Data Security and Privacy Issues in Healthcare

Samed BAJRIĆ *

Jožef Stefan Institute, Laboratory for Open Systems and Networks, Jamova cesta 39, 1000 Ljubljana, Slovenia.
E-mail: samed@e5.ijs.si

* Author to whom correspondence should be addressed; Tel.: +386 1 477 37 58

Received: August 23, 2019 /Accepted: March 22, 2020 / Published online: March 30, 2020

Abstract

The entire e-healthcare systems need to be protected from any kind of threat at all times, from sensors to employing the Internet of Things to the core network and everything in between. This paper briefly carried out in order to address the challenges of security and privacy of healthcare data, and the impact of this on interoperability in the e-healthcare setting. Understanding these challenges is crucial for anyone involved in healthcare, as the impact of e-healthcare will have a considerable effect on patients, clinicians, healthcare providers and deliveries.

Keywords: Security; Privacy; Data Protection; e-Health

Introduction

The need for development and organizing new ways of providing efficient healthcare services has been accompanied over the last decade. This has been done by significant progress in information technology, especially the ability to record easily and inexpensively information about each medical transaction and to access this information instantly no matter where it is stored. This change is allowing better health information sharing and it permits users to have control over their personal data more easily. The continuous development in the communication technology in the healthcare sector has led to a new concept called e-health, which refers to any electronic exchange of health-related data collected or analyzed through electronic connectivity for improving efficiency and effectiveness of healthcare delivery [1]. This new concept allows stakeholders and clinicians in executing their duties electronically, instead of using papers and related traditional utilities. When the health information is outsourced to store or process, it is organized as Electronic Health Record (EHR). According to the National Alliance for Health Information Technology EHR can be defined as an electronic record of health-related information on an individual, which is in accordance with nationally recognized standards and interoperability. Access to this information is provided to authorized clinicians and staff across more than one healthcare organization, who can also create and manage this information. Some of the reasons for the exchange of information and invoking authorized partners services in healthcare domain are the following:

- Informing the patient about their treatment and care;
- Monitoring and evaluation of the quality of care;
- Public health emergency preparedness and response capabilities;
- Population health measurement;
- Conducting research on existing and emerging treatment mechanisms.

As healthcare devices continue to evolve, so does their interconnectivity. This interconnectivity enables the digital collection of health data on a large scale, which ultimately results in accelerated development of future IoT applications. Interconnected technology outside of the clinical environment allows health professionals to monitor and adjust implanted devices without the need for a hospital visit or invasive procedures. EHRs can improve patient care by making health information more broadly available [2]. Although e-healthcare systems aim to reduce overall costs and at the same time to adequately improve healthcare quality, they also bring to light new patient issues. An extremely confidential patient data can be compromised at any point from sensors to cloud storage it from all threats. E-healthcare is currently one of the most targeted sectors. Reports highlight the growth of attacks and the rise in medical identity theft with millions of medical records stolen globally. Medical records and healthcare data are now up to 10 times more valuable for selling than other stolen data such as credit card numbers. According to SecureLink [3] the actual value of one medical record is up to $ 50 in comparison to credit card information for $1.50 or social security number for $3; or full medical records including date of birth, credit card details, social security number, address, and e-mails are offered for up to $1000 for U.S. consumers. The most significant attack on an e-healthcare enterprise resulted in the theft of the data of around 78 million people [4]. Medical records contain lots of information, such as personal full name, address, contact information, social security number, insurance details, treatments and more. If healthcare data falls into the wrong hands, it can be used for a variety of sinister purposes. A scammer can use the information to open bank accounts, apply for credit cards or loans, or even file tax returns. They can also be used for harassment or even blackmail. If a famous person's medical records are stolen, hackers could use the information to extort significant sums of money. In order to keep EHR's availability and integrity, as well as the quality of services, it is necessary to pay more attention to security policy and privacy issues. One of the biggest challenges of EHR adoption is understanding the security policy and privacy issues, especially it is important to understand how EHR is protected and what factors lead to significant improvement of a successful e-health system.

In this paper, the possible security and privacy issues in the adoption of EHR by healthcare organizations and services are discussed. It aims to help in understanding the critical security challenges in the entire environment of e-healthcare enterprises.

E-Healthcare Architectures

In order to better understand the essence of e-healthcare as well as the security requirements therein, it is necessary to understand an architectural overview of e-healthcare systems. There have been deployed several EHR architectures throughout the world. The most commonly recognized [5] are the following.

Centralized (Fully Integrated) Model

It has a unique repository of health data and exchanges information with representatives from each member hospital (see Figure 1). In this model, patient health information is transmitted electronically by each member hospital to the clinical data repository. All transmitted information is securely stored and since e-health authority is directly connected to each hospital's patient data repository, the information is keep updated through different interfaces. The cost of establishing and maintaining this model is relatively high because it is necessary to invest in technology in the form of servers, which need to be monitored and stored in a secure, separate location. In addition, all the responsibilities related to this model, including cybersecurity, are exclusively within the jurisdiction of one body, this might be the Ministry of health or the National e-health center.

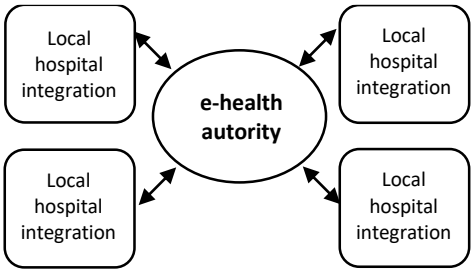

Figure 1. Centralized model

Decentralized (Federated) Model

In this model, as opposed to centralized, patient health information is not stored in a centralized location, but it is locally stored with the regional central authority (see Figure 2). The centralized model agrees to provide the overreaching state or central authority with their unique patient identifier information, which is stored in the patient's registry, or record locator service. In addition, in the decentralized model, EHR is powered by the central authority but instances exist in several healthcare organizations.

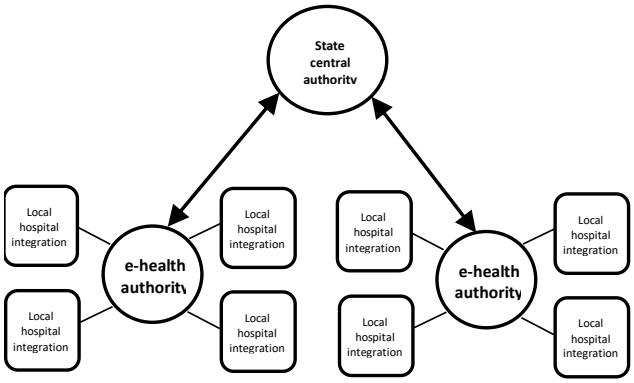

Figure 2. Decentralized model

Hybrid Model

This model is a combination of a centralized and decentralized model as can be seen in Figure 3.

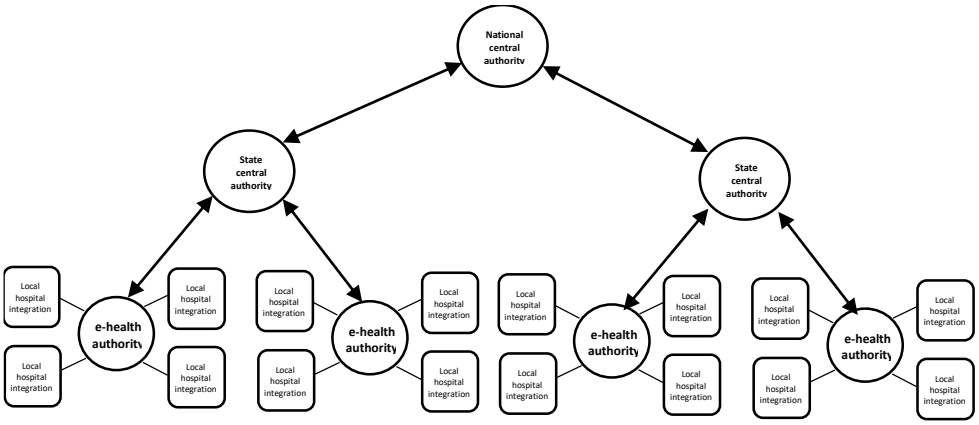

Figure 3. Hybrid model

Therefore, regarding the performed studies, the electronic health record architecture can be defined as the science of study and characterizing its components (content and structure), the

relationship among components, and the relationship between the set of components and the environment (confidentiality and security). The main components of any e-healthcare system are [6]:

- **Core network:** It contains all the information and servers.
- **Body area network (BAN):** It contains sensors and provides necessary information about patient healthcare parameters.
- **Users of the e-healthcare system:** It contains users possible located in a remote position with respect to the system's core network (physician, pharmacist, stakeholders).
- **Communication link:** It connects each of these to form a single uniform system.

Regarding architecture of the electronic health record, answers are sought to determine how, by whom and in which structure the data should be collected, to whom they should be accessible and how the access of others should be limited. In other words, in order to establish the electronic health record, all the information required to establish the record content should be identified and defined and their structure must be specified and standardized and that privacy and security of data should be considered as a critical issues [7].

Advantages and Disadvantages of EHR

With the advent of digital storage, there has also been a debate over-contribution which way is better for storing data, digital or traditional with the paper. Of course, healthcare has not bypassed this debate either. In this regard, one of the conclusions of this debate that can be found in the literature is that EHRs offer more significant advantages over paper records, though EHRs themselves are not without drawbacks. Below we describe some of the major advantages and disadvantages of EHR that can be found in the literature.

The main advantages of EHR can be summarized as follows:

- ***Time.*** Weekly savings in documentation using EHRs are an average of 15 hours, which is valuable time that can be spent on a patient. On the other hand, some experts have found that healthcare providers spend too much time learning to use EHRs, which results in physicians moving away from patients, i.e. physicians paying less attention to patients.
- ***Quality improvement.*** The EHR has tremendous potential to improve quality in health care and reduce medical errors. Patients may find EHR attractive because doctors report that with the EHR, health issues can be resolved with fewer in-office interactions since many visits were replaced with telephone encounters and a secure e-mail messaging, saving the patient travel time [8].
- ***Security***. It is well-known that paper records are vulnerable in two ways. The first one is by being misplaced, and the second is by getting stolen. On the other hand, EHRs are at risk due to a massive increase in the number of successful cyberattacks over the past years.
- ***Illegibility.*** Anyone who has visited a doctor at least once in his life knows that doctor's notes are illegible. Also, due to insufficient space on the paper, most of what is written is not legible. With EHRs, this cannot happen, because the doctors have an unlimited amount of space for writing, which leads to the fact that it is not necessary to write illegible abbreviations. Moreover, everything is typed and is easily legible.
- ***Patient access.*** With the more comprehensive use of electronic health records, and improving the health treatment services, online portals have been created by medical providers, which enables patients to have access to their medical records. The patients have the opportunity to access their medical records at any time and to see a treatment plan prescribed by their doctor.

The main disadvantages of EHR can be summarized as follows:

- ***Access to the patient file.*** An employee should not access to a patient's file without prior permission. Also, if a doctor who has access to a patient's file provides detailed information about his health to his family without the patient's prior consent, it could be considered as a privacy violation. Therefore, proper training of medical staff is required to avoid such things.

- ***EHR must be updated.*** In order to ensure compatibility and smooth operation, an electronic health record platform should always be updated/upgraded to the latest version. This is very important since an outdated system can leave some software vulnerabilities and exploit some security holes.
- ***EHR systems are not cheap.*** The main obstacles to the EHR are high cost, lost income during the transitional period, while doctors learn to use the system and uncertain financial benefits. This is why many facilities need to hire additional IT professionals to transfer their knowledge to employees and enable them a very simple and easy to use electronic health record platform.

Privacy and Security Challenges in EHR

The security aspects of the e-health system have been an active research field among researchers. Privacy is one of the biggest obstacles preventing e-health providers from gaining patient trust and implementing e-health system in full capacity. It is often defined as having the ability to facilitate or promote fundamental values such as personal autonomy (the ability to make personal decisions) or individuality or human dignity. It also enables individuals to control how their e-healthcare information is managed and used by clinicians and other users in domains other than healthcare. In order to exercise the privacy rights of individuals as efficiently as possible, it is governed by the law, which imposes an obligation on specific systems to ensure this issue. Within the healthcare community, both privacy and confidentiality are so closely related that sometimes the two have come to be considered as the same, and are sometimes used interchangeably. Therefore, confidentiality is seen as protecting the interest of the organization and privacy as protecting the autonomy of the individual, while in common medical usage both privacy and confidentiality mean the same [9]. In addition, the success of e-healthcare and the realization of its promises is reflected in protecting the privacy of patients' identifiable health information. The secure exchange of e-healthcare information inside the organization itself or more of them requires standards for security measures and privacy protection. Therefore, the EHR systems need to implement global security and privacy conceptualizations that include global standards for clinician's roles, patient consent, and semantically interoperable audit trails and logs. Some of the major privacy and security challenges in EHR systems are listed below.

Access Control and Authentication

Access control is necessary for ensuring proper authorization and confidentiality for patient records. Robust, reliable and standards forms of authentication are a particularly important requirement for protecting the privacy of patient records. It is the initial stage of the users' validation in order to determine their identity which is necessary to ensure that they are authorized to access the system [10]. By privacy rule patients should have full visibility of how their health records are used and for what purposes. However, this aspect has not been fully addressed by concerned parties and continues to be under violation. In addition, the patient's involvement in the management of their health data in EHR would probably improve the privacy issues.

Data Integrity

Ensuring integrity is one of the most crucial keys in the EHR system since it guarantees the accuracy of data thus minimizing errors and improving the safety of patients [11]. Incorrect input of the information by staff or miscommunication between the paper and electronic medical records, or insufficient knowledge of the use of standard information exchange protocols leads to such errors.

System Availability

It is essential for achieving the continuity of electronic healthcare in order to ensure the best services. For instance, if the network is down, the healthcare providers will not be able to access the

patient's data and cannot prescribe. It is therefore considered that the availability of networks and information systems are very critical. The system should not be considered to a specific time of the day; otherwise the physician's job will be made complex since decisions cannot be made in real-time as required [12].

Data Loss

In this framework, considering that personal and confidential data are stored digitally, it is essential to protect the data from loss. In the case of data loss, it is necessary to achieve data recovery which can be challenging due to software and hardware errors, network errors, or security attacks.

Network Security

Data protection becomes crucial when the security of other critical assets relies on network security. Disruption to network functionality and for instance, denial service attacks can have a major impact on healthcare delivery. One of the most common network security technique is the use of firewalls. Using a firewall is a very successful approach to keep an organization network and the protected health information as secure as possible. On the other side, the use of a firewall can be costly and vary based on many factors, such as the work environment and size of an organization, and the budget criteria.

Existing Security Solutions in E-Health

One of the ways of providing a better quality of healthcare delivery is to share patient's data across a variety of users. However, as a consequence of this way is that specific patient's data may be compromised. On the other hand, the use of different cryptographic algorithms for keeping the sensitivity of personal medical information requires high costs, primarily when modification techniques are employed. Some of the existing security solutions are described below:

- ***Data encryption.*** Encryption is the traditional solution used. Although it provides simple access control, it is not applicable to complex EHR systems that require various access requirements. The main role in the security process of e-health communications plays the key management protocols. Moreover, the transmission rate is highly influenced by complex encryption algorithms or transmission protocols that sometimes fail to perform data transmission. Gong et al. [13] designed a prototype system based on a lightweight private homomorphism algorithm and an encryption algorithm improved from the Data Encryption Standard. Secure authentication and key agreement scheme based on the concept of Diffie-Hellman key exchange, which can create secure ways for the system participants when they register has proposed by Li et al. [14]. This scheme is suitable for implementation in the current mobile emergency medical systems.
- ***Data access control***. There are various encryption methods such as symmetric key encryption, asymmetric key encryption, and attribute-based encryption that can be applied in access control. However, it is evident that in health information systems exist some drawbacks for authorization in meetings, the needs of patient health information. This is particularly related to noncryptographic approaches lacking a secure and reliable mechanism for access policy enforcement, while cryptographic approaches being too expensive, complex, and limited in specifying policies. Lounis et al. [15] presented an architecture based on attribute-based encryption which has a data value to express validity data of the emergency key. Researchers, Li et al. [16] proposed a novel framework based on attribute-based encryption techniques to encrypt each patient's data file to guarantee a high degree of patient privacy. In addition, role-based access control and attribute-based access control are the most popular models for healthcare application clouds.
- ***Data search.*** In order to better protect the privacy of data, it is necessary to encrypt sensitive data before sending them through a network. But, once the data is encrypted, then it is not possible to use plaintext keyword search, which means that enabling an encrypted cloud data

search is of great importance. In addition, if the encrypted data search results cannot be applied promptly, then all measures of security and privacy have less meaning. Miao et al. [17] proposed a multi-keyword search scheme over encrypted personal health records in a more challenging multi-owner setting supporting both fine-grained access control and multi-keyword search in cloud storage. Recently, Guo et al. [18] proposed a decryptable attribute-based keyword search scheme that can resist chosen plaintext attack and chosen keyword attack. This scheme can be implemented in the eHealth cloud platforms, especially in a telemedicine system.

- ***Data anonymization.*** Patient sensitive data can be divided into three categories: explicit identifiers (ID number, name, cell phone), quasi-identifiers (age, birth date, address), and privacy attributes (illness, income). Data anonymous technology can be efficiently used to solve issues such as k-anonymity, l-diversity, and confidence bounding. Liu and Li [19] proposed a specific threat model about the data sharing process of wearable devices' data based on the k-anonymity algorithm as the building block of privacy. For instance, k-anonymity is used as the privacy criteria in real applications such as the Family educational rights and privacy act of United States [20].
- ***Trusted third-party auditing.*** To ensure correctness of data, a third-party auditor can verify the integrity of the data stored in the cloud. Whenever the audit request comes from client, the third-party auditor sends the challenge request to the cloud service provider. It then compares the challenge response to ensure the data integrity and availability. Also auditor can efficiently audit the cloud data storage without demanding the local copy of data. Many researchers have been presented auditing methods over the past decades. For inst ance, Govaert et al. [21] presented a review showing the effects of surgical auditing on hospital costs. They showed that surgical auditing can function as a quality instrument and therefore as a tool to reduce costs. Hence, the third-party auditor can be implemented in the mobile user's computational resource thus achieving cost-effectiveness to gain trust in the cloud storage server.

Future Challenges of Privacy and Security in EHR

Protecting healthcare information security, privacy and confidentiality is a continuous process and serious responsibility of every health care organization. Although EHRs are increasingly used by patients, doctors and other healthcare professionals because of several advantages but it brings several privacy and security problems together. In the following, we present several challenges that require special attention.

In order that e-healthcare organizations to successfully implement widely accepted security standards, it is necessary to establish secure connections over the network, particularly in the domains of audit logs, data encryption, TLS assertions, access rights policy, and many more related to data integrity and resilience of systems. Therefore, correct interoperability will gradually increase end-user experience which will also lead to the establishment of a new type of service over open networks and not in closed and private networks as it is so far.

The protection against traffic analysis to prevent data forensics by inference and to improve obfuscation while maintaining accountability and the privacy of individual transactions. This needs further attention as every member of the Blockchain can see all transactions. This Blockchain technology offers a secure platform for storing medical and other health information with certain benefits such as security, anonymity and integrity of data without third party intervention. It was introduced by Nakamoto [22], to have a cryptographically secured and decentralized currency that would be helpful for financial transactions. But soon this new technology is being used in many other applications [23]. Blockchain technology could be a future solution for common problems in healthcare such as EHR interoperability, auditing, privacy and granting of data access control by patients. In addition, it could provide a new model for health information exchange by making EHR more efficient and secure.

The major issues in cloud computing are data security and it has many aspects like confidentiality, integrity, reliability, availability, backup and recovery. The potential research direction would be to find ways to store and process data in a way that does not breach privacy and security.

Conclusions

As we can see, there have been developed numerous security techniques that can be used in e-healthcare to provide unauthorized access to sensitive patient data. Using these security techniques properly depend on many factors such as the work environment and size of an organization, and the budget criteria. On the other hand, it is very difficult to say when e-healthcare information and its management environment are secure from breaches of privacy. It is well-known that absolute security is impossible to attain. Therefore, a secure technological environment that is based on privacy laws and policies must manage e-healthcare information. Moreover, the implementation of a security and privacy technique throughout all levels of the underlying stack is the only promising approach for secure e-health data.

Conflict of Interest

The author declares that he has no conflict of interest.

Acknowledgements

This work is supported by research project "Technology and business aspects of the future e-health ecosystem" founded by Ministry of education, science and sport, Republic of Slovenia.

References

1. Cashen M, Dykes P, Gerber B. E-Health technology and internet resources: barriers for vulnarable populations. Journal of Cardiovascular Nursing 2004;19(3):209-14.
2. Shenoy A, Appel JM. Safeguarding confidentiality in electronic health records. Cambridge Quarterly of Healthcare Ethics 2017;26(2):337-41.
3. Selck-Paulsson D. Why is the healthcare vertical such an attractive target? [Online] 2019 [Cited 2020 March 3] Available from: https://securelink.net/de-de/insights/why-is-healthcare-an-attractive-target/
4. Mathews W. Anthem: Hacked Database Included 78.8 Million People. [Online] 2015 [Cited 2019 October 18]. Available: https://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364.
5. Health Information Exchange: Architecture Types. [Online] 2012 [Cited 2019 October 18] Available: https://corepointhealth.com/health-information-exchange-architecture-types/
6. Miao F, Jiang L, Li Y, Zhang Y-T. Biometrics based novel key distribution solution for body sensor networks. 2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Minneapolis, MN, 2009, pp. 2458-61. doi: 10.1109/IEMBS.2009.5334698
7. Fernández-Alemán JL, Senor IC, Lozoya PAO, Toval A. Security and privacy in electronic health records: a systematic literature review. Journal of Biomedical Informatics 2013;46(3):541-62.
8. Chen C, Garrido T, Chock D, Okawa G, Liang L. The Kaiser permanente electronic health record: transforming and streamlining modalities of care. Health Affairs 2009;28(2):323-33.
9. Shoniregun CA, Dube K, Mtenzi F. Electronic healthcare information security. New York: Springer, 2010.
10. Lillian R. Access control in healthcare information systems. [Online] 2009 [Cited 2019 October 18]. Available from: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/249994

11. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. International Journal of Internet and Enterprise Management 2010;6(4):279-314.
12. Sicuranzsa M, Esposito A, Ciampi M. A semantic access control for easy management of the privacy for EHR systems. 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Guangdong, 2014, pp. 400-5. doi: 10.1109/3PGCIC.2014.84.
13. Gong T, Huang H, Li P, Zhang K, Jiang H. A medical healthcare system for privacy protection based on IoT. 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Nanjing, 2015, pp. 217-22. doi: 10.1109/PAAP.2015.48.
14. Li C-T, Lee C-C, Weng C-Y. A secure cloud-assisted wireless body area network in mobile emergency medical care system. Journal of Medical Systems 2016;40(5) 1-15.
15. Lounis A, Hadjidj A, Bouabdallah A, Challal Y. Secure medical architecture on the cloud using wireless sensor networks for emergency management. 2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications, Compiegne, 2013, pp. 248-52. doi: 10.1109/BWCCA.2013.142
16. Li M, Yu S, Zheng Y. Scalable and secure sharing of personal health records in cloud computing using attribute based encryption. IEEE Transactions on Parallel and Distributed Systems 2012;24(1):131-43.
17. Miao Y, Ma J, Liu X, Wei F, Liu Z, Wang XA. m2- ABKS: attribute-based multi-keyword search over encrypted personal health records in multi-owner setting. Journal of Medical Systems 2016;40(11):1-12.
18. Guo L, Li Z, Yau W-C, Tan S-Y. A decryptable attribute-based keyword search scheme on eHealth cloud in Internet of things platforms. IEEE Access 2020;8:26107-18.
19. Liu F, Li T. A clustering k-anonymity privacy-preserving method for wearable IoT devices. Security and Communication Networks 2018;2018:1-8.
20. Family Educational Rights and Privacy Act. [Online] 2015 [Cited 2019 October 18]. Available from: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
21. Govaert JA, Van Bommel ACM, Van Dijk WA, Van Leersum NJ, Tollenaar RAEM, Wouters MWJM. Reducing healthcare costs facilitated by surgical auditing: a systematic review. World Journal of Surgery 2015;39(7) 1672-80.
22. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. [Online] 2008 [Cited 2019 October 18]. Available from: https://bitcoin.org/bitcoin.pdf.
23. Qamar SU, Khalid A. Using Blockchain for electronic health records. IEEE Access 2019;7:147782-95.