JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 03 Issue 01
2022

Research Article

Towards Developing Secure Transmission of Electronic Medical Records using Mobile Devices

Hamza Tariq[1,*] Arslan Iftikhar[2] and Adil[3]

[1]Department of Computer Science, NFC-Institute of Engineering & Technology, Multan, Pakistan
[2]Department of Telecommunication, Bahauddin Zakariya University, Multan, Pakistan
[3]Department of Information Technology, Muhammad Ali Jinnah University, Karachi, Pakistan
[*]Corresponding Author: Hamza Tariq. Email: hamzagujjar236@gmail.com

Received: December 16, 2021 **Accepted:** February 21, 2022 **Published:** March 15, 2022

Abstract: Establishing a secure exchange of health information through mobile devices is a major concern in health care initiative due to the advancement in ICT era; however, this task poses challenges. This study aims to shed light on conducting a survey on secure transmission technique that employs health information through mobile devices to encourage researchers to study these techniques. In this study, we discuss the mobile data transmission. We also elaborate on the security issues with mobile transmission, along with the possible difficulties it may present. This study also analyzes the techniques of transmission methods and security methods related to mobile EMR and discuss their strengths and weaknesses.

Keywords: Healthcare; ICT; Mobiledata Transmission; Security; EMR

1. Introduction

Mobile devices nowadays are very hot topic, especially after introducing the smart phones and the high competition between the smart phones manufacturers in the market. Numerous applications have been developed by programmers to provide different facilities and utilities to the users. No exception is the use of mobile devices to send and receive medical data. Due to the nature of EMRs and the information it contain, it is very important to ensure that these records are kept and managed securely (van der Linden, Kalra, Hasman, & Talmon, 2009). Ensuring the security of electronic medical records is one of the very important topics nowadays(Ting, 2011), particularly when these records are being transmitted from one place to another. According to(Ruotsalainen & Manning, 2007)the security requirements for EMR involve authentication, authorization, integrity, non-repudiation, privacy and confidentiality. According to (van der Linden et al., 2009)confidentiality is one of the major issues with EMRs. EMRs need to be kept highly confidential (van der Linden et al., 2009) especially during its transmission time. Serious problems could occur if the requested EMRs are not transmitted in secure manner. For example, unauthorized modification of any records could result in serious repercussion in patient diagnosis by the doctors. Thus, the aim of this article is to study the possible methods to transmit medical data securely via mobile devices through wireless networks. In addition there are also some other important features that must be available in the medical systems such as scalability, availability, speed and integration. Medical systems should be scalable enough to accommodate maximum number of users at a given point of time without degradation of the performance metrics (Xue et al., 2012) EMR systems need to be instantly available and operational whenever needed. Availability of EMR is considered as a very important factor(Xue et al., 2012). In addition the system should be fast enough, records need to be retrieved fast to provide timely care to patients(Lucas, 2010). Finally, Integration of EMR systems has to be taken under concern, EMR systems require to be fully

integrated with other scattered systems whenever necessary in order to facilitate the exchange of medical data among them(Rose et al., 2005). In the following section we will discuss the methods used in sending and receiving data through mobile devices.

2. Mobile Data Transmission

As shown in (Figure 1) data can be transmitted through a mobile device using either data packets via cellular network or through a wireless LAN network. When a mobile device uses wireless LAN networks, in this case the normal standard protocols identified by the internet service providers are used. However, when the mobile device uses cellular network to transmit and receive data, the protocols identified by the mobile companies are used and applied.

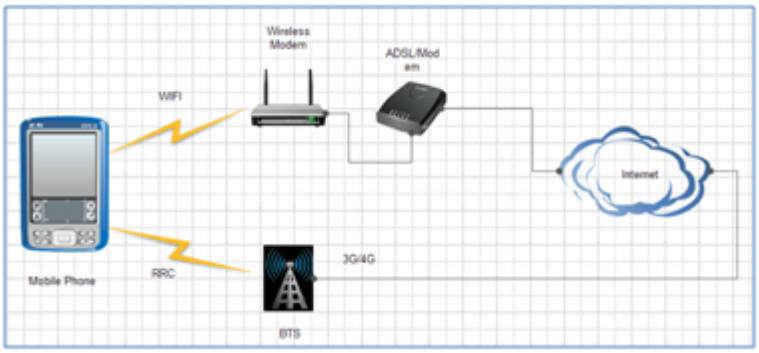

Figure 1. This Image represents mobile data transmission.

3. Security Issues with Mobile Data Transmission

According to (Zhao, Aggarwal, & Liu, 2008) GSM networks were not designed to transmit sensitive data. Hence, transmitting sensitive data through mobile networks needs additional security capabilities such as applying encryption techniques, authentication, and etc. With high usage of wireless networks through mobile devices nowadays, the security need to be taken under concern (Abomhara et al., 2010; Ahmed, Kiah, Zaidan, & Zaidan, 2010). There are number of encryption algorithms such as RSA, AES, NTRU, ECC, etc. which are in common use of traditional computers, in the following section the possibility of applying these algorithms on mobile devices are discussed.

3.1 RSA Algorithm

RSA is asymmetric algorithm acronym which stands for Rivest, Shamir and Adleman. It is a public key cryptography algorithm which is believed to be sufficiently secure as it has long keys (Gottesman & Lo, 2001). RSA involves 3 steps namely key generation, encryption and decryption. Many weaknesses were reported on RSA such as it is slow and not secure if the same message is encrypted to several receivers. RSA also requires longer keys in order to be very secure.

3.2 NTRU

NTRU was introduced in 2009 as a new standard for public key cryptography. NTRU has several advantages compared to RSA and ECC. Such as similar security level with smaller key size, faster speed, faster key generation, less computation power. Unlike RSA and ECC there is no successful attack that has been noted to break the security of NTRU (Manasa & Maheswar, 2012). The ability of NTRU to work under limited computing capability environment such as in case of mobile devices is considered as very important feature of this algorithm (Al-Bakri, Kiah, Zaidan, Zaidan, & Alam, 2011). NTRU is apparent to resist against quantum attacks (Howgrave-Graham, 2007). NTRU is faster comparing with RSA and ECC. However, it is around 20 times slower than AES (Hermans, Vercauteren, & Preneel, 2010). The computation power required by RSA, ECC and ElGamal is too high for some applications such as smart cards and mobile personal devices. These features and more made NTRU forefront on the mobile environment. The most important advantage of NTRU algorithm is the ability to work in limited computing capability environments. The benefit of using this algorithm in the mobile devices is that, it works efficiently and does not

have a bad effect on the performance of the mobile devices. Hence, NTRU is more reasonable for public key cryptography implementation on the mobile devices.

3.3 ECC

Elliptic curve cryptography (ECC) is based on algebraic structure of elliptic curves which is an approach to public-key cryptography. ECC is an attractive public-key cryptosystem for mobile/wireless environments. Comparing with RSA, ECC offers equivalent security with smaller key sizes, which results in faster computations, lower power consumption, as well as memory and bandwidth savings (Gupta, Gupta, Chang, & Stebila, 2002). There are number of successful attacks recorded on ECC, therefore, privacy and confidentiality cannot be achieved using this algorithm. Speed and scalability can be achieved with ECC under certain architectural designs (Aydos, Yanik, & Koc, 2001). Similar to RSA, ECC does not provide integration. ECC is faster than RSA (Vincent, Folorunso, & Akinde, 2010). ECC-160 has 6× smaller key-size than RSA-1024 and can generate a signature 12 times faster than RSA (Balitanas, Robles, Kim, & Kim, 2009). ECC is faster, and occupies less memory space than an equivalent RSA system (Kapoor, Abraham, & Singh, 2008), ECC is more efficient than the ubiquitous RSA based schemes because ECC utilizes smaller key sizes for equivalent security.

3.4 AES Algorithm

AES is symmetric algorithm which stands for Advanced Encryption Standard. AES is accessible publically and it is the first cipher approved by National Security Agency (NSA) for top secret information. AES has fixed block sizes of 128 bits, 192 or 256 bits. An attack against AES 256 bit key will require 2200 operation to break it which is longer than the age of universe to complete. In other words, AES algorithm is secure. AES demands small computing power (Lisonek & Drahansky, 2008) and therefore it can be adopted in mobile devices. However the disadvantage of this algorithm is that it requires secure channel to exchange the encryption keys (Lisonek & Drahansky, 2008). Furthermore, AES algorithm provides more physical security as well as higher speed (Xinmiao & Parhi, 2004). AES algorithm is so popular that it is now being used as authentication protocol. According to Itani and Kayssi (2004), AES block cipher can provide data integrity. However, some researchers have criticized the ability of AES alone to provide data integrity without the help of other integrity checking algorithms (Elbaz, Torres, Sassatelli, Guillemin, & Bardouillet, 2006). Several studies have been done to test the scalability of AES algorithms and it is proved that AES can achieve a very high throughput of 500 Gbits/s and hence AES is believed to be as extremely scalable (Bouhraoua, 2006). AES provides exceptionally great scale integration. It can be integrated without requiring changes in the infrastructure or protocols (Shen-Fu, Ming-Chih, & Chia-Shin, 2006). AES is very efficient and can operate on a wide range of devices and processor types simultaneously (Itani & Kayssi, 2004), this makes AES available for the users request at any time or moment.

3.5 Blowfish (Cipher) & RC6

Another symmetric block cipher named as blowfish was developed by Bruce Schneier in 1993. It is considered as fast block cipher except when changing keys as it requires preprocessing for each new key equivalent to encrypting about 4 kilobytes of text which is considered as very slow. Hence, this prevents its use in certain applications. Blowfish is freely available and no license is required. It is most suitable and efficient for hardware implementation (Lin & Lin, 2000). According to (Lo & Bishop, 2003) this algorithm can be adopted in mobile devices to provide end to end message encryption. RC6 is another type of symmetric key block cipher which was designed to meet the requirements of AES. RC6 design was based on RC5. Some modifications have been applied to make RC6 stand against successful attacks on RC5.

3.6 SHA-1 & MD5

SHA-1 in an acronym for Secure Hash Algorithm and it was designed by National Security Agency. SHA-1is the most widely used among the exiting three SHA hash functions i.e. SHA-0, SHA-1, and SHA-2. Hash algorithms are always used within other cryptographic algorithms and protocols for the purpose of protection of sensitive information. In hash algorithm the encryption is based on a hash value. This value is calculated from a base input number using a hashing algorithm. Basically the hash value is a summary

of the original value. Scalability can be accomplished with the use of hash functions (Stoica, Morris, Karger, Kaashoek, & Balakrishnan, 2001). Hash function speed is dependent on the algorithm and application complexity (Xiao, Liao, & Deng, 2005). SHA-1 algorithm has the capability of integration with other algorithms such as MD5 (Mao-Yin, Chih-Pin, Chih-Tsun, & Cheng-Wen, 2004). SHA-1 can be used for implementing a key exchanging mechanism (Traw & Aucsmith, 1999). Finally SHA-1 has been used with other encryption techniques to secure mobile based bank payment system (Hassinen, Hyppönen, & Haataja, 2006). MD5 is another widely used hash algorithm. It is a strengthened version of MD4 (Wang & Yu, 2005). MD5 has been used in different mobile payment services (Massoth & Bingel, 2009). However, it was criticized due to some successful attacks recorded.

3.7 XML/SOAP

XML is considered nowadays as the universal language for data transmission or exchange over the Internet. XML has been also used in data transmission over the mobile devices (Figueredo & Dias, 2004). Several enhancements have been done to XML to improve its security and privacy features through XML encryption, XML signature and XML Key Management Specification. Since XML is platform and language independent it make any XML based solution very flexible as it has the ability to integrate with any other systems (Chester, 2001). The flexibility, simplicity and the interconnection capabilities makes XML an excellent language for data exchange over the Internet. SOAP is becoming a de facto standard as it is a light weight protocol for exchanging structured and typed information (Jia & Jen-Yao, 2002). SOAP is based on XML and therefore it is able to communicate through the internet independent of the platform and programming language used. According to (Brose, 2003) SOAP does not provide any message security at all and therefore other way of securing SOAP messages is necessary. Hence, SOAP with XML can be used to send messages over the net with some level of security. However to achieve a high level of security, the support of other security algorithms are needed. Since SOAP is a protocol which communicates using XML, it therefore fully inherits the openness, scalability and availability of XML (Ping, Zhiyong, Tao, & Xinxing, 2010). Like XML, SOAP also assists in integration of most of the applications (Chester, 2001).

From the above discussion we can conclude that in order to secure the EMRs transmission in mobile devices fast and light weight (demanding less computing power) security algorithms must be adopted. Since EMRs are considered as highly sensitive data, it's very important to select a proper and secure algorithm from the above discussed algorithms. For example one can use AES or NTRU along with SOAP/XML to provide strong security service with efficient computing power while data transmission.

4. Literature Survey

Several research studies have been done on transmitting EMRs through mobile devices. A few recent studies were selected and tabulated below for the purpose of literature survey. In the following Table 1, the papers were evaluated based on some specific criteria. These criteria have been divided into two basic groups which are the transmission methods and the security methods. For example in the transmission section some transmission protocols such as SOAP/XML were checked whether they have been used or not. In addition the use of cloud, wireless LAN network, and cellular network has been checked. When discussing the security aspects in the papers, the criteria on which papers are evaluated is whether any encryption algorithm is used, hashing algorithms are applied, or key exchanging method is applied.

Table 1: Literature Survey on Mobile Based EMR Transmission.

Authors	*Transmission Method*				*Security Methods*			
	Use of	*Use of Cloud*	*Use of Wireless*	*Use of Mobile Network*	*Others*	*Algorithm Used*	*Hashing Method*	*Key Exchange*	*Others*

(Fritz, Balhorn, Riek, Breil, & Dugas, 2012)	*x*	*x*	*x*	*x*	*Have not been discussed*	*x*	*x*	*x*	*Have not used or proposed a security method*
(Hsieh et al., 2010)	√	*x*	√	*X*	*HL7 communication standards have been adopted in designing the system.*	*x*	*x*	*x*	*To ensure data security and integrity user interfaces, subsystems and database accessing have been separated in layers.*
(Liu, Chung, Chiang, Chen, & Wang, 2012)	√	√	*x*	*X*	*Use of mobile agent for accessing data*	*x*	*x*	*x*	*Securing data by having mobile agent for collecting electronic patient records.*
(Holzinger et al., 2011)	√	*x*	√	√	*A client–server system with a thin client solution at the front-end using a mobile device has been proposed*	*x*	*x*	*x*	*The importance of privacy and security was mentioned but how it can be achieved has not been discussed*
(Dmitrienko, Hadzic, Löhr, Winandy, & Sadeghi, 2011)	√	*x*	√	√	*TruWallet architecture has been adopted which is based on security kernel*	*x*	*x*	*x*	*Combination of the concept of security kernel and hardware security features.*
(Karahoca, Bayraktar, Tatoglu, & Karahoca, 2010)	√	*x*	√	*x*	*The proposed system could work on tablet PCs via Wi-Fi network*	*x*	*x*	*x*	*Security issues have not been discussed or proposed.*
(Vatsalan et al., 2010)	*x*	*x*	*x*	√	*ADSL, 3G and GSM mobile technologies have been used for communication.*	*x*	*x*	*x*	*Security issues have not been discussed or proposed*
(Klein, Mannweiler, Schneider, & Schotten, 2010)	*x*	√	√	*x*	*A formal method assessing link quality based on available context information has been developed for triggering handover mechanisms*	*x*	*x*	*x*	*Centralized maintenance of security-critical software is proposed.*
(Aversa, Di Martino, Rak, &	√	√	*x*	*x*	*The architecture proposed aims at integrating three*	*x*	*x*	*x*	*Security issues have not been discussed or proposed*

Venticinque, 2010)					*different technologies: GRID, Cloud and Mobile Agents.*				
(Huerta-Canepa & Lee, 2010)	√	√	√	*x*	*Communication between devices is done based on the Extensible Messaging and Presence Protocol (XMPP)*	*x*	*x*	*x*	*Security issues have not been discussed or proposed*
(Nkosi & Mekuria, 2010)	*x*	√	√	*x*	*The proposed framework uses a Cloud Computing protocol management model which intends to provide multimedia sensor signal processing & security as a service to mobile devices*	*x*	*x*	*x*	*Security concerns have been addressed with regard to mobile cloud computing*
(Ott, 2006)	*x*	*x*	√	*x*	*Solution using DTN with asynchronous message passing was proposed for flexible mobile communication*	√	*x*	√	*End-to-end security mechanisms such as S/MIME with public key cryptography have been suggested.*
(Huang, Zhang, Kang, & Luo, 2010)	*x*	√	√	√	*The objective of this research is to use a systematic approach to investigate both cloud computing and mobile ad hoc Networks(MANETs) technologies*	*x*	√	*x*	*Virtual trusted and provisioning domain (VTaPD)" was introduced to isolate information flows belonging to different security domains using programmable router technologies*
(Houmansadr, Zonouz, & Berthier, 2011)	*x*	√	√	*x*	*Cloud based Smartphone specific intrusion detection and response Engine system was proposed which continuously performs an in-depth forensics analysis on the smartphone to detect any misbehavior*	*x*	*x*	*x*	*Cloud based service was presented to provide security and tolerance to resource limited mobile phone devices*

(Landman, 2010)	*x*	√	√	√	*All the network access mechanisms were discussed but not implemented.*	*x*	*x*	*x*	*Security solutions have been discussed but not implemented.*

5. Proposed solution

From the previous discussion in this paper, it becomes obvious that mobile devices are still lacking in security while data are being transmitted. SOAP/XML have been used in several studies as a medium of transmission in mobile devices, however, security techniques have not been applied. Since EMRs transmission through mobile devices requires high level of security, one method to achieve this is proposed in this section. Encryption is one of the widely used techniques to protect the data. Here we can encrypt the data itself inside the XML message packets while it's being transmitted from the source to destination, or enhance the security of HL7 health standard by adding advanced encryption techniques. XML massage encryption is one of the possible and very robust solutions. The SOAP/XML techniques along with hybrid of encryption and hashing algorithms have been implemented in previous studies. (Kiah, Nabi, Zaidan, & Zaidan, 2013) implemented a solution based on AES hybrid with SOAP/XML and SHA-1 to provide security for EMRs during transmission. In this study the entire SOAP/XML message is encrypted at the sender side and then transmitted. At the receiver side the whole message is decrypted and then the information is extracted. In similar way we can apply AES hybrid with SOAP/XML and SHA-1 to secure the message transmission in mobile devices. Using this technique will enhance the security of mobile devices and it will provide the required solution for the security problems faced so far while using mobile devices to send sensitive data.

6. Highlights

- In this article a deep study has been performed on the ability of mobile devices to send and receive sensitive health records.
- A review has been conducted to determine up to what extent studies have been done so far on the ability of mobile devices to send and receive health records.
- A solution has been suggested based on the review and different techniques available.
- SOAP/XML can be efficiently used with mobile devices for data transmission.
- Encryption techniques can be applied with SOAP/XML in order to allow transmission of sensitive data using mobile devices.
- Only the sensitive data within the XML message can be encrypted rather than encrypting the entire message

7. Conclusion

On the basis of this review, it is obvious that there are several studies focusing on the mobile based EMR transmission. The importance of the security issues has been discussed in several articles. However, a complete solution for transmitting EMRs based on mobile devices has not been proposed yet. Mobile devices are used nowadays in health applications. Transmission of EMRs needs to be achieved through mobile applications. Encryption algorithms for mobile devices are available and can be adopted according to the requirements. A complete and secure mobile based EMR framework has not been built yet. In this paper, an overview of cellular network access mechanisms and security algorithms capable of being implemented in mobile environment is presented. By using encryption techniques such as NTRU and AES one can achieve a secure EMR transmission through mobile devices.

8. Future Study

The challenge for ongoing mobile cloud computing researches is to take the needs and requirements of different health care professionals and consumers in the development of EMRs. A further challenge is obtaining the law facts associated with the country where the medical system would be used.

References

1. Abomhara, M., Khalifa, O. O., Zakaria, O., Zaidan, A., Zaidan, B., & Alanazi, H. O. (2010). Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview. J. Appl. Sci, 10(15), 1656-1661.
2. Ahmed, M. A., Kiah, M. L. M., Zaidan, B., & Zaidan, A. (2010). A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. Applied Sci, 10, 59-64.
3. Al-Bakri, S. H., Kiah, M. L. M., Zaidan, A., Zaidan, B., & Alam, G. M. (2011). Securing peer-to-peer mobile communications using public key cryptography: New security strategy. International Journal of the Physical Sciences, 6(4), 930-938.
4. Aversa, R., Di Martino, B., Rak, M., & Venticinque, S. (2010). Cloud agency: A mobile agent based cloud system. Paper presented at the Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference on.
5. Aydos, M., Yanik, T., & Koc, C. K. (2001). High-speed implementation of an ECC-based wireless authentication protocol on an ARM microprocessor. Communications, IEE Proceedings-, 148(5), 273-279. doi: 10.1049/ip-com:20010511
6. Balitanas, M. O., Robles, R.-J., Kim, N., & Kim, T. (2009). Crossed crypto-scheme in WPA PSK mode. Paper presented at the Bio-inspired Learning and Intelligent Systems for Security, 2009. BLISS'09. Symposium on.
7. Bouhraoua, A. (2006, 16-19 Dec. 2006). Design Feasibility Study For A 500 Gbits/s AES Cypher Decypher Engine. Paper presented at the Microelectronics, 2006. ICM '06. International Conference on.
8. Brose, G. (2003). Securing web services with SOAP security proxies. Paper presented at the Proc. Int'l Conf. Web Services (ICWS'03).
9. Chester, T. M. (2001). Cross-platform integration with XML and SOAP. IT Professional, 3(5), 26-34.
10. Dmitrienko, A., Hadzic, Z., Löhr, H., Winandy, M., & Sadeghi, A.-R. (2011). A security architecture for accessing health records on mobile phones. Paper presented at the Proceedings of the 4th International Conference on Health Informatics (HEALTHINF 2011).
11. Elbaz, R., Torres, L., Sassatelli, G., Guillemin, P., & Bardouillet, M. (2006, 0-0 0). PE-ICE: Parallelized Encryption and Integrity Checking Engine. Paper presented at the Design and Diagnostics of Electronic Circuits and systems, 2006 IEEE.
12. Figueredo, M. V. M., & Dias, J. S. (2004, 1-5 Sept. 2004). Mobile Telemedicine System for Home Care and Patient Monitoring. Paper presented at the Engineering in Medicine and Biology Society, 2004. IEMBS '04. 26th Annual International Conference of the IEEE.
13. Fritz, F., Balhorn, S., Riek, M., Breil, B., & Dugas, M. (2012). Qualitative and quantitative evaluation of EHR-integrated mobile patient questionnaires regarding usability and cost-efficiency. International Journal of Medical Informatics, 81(5), 303-313. doi: http://dx.doi.org/10.1016/j.ijmedinf.2011.12.008
14. Gottesman, D., & Lo, H. K. (2001). From quantum cheating to quantum security. Arxiv preprint quant-ph/0111100.
15. Gupta, V., Gupta, S., Chang, S., & Stebila, D. (2002). Performance analysis of elliptic curve cryptography for SSL. Paper presented at the Proceedings of the 1st ACM workshop on Wireless security, Atlanta, GA, USA.
16. Hassinen, M., Hyppönen, K., & Haataja, K. (2006). An Open, PKI-Based Mobile Payment System. In G. Müller (Ed.), Emerging Trends in Information and Communication Security (Vol. 3995, pp. 86-100): Springer Berlin Heidelberg.
17. Hermans, J., Vercauteren, F., & Preneel, B. (2010). Speed Records for NTRU. In J. Pieprzyk (Ed.), Topics in Cryptology - CT-RSA 2010 (Vol. 5985, pp. 73-88): Springer Berlin Heidelberg.
18. Holzinger, A., Kosec, P., Schwantzer, G., Debevc, M., Hofmann-Wellenhof, R., & Frühauf, J. (2011). Design and development of a mobile computer application to reengineer workflows in the hospital and the methodology to evaluate its effectiveness. Journal of Biomedical Informatics, 44(6), 968-977. doi: http://dx.doi.org/10.1016/j.jbi.2011.07.003
19. Houmansadr, A., Zonouz, S. A., & Berthier, R. (2011). A cloud-based intrusion detection and response system for mobile phones. Paper presented at the Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on.
20. Howgrave-Graham, N. (2007). A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU. In A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007 (Vol. 4622, pp. 150-169): Springer Berlin Heidelberg.
21. Hsieh, S.-H., Hou, I. C., Cheng, P.-H., Tan, C.-T., Shen, P.-C., Hsu, K.-P., . . . Lai, F. (2010). Design and Implementation of Web-Based Mobile Electronic Medication Administration Record. Journal of medical systems, 34(5), 947-958. doi: 10.1007/s10916-009-9310-9
22. Huang, D., Zhang, X., Kang, M., & Luo, J. (2010). MobiCloud: building secure cloud framework for mobile computing and communication. Paper presented at the Service Oriented System Engineering (SOSE), 2010 Fifth IEEE International Symposium on.
23. Huerta-Canepa, G., & Lee, D. (2010). A virtual cloud computing provider for mobile devices. Paper presented at the Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services: Social Networks and Beyond, San Francisco, California.
24. Itani, W., & Kayssi, A. (2004). J2ME application-layer end-to-end security for m-commerce. Journal of Network and Computer Applications, 27(1), 13-32. doi: 10.1016/s1084-8045(03)00030-4
25. Jia, Z., & Jen-Yao, C. (2002, 2002). A SOAP-oriented component-based framework supporting device-independent multimedia Web services. Paper presented at the Multimedia Software Engineering, 2002. Proceedings. Fourth International Symposium on.
26. Kapoor, V., Abraham, V. S., & Singh, R. (2008). Elliptic curve cryptography. Ubiquity, 9(20), 1-8.

27. Karahoca, A., Bayraktar, E., Tatoglu, E., & Karahoca, D. (2010). Information system design for a hospital emergency department: A usability analysis of software prototypes. J. of Biomedical Informatics, 43(2), 224-232. doi: 10.1016/j.jbi.2009.09.002
28. Kiah, M. L. M., Nabi, M., Zaidan, B. B., & Zaidan, A. A. (2013). An Enhanced Security Solution for Electronic Medical Records Based on AES Hybrid Technique with SOAP/XML and SHA-1. Journal of medical systems, 37(5), 1-18. doi: 10.1007/s10916-013-9971-2
29. Klein, A., Mannweiler, C., Schneider, J., & Schotten, H. D. (2010). Access schemes for mobile cloud computing. Paper presented at the Mobile Data Management (MDM), 2010 Eleventh International Conference on.
30. Landman, M. (2010). Managing smart phone security risks. Paper presented at the 2010 Information Security Curriculum Development Conference, Kennesaw, Georgia.
31. Lin, M. C.-J., & Lin, Y.-L. (2000). A VLSI implementation of the blowfish encryption/decryption algorithm. Paper presented at the Proceedings of the 2000 Asia and South Pacific Design Automation Conference, Yokohama, Japan.
32. Lisonek, D., & Drahansky, M. (2008, 13-15 Dec. 2008). SMS Encryption for Mobile Communication. Paper presented at the Security Technology, 2008. SECTECH '08. International Conference on.
33. Liu, C.-H., Chung, Y.-F., Chiang, T.-W., Chen, T.-S., & Wang, S.-D. (2012). A Mobile Agent Approach for Secure Integrated Medical Information Systems. Journal of medical systems, 36(5), 2731-2741. doi: 10.1007/s10916-011-9749-3
34. Lo, J. L.-C., & Bishop, J. (2003). Component-based interchangeable cryptographic architecture for securing wireless connectivity in Java^{TM} applications. Paper presented at the Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology.
35. Lucas, L. (2010). Partnering to Enhance the Nursing Curriculum: Electronic Medical Record Accessibility. Clinical Simulation in Nursing, 6(3), e97-e102. doi: 10.1016/j.ecns.2009.07.006
36. Manasa, C., & Maheswar, M. (2012). Secure Mobile IM System Using NTRU. International Journal of Engineering, 1(9).
37. Mao-Yin, W., Chih-Pin, S., Chih-Tsun, H., & Cheng-Wen, W. (2004, 27-30 Jan. 2004). An HMAC processor with integrated SHA-1 and MD5 algorithms. Paper presented at the Design Automation Conference, 2004. Proceedings of the ASP-DAC 2004. Asia and South Pacific.
38. Massoth, M., & Bingel, T. (2009, 24-28 May 2009). Performance of Different Mobile Payment Service Concepts Compared with a NFC-Based Solution. Paper presented at the Internet and Web Applications and Services, 2009. ICIW '09. Fourth International Conference on.
39. Nkosi, M., & Mekuria, F. (2010). Cloud computing for enhanced mobile health applications. Paper presented at the Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on.
40. Ott, r. (2006). Application protocol design considerations for a mobile internet. Paper presented at the Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture, San Francisco, California.
41. Ping, Z., Zhiyong, L., Tao, Q., & Xinxing, J. (2010, 22-24 Oct. 2010). Research based on XML/SOAP BACnet and internet integration technology. Paper presented at the Intelligent Computing and Integrated Systems (ICISS), 2010 International Conference on.
42. Rose, A. F., Schnipper, J. L., Park, E. R., Poon, E. G., Li, Q., & Middleton, B. (2005). Using qualitative studies to improve the usability of an EMR. Journal of Biomedical Informatics, 38(1), 51-60. doi: 10.1016/j.jbi.2004.11.006
43. Ruotsalainen, P., & Manning, B. (2007). A notary archive model for secure preservation and distribution of electrically signed patient documents. International Journal of Medical Informatics, 76(5–6), 449-453. doi: 10.1016/j.ijmedinf.2006.09.011
44. Shen-Fu, H., Ming-Chih, C., & Chia-Shin, T. (2006). Memory-free low-cost designs of advanced encryption standard using common subexpression elimination for subfunctions in transformations. Circuits and Systems I: Regular Papers, IEEE Transactions on, 53(3), 615-626.
45. Stoica, I., Morris, R., Karger, D., Kaashoek, M. F., & Balakrishnan, H. (2001). Chord: A scalable peer-to-peer lookup service for internet applications. SIGCOMM Comput. Commun. Rev., 31(4), 149-160. doi: 10.1145/964723.383071
46. Ting, D. (2011). Securing access to healthcare. Biometric Technology Today, 2011(2), 10-11. doi: 10.1016/s0969-4765(11)70037-6
47. Traw, C. B. S., & Aucsmith, D. W. (1999). Content protection for transmission systems: Google Patents.
48. van der Linden, H., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter-organizational future proof EHR systems: A review of the security and privacy related issues. International Journal of Medical Informatics, 78(3), 141-160. doi: http://dx.doi.org/10.1016/j.ijmedinf.2008.06.013
49. Vatsalan, D., Arunatileka, S., Chapman, K., Senaviratne, G., Sudahar, S., Wijetileka, D., & Wickramasinghe, Y. (2010). Mobile technologies for enhancing eHealth solutions in developing countries. Paper presented at the eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED'10. Second International Conference on.
50. Vincent, O., Folorunso, O., & Akinde, A. (2010). Improving e-payment security using Elliptic Curve Cryptosystem. Electronic Commerce Research, 10(1), 27-41.
51. Wang, X., & Yu, H. (2005). How to Break MD5 and Other Hash Functions. In R. Cramer (Ed.), Advances in Cryptology – EUROCRYPT 2005 (Vol. 3494, pp. 19-35): Springer Berlin Heidelberg.
52. Xiao, D., Liao, X., & Deng, S. (2005). One-way Hash function construction based on the chaotic map with changeable-parameter. Chaos, Solitons & Fractals, 24(1), 65-71. doi: 10.1016/j.chaos.2004.07.003
53. Xinmiao, Z., & Parhi, K. K. (2004). High-speed VLSI architectures for the AES algorithm. Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, 12(9), 957-967.

54. Xue, Y., Liang, H., Wu, X., Gong, H., Li, B., & Zhang, Y. (2012). Effects of electronic medical record in a Chinese hospital: A time series study. International Journal of Medical Informatics, 81(10), 683-689. doi: 10.1016/j.ijmedinf.2012.05.017
55. Zhao, S., Aggarwal, A., & Liu, S. (2008). Building secure user-to-user messaging in mobile telecommunication networks. Paper presented at the Wireless Telecommunications Symposium, 2008. WTS 2008.