An Elliptic Curve Digital Signature Algorithm (ECDSA) for Securing Data: An Exemplar of Securing Patient's Data

Philomena Waruhari

Department of Electrical & Electronic Engineering
School of Electrical, Electronic & Information Engineering
Jomo Kenyatta University of Agriculture and Technology
pwaruhari@jkuat.ac.ke

Lawrence Nderu

Department of Computing
School of Computing and Information Technology
Jomo Kenyatta University of Agriculture and Technology
lnderu@jkuat.ac.ke

Abstract **- In this paper, we present the progress of our work in the creation and implementation of an Elliptic Curve Digital Signature Algorithm (ECDSA). We present the design of the algorithm and its implementation in encryption of medical data. ECDSA PHP ECC code has been used to implement the digital signatures over elliptic curve P-256. The work presented highlights practical implementation of ECDSA signature generation to secure and authenticate patient laboratory test results in a Laboratory Information System (LIS). Future work will demonstrate the implementation of decryption using the ECDSA. With the inherent superiority capability of Elliptic Curves (EC) in securing data, our algorithm is highly secure and can be adapted in many areas where data privacy and security is paramount.**

Keywords **- Security, Encryption, Digital signature, Elliptic Curve Digital Signature Algorithm (ECDSA)**

I. INTRODUCTION

The proliferation of Information and Communication Technologies (ICTs) today has seen most businesses computerize their operations. This is due to the accrued benefits such as better data management, evidenced based decision support, cost saving, efficiency among others. Most importantly, the driving factor to adopting ICTs in business is the competitive advantage/edge gained in the prevailing markets competition. Information is now more readily available than ever before any where any time just by a click of a button. However, this has at the same time exposed organizations to numerous security threats and breaches resulting to great losses in revenue as well as customer confidence. The fact that security breaches emanate from either internal or external sources or both [1], has given organizations a headache and has forced them to greatly focus on security mechanisms to curb unauthorized access or manipulation of organizational data. Consequently, different security mechanisms are continually being devised to prevent these malicious attacks.

In health care industry, different types of information systems such as clinical information systems (CIS), Electronic Medical Records (EMR), Pharmacy Systems (PS) and Hospital Management Information Systems (HMIS) have been deployed to support care and treatment. This has resulted to improved health outcomes as well as healthcare cost reduction [2]. On the other hand, Laboratory Information Systems (LISs) solutions are also vital in supporting evidence-based medicine which has further improved quality of health care [3]. All these information systems are designed to capture, store, process and communicate health information which is highly personal. Therefore, it is detrimental if this information falls in the wrong hands. This is further compounded by the ease of sharing electronic data.

Storage or transmission of data in digital form posses a great security threat due to very sophisticated technologies used by hackers to gain access to sensitive data of their choice through eavesdropping , password attack, Denial of Service (DoS), Social Engineering among others techniques [4]. Patients' trust on the integrity of the outcome of their laboratory test results should be guaranteed by employing appropriate security measures [5].

Information security standards have been enforced through cryptographic and digital signatures techniques to ensure electronically stored or transmitted data is authentic and free from alterations [6]. Digital signatures are used to validate and authenticate electronic documents. Digital signatures are non-forgeable due to the algorithms used to derive them. Rivet Shamir Adelman (RSA), Deffie Hellman (D-H) and Elliptic Curve Digital Signature Algorithm (ECDSA) are the standardized digital signature schemes [7]. The choice on the best algorithm is based on the level of security they provide as well as size of the signature [8],[9]. The size of the signature has a direct effect on storage space, bandwidth, power consumption and computational power needed. ECDSA is a better choice as it has smaller key size leading to faster computations among other benefits [10]. Thus ECDSA is suitable in portable devices such as cellular phones, medical implants and smart cards [11], [12], [13]. In addition, ECDSA provides greater security compared to other digital signature schemes as its algorithm is based on elliptic curves which provides greater strength-per-key bit [14],[15]. In this paper, we discuss how ECDSA may be applied in securing patient laboratory test results data.

The reminder of this paper is organized as follows: In section II, we discuss information security and types of security mechanisms followed by a discussion on

cryptography and its implementation in elliptic curves in section III. In Section IV, we discuss digital signatures with particular focus on elliptic curve digital signature algorithm. In section V we show the implementation and results of ECDSA design in securing patient data in a laboratory information system. In sections VI and VII we present a discussion and conclusion respectively.

II. INFORMATION SECURITY

Many organisations store volumes of sensitive data and information as a result of computerization of their services. Information in digital information is much easier to manipulate and hence the need to safe guard it from unauthorized access. Information security encompasses aspects to do with electronic information assets protection against security threat [16]. Information security is based on three pillars: Confidentiality, Integrity and Availability (CIA) triad. However, Authentication and non-repudiation have also been added as information security properties [17]. Confidentiality is enforced when measures are put in place to ensure information is accessed by authorised persons only. In health care setting, confidentiality is applied in all aspects of handling a patient from the conversations with doctors to handling patients' records. In fact, even medical practitioners are prevented from revealing some of their discussions with patients due to legal protections even under oath in court. Integrity is ensured when the received message is as it was sent from the transmitting side and hence a guarantee that no alterations has taken place in the process of transmission. Information systems are said to serve their purpose if the information they store and process is available when needed [18]. Therefore the access control measures implemented to enforce information security and the communication channels for its transmission should be functional at all times. These three information security properties known as CIA triad encompasses the fundamental security concerns for both data/information and computing services [19]. Authentication is the process of proving one's identity while non-repudiation is a way of proving that the message has actually been sent by the claimed sender [6].

In healthcare systems, various standards and legislation are enforced to ensure security of healthcare data. For instance US comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which directs that all patient-related information should be protected and encrypted when being transported electronically [12]. In addition, HIPAA also ensures that stored patient's information is confidential, reliable and available when needed. In the UK, organizations are required to comply with Data Protection Act 1998 [1] which regulates processing of information or data relating to its collection, storage and disclosure. In Kenya, The Kenya Information and Communication Act 2009 regulates matters touching electronic data in the Electronic Transactions section of the laws (Kenya Laws, 2009).

III. CRYPTOGRAPHY WITH ELLIPTIC CURVES

Katz & Lindel [21] defines cryptography as "*scientific study of techniques for securing digital information, transactions and distributed computations"* by transforming data from one format to another using a key (k) such that the data is unintelligible to unauthorized parties and hence cannot be tampered with. Historically, the military and intelligence organizations were the major consumers of cryptography [21]. However, today, cryptography is everywhere due to the increased usage of computers and Information and Communications Technologies (ICTs) resulting to modern security mechanisms.

Security behind public key cryptosystems is based on one-way function mathematical functions that are easy to compute but their inverse function is very difficult to compute [22]. The three problems on which public key cryptosystems are founded on are Integer Factorization Problem used by RSA [23], Discrete Logarithm Problem applied by DSA, Diffie-Hellman, ElGamal and Elliptic Curve Discrete Logarithm Problem used in ECDSA [24].

Elliptic curve cryptosystems (ECC) came into being as a result of the use of points on elliptic curve by the public key cryptosystems independently proposed by Neal Koblitz and Victor Miller in 1985 [9],[14]. Elliptic curves are defined over finite fields F(p) also referred to as Galois field GF(p) and they require unique mathematical operations. ECC is based on the difficulty of computing point Q given P, R and the curve $y^2 = x^3 + ax + b$ shown in Fig. 1. According to Najlae & Said [10], elliptic curve cryptography is a choice for those in search for public key cryptosystem that has smaller keys and faster and at the same time offering high security. This is mostly preferred especially in constrained environments where computational power and size of devices is of concern [12],[13].

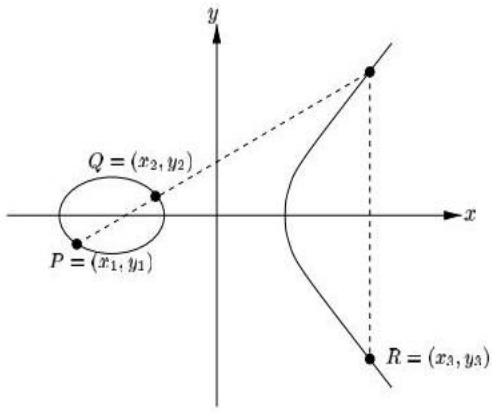

Fig. 1 An illustration of elliptic curve cryptography [8]

Table 1 evidently shows that ECC gives same security as compared to the other cryptosystems but with small key size. This is more pronounced in higher security levels. For example, where methods like RSA requires 1024 bit keys, elliptic curve only requires 160 bit keys for equivalent security. Digital signatures schemes are one of the major applications of public key cryptography.

TABLE 1
NIST RECOMMENDED KEY SIZES (IN BITS) FOR EQUIVALENT SECURITY [11]

Symmetric key size	RSA and Deffie-Hellman key size	Elliptic curve key size	Key Ratio
56	512	112	5:1
80	1024	160	6:1
112	2048	224	9:1
128	3072	256	12:1
192	7680	384	20:1
256	1560	512	30:1

IV. DIGITAL SIGNATURES

Digital signatures are used to validate and authenticate electronic documents [25]. NIST FIPS PUB 186-3, defines a digital signature as "*the result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation"* [26]. In the first step of digital signature generation, the data message is compressed by subjecting it to a hash function resulting to a fixed-size message digest. The hash algorithms provide another level of security as they are designed in such a way that it is impossible for two messages which are not similar to be assigned the same hash value [25]. On the other hand, it is impossible to determine the contents (message) by reverse engineering the message digest. Message-digest 5 (MD5) and Secure Hash Algorithm (SHA) are some of the hash functions in common use today. FIPS 180 specifies SHA-2 as the current hashing standard for encryption [26]. In the second stage of digital signature generation, the resulting message digest is signed using the signatory's private key. Consequently, the digitally signed message is then sent to the receiver. Finally on the receiving end, the signature is verified by the use of the signatory's public key. If the hash values are equal, then the signature is valid meaning the integrity of the message intact and it is authentic. In case a hacker alters the message even a single bit, the hash values will not be equal thereby invalidating the signature. Fig. 2 illustrates the digital signature process.

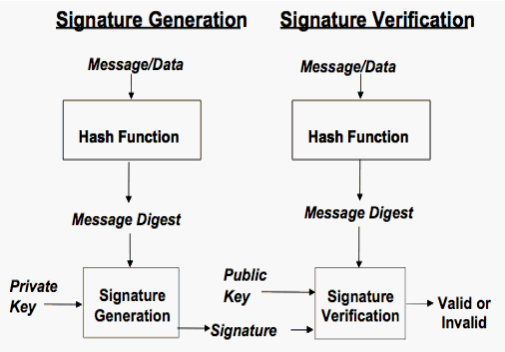

Fig. 2 Digital signature process [11]

There are a number of digital signature schemes but the standardized ones include ElGamal digital signature scheme, digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA). *"The Elliptic Curve Digital Signature Algorithm is the elliptic curve analogue of the Digital Signature Algorithm (DSA)"* [9],[13]. This signature scheme is widely standardized in ANSI X9.62, FIPS 186-2, IEEE 1363- 2000 and ISO/IEC 15946-2 standards as well as several other draft standards. The ECDSA processes involve key generation, signature generation and signature validation. Just like public cryptosystems, digital signatures consists of four algorithms: domain parameter generation algorithm, key generation algorithm, encryption and a decryption algorithm [7],[27].

A signature scheme is considered to be secure if it is impossible to forge it by using any form of computations [9]. This means that an adversary cannot obtain a valid signature of new messages given messages from a legitimate signer. Since it is impossible to predict the potential of an adversary in different settings, it is upon the designer of the signature scheme to ensure that it is very secure. Digital signatures not only provide security of data but mainly enforce authentication, integrity and non-repudiation. This is extremely important in the medical field as accountability is highly demanded as the data handled means life.

V. IMPLEMENTATION AND RESULTS

Patients' laboratory test results are deemed very sensitive and hence should be safe guarded from falling into wrong hands. Therefore, we implemented digital signatures using ECDSA on test results in a Laboratory Information System (LIS) for JKUAT hospital in order to enforce security to this highly sensitive patient information. The test results are encrypted and digitally signed on clicking the save test results button by laboratory technologist once the results are captured from the clinical analyzers. Therefore the results in the LIS MySQL database are encrypted making them secure from any malicious attack both internal and external. The implementation design layout is shown in the Fig. 3.

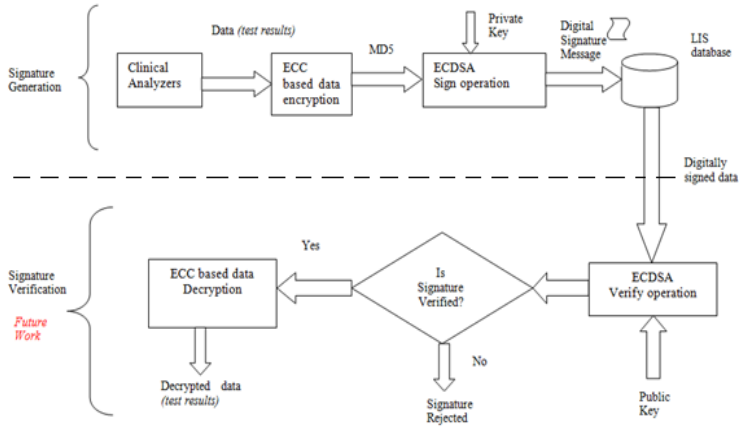

Fig. 3 ECDSA implementation Design Layout

ECDSA PHP ECC code shown below was used to implement the digital signatures over elliptic curve P-256. NIST curves were used because they are standardized as secure by FIPS-186-2. The ECDSA processes involve key generation, signature generation and signature validation. The

NIST curve selected was 256. The steps of digitally signing patient results in LIS were implemented as shown in Fig. 4 via the technologist's role in the LIS system. The output is shown in Fig. 6.

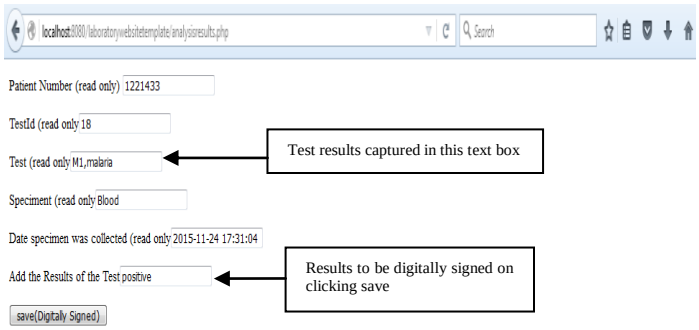

Fig.4 Test results capture interface

The code for generating the key pair is shown in Fig. 5 (https://github.com/phpecc/phpecc).

```
//Use base 256
define('MAX_BASE', 256);

//Force Either BCMATH or GMP, Autodetected otherwise, prefers GMP
//if(!defined('USE_EXT')) define ('USE_EXT', 'BCMATH');
//if(!defined('USE_EXT')) define ('USE_EXT', 'GMP');

include 'autoload.inc.php';
include 'classes/PHPECC.class.php';
include 'classes/SECurve.class.php';

$keypair = PHPECC::hex_keypair_generate();
$signed = PHPECC::hex_keypair_generate($result);
```

Classes that do the keys generation

Fig. 5 Code for generation of key pair

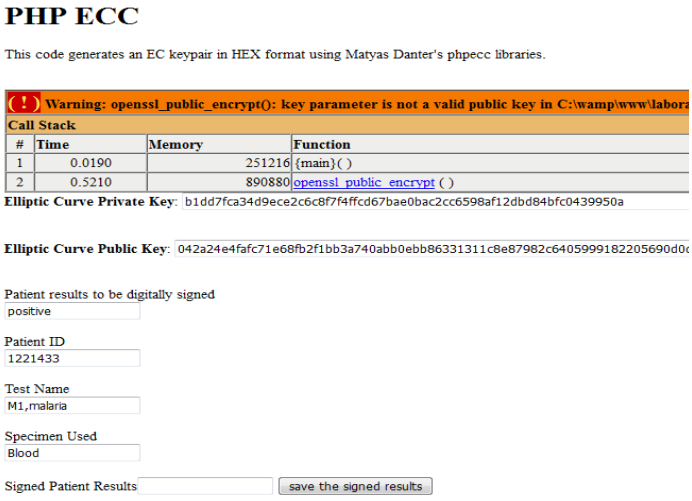

Fig. 6 Generation of private and public key pair

The test results were digitally signed using the generated private key and saved in the LIS database as shown in Fig. 7. Future work will demonstrate the signature verification part of digital signature process using the generated public key.

Confidentiality of patient data is enforced further by authentication of the system users through role based system access via personal login username and password credentials.

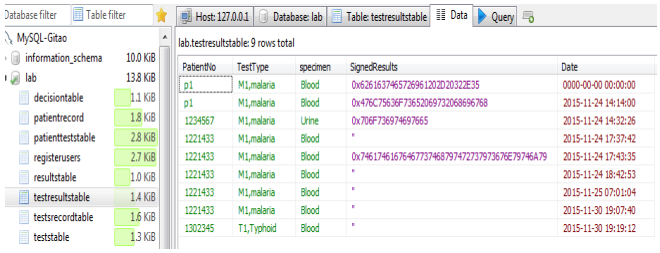

Fig. 7 Digitally signed test results in the LIS database

VI. DISCUSSION

We have implemented ECDSA digital signature to secure healthcare data in storage. This is a 'Data at Rest' security solution. The system generates a unique key pair for every click on the save results button. Therefore even if the test result outcome is the same for two different patients, the digitally signed results appear different in the database. For example malaria test results may be positive for two different patients but the generated signature is for each different. On the other hand, signing the message digest rather than the message improves the efficiency as well as doubling the security of the message. The message digest usually is smaller in size than the message. At the same time the verifier of the digital signature must use the same hash algorithm as was used by the creator of the digital signature as well as the public key of the generated key pair. We used Secure Hashing Algorithm (SHA1) for its known security as it is computationally impossible to find two different messages produced by the same message digest. The resulting digitally signed laboratory test results can also be transmitted over insecure public communication links to other hospitals without potential risks of malicious attacks, hence making our solution viable for use in public health laboratories.

VII. CONCLUSION

In this paper we have presented a practical implemented of ECDSA signature generation to secure and authenticate patient laboratory test results in a LIS. ECDSA offers smaller keys than conventional algorithms like RSA without compromising the level of security. The empirical results demonstrate the use of ECDSA in securing patient data on healthcare devices. Comprehensive security of healthcare data is guaranteed when encryption, signature and authentication entities are combined together. Our future work will demonstrate the verification process.

REFERENCES

[1] G. Kelly and B. McKenzie, "Security, privacy, and confidentiality issues on the Internet," *Journal of Medical Internet Research*, vol. Vol:4, no. 2, 2002.

[2] F. Robert G., R. Kohli, and R. Krishnan, "Healthcare : Current Research and Future Trends The Role of Information Systems in Healthcare : Current Research and Future Trends," *Information Systems Research*, vol. 22, no. January 2014, pp. 419–428, 2011.

[3] Eisenberg M. John, "Evidence-Based Medicine," *Expert Voices, Agency for healthcare Research and Quality*, no. 1, pp. 1–2, 2001.

[4] S. Chen, J. Xu, and E. Sezer, "Non-control-data attacks are realistic threats," *Proceedings of the 14th USENIX Security Symposium*, vol. 14, pp. 177–191, 2005.

[5] A. L. McGuire, R. Fisher, P. Cusenza, K. Hudson, M. a Rothstein, D. McGraw, S. Matteson, J. Glaser, and D. E. Henley, "Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider.," *Genetics in medicine : official journal of the American College of Medical Genetics*, vol. 10, no. 7, pp. 495–499, 2008.

[6] G. C. Kessler, "An overview of cryptography," *Online: http://www. garykessler. net/library/crypto. html*, vol. 1998, no. May 1998, pp. 1–23, 2007.

[7] W. Stallings, "Digital Signature Algorithms," *Cryptologia*, vol. 37, no. 4, pp. 311–327, 2013.

[8] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[9] D. Hankerson, a J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. 2003.

[10] Najlae Hameed Al-Saffar and M. R. M. Said, "On the Mathematical Complexity and the Time Implementation of Proposed Variants of Elliptic Curves Cryptosystems," *International Journal of Cryptology Research*, vol. 4, no. 1, pp. 42–54, 2013.

[11] A. Khalique, K. Singh, and S. Sood, "Implementation of Elliptic Curve Digital Signature Algorithm," *International Journal of Computer Applications*, vol. 2, no. 2, pp. 21–27, 2010.

[12] K. Malhotra, S. Gardner, and W. Mepham, "A novel implementation of signature, encryption and authentication (SEA) protocol on mobile patient monitoring devices.," *Technology and health care : official journal of the European Society for Engineering and Medicine*, vol. 16, no. 4, pp. 261–272, 2008.

[13] R. Afreen and S. C. Mehrotra, "A Review of Elliptic Curve Cryptography for Embedded Systems," *International Journal of Computer Science & Informatiion Technology*, vol. 3, no. 3, pp. 84–103, 2011.

[14] Teo Kai Meng, "Curves For the Elliptic Curve Cryptosystem," *Research opportunity programme in computer science*, 2001.

[15] M. N. Nabi, M. L. Rahman, and M. L. Rahman, "Implementation and Performance Analysis of Elliptic Curve Digital Signature Algorithm," pp. 28–33, 2000.

[16] E. H. Spafford, "Computers and Security: Editorial," *Computers and Security*, vol. 30, no. 4, p. 171, 2011.

[17] P. S. Browne, "Computer security," *ACM SIGMIS Database*, vol. 4, no. 3, pp. 1–12, 2001.

[18] H. F. Tipton, *Information Security Management Handbook, Fourth Edition, Volume 3*, 4th Editio. United States of America: CRC Press, 2014.

[19] W. Stallings, M. Bauer, and E. M. Hirsch, *Computer Security. Principles and Practice.*, Second Edi. Pearson Education, Inc, 2013.

[20] Laws of Kenya, "LAWS OF KENYA The Kenya Information And Communications Act," vol. 2009, no. 1998, 2009.

[21] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. 2007.

[22] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," *Lecture notes in computer science*, pp. 119–132, 2004.

[23] R. L. Rivest, A. Shamir, and L. Adleman, "A Method of Obtaining Digital Signatures and Public-Key Crytosystems," 1978.

[24] Rhea Stadick, "Rhea StadickThesis 12-05." pp. 1–72, 2005.

[25] S. R. Subramanya and B. K. Yi, "Digital signatures," *IEEE Potentials*, vol. 25, no. April, pp. 5–8, 2006.

[26] T. A. Hall, "The FIPS 186-4 Digital Signature Algorithm Validation System (DSA2VS)," 2014.

[27] N. Carruthers, "Digital Signature Schemes," *Department of Math and Computer Science*, 1997.