fig. 8.13, the SSO process involves at least one identity provider (IdP), service provider (SP), as well as the "where-are-you-from" (WAYF) service. Upon receiving an access request, the SP can redirect the requestor to a WAYF site where he/she can select an IdP to verify the identity. Based on the trust associations among organizations, requested sites should be able to authenticate remote clients based on a local authentication at their home site, and thus enable the same clients to sign in and use multiple services (hosted by different SPs).

8.3.2 Privacy-aware access control

Access control policies are predominantly used to determine "who is allowed to access data and use services." Traditional access control can partially meet the demands in the s-Health context. With the implementation of monitoring, an emergency access control paradigm is demanded to allow save patient lives in some dangerous scenarios. Besides patient-centric methods are studied in smart healthcare. By returning data control back to patients (data owners), patients will be highly motivated to participate in various health-related activities.

8.3.2.1 Patient-centric access control

While using healthcare services, (patient) customers demand to store, use and share health information with their trusted professionals. To encourage their participation, current systems tend to return the control back to users. Here the core idea is to rely on user-centric authentication and authorization for secure data management. In this regard, OpenID and

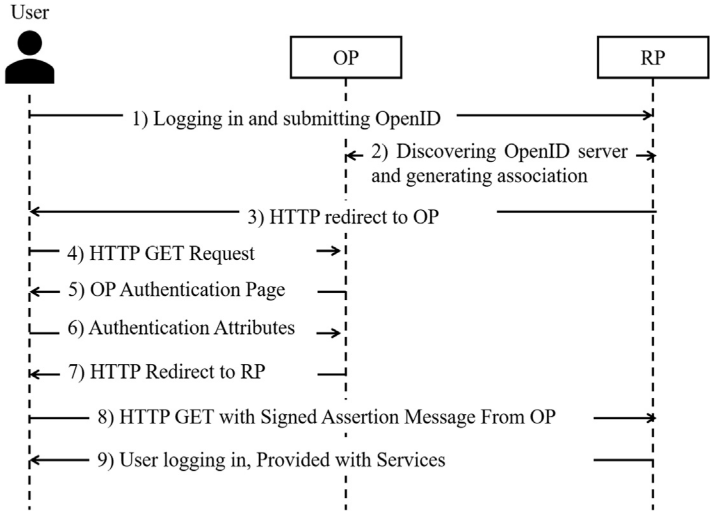

Figure 8.14
OpenID protocol flows.

OAuth can be used together to allow users to be signed in to multiple services with a single identifier and decide whether to authorize specific operations on resources by creating access tokens (Hardt, 2012; Recordon & Reed, 2006). As shown in Fig. 8.14, a typical process should involve at least one user, OpenID provider (OP) and Replaying Party (RP) (Recordon & Reed, 2006). On this basis, OAuth can be implemented among clients, resource owners, resource servers and authorization servers (Hardt, 2012). With this being implemented, resource servers will release online information only when the client presents the verified access tokens by the authorization server (Leiba, 2012).

Google Health and Microsoft HealthVault are featured as user control. Specifically, Google Health users can add their medical information (e.g., history medications, allergies, test results) and define access policies to protect their records at any time. What's more, Google assures that health records will not be shared without users' agreement.[6] Similarly, Microsoft's HealthVault brings users' medical records to an online platform. Through the web-based interface, patients can decide to upload, store in an encrypted database or share health documents with their providers (Gupta, Agrawal, Chhabra, & Dhir, 2016). In the e-health sector, similar access models are developed based on informed consent, one of the essential ethical principles (Kunneman & Montori, 2017; O'Keefe, Greenfield, & Goodchild, 2005). The idea is to let patients decide whether to permit access requests through issuing their consents.

[6] Lohr, S. Google and Microsoft Look to Change Health Care, 2007. Retrieved from https://www.nytimes.com/2007/08/14/technology/14healthnet.html.

8.3.2.2 Staff access control

The role-based access control (RBAC) model was designed for simplifying permission management by creating roles and permissions (Gilbert, 1995). Due to the flexibility, RBAC has been widely applied in e-health systems (Sahi et al., 2018). As shown in Fig. 8.15, nurses may need the writing privilege to input medical records to the database while reading is not necessary in typical healthcare scenarios. Due to their job contents, both pharmacists and physicians need to access related information before prescribing medicines to patients. In addition, some efforts are made to satisfy ethical and legitimate requirements, for example, as required to implement access control models underpinning clinical treatment and research (Brown, Brown, & Korff, 2010; Sicuranza & Esposito, 2013).

RBAC variants were proposed to satisfy special security demands from different systems. For instance, more powerful authorization can be realized by extending with contextual factors (Bertino, Bonatti, & Ferrari, 2001; Hansen & Oleshchuk, 2003). Considering the discrepancy of "roles" in different contexts, semantic technology was applied to formulate such a policy model (Lu & Sinnott, 2015). For general purposes, attribute-based access control was suggested to address requirements about the subject (user), object (health-related records), action (operations), and environment (accessing time, location, etc.), specified in eXtensible Access Control Markup Language (XACML) (Hu et al., 2013; Lu & Sinnott, 2016). Dealing with heterogeneous information silos, the access control should ideally incorporate inference capabilities rather than purely static description and comparison (Lu, Sinnott, & Verspoor, 2018; Lu, Sinnott, Verspoor, & Parampalli, 2018). As shown in Fig. 8.16, a semantic-enhanced framework enables reasoning on related knowledge formalized into ontology

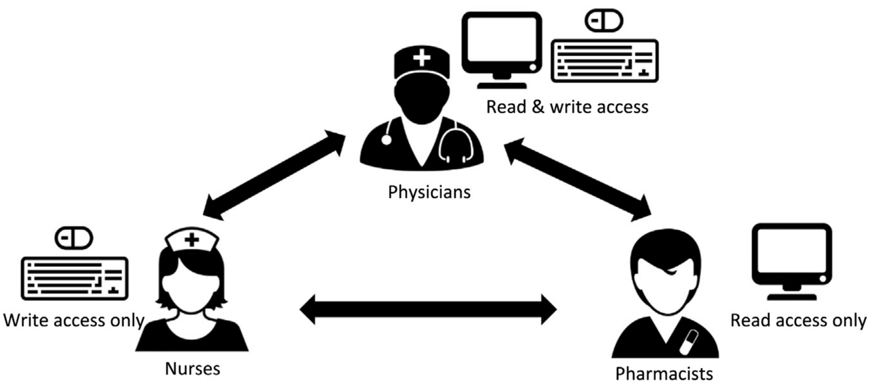

Figure 8.15
Staff access model in healthcare systems (Sahi et al., 2018).

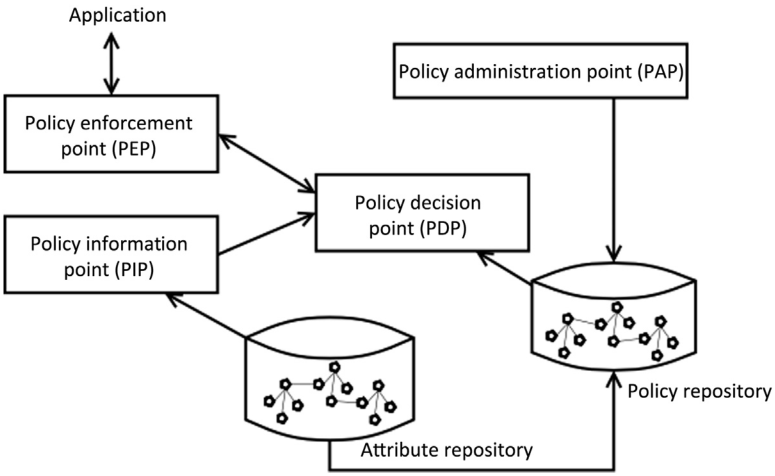

Figure 8.16
Sematic-extended XACML framework.

and semantic rules (Lu & Sinnott, 2018). In addition to deciding the access rights, an obligation component was built on a semantic rule set to infer the level of data disclosure.

8.3.2.3 Break-glass access control

Patient-centric access control is preferred to be used in smart healthcare applications; however, in the situations of emergency, data owners (patients) may not be able to grant access to any doctors for urgent needs. Towards the potential risk, break-glass solutions are introduced as a quick means for extending a person's access rights (Brucker & Petritsch, 2009). Usually, break-glass solutions need to distribute prestaged user accounts in advance. To secure end-to-end communication, Brucker, Petritsch, and Weber (2010) proposed a break-glass solution with ABE techniques being extended. To detect unknown conflicts, a novel break-glass model, Rumpole was formalized in a logic programming language and thus can be extended with reasoning capabilities (Marinovic, Craven, Ma, & Dulay, 2011). As shown in Fig. 8.17, a generic break-the-glass access control architecture (BTG-AC) was proposed within a normal authorization component, that is, policy enforcement point performing as an authentication service provider between users and sensors, and policy decision point making decisions. In the access control module, three types of policies are developed and executed (Maw, Xiao, Christianson, & Malcolm, 2016). Specifically, authorization policies are used to make access decisions, checking if user requests should be permitted or denied; BTG policies are used to perform emergent operations on targeted objects; Obligation policies are used along with authorization and BTG policies in certain situations. For instance, an obligation policy can allow the administrator to take emergent

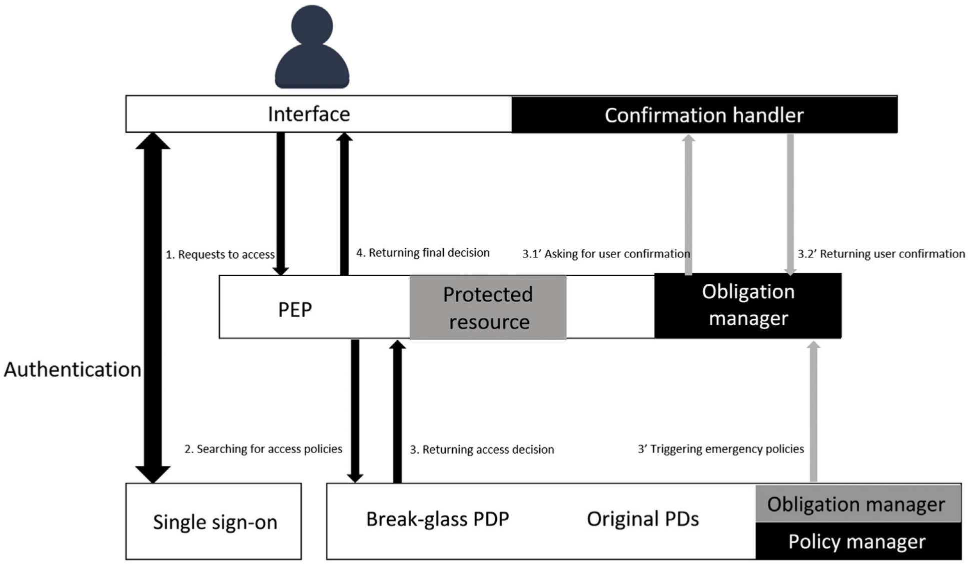

Figure 8.17
Break-glass architecture and message flows.

actions when the "glass is broken," while BTG policies can be defined for emergency situations where urgent access is required.

8.3.3 Anonymization

Privacy preservation is regarded as a personal right to be guaranteed. However, the implementation of monitoring systems may threaten patients' privacy due to unauthorized disclosures of attributes. Aside from patient demands, requirements defined in the ethical and legitimate regulations need to be satisfied in the process of data sharing. For instance, one of the most desirable cases is to ensure no one can be identified from health datasets released for research purposes (Harrelson & Falletta, 2007). When it involves health data analytics, it is necessary to focus on balancing preserving levels and information loss while modifying original values aiming for anonymization.

8.3.3.1 Statistical disclosure control

Statistical disclosure control (SDC) methods offer privacy protection by modifying (identifiable and non-identifiable) attributes at the cost of data utility (Shlomo, 2007). As shown in Fig. 8.18, a Risk-Utility map can be used to describe the trade-off exists between data utility and the privacy preservation: given a maximum tolerable risk level accepted by data custodians (e.g., hospitals) and data subjects (e.g., patients), the optimal SDC strategy should only incur the least information loss (Duncan, Keller-McNulty, & Stokes, 2004).

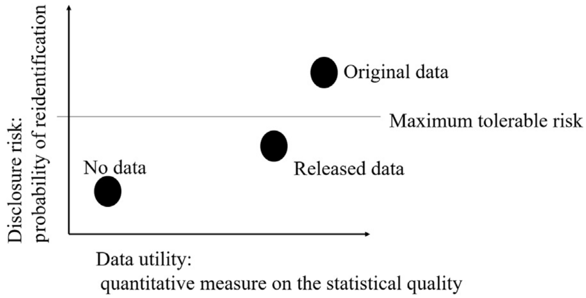

Figure 8.18
Risk-Utility map (Hundepool et al., 2012).

Age	Postcode	Reward
17	3001	1000
19	3002	1200
21	3003	1500
27	3005	5000
29	3117	45,000
34	3128	57,000
45	3159	31,000

Age	Postcode	Reward	
17,27	300*	1000	Group 1
17,27	300*	1200	Group 1
17,27	300*	1500	Group 1
17,27	300*	5000	Group 1
29,45	31**	45,000	Group 2
29,45	31**	57,000	Group 2
29,45	31**	31,000	Group 2

Figure 8.19
Group privacy in the k-anonymized dataset ($k = 3$).

Under such statistical requirements, k-anonymity and its variants are designed to deliver privacy protection by mitigating reidentification chance. Based on a set of predefined quasi-identifiers, k-anonymity requires any target individuals are obscured with $k-1$ other individuals (Sweeney, 2002). For instance, Fig. 8.19 describes an example scenario where a company payroll implements 3-anonymity. After generalizing atomic items, the original records will be released in two (equivalent) groups. On this basis, sensitive values in the *Reward* column can be hidden from illegal access requests.

While considering threats incurred by homogeneity attacks, methods such as l-diversity were designed to prevent sensitive knowledge disclosure from each equivalence group (Machanavajjhala, Johannes, Daniel, & Muthuramakrishnan, 2007). In other words, sanitized data should ensure that there is "diversity" across the sensitive attributes. This requires each group contains at least "l sensitive attribute types." If the target individual is known falling in the second group, his/her salary level can be inferred relatively high. Furthermore, t-closeness provides finer-grained deidentification by controlling the "closeness" among sensitive attributes within each group (Li, Li, & Venkatasubramanian, 2007). Apart from the protection based on mathematic models, SDC methods can be designed in case anyone collects deidentified information and seek out private information in an on-going "requesting and releasing" scenario. To address this issue, the m-invariance model was designed to disallow sensitive attributes updates during a time span (Xiao & Tao, 2007). By tracking the "historical release," τ-safety scheme was designed to adjust attribute combinations in case any disclosure may take place (Anjum & Raschia, 2013).

8.3.3.2 Privacy-preserving big data

Smart healthcare mostly represents a complex system. As a result, the involved activities rely on the integrated analysis on social, economic, political, and cultural information in the healthcare domain. For instance, Marco and Miltiadis (2018) designed an adaptive component by incorporating knowledge discovery into the science research framework. The prototype shows their method empowers the development of patient-centric healthcare with advanced applications, such as personalized medication. In addition, record linkage as a data integration technique has been applied in population-based studies. By comparing individual attributes, records about the same patients can be found and combined as record linkage (or linked records). A typical probabilistic record linkage (PRL) process is shown in Fig. 8.20: by evaluating record pairs against a pre-agreed "threshold", pairwise records can be classified as *Matched*, *Nonmatched*, and *Possibly matched*. In addition, data privacy needs attention to the linkage process (Christen, 2012). Correspondingly,

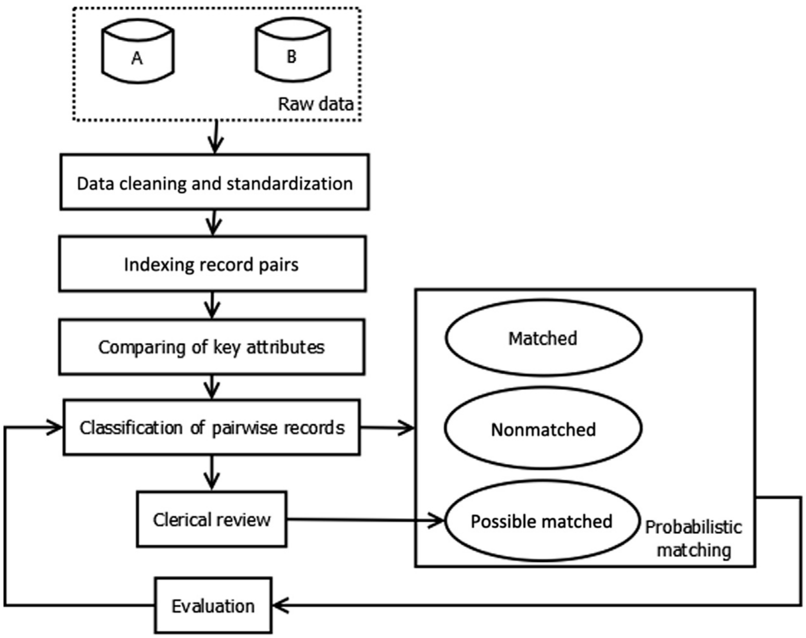

Figure 8.20
Probabilistic record linkage (Schmidlin, Clough-Gorr, & Spoerri, 2015).

privacy-preserving data linkage techniques are developed to match records across databases without revealing confidential information to any external stakeholders (Vatsalan, Sehili, Christen, & Rahm, 2017). Through the implementation of encoding methods on identifiers, high-quality linkage services can be delivered without relying on a "trusted third party" to conduct linkage. Fig. 8.21 depicts the practical model, secure multiparty computation (SMC), which disallows researchers to request the raw data but processed values (Dibben, Elliot, Gowans, Lightfoot, & Data Linkage Centres, 2015). Instead, statistical summaries can be shared among data holders (dashed lines) based on the linkage made with the submitted identifiers (solid lines). In the two-party secure computation protocol, a bloom filter can be used to compare strings and then records (Vatsalan, Christen, & Verykios, 2013). As shown in Fig. 8.22, through exchanging the resultant matrix, it enables similarity calculation based on the "number of edits" (Grannis, Overhage, & McDonald, 2004). To guarantee the privacy and security in results, certain disclosure policies can be added as an extra layer of protection to support SMC models (Durham et al., 2014).

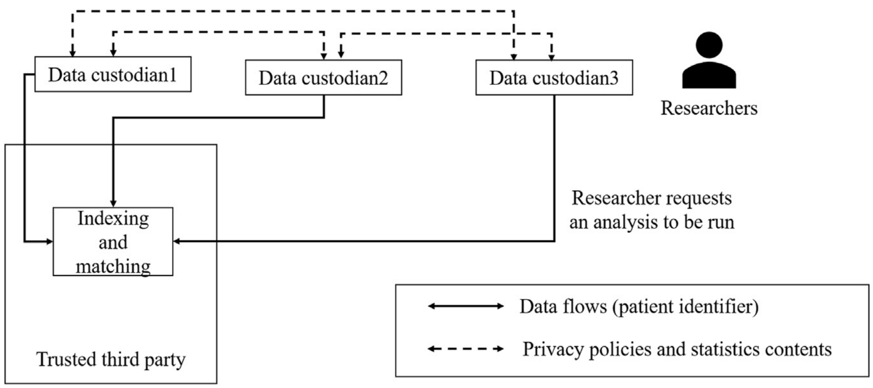

Figure 8.21
Secure multiparty computation linkage (Dibben et al., 2015).

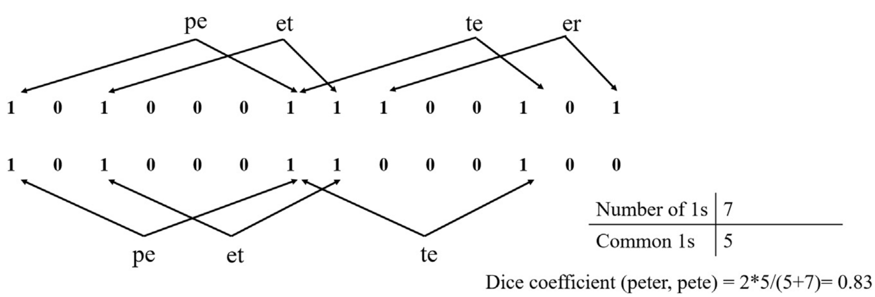

Figure 8.22
An example of bloom filter-based similarity calculation.

8.4 Discussion

Table 8.1 shows a systematic evaluation of selected security and privacy solutions in s-health systems. Specially, all of the key characteristics are identified from the earlier studies on security and privacy protection, as well as techniques implemented in the smart

Table 8.1: Characterization of selected solutions for security and privacy preservation.

	Research issues	Sources	C	A	I	*Novelty*	*Mobility*	*Complexity*	*Richness*
Authentication	IoT authentication	Rahman et al. (2017)	✓	✓		✓✓	✓✓✓	✓✓	✓
	User authentication	De Luca et al. (2015)	✓	✓		✓✓	✓✓✓	✓	✓
		Murillo-Escobar et al. (2015)	✓	✓	✓	✓✓	✓✓	✓✓	✓✓
		Hejazi et al. (2016)	✓	✓		✓✓✓	✓	✓✓✓	✓✓✓
		Zhang et al. (2018)	✓	✓		✓✓✓	✓	✓	✓
	Distributed authentication	Perlman (1999)	✓		✓	✓	✓	✓	✓
		Pashalidis and Mitchell (2003)	✓		✓	✓	✓✓	✓	✓
		Aberer et al. (2005)	✓		✓	✓	✓	✓	✓
		Goyal et al. (2006)	✓		✓	✓✓	✓	✓✓	✓✓
		Bethencourt et al. (2007)	✓		✓	✓✓	✓	✓✓	✓✓
		Watt and Sinnott (2011)	✓	✓	✓	✓	✓	✓	✓
		Chadwick and Fatema (2012)	✓	✓		✓	✓	✓✓	✓
		Ambrosin et al. (2016)	✓		✓	✓	✓	✓	✓
Privacy-aware access control	Patient-centric access control	O'Keefe et al. (2005)	✓	✓		✓✓	✓✓	✓	✓
		Gupta et al. (2016)	✓	✓		✓✓	✓✓	✓✓	✓
		Kunneman and Montori (2017)	✓	✓	✓	✓✓✓	✓✓✓	✓	✓
	Staff access control	Sicuranza and Esposito (2013)	✓	✓		✓	✓	✓	✓
		Brown et al. (2010)	✓	✓		✓	✓	✓	✓
		Sahi et al. (2018)	✓	✓		✓	✓	✓	✓
		Lu, Sinnott & Verspoor (2018)	✓	✓		✓✓	✓	✓✓	✓✓✓
	Break-glass access control	Brucker et al. (2010)	✓	✓		✓✓	✓✓	✓	✓
		Marinovic et al. (2011)	✓	✓		✓✓	✓✓	✓✓	✓
		Maw et al. (2016)	✓	✓		✓✓	✓✓	✓✓	✓✓
Anonymization	Statistical disclosure control	Sweeney (2002)	✓			✓	✓	✓✓	✓
		Machanavajjhala et al. (2007)	✓			✓	✓	✓✓	✓✓
		Xiao and Tao (2007)	✓			✓	✓	✓✓	✓✓
		Anjum & Raschia (2013)	✓			✓	✓	✓✓✓	✓✓
	Privacy-preserving big data	Grannis et al. (2004)	✓			✓	✓	✓✓	✓
		Durham et al. (2014)	✓			✓✓	✓	✓✓	✓✓✓
		Dibben et al. (2015)	✓			✓	✓	✓	✓

cities. The CIA concepts on the left side stand for the general security and privacy requirements. As for the compliance with s-health services, we select *Novelty*, *Mobility*, *Complexity*, and *Richness* as the indicators of assessing related solutions. Depending on the requirements such as "less utility but strong security," stakeholders can decide to configure which solutions in the system for security risk mitigation. A reliable solution (combination) should cover all three aspects—*Authentication*, *Access control*, *Anonymization*, and jointly satisfy the CIA requirements. For each solution, more ✓ showing in one cell means better performance in one certain aspect. As the study continues, Table 8.1 can be certainly enriched within multiple dimensions, such as considering patients' social awareness (e.g., *Immersion* and *Interaction*) and the *Smartness* of methods, depending on to what extents services can be enhanced by using machine learning technologies. Individuals' privacy concerns may cause different expectations. As a result, we suggest it should be considered while assessing the method *Effectiveness*.

8.5 Conclusions and open research issues in future

The adoption of sensors and mobile technologies leads to the provision of healthcare services in a pervasive manner. Through analyzing related concepts of smart city, electronic health (e-health), and mobile health (m-health), it is clear to see smart health (s-health) as a subfield of smart cities, keeping certain characteristics of e-health and m-health frameworks. As health-related activities emerge with ICT applications, it is essential to design the security and privacy solutions accordingly. Existing studies on authentication, access control, and anonymization can generally secure the access to and use of health records while special considerations on "smart features" should be addressed as well. Considering customer trust is intertwined with service quality and privacy concerns, this chapter selectively reviews security and privacy-preserving solutions developed in s-health contexts, and evaluates the potentials of satisfying privacy requirements as well as the assurance of service quality in a data-rich world. Future studies are still necessary for improving current solutions:

1. Processing a huge amount of data about home facilities, traffic, medical cares, and human information, data analytical methods need to be lightweight so as to provide seamless, real-time services. In terms of security and privacy, a highly efficient cryptographic algorithm would be rather desired while exchanging patients' information among platforms—it can guarantee the confidentiality and integrity at a minimal computation cost.
2. Making policies to restrict data collection by sensors and other IoT devices is always seen as a security procedure in smart cities. Sensors are widely deployed to collect patient information, which is then used for performing online data analysis. However, the majority of such data contains personal information and sensitive attributes, which could cause serious privacy issues. In addition to anonymizing personal records, government policies defined for increasing transparency can help strike a balance between benefits and security risks (Visvizi, Lytras, Damiani, & Mathkour, 2018).

3. The establishment of smart health systems relies on the sensing devices usually deployed in the open environment where numerous security risks exist. Therefore, it is essential to design a framework to assess and mitigate potential threats. This can benefit a great number of patients who choose the provided services. However, due to the heterogeneity of information collected by sensors, it is challenging to conceptualize such a knowledge model defining all possible risks and factors that are relevant to the evaluation. Besides, developing techniques for mitigating each treat model is not efficient. Ideally, techniques can be used in combinations to ensure security and privacy preservation in s-health applications (Lytras & Visvizi, 2018).
4. People are always in the center of smart cities (Visvizi & Lytras, 2018). When it comes to health data, patients should be given the rights of deciding with whom their data are shared and how it will be used. Their decisions will impact the quality of s-health services, and in return, their experience may continuously affect their choices. Therefore, the first step of designing security and privacy solutions is to understand individuals' privacy concerns about data exchange and services in smart health systems. The incorporation of these subjective factors to the model (suggested in the last point) can guarantee the correctness of solution formation.

8.6 Teaching assignments

- Q1: In addition to the privacy issues mentioned, what potential risks have you found in existing SHSs? Please discuss in groups and list three to five examples.
- Q2: Based on the answer of Q1, please rank the issues according to their potential impacts and explain why.
- Q3: To the issue ranked at the first place, is there any solutions have been developed can deal with it? If so, please discuss. If not, can you suggest a possible solution?
- Q4: Can you distinguish the concepts "Mobile Health (m-health)", "Smart Health (s-health)" and "Electronic Health (e-health)"? Explain their similarities and differences in your words.
- Q5: Can you summarize the security and privacy requirements in each of fields mentioned in Q4?

References

Aberer, K., Datta, A., & Hauswirth, M. (2005). A decentralized public key infrastructure for customer-to-customer e-commerce. *International Journal of Business Process Integration and Management*, *1*, 26–33. (LSIR-ARTICLE-2005-001).

Ambhati, R. K., Kota, V. K., Chaudhari, S. Y., & Jain, M. (March 2017). *E-IoT: Context-oriented mote prioritization for emergency IoT networks. International conference on wireless communications, signal processing and networking (WiSPNET)* (pp. 1897–1903). IEEE.

Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S. R., Rahmani, A. M., & Liljeberg, P. (2016). On the feasibility of attribute-based encryption on internet of things devices. *IEEE Micro*, *36*(6), 25–35.

Amendola, S., Lodato, R., Manzari, S., Occhiuzzi, C., & Marrocco, G. (2014). RFID technology for IoT-based personal healthcare in smart spaces. *IEEE Internet of Things Journal*, *1*(2), 144–152.

Amrutha, K. R., Haritha, S. M., Haritha Vasu, M., Jensy, A. J., & Charly, J. K. (2017). IOT based medical home. *Network, 1*, 6.

Anjum, A., & Raschia, G. (March 2013). *Anonymizing sequential releases under arbitrary updates*. *Proceedings of the joint EDBT/ICDT 2013 workshops* (pp. 145–154). ACM.

Baig, M. M., & Gholamhosseini, H. (2013). Smart health monitoring systems: An overview of design and modeling. *Journal of Medical Systems*, *37*(2), 9898.

Bertino, E., Bonatti, P. A., & Ferrari, E. (2001). TRBAC: A temporal role-based access control model. *ACM Transactions on Information and System Security (TISSEC)*, *4*(3), 191–233.

Bethencourt, J., Sahai, A., & Waters, B. (May 2007). *Ciphertext-policy attribute-based encryption*. *IEEE symposium on security and privacy 2007 (SP'07)* (pp. 321–334). IEEE.

Brown, I., Brown, L., & Korff, D. (2010). Using NHS patient data for research without consent. *Law, Innovation and Technology*, *2*(2), 219–258.

Brucker, A. D., & Petritsch, H. (June 2009). *Extending access control models with break-glass*. *Proceedings of the 14th ACM symposium on access control models and technologies* (pp. 197–206). ACM.

Brucker, A. D., Petritsch, H., & Weber, S. G. (April 2010). *Attribute-based encryption with break-glass*. *IFIP international workshop on information security theory and practices* (pp. 237–244). Berlin, Heidelberg: Springer.

Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., & Tarricone, L. (2015). An IoT-aware architecture for smart healthcare systems. *IEEE Internet of Things Journal*, *2*(6), 515–526.

Chadwick, D. W., & Fatema, K. (2012). A privacy preserving authorization system for the cloud. *Journal of Computer and System Sciences*, *78*(5), 1359–1373.

Cherdantseva, Y., & Hilton, J. (2013). *A reference model of information assurance and security*. *8th international conference on availability, reliability and security (ARES)* (pp. 546–555). IEEE.

Christen, P. (2012). *Data matching: Concepts and techniques for record linkage, entity resolution, and duplicate detection*. Springer Science & Business Media.

Cody-Allen, E., & Kishore, R. (April 2006). *An extension of the UTAUT model with e-quality, trust, and satisfaction constructs*. *Proceedings of the 2006 ACM SIGMIS CPR conference on computer personnel research: Forty-four years of computer personnel research: achievements, challenges & the future* (pp. 82–89). ACM.

Dafa-Alla, A. F., Kim, E. H., Ryu, K. H., & Heo, Y. J. (2005). *PRBAC: An extended role based access control for privacy preserving data mining*. *Fourth annual ACIS international conference on computer and information science* (pp. 68–73). IEEE.

De Luca, A., Hang, A., Von Zezschwitz, E., & Hussmann, H. (April 2015). *I feel like I'm taking selfies all day: Towards understanding biometric authentication on smartphones*. *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (pp. 1411–1414). ACM.

Demirkan, H. (2013). A smart healthcare systems framework. *It Professional*, *15*(5), 38–45.

Dibben, C., Elliot, M., Gowans, H., Lightfoot, D., & Data Linkage Centres. (2015). The data linkage environment. *Methodological Developments in Data Linkage*, 36–62.

Domingue, J., Galis, A., Gavras, A., et al. (Eds.), (2011). *The future internet*. Berlin, Heidelberg: Springer. Available from https://doi.org/10.1007/978-3-642-20898-0.

Duncan, G. T., Keller-McNulty, S. A., & Stokes, S. L. (2004). Database security and confidentiality: Examining disclosure risk vs. data utility through the RU confidentiality map. National Institute of Statistical Sciences. *Technical Repor*, 142, 1–24.

Durham, E. A., Kantarcioglu, M., Xue, Y., Toth, C., Kuzu, M., & Malin, B. (2014). Composite bloom filters for secure record linkage. *IEEE Transactions on Knowledge and Data Engineering*, *26*(12), 2956–2968.

Fairchild, A. L., Gable, L., Gostin, L. O., Bayer, R., Sweeney, P., & Janssen, R. S. (2007). Public goods, private data: HIV and the history, ethics, and uses of identifiable public health information. *Public Health Reports*, *122*(1_suppl), 7–15.

Firth-Cozens, J. (2004). Organisational trust: The keystone to patient safety. *BMJ Quality & Safety*, *13*(1), 56–61.

Ghamari, M., Janko, B., Sherratt, R. S., Harwin, W., Piechockic, R., & Soltanpur, C. (2016). A survey on wireless body area networks for ehealthcare systems in residential environments. *Sensors*, *16*(6), 831.

Gilbert, M. D. M. (1995). *An examination of federal and commercial access control policy needs*. *National computer security conference, 1993 (16th) Proceedings: Information systems security: User choices* (p. 107) DIANE Publishing.

Gope, P., & Hwang, T. (2016). BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sensors Journal*, *16*(5), 1368–1376.

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (October 2006). *Attribute-based encryption for fine-grained access control of encrypted data*. *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89–98). ACM.

Grannis, S. J., Overhage, J. M., & McDonald, C. J. (2004). Real world performance of approximate string comparators for use in patient matching. *In Medinfo*, 43–47.

Grossman, R. L., Heath, A. P., Ferretti, V., Varmus, H. E., Lowy, D. R., Kibbe, W. A., & Staudt, L. M. (2016). Toward a shared vision for cancer genomic data. *New England Journal of Medicine*, *375*(12), 1109–1112.

Gupta, P., Agrawal, D., Chhabra, J., & Dhir, P. K. (March 2016). *IoT based smart healthcare kit*. *International conference on computational techniques in information and communication technologies (ICCTICT)* (pp. 237–242). IEEE.

Hansen, F., & Oleshchuk, V. (2003). SRBAC: A spatial role-based access control model for mobile systems. In *Proceedings of the 7th nordic workshop on secure IT systems (NORDSEC'03)* (pp. 129–141).

Hardt, D. (2012). *The OAuth 2.0 authorisation framework*. Technical Report.

Harrelson, J. M., & Falletta, J. M. (2007). *The privacy rule (HIPAA) as it relates to clinical research*. *Cancer clinical trials: Proactive strategies* (pp. 199–207). Boston, MA: Springer.

Hejazi, M., Al-Haddad, S. A. R., Singh, Y. P., Hashim, S. J., & Aziz, A. F. A. (2016). ECG biometric authentication based on non-fiducial approach using kernel methods. *Digital Signal Processing*, *52*, 72–86.

Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., & Scarfone, K. (2013). *Guide to attribute-based access control (ABAC) definition and considerations*. NIST Special Publication, 800(162).

Hundepool, A., Domingo-Ferrer, J., Franconi, L., Giessing, S., Nordholt, E. S., Spicer, K., & De Wolf, P. P. (2012). *Statistical disclosure control*. John Wiley & Sons.

Khan, M., Jilani, M. T., Khan, M. K., & Ahmed, M. B. (2017). *A security framework for wireless body area network based smart healthcare system*. *International conference for young researchers in informatics* (pp. 80–85). Kaunas, Lithuania: Mathematics and Engineering (ICYRIME).

Kostadinovska, A., de Vries, G. J., Geleijnse, G., & Zdravkova, K. (2015). *Employing personal health records for population health management*. *ICT innovations 2014* (pp. 65–74). Cham: Springer.

Kumar, R. S., & Saxena, A. (January 2011). *Data integrity proofs in cloud storage*. *3rd international conference on communication systems and networks (COMSNETS)* (pp. 1–4). IEEE.

Kunneman, M., & Montori, V. M. (2017). When patient-centred care is worth doing well: Informed consent or shared decision-making. *BMJ Quality & Safety*, *26*, 522–524.

Leiba, B. (2012). Oauth web authorization protocol. *IEEE Internet Computing*, *16*(1), 74–77.

Li, N., Li, T., & Venkatasubramanian, S. (April 2007). *t-closeness: Privacy beyond k-anonymity and l-diversity*. *IEEE 23rd international conference on data engineering 2007 (ICDE 2007)* (pp. 106–115). IEEE.

Lohr, S. (August 14, 2007). Google and Microsoft Look to Change Health CareWater aerobics. Retrieved from http://www.buzzle.comhttps://www.nytimes.com/2007/08/14/technology/14healthnet.html.

Lowrance, W. (2003). Learning from experience: Privacy and the secondary use of data in health research. *Journal of Health Services Research & Policy*, *8*(1_suppl), 2–7.

Lu, Y., & Sinnott, R. O. (2015). *Semantic security for e-Health: A case study in enhanced access control*. *Ubiquitous intelligence and computing and 2015 IEEE 12th international conference on autonomic and trusted computing and 2015 IEEE 15th international conference on scalable computing and communications and its associated workshops (UIC-ATC-ScalCom)* (pp. 407–414). IEEE.

Lu, Y., & Sinnott, R. O. (August 2016). *Semantic-based privacy protection of electronic health records for collaborative research*. *IEEE trustcom/BigDataSE/ISPA* (pp. 519−526). IEEE.

Lu, Y., & Sinnott, R. O. (2018). Semantic privacy-preserving framework for electronic health record linkage. *Telematics and Informatics*, *35*(4), 737−752.

Lu, Y., Sinnott, R. O., & Verspoor, K. (2018). *Semantic-based policy composition for privacy-demanding data linkage*. *2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)* (pp. 348−359). IEEE.

Lu, Y., Sinnott, R. O., Verspoor, K., & Parampalli, U. (2018). *Privacy-preserving access control in electronic health record linkage*. *2018 17th IEEE international conference on trust, security and privacy in computing and communications* (pp. 1079−1090). IEEE.

Lytras, M., & Visvizi, A. (2018). Who uses smart city services and what to make of it: Toward interdisciplinary smart cities research. *Sustainability*, *10*(6), 1998.

Machanavajjhala, A., Johannes G., Daniel K., & Muthuramakrishnan V. (2007). l-Diversity: Privacy beyond k-anonymity. In *ACM transactions on knowledge discovery from data (TKDD) 1.1* (p. 3).

Malik, S., & Park, S.-H. (2008). Integrated service platform for personalized exercise & nutrition management. In 10th international conference on advanced communication technology 2008 (ICACT 2008) (Vol. 3, pp. 2144−2148). IEEE.

Marco, S., & Miltiadis, L. (2018). Applied data science in patient-centric healthcare: Adaptive analytic systems for empowering physicians and patients. *Telematics and Informatics*, *35*(4), 643−653. Available from https://doi.org/10.1016/j.tele.2018.04.002.

Marinovic, S., Craven, R., Ma, J., & Dulay, N. (June 2011). *Rumpole: A flexible break-glass access control model*. *Proceedings of the 16th ACM symposium on access control models and technologies* (pp. 73−82). ACM.

Maw, H. A., Xiao, H., Christianson, B., & Malcolm, J. A. (2016). BTG-AC: Break-the-glass access control model for medical data in wireless sensor networks. *IEEE Journal of Biomedical and Health Informatics*, *20*(3), 763−774.

Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., & López-Gutiérrez, R. M. (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Systems with Applications*, *42*(21), 8198−8211.

Nguyen, L., Bellucci, E., & Nguyen, L. T. (2014). Electronic health records implementation: An evaluation of information system impact and contingency factors. *International Journal of Medical Informatics*, *83*(11), 779−796.

O'Keefe, C. M., & Connolly, C. J. (2010). Privacy and the use of health data for research. *Medical Journal of Australia*, *193*(9), 537−541.

O'Keefe, C. M., Greenfield, P., & Goodchild, A. (2005). A decentralized approach to electronic consent and health information access control. *Journal of Research and Practice in Information Technology*, *37*(2), 161.

Pashalidis, A., & Mitchell, C. J. (October 2003). *Single sign-on using trusted platforms*. *International conference on information security* (pp. 54−68). Berlin, Heidelberg: Springer.

Prakash, R., & Balaji Ganesh, A. (2019). *Internet of Things (IoT) enabled wireless sensor network for physiological data acquisition*. *International conference on intelligent computing and applications* (pp. 163−170). Singapore: Springer.

Prasser, F., Kohlmayer, F., Spengler, H., & Kuhn, K. A. (2018). A scalable and pragmatic method for the safe sharing of high-quality health data. *IEEE Journal of Biomedical and Health Informatics*, *22*(2), 611−622.

Provost, F., & Fawcett, T. (2013). *Data science for business: What you need to know about data mining and data-analytic thinking*. O'Reilly Media.

Perlman, R. (1999). An overview of PKI trust models. *IEEE Network*, *13*(6), 38−43.

Rahman, F., Bhuiyan, M. Z. A., & Ahamed, S. I. (2017). A privacy preserving framework for RFID based healthcare systems. *Future Generation Computer Systems*, *72*, 339−352.

Recordon, D., & Reed, D. (November 2006). *OpenID 2.0: A platform for user-centric identity management*. *Proceedings of the 2nd ACM workshop on digital identity management* (pp. 11−16). ACM.

Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., & Yaseen, A. (2018). Privacy preservation in e-healthcare environments: State of the art and future directions. *IEEE Access*, *6*, 464–478.

Sakr, S., & Elgammal, A. (2016). Towards a comprehensive data analytics framework for smart healthcare services. *Big Data Research*, *4*, 44–58.

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Schmidlin, K., Clough-Gorr, K. M., & Spoerri, A. (2015). Privacy preserving probabilistic record linkage (P3RL): A novel method for linking existing health-related data and maintaining participant confidentiality. *BMC Medical Research Methodology*, *15*(1), 46.

Shlomo, N. (2007). Statistical disclosure control methods for census frequency tables. *International Statistical Review*, *75*(2), 199–217.

Sicuranza, M., & Esposito, A. (December 2013). *An access control model for easy management of patient privacy in EHR systems*. *8th international conference for Internet technology and secured transactions (ICITST)* (pp. 463–470). IEEE.

Solanas, A., Patsakis, C., Conti, M., Vlachos, I. S., Ramos, V., Falcone, F., & Martinez-Balleste, A. (2014). Smart health: A context-aware health paradigm within smart cities. *IEEE Communications Magazine*, *52*(8), 74–81.

Sweeney, L. (2002). k-Anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(05), 557–570.

Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *6*, 24–31.

Vatsalan, D., Christen, P., & Verykios, V. S. (2013). A taxonomy of privacy-preserving record linkage techniques. *Information Systems*, *38*(6), 946–969.

Vatsalan, D., Sehili, Z., Christen, P., & Rahm, E. (2017). *Privacy-preserving record linkage for big data: Current approaches and research challenges*. *Handbook of Big Data technologies* (pp. 851–895). Cham: Springer.

Visvizi, A., & Lytras, M. D. (2018). Rescaling and refocusing smart cities research: From mega cities to smart villages. *Journal of Science and Technology Policy Management*, *9*(2), 134–145.

Visvizi, A., Lytras, M. D., Damiani, E., & Mathkour, H. (2018). Policy making for smart cities: Innovation and social inclusive economic growth for sustainability. *Journal of Science and Technology Policy Management*, *9*(2), 126–133.

Wang, H., Lee, M. K., & Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM*, *41*(3), 63–70.

Wang, X., Gui, Q., Liu, B., Jin, Z., & Chen, Y. (2014). Enabling smart personalized healthcare: A hybrid mobile-cloud approach for ECG telemonitoring. *IEEE Journal of Biomedical and Health Informatics*, *18*(3), 739–745.

Watt, J., & Sinnott, R. O. (May 2011). *Supporting federated multi-authority security models*. *Proceedings of the 2011 11th IEEE/ACM international symposium on cluster, cloud and grid computing* (pp. 620–621). IEEE Computer Society.

Xiao, X., & Tao, Y. (2007). *M-invariance: towards privacy preserving re-publication of dynamic datasets*. *Proceedings of the 2007 ACM SIGMOD international conference on Management of data* (pp. 689–700). ACM, June.

Zhang, Y., Gravina, R., Lu, H., Villari, M., & Fortino, G. (2018). PEA: Parallel electrocardiogram-based authentication for smart healthcare systems. *Journal of Network and Computer Applications*, *117*, 10–16.

Zhao, X., You, Z., Zhao, Z., Chen, D., & Peng, F. (2010). *Availability based trust model of clusters for MANET*. *7th international conference on service systems and service management (ICSSSM)* (pp. 1–6). IEEE, June.

Further reading

Yue, C. (2013). *The devil is phishing: Rethinking web single sign-on systems security*. *Presented at 6th USENIX workshop on large-scale exploits and emergent threats*. Washington, DC: USENIX.