A Study on Authentication Factors in Electronic Health Records

Manoj Jayabalan[1], Thomas O'Daniel[2]
[1,2]School of Computing & Technology, Asia Pacific University of Technology & Innovation,
57000 Kuala Lumpur, Malaysia
[1]manoj@apu.edu.my, [2]dr.thomas.odaniel@apu.edu.my

Abstract— **Privacy and security are one the major challenge for the healthcare providers to maintain with increasing security breaches. User authentication is an essential factor to implement in Electronic Health Records (EHRs) to protect patient data and prevent malicious users from gaining access to the medical server. As Single Factor Authentication (SFA) are prone to vulnerabilities, due to the user using weak passwords and hackers are able to crack the passwords in sophisticated techniques such as brute force, dictionary attack, etc. The International Standards require the healthcare organizations using the Multi-Factor Authentication (MFA) to protect patient privacy and security. The complexity of authentication can be increased using the combination of two or more independent factors (smartcard, security hardware token, biometrics, etc.). This study presents the review of different authentication factors employed in EHRs such as secure communications, handheld devices, smart card, and biometric. It will be beneficial for the researchers to know the current trends and understand the areas that require improvement in the authentication framework.**

Index Terms— **Authentication, Healthcare, Electronic health records, Smart card, Biometric**

1. Introduction

With the advancement of information technology and the pervasive nature of digital services in healthcare leads to the massive explosion of data. Privacy and security are one the major challenge for the healthcare to maintain with increasing security breaches. Authentication is one of the fundamental methods to ensure the confidentiality and availability of data to the legitimate user. Typically, the first step/component in the access control model consists of user verification; once it is satisfied, the user is given access to the patient's critical data (Grassi et al., 2017). The traditional and most widely used approach used to identify the legitimacy of the user consists of supplying a username and password, a system known as Single Factor Authentication (SFA).

In Raza et al. (2012) argue that SFA is the most straightforward method to implement and inexpensive, but it is prone to vulnerabilities such as users using weak passwords that are easily cracked, phishing attacks, and other conventional hacker techniques. As such, there is apparently a need for healthcare organizations to employ Multi-Factor Authentication, such as using a combination of two or more independent authentication factors (passwords, smart cards, biometrics, security tokens, user behavior, etc.), offers extra security protection (ISO, 2014).

This study discusses the different authentication factors employed in electronic health records. It will be beneficial for researchers to understand the areas that require improvement in the authentication framework and current trends.

2. Electronic Health Records

The Electronic Health Records (EHRs) is an information system consisting of patient medical data such as treatments, medical histories, radiology image, etc., in a digital format. It benefits the healthcare providers to streamline the workflow, to provide a better decision on patient care, timely service and share the patient medical data among the participating entities (HealthIT.gov, 2013).

The scope of EHR is broader in terms of the user accessing the medical data from the ubiquitous environment, and patients' information is collected from different sources such as laboratory, pharmacy, sensors, wearable devices, etc. This information can assist healthcare and government agencies to analyze patients' behavior, diseases severity, and groundbreaking discoveries, which required safeguarding from adversaries at any cost. (Eikey et al., 2015) says privacy violation can lead to penalties from the respective agencies in their country, such as Health Insurance Portability Accountability Act (HIPAA) in the United States of America, European Data Directive 95/46/EC in the European Union, etc. Security of healthcare information commences with the protection of patient medical records by guaranteeing that privacy, confidentiality, integrity, and availability of the EHR system. Technology advancement is rapid as never before, but, the aspect of privacy and security concerns in EHR remain unclear towards consumers as a result of prevailing breach thus lowering the trust (Papoutsi et al., 2015).

According to the US Department of Health & Human Services, five pillars of healthcare security are access control, audit control, authentication, integrity, and transmission security (Centers for Medicare and Medicaid Services, 2007). The first three components can be combined into a single logical unit (access control) used for protecting the patient data throughout the active application level whereas the "transmission security" focus towards encrypting the data either in rest or motion. The integrity is implicitly achieved through access control and authentication via allowing only the legitimate user to perform a set of actions in the patient data. The explanation of the different authentication factors employed in electronic health records are given in the below section, and access control, audit control, and transmission security is left beyond the scope of this study.

3. Authentication Factors

This study presents a comprehensive review of the literature and patent of authentication for electronic health record to protect patient's privacy and security. Articles from 2006 to 2017 were extracted from the IEEE Xplore Digital Library, Science Direct, MEDLINE, and MetaPress using broad eligibility criteria, and the patents from 2006 to 2017 filing date were extracted from the patent office (USA, Canada, Europe, and the UK) which are indexed in Google Patent Search. Authentication methods proposed only for EHR are considered and the authentication models for medical logistic authentication, medical device authentication, etc. were left outside the scope of this review.

The password is the oldest and predominant authentication factor that exists in the information security world. Four broad areas of authentication are being actively investigated and developed; secure communication, a handheld device, smart card and biometric. Transmitting the password/credentials in the secure protocol between the client and medical server are typical security features. Nearly, 84% of the research clustered into smart card (67%) and handheld device (17%) as a factor to perform the authentication. There is an increase in the amalgamation of biometric authentication systems in smart cards and handheld devices since these grant access only after validating a subject's unique characteristics.

Few articles are chosen for this review focus on multifactor authentication to enforce additional protection at the primary point of entry to the system. This is not surprising as multifactor authentication is usually closely associated with cryptography (even in ISO 22600-1:2014), and cryptographic standards and methods have been ruled outside the scope of this study.
Location is used as an authentication factor in (Choi et al., 2013) to determine the access using proximity bounding protocol. Many Bluetooth devices rather than an expensive device can be installed in trusted regions in order to authenticate access to EHR. Multifactor authentication is applied to risk adaptive authentication in (Boonyarattaphan et al., 2010) as a solution for normal, abnormal and critical situations. The normal situation is performed with one-factor authentication, and for other situations the authentication process checks spatial and temporal parameters to determine the authenticity of the user.

Two articles (Khan & Sakamura, 2012, 2015) have shown interest in using the eTRON tamper-resistant smart card/SIM card/USB for authentication. The eTRON device contains a unique identifier and is given to every individual user (doctor and nurse), so it can be used to perform mutual authentication and provide a secure connection using public key cryptography.

3.1. Secure Communications

The password is the oldest and predominant authentication factor that exists in the information security world. Transmitting the password in the secure protocol between the client and medical server are therefore typical security features (Lee et al., 2013b; Odelu et al., 2016). The simple group password-based authentication reduces the complexity of managing multiple public keys in the server through sharing common session key based on the user role. The individual user password act as a separate private key to join the group and securely communicate (Lee et al., 2013b). The improvements have been proposed in the dynamic group password-based authentication to join the user in a group through randomly generated server key and deleted when the user leaves the session (Odelu et al., 2016).

Integrating the Healthcare Enterprise (IHE) promotes the standards for disconnected healthcare organizations to utilize Cross-Enterprise Document Sharing using Portable Media (XDM). Authenticating the subjects accessing the EHR in rural areas is a big challenge without proper IT infrastructure and Internet connection. Thus a protocol was proposed using the security assertion markup language with a security token to verify the individual identity (Masi et al., 2011).
Exchanging the patient data among the participating healthcare requires a secure framework considering several security components. One article proposes mutual authentication using digital certificates to be exchanged while requesting access to the data to prevent man-in-the-middle attack and replay attack (Ibrahim et al., 2016).

Two studies (Ray & Biswas, 2014; Choe & Yoo, 2008) utilize PKI that is issued to the patient, doctor, and nurse upon registration to the system and access to medical data are granted based on the verification of certificates. The mutual authentication between the parties is controlled through a registration key generated using a Diffie-Hellman (DH) technique (Ray & Biswas, 2014).

Three articles (Sahi et al., 2016; Lin & Lee, 2014; Lee, 2014) adopted the three-party key authenticated exchange protocol (3PAKE) protocol based on the DH, one article (Xie et al., 2014a) with 3PAKE based on Elliptic Curve Cryptography (ECC) for the verifier-based authentication that does not require to manage keys in the server and (Lin & Lee, 2014) extended with chaotic map. The cloud service further extended with pairing based cryptography (based on identity-based cryptography) to perform mutual authentication between the parties (patient, doctor) and digital signature to nonrepudiation the information (Chen et al., 2014).

Authentication to the medical server is improved with fewer key management and computation time using the Shamir's threshold scheme and Schnorr's digital scheme since they benefit in forwarding secure function (Yu & Hou, 2014). It maintains the trustworthiness of the records even after the private keys are renewed.

3.2. **Handheld devices**

The advancement in mobile technology has led to a rapid evolution in the user behavior towards communicating to the system. The ubiquitous computing allows healthcare practitioners to access patient medical data with different devices, and the access request is increasing through mobile devices. There is a need to provide secure network system architecture through two-step authentication in order to protect from compromised networks, phishing attack or unwanted remote access. The secure token also known as One Time Password (OTP) generated by the server are sent to the user mobile device to verify the identity is the usual approach for authentication (Setianto & Utami, 2014; Mirkovic et al., 2011; Goncalves et al., 2015; Abdellaoui et al., 2016) and suggest to encrypt the data for better protection (De Luca et al., 2016).

There is a gradual migration from the healthcare industries to move patient data into the cloud which require additional protection to safeguard the data stored in the vendor data center. The ready-to-go architecture proposed based on hybrid encryption and the two-factor authentication to combine the passwords with tokens generated by mobile devices (Goncalves et al., 2015). Two article suggest using a hash function for the password, ECC for signature and symmetric algorithm for encrypting the patient data (Chiou et al., 2016; Abdellaoui et al., 2016) and further extended with image-based password (Abdellaoui et al., 2016). One article (Siddiqui et al., 2014) suggest to include bio-metric characteristics as an additional factor to increase the complexity in the cloud.

The cryptography technologies are extended in the smartphone to protect attribute disclosure in the sensitive domain. U-Prove is a token-based approach applied for authenticating to patient medical data through mobile devices. The token is similar to PKI but differs in providing minimal disclosure of attribute and traceability which can significantly reduce the mobile phone related attacks (Zeb et al., 2016). One study proposed attribute-based authentication to eliminate the linkability between identities and patient information to preserve the attribute disclosure (Guo et al., 2014). The approach was designed for mobile communication between the patients and doctors in a decentralized system. The authentication between the participating entities is achieved through identity-based cryptography and zero-knowledge proofs.

Impersonation is one of the threats in pervasive computing that can be overcome through the utilization of Near Field Communication (NFC) to exchange message between the mobile device and tags installed within the Local Area Network (LAN) (Quincozes & Kazienko, 2016). The impersonation solution beyond the LAN was suggested by the inventor (Kia Ebrahimi, 2011) utilizing the unique user identifier, device id and the passphrase (spoken voice phrase) are encrypted and verified in the medical server to initiate data exchange. The probabilities of the false alarm are maintained to a minimum through restricting the passphrase to the username. The Markov Models algorithm suggested to analysis biometric characteristic with different parameters such as acoustic, phonotactic and prosodic subsystem for better performance. The user anonymity are achieved through the chaotic map and bio-hashing function (Das & Goswami, 2014).

Further, the mobile device extended as identity management to ease doctor, without the need to type credentials in web-based EHR (Xie et al., 2013a). The doctors are required to launch the mobile application to enter the master password to verify their identity in the trusted server, and OTP pushed to the mobile device that needs to be entered into the EHR for authentication.

3.3. **Smart cards**

The smart card provides convenience to verify the practitioner requesting to access data/resource. Password-based user authentication scheme (Wu et al., 2012c) proposed for the integrated healthcare to share patient medical data with the combination of smart card and password to identify the subject.

The one-way hash function to secure password storage/medical history due to the capabilities to generate the digital signature and to ensure the authenticity of the smart card (Li & Hwang, 2010; Das, 2015a; Lee et al., 2013a; Li et al., 2015a; Wang et al., 2016; Wu et al., 2012b, 2012c; Li et al., 2014b; Xie et al., 2013b; Wu & Xu, 2012; Lee, 2013; Wen & Guo, 2014; Mir et al., 2015; Wei et al., 2012; Debiao et al., 2012; Sutrala et al., 2016).

Four articles (Das, 2015a; Li et al., 2015a; Wu et al., 2012c; Chen et al., 2012) have included bitwise operations to increase the computation for the variable length and one article (Wu et al., 2012b) proposed Advanced Encryption Standard (AES) protect patient medical data, two articles (Wu & Xu, 2012; Wu et al., 2012a) utilized AES and RSA (Chandrakar & Om, 2015; Giri et al., 2015) for mutual communication. One article (Xie et al., 2013b) uses Rabin encryption to the password stored in the smart card. One article (Khan & McKillop, 2013) describe the use of the eTRON tamper-resistant smart card/SIM card/USB for authentication. The eTRON device contains a unique identifier and is given to every individual user (doctor and nurse), so it can be used to perform mutual authentication and provide a secure connection using public key cryptography.

Two articles suggest to include the patient and doctor smart cards together for efficient data exchange and authentication (Kardas & Tunali, 2006; Lee & Lee, 2008). Smart cards with an encryption key (Data Encryption Standard (DES)) and digital signature are used to secure the data stored on the card and doctors are allowed to access the patient data only when both the cards are inserted into the reader (Kardas & Tunali, 2006). The session based solution proposed for the efficient storage of patient information in the smart card and master key for authentication. Doctors can access the patient information only when they physically present the smart card to concern person, which in-turn increase the privacy. However, suffers from the availability of information in an emergency situation and require massive data storage capacity to store medical history (Lee & Lee, 2008).

Further, smart card security has been extended with hybrid PKI to secure the communication (Hu et al., 2010; Giri et al., 2015). The key generation and management using PKI require a higher resource, in order to decrease the computation complexity and increase the performance of smart card based authentication, ECC and its variants was proposed (Huang & Liu, 2011; Amin et al., 2015b, 2015a; Xu et al., 2014; Xie et al., 2014b; Arshad et al., 2015; Liu & Chung, 2016). The communication security between the parties is extended with 3PAKE and a signature scheme based on discrete logarithmic for efficient identification of smart cards (Islam & Biswas, 2015). The inventor proposes to secure the smart card password communication using Strong Password-Only Authentication Key Exchange (SPEKE), Diffie-Hellman Encrypted Key Exchange (DH-EKE), Bellovin-Merritt protocol or Password Authenticated Connection Establishment (PACE) (Gotthardt, 2011).

User anonymity is an essential consideration to personal privacy of the user in the healthcare and extended to authentication framework using the dynamic identity-based authentication and chaotic maps for hiding real user identity (Li et al., 2016; Hao et al., 2013). Further improvements were proposed with extending the chaotic maps and its variants, one-way hash function, and/or fuzzy extractor to protect the biometric information stored in the smart card (Wang et al., 2016; Li et al., 2014b; Wang et al., 2015; Li et al., 2014a; Jiang et al., 2014; Awasthi & Srivastava, 2013; Tan, 2014; Lou et al., 2015).

The user anonymity and overhead of managing the credentials in the trusted server achieved through storing the biometric template and password in the smart card for authentication (Li & Hwang, 2010). Three articles (Amin et al., 2015b; Mishra & Barnwal, 2015; Mishra et al., 2014) uses bio-hashing on the fingerprint templates stored in the smart card for “genuine user identification” and reduce false rate. One article (Islam & Khan, 2014) suggest using ECC based mutual authentication such that it is secured against the hardness assumption of computational DH problem. The privacy of the patient information the smart care is achieved through Cipher Block Chaining which preserves the plaintext which is being encrypted and minor alteration in any of the block causes the entire data to be corrupt (Jiang et al., 2013) and one article (Guo et al., 2015) suggest ID-mBJM model to improve the privacy.

Paruchuri (Paruchuri, 2015) invented the authentication using the smart card technology with fingerprint authentication. The frameworks work with PKI, digital certificates and the medical data stored in the card are encrypted using RSA. The healthcare practitioners can view patient medical data through exchanging the pseudorandom number for proving legitimacy. The two-factor authentication utilizing password and biometric verification is proposed to improve the security (Maitra & Giri, 2014). In order to increase the security inpatient data either in the cloud or medical server, the author suggested using three-factor authentication such as password, smart card and biometric (Jiang et al., 2016; Das, 2015b). The approach provides a patient-centric model to control their medical data utilizing ECC protocol, and the biometric templates use a fuzzy extractor since its ability to extract the string from the template with error tolerance unlike the conventional hash function, which is sensitive to minor variation in the input.

Network attacks and user anonymity are the common issues in the smart card based authentication, Wen et.al proposed quadratic residue to overcome the issue (Wen, 2014). Islam et.al (Islam et al., 2015) extended Wen et.al with the intractable assumption of the quadratic residue problem in the multiplicative group to validate the correctness of identity and password in the login and password change phase. Both the Wen et.al (Wen, 2014) and Islam et.al (Islam et al., 2015) were unable to support the password change in offline that was overcome by Ta Li (Li et al., 2015b).

The identity-based cryptography is an exciting proportion applied to the smart card to ensure only the legitimate person can decrypt the message using the master private key issued by the trusted central authority and patient public key (Mao et al., 2015). One article showed the zero knowledge protocol for authentication in cloud service to verify using the secret id provided during the registration and responding the challenge to grant access (Kahani et al., 2016).

With the advancement and innovation of smart card to store patient medical data, the authors extended the capabilities to derive questions based on the medical history to be used as a Q&A challenges. The medical data are abstracted using the attribute value taxonomies into a hierarchical data tree (Fong & Zhuang, 2012).

Two articles (Wen, 2013; David et al., 2015) proposed secure protocol using a counter-based authentication mechanism and dynamic-id based authentication adopted from 3rd Generation Partnership Project (3GPP) standard for cellular networks. The extension of the OpenID 2.0 was proposed with the smart card to leverage the secure infrastructure to transmit patient records (Falcao-Reis & Correia, 2010).

The badge based approach was proposed to improve the usability of the authentication through limiting the frequent need for the password to be entered into the system for accessing medical data. The location and time constraints are included with the authentication module to validate the access request through RFID tags (Jin & Qihua, 2012; Graves et al., 2010).

3.4 **Biometric**

The biometric properties of a user for authentication are gaining immense interest from the recent software products or organizations, as it tackles the issue of transferability of credentials (Caldwell, 2015). There are different biometric characteristic such as iris, voice, face, fingerprint, etc., to measure a unique characteristic of the user for securing authentication from different threats.

Biometric-based authentication is categorized into the physiological and behavioral property of the user. The physiological property covers the visible part of the human body such as the retina, fingerprint, etc. On the other hand, behavioral property analyzes the behavior of a user through user profiling, gait, mouse dynamics, keystroke dynamics, etc. These unique behavior properties can be used to enhance user verification process and develop multi-modal user authentication system. For instance, by implementing user behavior profiling alongside with password-based authentication system, the impostor will not only need to obtain the knowledge of the password but also the knowledge of how the user behaves to a different application.

SpeechXRays is implemented for EHR that can perform user authentication with voice acoustics and audio-visual identity verification. This approach tries to replace the traditional authentication factor (username and password). It may suffer from a high false rejection rate during the emergency situation, and/or low ambient setting but provides superior anti-spoofing capabilities (Spanakis et al., 2016). Fingerprint and pin for authentication proposed in the EHR for efficient identification (Han et al., 2006).

The inventor claims the RFID tag and Vascular Infrared Verification (VIV) will provide better authentication for the in-patient. The tag will assist to verify the proximity of the patient and healthcare practitioner while performing a transaction and VIV provide additional security with better accuracy (Bryant, 2013).

The behavioral biometric strike the balance between security and usability via monitoring the user behavior throughout the active session. According to Global Opportunity Report 2017, "*Behavioral biometrics analyses specific human behavior with intelligent software, adding a new layer of security to verifying identification that is nearly impossible to replicate, without any additional stress for the user. Products and services in this market are moving digital security beyond simple passwords, ensuring that as cybercriminals become more advanced, so too do everyday users*" (DNV GL AS, 2017).

The behavioral biometrics such as keystrokes, mouse dynamics, which are usually captured under static and controlled conditions. These approaches are vulnerable to replay attacks, human interaction simulation, and advanced malware injections. However, the behavioral biometrics are trained as the user operates the system which is difficult to be mimic by the robots due to the "invisible challenge" and improve security with the cognitive fingerprint of the user (Turgeman & Zelazny, 2017; Ferbrache, 2016).

4. **Conclusions**

This study discusses the different authentication factors employed in the electronic health records. The articles discussing secure communication were mainly interested in reducing the key exchange between the client and the medical server. Transmitting the password in the secure protocol between the client and medical server are therefore typical security features. Smart cards can be used for authentication and can also double up as a secure means to store and transport medical history. The recent interest on the smart card was towards user anonymity, and finally, the biometric authentication is gaining immense interest in the healthcare. The two main drawbacks are that smartcard data storage is limited and a particular reader is required for validation.

Similarly, the smartphone was also used to store medical history, interact with EHR, and extended to perform authentication. There is an increase in biometric authentication systems in healthcare organizations since these grant access only after validating a subject's unique characteristics. Three-factor authentication using a combination of the above can offer greater security, but as it is more complicated, and organizations have to maintain acceptable efficiency levels.

References

Abdellaoui, A., Khamlichi, Y.I. & Chaoui, H. (2016). A Robust Authentication Scheme for Telecare Medicine Information System. *Procedia Computer Science*. 58. p.pp. 584–589.

Amin, R., Islam, S.H., Biswas, G.P., Khan, M.K. & Kumar, N. (2015a). An Efficient and Practical Smart Card Based Anonymity Preserving User Authentication Scheme for TMIS using Elliptic Curve Cryptography. *Journal of Medical Systems*. 39 (11).

Amin, R., Islam, S.H., Biswas, G.P., Khan, M.K. & Obaidat, M.S. (2015b). Design and Analysis of an Enhanced Patient-Server Mutual Authentication Protocol for Telecare Medical Information System. *Journal of Medical Systems*. 39 (11).

Arshad, H., Teymoori, V., Nikooghadam, M. & Abbassi, H. (2015). On the Security of a Two-Factor Authentication and Key Agreement Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems*. 39 (8).

Awasthi, A.K. & Srivastava, K. (2013). A biometric authentication scheme for telecare medicine information systems with nonce. *Journal of Medical Systems*. 37 (5). p.pp. 1–4.

Boonyarattaphan, A., Bai, Y., Chung, S. & Poovendran, R. (2010). Spatial-Temporal Access Control for E-health Services. In: *2010 IEEE Fifth International Conference on Networking, Architecture, and Storage*. 2010, pp. 269–276.

Bryant, B.J. (2013). *Computer system and method for managing medical care*.

Caldwell, T. (2015). Market report: healthcare biometrics. *Biometric Technology Today*. 2015 (1). p.pp. 5–10.

Centers for Medicare and Medicaid Services (2007). Security Standards: Technical Safeguards. *HIPAA Security Series*. [Online]. 2. p.pp. 1–17. Available from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf.

Chandrakar, P. & Om, H. (2015). RSA Based Two-factor Remote User Authentication Scheme with User Anonymity. *Procedia Computer Science*. 70. p.pp. 318–324.

Chen, C.-L., Yang, T.-T., Chiang, M.-L. & Shih, T.-F. (2014). A privacy authentication scheme based on cloud for medical environment. *Journal of medical systems*. 38 (11). p.p. 143.

Chen, H.-M., Lo, J.-W. & Yeh, C.-K. (2012). An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems*. 36 (6). p.pp. 3907–3915.

Chiou, S.Y., Ying, Z. & Liu, J. (2016). Improvement of a Privacy Authentication Scheme Based on Cloud for Medical Environment. *Journal of Medical Systems*. 40 (4). p.pp. 1–15.

Choe, J. & Yoo, S.K. (2008). Web-based secure access from multiple patient repositories. *International Journal of Medical Informatics*. 77 (4). p.pp. 242–248.

Choi, S., Gutierrez, C., Lim, H.-S., Bagchi, S. & Bertino, E. (2013). Secure and resilient proximity-based access control. In: *International workshop on Data management & analytics for healthcare - DARE '13*. 2013, ACM, pp. 15–20.

Das, A.K. (2015a). A secure and robust password-based remote user authentication scheme using smart cards for the integrated EPR information system. *Journal of medical systems*. 39 (3). p.p. 25.

Das, A.K. (2015b). A Secure User Anonymity-Preserving Three-Factor Remote User Authentication Scheme for the Telecare Medicine Information Systems. *Journal of Medical Systems*. 39 (3).

Das, A.K. umar & Goswami, A. (2014). An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. *Journal of medical systems*. 38 (6). p.p. 27.

David, D.B., Rajappa, M., Karupuswamy, T. & Iyer, S.P. (2015). A Dynamic-Identity Based Multimedia Server Client Authentication Scheme for Tele-Care Multimedia Medical Information System. *Wireless Personal Communications*. 85 (1). p.pp. 241–261.

Debiao, H., Jianhua, C. & Rui, Z. (2012). A More Secure Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems*. 36 (3). p.pp. 1989–1995.

DNV GL AS (2017). *Global Opportunity Opportunity*.

Eikey, E. V., Murphy, A.R., Reddy, M.C. & Xu, H. (2015). Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings. *International Journal of Medical Informatics*. 84 (12). p.pp. 1065–1075.

Falcao-Reis, F. & Correia, M.E. (2010). Patient empowerment by the means of citizen-managed Electronic Health Records: web 2.0 health digital identity scenarios. *Studies in health technology and informatics*. 156. p.pp. 214–228.

Ferbrache, D. (2016). Passwords are broken – the future shape of biometrics. *Biometric Technology Today*. 2016 (3). p.pp. 5–7.

Fong, S. & Zhuang, Y. (2012). Using medical history embedded in biometrics medical card for user identity authentication: data representation by AVT hierarchical data tree. *Journal of biomedicine & biotechnology*. 2012. p.p. 539395.

Giri, D., Maitra, T., Amin, R. & Srivastava, P.D. (2015). An Efficient and Robust RSA-Based Remote User Authentication for Telecare Medical Information Systems. *Journal of Medical Systems*. 39 (1).

Goncalves, R., Leonova, E., Puttini, R. & Nascimento, A. (2015). A privacy-ensuring scheme for health data outsourcing. In: *2015 International Conference on Cloud Technologies and Applications (CloudTech)*. June 2015, IEEE, pp. 1–7.

Gotthardt, F. (2011). *Communication method of an electronic health insurance card with a reading device*.

Grassi, P.A., Garcia, M.E. & Fenton, J.L. (2017). *Digital identity guidelines: revision 3*. [Online]. Gaithersburg, MD. Available from: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

Graves, A.F., Johnson, B. & Jeff, F. (2010). *Use of location awareness to establish and suspend communications sessions in a healthcare environment*.

Guo, D., Wen, Q., Li, W., Zhang, H. & Jin, Z. (2015). A Novel Authentication Scheme Using Self-certified Public Keys for Telecare Medical Information Systems. *Journal of Medical Systems*. 39 (6).

Guo, L., Zhang, C., Sun, J. & Fang, Y. (2014). A privacy-preserving attribute-based authentication system for mobile health networks. *IEEE Transactions on Mobile Computing*. 13 (9). p.pp. 1927–1941.

Han, S., Skinner, G., Potdar, V., Chang, E. & Wu, C. (2006). New Framework for Authentication and Authorization for e-Health Service Systems. In: *2006 IEEE International Conference on Industrial Technology*. 2006, IEEE, pp. 2833–2838.

Hao, X., Wang, J., Yang, Q., Yan, X. & Li, P. (2013). A Chaotic Map-based Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems*. 37 (2). p.p. 9919.

HealthIT.gov (2013). *What is an electronic health record (EHR)*. [Online]. 2013. Available from: https://www.healthit.gov/providers-professionals/faqs/what-electronic-health-record-ehr. [Accessed: 2 February 2017].

Hu, J., Chen, H.-H.H. & Hou, T.-W.W. (2010). A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. *Computer Standards and Interfaces*. 32 (5–6). p.pp. 274–280.

Huang, H.-F.F. & Liu, K.-C.C. (2011). Efficient key management for preserving HIPAA regulations. *Journal of Systems and Software*. 84 (1). p.pp. 113–119.

Ibrahim, A., Mahmood, B. & Singhal, M. (2016). A Secure Framework for Medical Information Exchange (MI-X) between Healthcare Providers. In: *2016 IEEE International Conference on Healthcare Informatics (ICHI)*. October 2016, IEEE, pp. 234–243.

Islam, S.H. & Biswas, G.P. (2015). Cryptanalysis and improvement of a password-based user authentication scheme for the integrated EPR information system. *Journal of King Saud University - Computer and Information Sciences*. 27 (2). p.pp. 211–221.

Islam, S.H. & Khan, M.K. (2014). Cryptanalysis and Improvement of Authentication and Key Agreement Protocols for Telecare Medicine Information Systems. *Journal of Medical Systems*. 38 (10).

Islam, S.K.H., Khan, M.K. & Li, X. (2015). Security Analysis and Improvement of 'a More Secure Anonymous User Authentication Scheme for the Integrated EPR Information System'. *PloS one*. 10 (8). p.p. e0131368.

ISO (2014). *BS EN ISO 22600-1:2014: Health informatics. Privilege management and access control. Overview and policy management*.

Jiang, Q., Khan, M.K., Lu, X., Ma, J. & He, D. (2016). A privacy preserving three-factor authentication protocol for e-Health clouds. *The Journal of Supercomputing*. 72 (10). p.pp. 3826–

3849.

Jiang, Q., Ma, J., Lu, X. & Tian, Y. (2014). Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. *Journal of medical systems*. 38 (2). p.p. 12.

Jiang, Q., Ma, J., Ma, Z. & Li, G. (2013). A privacy enhanced authentication scheme for telecare medical information systems. *Journal of Medical Systems*. 37 (1).

Jin, H. & Qihua, W. (2012). *Secure and usable authentication for health care information access*.

Kahani, N., Elgazzar, K. & Cordy, J.R. (2016). Authentication and Access Control in e-Health Systems in the Cloud. In: *Proceedings - 2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and S*. 2016, pp. 13–23.

Kardas, G. & Tunali, E.T. (2006). Design and implementation of a smart card based healthcare information system. *Computer Methods and Programs in Biomedicine*. 81 (1). p.pp. 66–78.

Khan, A. & McKillop, I. (2013). Privacy-Centric Access Control for Distributed Heterogeneous Medical Information Systems. In: *IEEE International Conference on Healthcare Informatics*. 2013, Philadelphia, PA: IEEE, pp. 297–306.

Khan, M.F.F. & Sakamura, K. (2012). Context-awareness: exploring the imperative shared context of security and ubiquitous computing. In: *14th International Conference on Information Integration and Web-based Applications & Services*. 2012, pp. 101–110.

Khan, M.F.F. & Sakamura, K. (2015). Fine-grained access control to medical records in digital healthcare enterprises. In: *International Symposium on Networks, Computers and Communications, ISNCC 2015*. 2015, pp. 1–6.

Kia Ebrahimi, O. (2011). *Secure and Mobile Biometric Authentication for Electronic Health Record Management*.

Lee, T.-F., Chang, I.-P., Lin, T.-H. & Wang, C.-C. (2013a). A secure and efficient password-based user authentication scheme using smart cards for the integrated EPR information system. *Journal of medical systems*. 37 (3). p.p. 9941.

Lee, T.-F.F. (2014). Verifier-based three-party authentication schemes using extended chaotic maps for data exchange in telecare medicine information systems. *Computer Methods and Programs in Biomedicine*. 117 (3). p.pp. 464–472.

Lee, T.F. (2013). An efficient chaotic maps-based authentication and key agreement scheme using smartcards for telecare medicine information systems. *Journal of Medical Systems*. 37 (6).

Lee, T.F., Chang, I.P. & Wang, C.C. (2013b). Simple group password-based authenticated key agreements for the integrated EPR information system. *Journal of Medical Systems*. 37 (2).

Lee, W. Bin & Lee, C.D. (2008). A cryptographic key management solution for HIPAA privacy/security regulations. *IEEE Transactions on Information Technology in Biomedicine*. 12 (1). p.pp. 34–41.

Li, C.-T. & Hwang, M.-S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*. 33 (1). p.pp. 1–5.

Li, C.-T., Weng, C.-Y., Lee, C.-C. & Wang, C.-C. (2015a). A Hash Based Remote User Authentication and Authenticated Key Agreement Scheme for the Integrated EPR Information System. *Journal of medical systems*. 39 (11). p.p. 144.

Li, C.-T., Weng, C.-Y., Lee, C.-C. & Wang, C.-C. (2015b). Secure User Authentication and User Anonymity Scheme based on Quadratic Residues for the Integrated EPRIS. In: *Procedia Computer Science*. 2015, pp. 21–28.

Li, C., Lee, C., Weng, C.-Y. & Chen, S. (2016). A Secure Dynamic Identity and Chaotic Maps Based User Authentication and Key Agreement Scheme for e-Healthcare Systems. *Journal of Medical Systems*. [Online]. 40 (11). p.p. 233. Available from: http://link.springer.com/10.1007/s10916-016-0586-2.

Li, C.T., Lee, C.C. & Weng, C.Y. (2014a). A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. *Journal of Medical Systems*. 38 (9).

Li, X., Wen, Q., Li, W., Zhang, H. & Jin, Z. (2014b). Secure Privacy-Preserving Biometric Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems*. 38 (11).

Lin, T.-H. & Lee, T.-F. (2014). Secure Verifier-Based Three-Party Authentication Schemes without Server Public Keys for Data Exchange in Telecare Medicine Information Systems. *Journal of Medical Systems*. 38 (5). p.p. 30.

Liu, C.-H. & Chung, Y.-F. (2016). Secure user authentication scheme for wireless healthcare sensor networks. *Computers & Electrical Engineering*. 000. p.pp. 1–12.

Lou, D.C., Lee, T.F. & Lin, T.H. (2015). Efficient biometric authenticated key agreements based on extended chaotic maps for telecare medicine information systems. *Journal of Medical Systems*. 39 (5).

De Luca, G., Brattstrom, M. & Morreale, P. (2016). Designing a secure e-health network system. In: *2016 Annual IEEE Systems Conference (SysCon)*. April 2016, IEEE, pp. 1–5.

Maitra, T. & Giri, D. (2014). An Efficient Biometric and Password-Based Remote User Authentication using Smart Card for Telecare Medical Information Systems in Multi-Server Environment. *Journal of Medical Systems*. 38 (12).

Mao, K., Chen, J., Liu, J. & Wang, M. (2015). Security enhancement on an authentication scheme for privacy preservation in Ubiquitous Healthcare System. In: *2015 4th International Conference on Computer Science and Network Technology (ICCSNT)*. 2015, pp. 885–892.

Masi, M., Pugliese, R. & Tiezzi, F. (2011). A standard-driven communication protocol for disconnected clinics in rural areas. In: *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*. June 2011, IEEE, pp. 304–311.

Mir, O., van der Weide, T. & Lee, C.C. (2015). A Secure User Anonymity and Authentication Scheme Using AVISPA for Telecare Medical Information Systems. *Journal of Medical Systems*. 39 (9).

Mirkovic, J., Bryhni, H. & Ruland, C.M. (2011). Secure solution for mobile access to patient's health care record. In: *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*. June 2011, IEEE, pp. 296–303.

Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, M.K. hurram & Chaturvedi, A. (2014). Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. *Journal of medical systems*. 38 (5). p.p. 41.

Mishra, R. & Barnwal, A.K. (2015). A Privacy Preserving Secure and Efficient Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems*. 39 (5). p.pp. 1–10.

Odelu, V., Das, A.K. & Goswami, A. (2016). A secure effective dynamic group password-based authenticated key agreement scheme for the integrated EPR information system. *Journal of King Saud University - Computer and Information Sciences*. [Online]. 28 (1). p.pp. 68–81. Available from: http://dx.doi.org/10.1016/j.jksuci.2014.04.008. [Accessed: 23 December 2016].

Papoutsi, C., Reed, J.E., Marston, C., Lewis, R., Majeed, A. & Bell, D. (2015). Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. *BMC medical informatics and decision making*. 15. p.p. 86.

Paruchuri, V.K. (2015). *Portable health record system and method*.

Quincozes, S.E. & Kazienko, J.F. (2016). A secure architecture based on ubiquitous computing for medical records retrieval. In: *2016 8th Euro American Conference on Telematics and Information Systems (EATIS)*. April 2016, IEEE, pp. 1–8.

Ray, S. & Biswas, G.P. (2014). A Certificate Authority (CA)-based cryptographic solution for HIPAA privacy/security regulations. *Journal of King Saud University - Computer and Information Sciences*. 26 (2). p.pp. 170–180.

Raza, M., Iqbal, M., Sharif, M. & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal*. 19 (4). p.pp. 439–444.

Sahi, A., Lai, D. & Li, Y. (2016). Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan. *Computers in Biology and Medicine*. 78. p.pp. 1–8.

Setianto, Y.B.D. & Utami, Y.R.W. (2014). A new patients' rights oriented model of EMR access security. In: *2014 International Conference on Advanced Computer Science and Information System*. [Online]. October 2014, IEEE, pp. 19–24. Available from: http://ieeexplore.ieee.org/document/7065858/.

Siddiqui, Z., Abdullah, A.H., Khan, M.K. & Alghamdi, A.S. (2014). Smart environment as a service: Three factor cloud based user authentication for telecare medical information system. *Journal of Medical Systems*. 38 (1).

Spanakis, E.G., Spanakis, M., Karantanas, A. & Marias, K. (2016). Secure access to patient's health records using SpeechXRays a mutli-channel biometrics platform for user authentication. In: *2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. August 2016, IEEE, pp. 2541–2544.

Sutrala, A.K., Das, A.K., Odelu, V., Wazid, M. & Kumari, S. (2016). Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems. *Computer Methods and Programs in Biomedicine*. 135. p.pp. 167–185.

Tan, Z. (2014). A user anonymity preserving three-factor authentication scheme for telecare medicine information systems. *Journal of Medical Systems*. 38 (3).

Turgeman, A. & Zelazny, F. (2017). Invisible challenges: the next step in behavioural biometrics? *Biometric Technology Today*. 2017 (6). p.pp. 5–7.

Wang, C., Zhang, X. & Zheng, Z. (2016). An improved biometrics based authentication scheme using extended chaotic maps for multimedia medicine information systems. *Multimedia Tools and Applications*. (37).

Wang, Z., Huo, Z. & Shi, W. (2015). A Dynamic Identity Based Authentication Scheme Using Chaotic Maps for Telecare Medicine Information Systems. *Journal of Medical Systems*. 39 (1).

Wei, J., Hu, X. & Liu, W. (2012). An Improved Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems*. 36 (6). p.pp. 3597–3604.

Wen, F. (2014). A More Secure Anonymous User Authentication Scheme for the Integrated EPR Information System. *Journal of Medical Systems*. 38 (5). p.p. 42.

Wen, F. (2013). A robust uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. *Journal of medical systems*. 37 (6). p.p. 9980.

Wen, F. & Guo, D. (2014). An improved anonymous authentication scheme for telecare medical information systems. *Journal of medical systems*. 38 (5). p.p. 26.

Wu, F. & Xu, L. (2012). Security analysis and Improvement of a Privacy Authentication Scheme for Telecare Medical Information Systems. *Journal of Medical Systems*. 37 (4). p.pp. 1–9.

Wu, Z.-Y., Lee, Y.-C., Lai, F., Lee, H.-C. & Chung, Y. (2012a). A Secure Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems*. 36 (3). p.pp. 1529–1535.

Wu, Z.-Y., Tseng, Y.-J., Chung, Y., Chen, Y.-C. & Lai, F. (2012b). A Reliable User Authentication and Key Agreement Scheme for Web-Based Hospital-Acquired Infection Surveillance Information System. *Journal of Medical Systems*. 36 (4). p.pp. 2547–2555.

Wu, Z.-Y.Y., Chung, Y., Lai, F. & Chen, T.-S.S. (2012c). A password-based user authentication scheme for the integrated EPR information system. *Journal of Medical Systems*. 36 (2). p.pp. 631–638.

Xie, M., Topaloglu, U., Powell, T., Peng, C. & Bian, J. (2013a). SIM: A smartphone-based identity management framework and its application to Arkansas trauma image repository. In: *2013 IEEE International Conference on Bioinformatics and Biomedicine*. December 2013, IEEE, pp. 53–60.

Xie, Q., Hu, B., Dong, N. & Wong, D.S. (2014a). Anonymous three-party password-authenticated key exchange scheme for telecare medical information systems. *PLoS ONE*. 9 (7). p.pp. 1–6.

Xie, Q., Liu, W., Wang, S., Han, L., Hu, B. & Wu, T. (2014b). Improvement of a uniqueness-and-anonymity-preserving user authentication scheme for connected health care. *Journal of Medical Systems*. 38 (9).

Xie, Q., Zhang, J. & Dong, N. (2013b). Robust anonymous authentication scheme for telecare medical information systems. *Journal of Medical Systems*. 37 (2).

Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H. & He, L. (2014). A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. *Journal of Medical Systems*. 38 (1).

Yu, Y.-C.C. & Hou, T.-W.W. (2014). An efficient forward-secure group certificate digital signature scheme to enhance EMR authentication process. *Medical and Biological Engineering and Computing*. 52 (5). p.pp. 449–457.

Zeb, K., Saleem, K., Muhtadi, J. Al & Thuemmler, C. (2016). U-prove based security framework for mobile device authentication in eHealth networks. In: *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*. September 2016, IEEE, pp. 1–6.