Secure Collaborative Mobile Platform for Transmission and Archival of Medical Images

TMKK Jinasena[1], RGN Meegama[1], and RB Marasinghe[2]

[1] Department of Computer Science, Faculty of Applied Sciences, University of Sri Jayewardenepura, Sri Lanka
[2] Department of Medical Education and Health Sciences, Faculty of Medical Sciences, University of Sri Jayewardenepura, Sri Lanka
#RGN Meegama; <rgn@sci.sjp.ac.lk>

Abstract— *Compromising security of sensitive medical data often lead to severe consequences such as death of a patient or financial loses to health workers. This becomes worse when we share electronic medical data among a large community through a public network; especially in a mobile environment. In this paper, we present the design and the implementation of a secure mechanism for authentication and integrity verification based on a novel, robust, and efficient public key cryptography method called Elliptic Curve Cryptography (ECC) to an Android based collaborative medical imaging application. Customized digital certificate system based on ECC is implemented to authenticate the stakeholders of the system. The Elliptic Curve Digital Signature Algorithm implemented in Spongy Castel library together with Secure Hash Algorithm (SHA)-256 hashing is used to sign the message and verify the integrity. Besides, Advanced Encryption Standard (AES) with 256 bits key size is used to impose the confidentiality of the message. A benchmark mobile application is developed to test run times of different algorithms, curves and key sizes to find the optimal configuration for a mobile device. Results indicate that AES and SHA sizes do not make any significant impact on the runtime but ECC does. Although the AES key generation time is* 61.0 μs, *the Initial Vector (IV) generation time is high as* 762.0 μs. *Moreover, the ECC sign time is less as 5 ms and the verification time is large as 200 ms. However, in all cases, the security increases when the key size increases. Though theoretically, ECC is much faster than the present RSA asymmetric encryption, practically it is not due to the unavailability of optimized libraries. However, due to less computation and space requirement of ECC compared to other public key cryptography methods, the proposed method is well suited for mobile devices.*

Keywords— **Computer Security, ECC, Mobile Computing, eHealth, mHealth**

I. INTRODUCTION

As the world grows and people become more mobile, the need to streamline routine work is fast becoming important and as a result, the mobile industry is growing exponentially. As health services are fundamental needs of human beings today, accessing recent health information from a distant place has grown tremendously. In eHealth, Tele-medicine and mHealth, such information is used in tele-consultation to obtain a second opinion, tele-diagnosing in emergencies, health training and education. Among them, mHealth is promising due to the rapid growth of wireless technologies and the exponential growth of mobile usage. However, the privacy of sensitive medical data is the most important concern in medicine next to patients' lives. The loss of privacy may cause colossal damage to patients, health workers and to the health institutions (Das & Mukhopadhyay 2011) (Chen, Yu & Feng 2000).

II. BACKGROUND

A. Growth of Mobile Usage and the Rising Security Challenges

According to statistics available, the number of smart phones in use during 2008 has exceeded the number of personal computers (PC) in the world. As predicted, there will be 10 billion mobile devices with the high speed 5G wireless data access by 2020. It is expected to have 15 billion mobile devices with real time access of high definition videos at 2020 Olympics. Figure 1 shows the growth of mobile phones relative to PCs, Laptops, and Tablets (Gozalvez 2015) (Dahlman 2014).

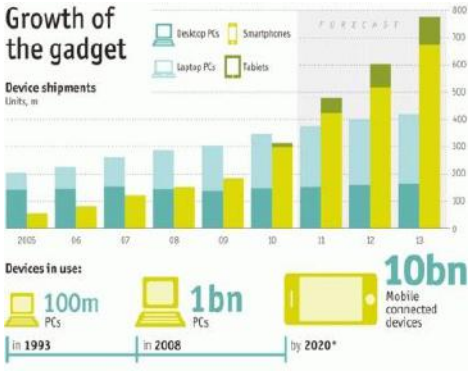

Figure 1: Mobile Growth (Hepburn 2013)

Digital theft is harder to detect compared to conventional robbery due to its unique characteristics such as identical original source and the copy. Such thefts cannot be detected because the original remains unchanged and the

theft can be in the other side of the world. This becomes worse in a wireless environment because the attacker can perform his activities without physically connecting to the network. As wireless environments are more vulnerable than wired, protecting digital data in a mHealth environment is always challenging (Das & Mukhopadhyay 2011) (Bagchi 2006) (Bedi 2003) (El-Iskandarani, Darwish & Abuguba 2008) (Georgiadis et al. 2006).

B. Loss of privacy in eHealth

Lack of security in sensitive medical data such as medical history, diagnoses, prescriptions, insurance details, social security numbers and patient's other personal details may lead to the patient's identity discloser, embarrassment, psychological distress, suicide, financial loses to the patient or to the hospital or health insurance companies and in extreme situations, the death of a patient due to unauthorized modifications such as allergies. Moreover, stolen medical records can be used to earn millions of dollars by false billing, to obtain medical services, prescription drugs, to access bank accounts or credit cards (Solove 2002) (LoPucki 2001) (Mancilla & Moczygemba 2009).

In USA, Medical Identity Theft (MIDT) is reported to be the most rising crime in recent times. A US firm was fined $250,000 by regulators in May 2009 for failing to prevent healthcare workers from accessing electronic health records (EHR) of a woman who had given birth to octuplets (Das & Mukhopadhyay 2011). In March 2012, another US hospital was fined 1.5 million dollars due to the loss of 57 hard drives that contained unencrypted health information (Foley et al. 2010). In France, medical records of a prominent racing car champion was stolen by a firm and sold to the media for 60,000 Swiss francs (Das & Mukhopadhyay 2011). All these cases emphasize the rising threats in eHealth systems (Walters & Betz 2012).

C. Computer Security

In computer security, we are basically focusing on assuring aspects such as Confidentiality, Integrity, Availability, Authentication, Access Control, Non-repudiation and Privacy. Given below is a brief account of each of these factors:

- **Confidentiality** ensures that information is not accessed by unauthorized persons.
- **Integrity** ensures that information is not altered in an unauthorized way by authorized or unauthorized persons.
- **Availability** makes information available to authorized users when needed.
- **Authentication** ensures that a user is the actual person that he claims to be.
- **Access control** makes sure that users access only those resources and services that they are entitled to access. Qualified users are not denied access to services that they legitimately expect to receive.
- **Non-repudiation** ensures that the originators of messages cannot deny that they in fact sent the messages.
- **Privacy guarantees that** individuals maintain the right to control what information is collected about them, how it is used, who has used it, who maintains it and what purpose it is used for (Demaerschalk et al. 2012) (El-Iskandarani, Darwish & Abuguba 2008) (Das, Mukhopadhyay & Shukla 2011).

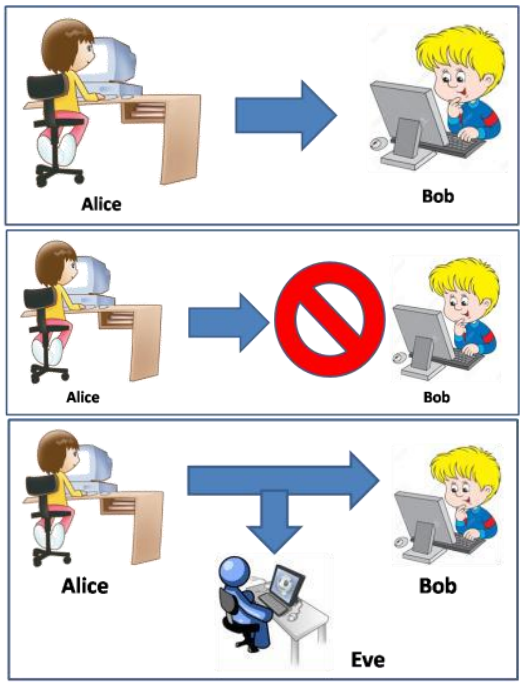

Figure 2: (Top) normal flow, (middle) interruption and (bottom) interception.

We have identified five possible attacks that will compromise the security of a system. Figure 2 (top) shows the normal flow of the system and the figure 2 (middle) shows one of the hardest attacks to deal with, losing availability due to interruption or jamming. Figure 2 (bottom) shows the case of Interception where another party is accessing information compromising privacy or confidentially. Figure 3 shows the case of flooding where another party is creating lots of traffic to the communication link resulting in the lose of availability (Das, Mukhopadhyay & Shukla 2011) (LoPucki 2001) (Mancilla & Moczygemba 2009).

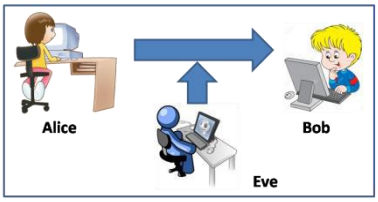

Figure 3: Flooding

Figure 4 shows the case of modification in which the integrity is lost. Figure 5 shows the case of fabrication where another party pretend as an authorized user compromising authentication

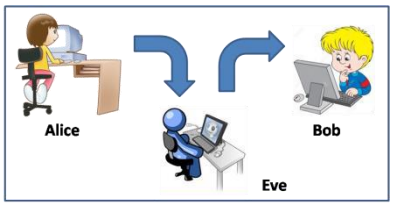

Figure 4: Modification

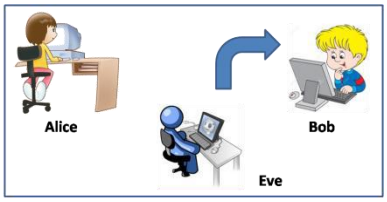

Figure 5: Fabrication / Impersonification

D. Symmetric key encryptions

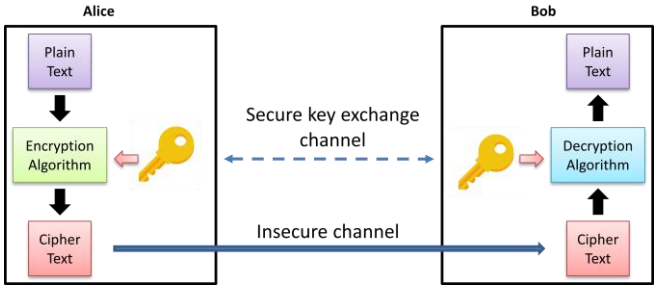

Figure 6: Symmetric-key Encryption

Symmetric key encryption, which is faster than Asymmetric key encryption, uses the same key for both encryption and decryption. However, it can only guarantee the confidentiality of data; neither the integrity nor the authentication can be achieved here.

E. Asymmetric encryption

In Asymmetric key, a pair of keys, known as private and public keys, is used to encrypt and decrypt the data. The private key is kept as a secret while the public key is known to everybody. The elegance of this mechanism is that if a person uses one key to encrypt it can only be decrypted by the other key.

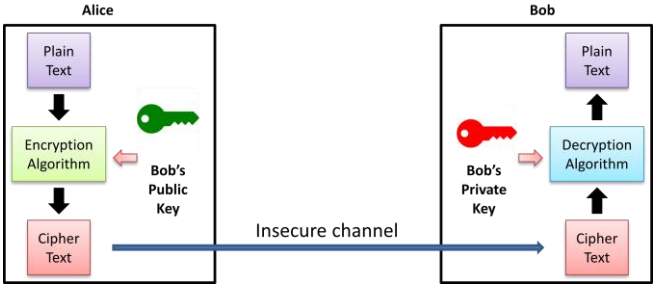

Figure 7: Asymmetric-key Encryption

For example, if Alice encrypts a message using her private key and sends it to Bob, Bob can use Alice's public key to open it. By doing so, Bob can authenticate the sender. On the other hand, if she encrypts it using Bob's public key, only Bob can decrypt the message ensuring confidentiality.

F. Hashing and Digital Signature

Where a digital signature is used to authenticate the sender, the sender first encrypts the message using his private key and then the recipient decrypts it using sender's public key as shown in Figure 8. This allows the recipient to verify the sender; because no other person possesses the sender's private key. However, this does not provide confidentiality because anyone who has the sender's public key can decrypt it.

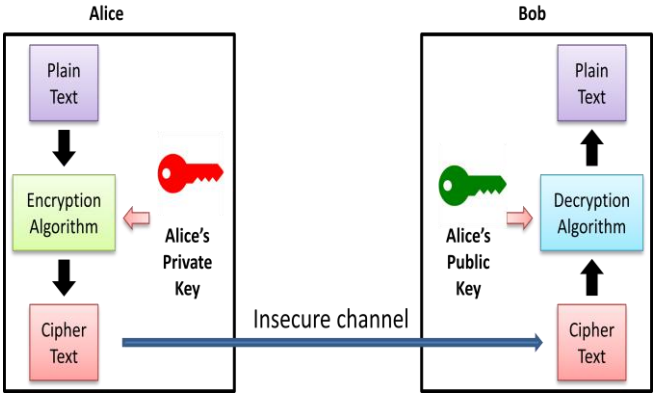

Figure 8: Sign and Authenticate

In practice, a combination of Asymmetric key cryptography and hashing is used to authenticate the sender as well as to verify the integrity. As shown in Figure 11, the digest of the original message is initially calculated using the selected hashing algorithm. Subsequently, it is transmitted along with the original message after encrypting with the sender's private key. Then, the recipient calculates the digest of the received message using the same hashing algorithm. Finally, the recipient uses the sender's public key

to decrypt the sender's digest and compare it with the calculated digest to verify the integrity of the message. If somebody alters the original message, the recipient digest will not match with the sender's digest. Thus, the recipient can verify the originality of the message.

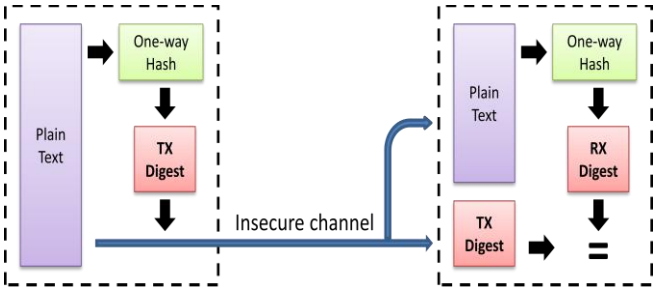

Figure 9: Sign and Verify

G. Digital Certificates and Public Key Infrastructure

One of the problems in public key cryptography is to verify the real owner of a public key. For example, Eve can put his public key and claim as he is Bob. There is no way for Alice to know whether he is actual Bob or not. This can be solved by having a third party known as Certificate Authority (CA) which is trusted by both parties. Each party has to give their details and get a certificate from the CA to confirm their identities shown in e Figure 10 (Gupta et al. 2012) (Han et al. 2010).

III. METHODOLOGY

In the proposed research, an Android application is implemented to transfer medical images over a mobile network with a mechanism to verify the integrity and the sender. This mechanism is based on a novel, robust and an efficient public key cryptography method called Elliptic curve cryptography (ECC). First, we create an elliptic curve (EC) based private and public key pairs for all the users in the system using the OpenSSL. As shown in Figure 10, we send details of users and their public keys to the CA to obtain the associated digital certificates. At this stage, we propose our own hierarchy of CA's to issue digital certificates in a distributive manner. However, we issue EC based digital certificates to all the stake holders of the system including the servers to confirm their identities.

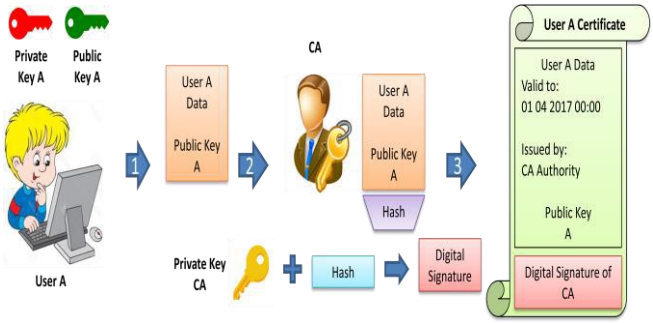

Figure 10: CA and Digital Certificates

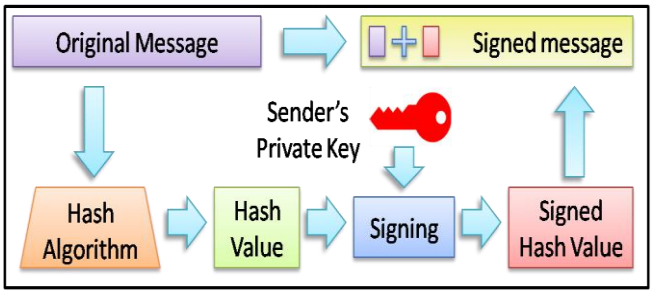

Figure 11: Signing a message

Next, we calculate the message digest or the hash value of the message using the SHA256 hashing algorithm. Then, as shown in Figure 11, it is signed using the sender's private key and concatenated to the original message. The ECC method implemented in the Spongy Castle library are used for this purpose. However, to assure the confidentiality, the content is encrypted using the AES symmetric key encryption method with a 256 bits key prior to hashing.

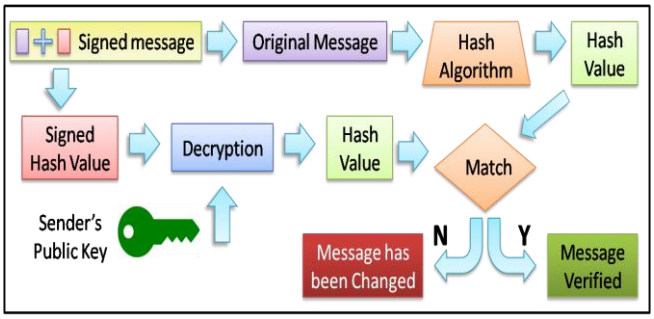

Figure 12: Verifying a Signed Message

At the next step, the validity of the Digital certificate is confirmed using the CA hierarchy at the recipient's end. If it is a valid certificate, the original content and the signed digest is separated from the received message and the digest is calculated again for the received content using the same hashing algorithm. Then, the public key is extracted from the certificate to decrypt the signed digest. Finally, the digest in the message and the newly calculated digest are compared to verify the integrity as shown in Figure 12.

IV. RESULTS AND DISCUSSION

The mobile application is tested using Android 5.1 on a Samsung Galaxy Core Prime phone with 1.2 GHz Quad-core Cortex-A53 CPU, Adreno 306 GPU and 1GB RAM. To obtain the best run time, each test is carried out 50 times to record the minimum run time.

Figure 13: Mobile Collaborative App

Figure 13 shows a screenshot of the Collaborative Mobile Application developed for this experiment. As seen, the images available for the current session are shown using floating thumbnails which allows selecting and zooming. Besides, it facilitates drawing and commenting on an image using a selected colour and a size. In addition, users can toggle between comments, voice, and videos of the current collaborative session.

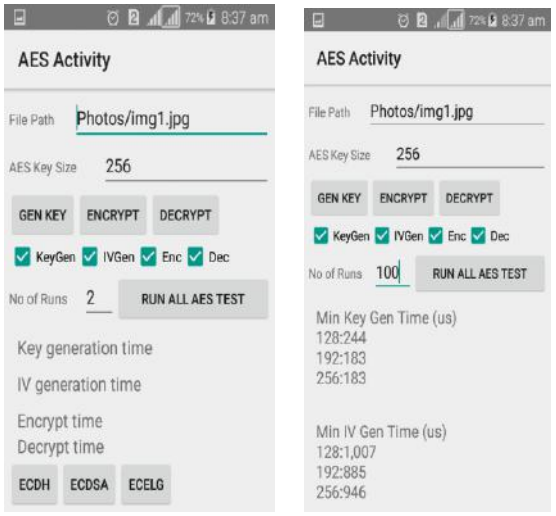

Figure 14: (Left) input parameters and (Right) performance results of AES Benchmark tests.

Figure 14 (Left) shows the AES benchmark application. AES key generation, IV generation, encryption, and decryption times can be tested separately or together for a given number of runs. The shortest times will be recorded and results will be shown as in Figure 14 (Right).

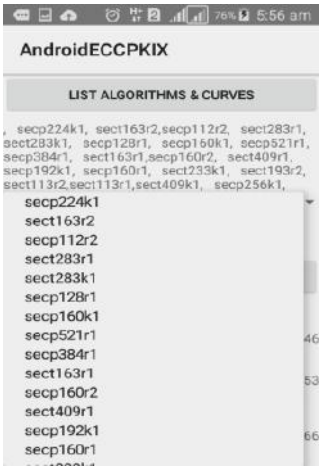

Figure 15: List of Supported Curves

Figure 15 shows the list of available elliptic curves used for the test.

Figure 16 (Left) shows generated ECC public and private keys and the shared session key between two users. Figure 16 (Right) shows the ECDH key exchange using a selected application and its run times.

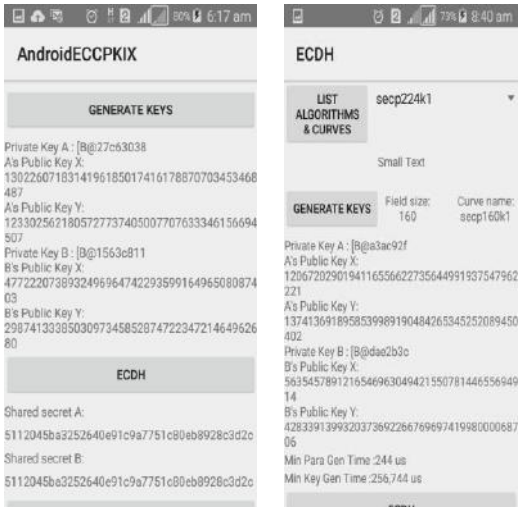

Figure 16: (Left) EC Key Generation, (Right) EC Diffie-Hellman Key Exchange

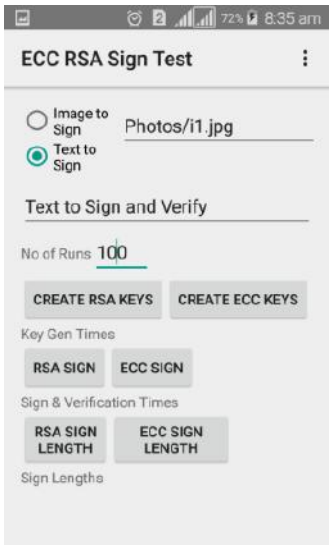

Figure 17: Benchmark to Test ECC and RSA Performances

Figure 17 shows the developed benchmark application to test the performance of the RSA and ECC algorithms. The Key generation times, sign and verification times, and signature lengths of both methods are tested. The selected tests are executed for given number of trails on a given text or image. In each iteration, the test is carried out on all curves and hash algorithms and the minimum times at each test is recorded.

As seen the EC sign time is significantly lower but the verification time is relatively higher. Moreover, both the sign and verification times get increased as the EC size increases. Though theoretically, the ECC is much faster than the present RSA asymmetric encryption, it is not due to the unavailability of optimized libraries in practice.

VI. CONCLUSION

In this paper, a secure mechanism for authentication and integrity verification based on a novel, robust and efficient public key cryptography method is implemented in an Android based collaborative medical imaging application using elliptic curve cryptography. Results indicate that the AES and SHA sizes do not make a significant impact on the runtime as the ECC. However, in all cases, the security increases as the key size increases. Due to less computation and space requirement of ECC, the method is well suited for mobile devices.

VII. REFERENCES

Bagchi, S 2006, 'Telemedicine in rural India', *PLoS medicine*, vol 3, no. 3, p. e82.

Bedi, BS 2003, 'Telemedicine in India: Initiatives and Perspective', *Health*.

Chen, Z, Yu, X & Feng, D 2000, 'Telemedicine system over the internet', *Selected papers from the*

Dahlman, EAMGAPSAEA 2014, '5G wireless access: requirements and realization', IEEE Communications Magazine, vol 12, no. 52, pp. 42--47.

Das, S & Mukhopadhyay, A 2011, 'Security and Privacy Challenges in Telemedicine'.

Das, S, Mukhopadhyay, A & Shukla, G 2011, 'A Framework for Determining the Hacker's Most Probable Path in a Wireless Telemedicine Network using Markov Model', E-Governance: Techno-Behavioural Implications, pp. 99-112.

Demaerschalk, BM, Vargas, JE, Channer, DD, Noble, BN, Kiernan, T-EJ, Gleason, EA, Vargas, BB, Ingall, TJ, Aguilar, MI & Dodick, DW 2012, 'Smartphone teleradiology application is successfully incorporated into a telestroke network environment', Stroke, vol 43, no. 11, pp. 3098-3101.

El-Iskandarani, MA, Darwish, S & Abuguba, SM 2008, 'A robust and secure scheme for image transmission over wireless channels', Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on, pp. 51-55.

Foley, L, Barney, K, Foley, J, Leeii, J, Fergerson, J, Sarrel, M, Nelson, C & Frank, M 2010, Identity theft: the aftermath 2009.

Georgiadis, P, Sidiropoulos, K, Hikimtzis, C, Banitsas, K, Dimitropoulos, N & Cavouras, D 2006, 'PDA-based teleradiology system with real-time voice conferencing capabilities', 2 nd

Gozalvez, J 2015, '5G Tests and Demonstrations [Mobile Radio]', Vehicular Technology Magazine, IEEE, vol 10, no. 2, pp. 16--25.

Gupta, S, Gill, PS, Mishra, A & Dwivedi, A 2012, 'A scheme for secure image transmission using ECC over the fraudulence network', International Journal of Advanced Research in Computer Science and Software Engineering, vol 02, no. 04, pp. 67-70.

Han, S, Nijdam, NA, Schmid, J, Kim, J & Magnenat-Thalmann, N 2010, 'Collaborative telemedicine for interactive multiuser segmentation of volumetric medical images', The Visual Computer, vol 26, no. 6-8, pp. 639-648.

Hepburn, A 2013, 'Infographic: 2013 mobile growth statistics', digitalbuzzblog. com, available on-line at www. digitalbuzzblog. com.

LoPucki, L 2001, 'Human identification theory and the identity theft problem', Texas Law Review, vol 80, pp. 89-134.

Mancilla, D & Moczygemba, J 2009, 'Exploring medical identity theft', Perspectives in health information management/AHIMA, American Health Information Management Association, vol 6, no. Fall.

Solove, DJ 2002, 'Identity theft, privacy, and the architecture of vulnerability', Hastings Lj, vol 54, p. 1227.

Walters, W & Betz, A 2012, 'Medical Identity Theft', Journal of Consumer Education, p. 75.