Enhanced tiny encryption algorithm for secure electronic health authentication system

Yunusa Simpa Abdulsalam*,
Olayemi Mikail Olaniyi and Aliyu Ahmed

Computer Engineering Department,
Federal University of Technology Minna,
Niger State, Nigeria
Email: abdulsalam.pg611937@st.futminna.edu.ng
Email: mikail.olaniyi@futminna.edu.ng
Email: aliyu.ahmed@futminna.edu.ng
*Corresponding author

Abstract: One of the main worries circling the globe today is how to provide efficient and effective quality health services. Conventionally, part of the constraints in making these efficient quality health services possible is the fact that patients and consultants must be physically present in the same location. Modern development in information technology have been able to raise the number of possible ways healthcare can be delivered remotely to reduce medical access restraints, but the issue of patient authentication remains paramount. As more delicate data is stored in electronic health record (EHR) systems, there is need to provide effective security to avoid malicious attacks through illicit access to EHRs. This paper presents an enhancement to tiny encryption algorithm for secure near frequency communication based EHR system. The conventional tiny encryption algorithm was enhanced with Yarrow pseudo random number generator for better key randomisation. Results of the performance evaluation of the developed enhanced algorithm showed that the scheme is capable of providing countermeasures against replay and tag cloning attacks in data communication channels of clinic tele-consultations.

Keywords: electronic health record; EHR; security; authentication; privacy; tiny encryption algorithm; TEA; healthcare.

Reference to this paper should be made as follows: Abdulsalam, Y.S., Olaniyi, O.M. and Ahmed, A. (2018) 'Enhanced tiny encryption algorithm for secure electronic health authentication system', *Int. J. Information Privacy, Security and Integrity*, Vol. 3, No. 3, pp.230–252.

Biographical notes: Yunusa Simpa Abdulsalam obtained his BEng in Electrical/Computer Engineering and Master's of Computer Engineering in 2015 and 2017, respectively, from Federal University of Technology, Minna, Nigeria. He is a promising computer network security expert. His research interests are in distributed systems design and computer network security.

Olayemi Mikail Olaniyi is a Senior Lecturer in the Department of Computer Engineering at Federal University of Technology, Minna, Niger State, Nigeria. He obtained his BTech and MSc in Computer Engineering and Electronic and Computer Engineering respectively. He had his PhD in Computer Security from Ladoke Akintola University of Technology, Ogbomosho, Oyo State, Nigeria. He has published in reputable journals and learned conferences. His areas of research include information and computer security, intelligent/embedded systems design and telemedicine.

Aliyu Ahmed is a Lecturer II in the Department of Computer Engineering at the Federal University of Technology, Minna, Niger State, Nigeria. He obtained his BEng in Electrical and Computer Engineering from the Federal University of Technology Minna and his MSc in Computer Networking from the University of Bedfordshire, UK. He is currently a Doctoral student at the Department of Computer Engineering Federal University of Technology, Minna, Niger state, Nigeria. His research interests include computer security, intelligent systems, embedded systems and wireless sensor networks.

1 Introduction

Healthcare service transformation from paper based systems to computerised networked environment raises alarms regarding privacy, safety and ethics. The fast growth of data, information gathering and management has led to unidentified challenges, in that medical data can now readily be available on shared networks, mobile devices, and distributed systems (Malin et al., 2013). The use of these technological devices to improve access and efficiency of healthcare records in digital environment raises security concerns as regards to patient privacy and legal authentication. These devices and tools has recently been integrated in e-health sector so as to enable and further facilitates ease of access to necessary services (Wamala and Augustine, 2016).

There is now a growing fear that unauthorised access to information may lead to lack of assurance and trust in electronic healthcare delivery, which can cause serious changes in the way users cooperate with the system. Such changes can reduce the real quality of healthcare delivered, as patient's can now choose either to visit another physician, give incomplete health information or even to self-medicate. According to the United Nations Sustainable Development Goals (SDGs), proper wellbeing and healthy lives of citizens should be preserved by year 2030 (Femi et al., 2017). These can only be achieved by the appropriate adoption of secured e-health schemes by enhancing and facilitating legitimate access to healthcare.

From the medical doctors' perspective, concerns as regards to authentication and privacy were discovered to deter doctors' approval and implementation of electronic health record (EHR) (Chao et al., 2013), thereby, showing how these concerns can further have negative impact on the use of EHR, which extends beyond patients' doubts. In light of these concerning issues and the developing mindfulness of potential privacy violation, the health system has now begun to implement several techniques in protecting privacy. Most health record systems have now adopted different techniques such as the pseudo-anonymity (Neubauer and Heurix, 2011). This concept of pseudo-anonymity allows third party access to medical information without in any way disclosing patient's identity. Other methods to protect patient's privacy is also access control. Most EHR systems now require authentication techniques such as digital credentials, electronic stamps and limited control access policies (Blobel, 2004; Fernández-Alemán et al., 2013). Failure to properly record medical activities can hinder the stability of healthcare delivery (Devendran et al., 2015; Mars, 2013). Therefore, it can be mostly seen that, patients had to carry laboratory tests and x-rays results that is not electronically available. To facilitate patients auto detection and overcome time challenges, near field communication (NFC) technology was adopted to allow patients be electronically

identified, making health records effortlessly manageable for record officers (Razmi and Sangar, 2016; Devendran et al., 2015; Kartik et al., 2015).

Addressing imminent security issues such as legal authentication of patients, will effectively increase the accessibility and quality of healthcare delivery by letting distant benefactors to diagnose, evaluate and treat patients efficiently. It can also provide an effective and efficient means for tertiary care advising and access by patients in remote areas. Increasing legitimate access to healthcare can enable patients seek early treatment, adhere to recommended treatments, and increase better quality life style for patients with prolonged ailment (Acharya et al., 2011).

In this paper we address the issue of authentication in NFC based EHR system using tiny encryption algorithm (TEA) which was enhanced with Yarrow pseudo random number generator to avert replay and tag cloning attacks in data communication channels of clinic tele-consultations. The rest of this paper is organised into four sections, Section 2 provides a review of related works and synthesis of existing works in literature, system methodology is presented in Section 3, results and discussions are presented in Section 4, while Section 5 concludes and provides scope for future works.

2 Literature review

A number of related works exist in literature. A common architecture for healthcare delivery using NFC for mobile health monitoring services was developed by Razmi and Sangar (2016). In this architectural scheme, provision of required secure health services according to available structure for patient's information in hospitals and treatment were addressed. Similar authentication technique for NFC based e-health system was developed by Devendran et al. (2015). The limitation to this technique was that 1k Mifare NFC tag which restricted storage clinical visit details was used and insecurity of transaction between tags and reader, which make the technique vulnerable to eavesdropping and replay attacks. Table 1 shows the chronological synthesis of related baseline works in literature.

In this work, we present an enhancement to conventional TEA for secure data transactions between NFC tags and readers to enhance existing secure authentication scheme for electronic health system in Abdelhalim et al. (2012), Devendran et al. (2015), Hameed et al. (2015, 2016) and Razmi and Sangar (2016). Our enhancement lies in the application of Feistel block architecture instead of the linear feedback shift registers (LFSR) which implemented the XOR mechanism similar to the traditional TEA. The implemented NFC application provides data integrity and information authentication, also in terms of symmetric ciphers which provides lowest storage requirements and processing latency for better power consumption and effective memory usage. The NFC applications have been known for several malicious attacks; either in the form of active or passive attacks. The decentralised areas of NFC applications are mostly inclined to invaders which typically are not the case when it comes to wired networks. A number of secure encryption mechanism have been implemented in NFC applications in other to increase and maintain privacy of information. In this paper, a well-defined enhancement to TEA have been designed to better suite NFC tags by creating strong security and mitigating attacks such as chosen plaintext attack, generate an unpredictable key circle and less time complexity in key generation.

Table 1 Review of NFC technology for electronic health authentication system

	Author	*Adopted methodology*	*Strength of adopted methodology*	*Limitations to adopted methodology*
1	Saito et al. (2004)	Proposed a method of re-encrypting encrypted RFID tag with the use of public key	Strengthening of cipher text by re-encryption, meaning encrypting a cipher text again.	Though the cipher text was repeatedly re-encrypted, the message could be acquired with the help of its private key.
2	Kinoshita et al. (2005)	Proposes a technique for protecting privacy in RFID tags.	Providing contextual information became certain and easier.	Limited application areas for active tags. lacked optimal privacy protection scheme.
3	Dunnebeil et al. (2011)	Proposed a SemTag. A prototype which utilised (NFC) technology.	The system showed memory storage advantages in comparison with other available options of healthcare data storage. SemTags could be read and encrypted without any physical contact.	The eHC is not yet accessible by all health facilities. Lacks storage capability for complete sets data and uses numerous scrambled keys at the same instance.
4	Saeed and Walter (2012)	Proposed an NFC tag that implemented off-line authentication framework.	The framework effectively differentiated legitimate tags from cloned ones, also had sufficient properties to perform cryptography.	Due to low cryptographic power, cryptography used on tags were fairly weak. If K_{cert} is compromised, a successful replica can be made even when protected by T_a.
5	Abdelhalim et al. (2012)	Proposed modified TEA (MTEA) using a linear feedback shift register as a pseudo random number generator (PRNG).	The MTEA proved to be more efficient as compared to the typical TEA algorithm.	Limitations were for power consumption, silicon area and throughput for RFID systems.
6	Ertl et al. (2013)	Adopted advanced encryption standard (AES) for tag encryption.	The enhancements allowed mutual authentication of reader and tag, based on a challenge response protocol.	AES high impact on memory space High RAM usage Not fast and inefficient Not easily implemented

Table 1 Review of NFC technology for electronic health authentication system (continued)

	Author	*Adopted methodology*	*Strength of adopted methodology*	*Limitations to adopted methodology*
7	Huang and Huang (2013)	Proposed a secured authentication based on one-time password (OTP) authentication for RFID tag.	The technique improved tags security for proper certification.	Encryption is not feasible for all tags, due to memory limitations.
				Time delay in the authentication process
			Effectively prevented security weaknesses such as replay attacks, tag forgery and eavesdropping.	
8	Jeddi et al. (2013)	Light weight encryption algorithm was proposed for RFID systems.	The scheme provided adequate integrity, confidentiality and legal authentication	Hardware implementation of the MAC generator consumed considerable amount of memory.
				Efficient but complex and difficult to implement
9	Özcanhan et al. (2014)	Proposed IMS-NFC suitable and efficient for NFC.	Evaluation showed that the system provided stronger security, improved patient welfare.	AES high impact on memory space
				High RAM usage
				Not fast and inefficient
				Not easily implemented
10	Hameed et al. (2014)	Proposed a security middleware for security weaknesses in NFC-based systems.	Performance evaluations depicted that security has little effect on CPU memory.	Lacks safeguards against common security attacks, such as tag spoofing and man-in-the-middle attack.
			Low latency middleware.	Lack of scalability
11	Aboelfotoh et al. (2014)	Proposed an (EHR) system that allowed exchange of medical data using mobile devices.	Mobile EHR was encrypted so no one can access health record.	Limited PHR storage space. Poor data management backup.
			Data entered do not go undetected.	Poor security assessment of the MPHR-DA protocol
12	Kartik et al. (2015)	Framework for presentation medical data on mobile device.	Secured medical tags.	Centralised security with the use of cryptographic server

Table 1 Review of NFC technology for electronic health authentication system (continued)

	Author	*Adopted methodology*	*Strength of adopted methodology*	*Limitations to adopted methodology*
13	Devendran et al. (2015)	Proposed an NFC tags carrying EHRs.	Access to data operation was adequately authenticated.	Lack of ultimate security.
			Data encoded were stored in raw form 100% availability	Lack of proper security framework
14	Hameed et al. (2015)	Proposed a set of signature algorithms which are more flexible to provide effective integrity of data storage in tags.	Flexible and efficient means of data integrity.	No data authentication.
			Scalable and no visible usability effect.	Messages are prone to eavesdropping attacks
			Room for variant hashing algorithms	Asymmetric ciphers high storage requirement.

3 Methodology and technique description

3.1 Securing NFC applications in patient auto-identification

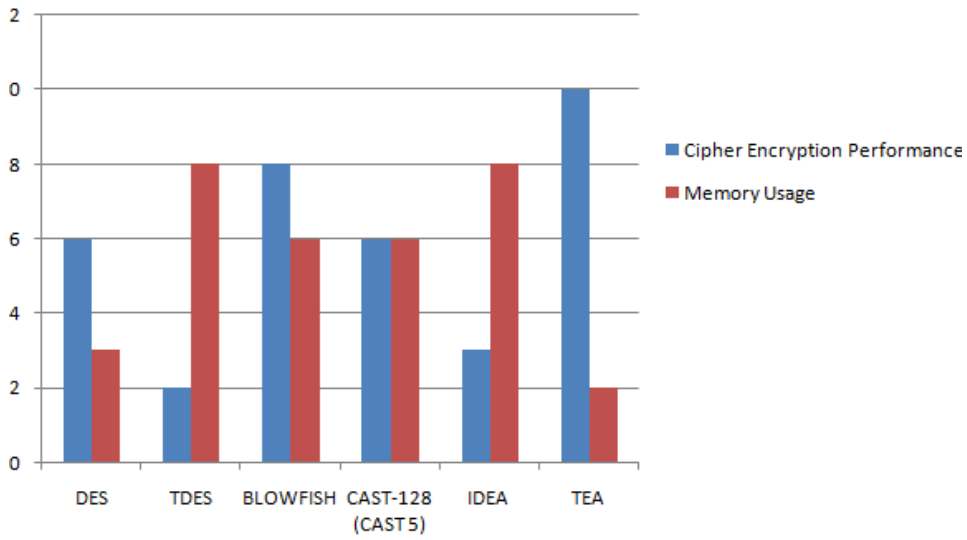
Patient emergency data are meant to be easily accessible by healthcare practitioners within short period of time and free of any possible interruption. Furthermore, healthcare information is a confidential information which should not be accessible by anyone without authorised access. In the light of providing efficient and effective access to medical information, NFC technology offers a unified flow of information and reliable transmission of secured data. This NFC feature will enable users access secure digital content contactless by a simple device connected to its proximity. There are multiple security issues involved in the application of NFC tags, such as relay and eavesdropping attacks. The applicable constraint taking into consideration for the implementation of NFC tags in this research however involves the reader/writer mode, where sensitive, encrypted data is to be stored and retrieved from NFC tags.

3.2 Security countermeasure by cryptographic algorithm

Cryptography, an essential mechanism for information protection in computing systems is also used to safeguard data in transit. Due to its integral part of a standard protocol, it comparatively makes it easy to integrate solid encryption in a wide variety of application. Therefore, the idea of cryptography comes to play, since it consists of symmetric and asymmetric algorithms, which can be used in securing NFC systems. Also, part of the solutions in remedying access to users is authentication by encryption, but, considering NFC tags memory limitations, the encryption algorithm should be sufficiently light to soothe these limitation (Jeddi et al., 2013).

Applying a suitable algorithm to a specific area of application requires proper knowledge of its limitation and strength. Subsequently, the performance evaluation of the developed algorithms centred on certain factors is highly paramount. For example, an algorithm's memory usage and consumption is defined as the total number of iterations carried out by an algorithm, the smaller memory usage and consumption, the greater its efficiency. Figure 1 represents generic scalability of different light weight cryptographic algorithms with respect to its memory usage performance and encryption. From the figure shown, it can be concluded that the TEA has better memory usage and high encryption performance.

Figure 1 Memory usage and encryption performance of different algorithm (see online version for colours)

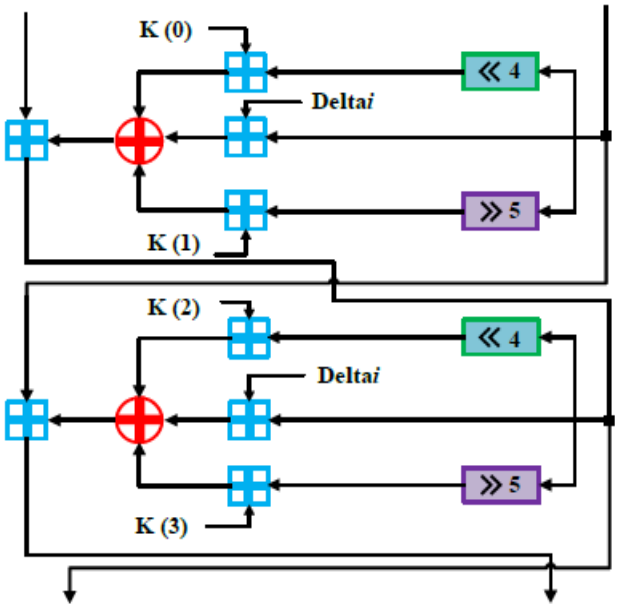


Source: Ebrahim et al. (2014)

3.3 Development of the enhanced tiny encryption algorithm

TEA was first proposed by Roger Needham and David Wheeler from Cambridge University (Alizadeh et al., 2012). TEA and other asymmetric algorithms are an example of lightweight cryptographic functions. This property makes them extremely suitable for high performance embedded systems (Abdelhalim et al., 2012; Olaniyi et al., 2017). TEA is a Feistel structure with different modes of operations which includes the ADD, SHIFT and XOR operations. Also, TEA has a block size of 64-bit and utilises 128-bit key rounds with 32 cycles (Abdelhalim et al., 2012; Ebrahim et al., 2014). TEA employs Shannon's twin structures namely diffusion and confusion, for adequate securing of cipher block as shown in Figure 2.

Figure 2 TEA structure (see online version for colours)



Source: Alizadeh et al. (2012)

In order to increase the TEA security against cryptanalysis, Yarrow PRNG was used to generate a new key every round as shown in Figure 3. The use of Yarrow as a PRNG was implemented due to its ability to handle cryptanalytic attacks. Yarrow utilises cryptographic hashing to sequentially generate input samples. Also, to preserve its secured updates, it combines the functions of the samples with existing key. This procedure ensures that attackers cannot manipulate input samples. In the developed algorithm, the secret key k is being generated by feeding input into the fast pool P_f and slow pool P_s respectively, to create enough entropy for key generation.

The random numbers from Figure 3 are produced by encrypting the value of the counter C using the secret key and the generated encryption function. The increment of the $n-bit$ counter C is done whenever a set of new random numbers are being generated:

$$C_{m+1} + C_m + 1 \left(\bmod 2^n \right) \tag{1}$$

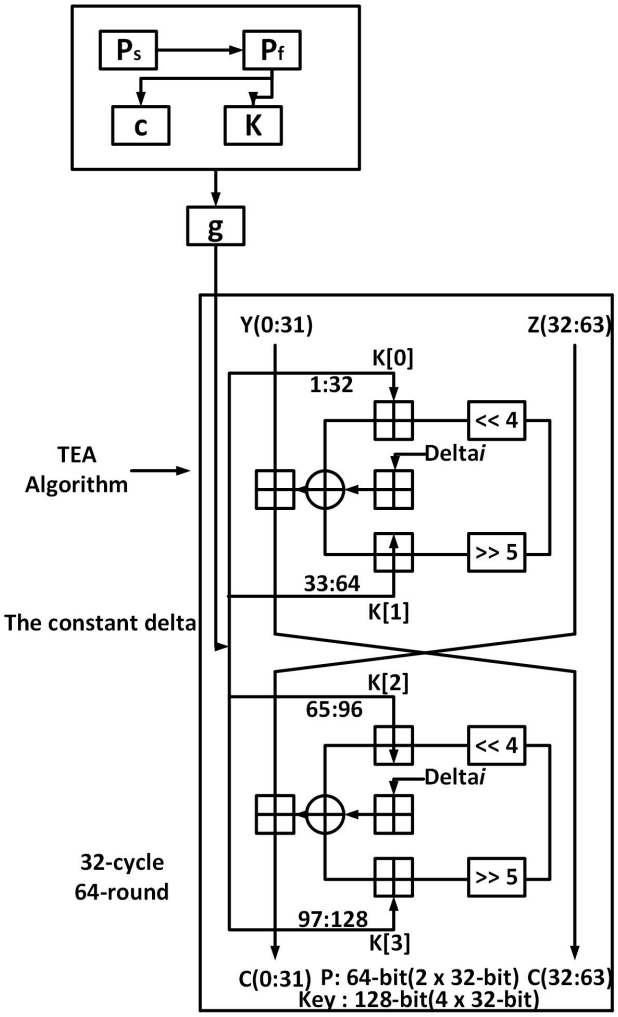
By encrypting C, produces the output O_m:

$$O_m = E_k \left(C_m \right) \tag{2}$$

As earlier stated, the traditional TEA operations depend on the use of ADD, SHIFT and XOR to deliver nonlinearity. The dual shift of the XOR operation creates a basis for all bits of the key and data to be varied repeatedly, and the 128-bit key K is split into four

32-bit blocks, k_0, k_1, k_2, k_3 and the 64-bit plaintext is split into two 32-bit blocks (Y_i, Z_j). After proper key generation and the value of delta is estimated, the Yarrow algorithm receives the generated key and randomly scramble it through the fast and slow pool to further generate a key that will be incremented by a counter after every encryption. In the developed enhanced algorithm in Section 3.3.1, after the data is been initiated, TEA registers the hash function and defines delta to be equal to yarrow k' for fast pool and entropy generation V_i for k_2' up to k_n' by the counter.

Figure 3 The developed enhanced TEA



In the decryption process, the cipher text is being initiated and the enhanced tiny encryption algorithm (eTEA) defines the generated PRNG to extract data. The structure of the enhancement of tiny encryption algorithm with Yarrow as a PRNG is depicted in Figure 3 as compared to the traditional TEA in Figure 2. The developed algorithm is show in Section algorithm 3.3.1 as follows.

3.3.1 Developed eTEA

Encryption process
Input: Plaintext
Output: Cypher text
Plaintext
Initiate data
$Delta = \left(\sqrt{5-1}\right) \times 2^n$
$Delta(i) = (i + 1) \times delta$
For $i = 0, 1, 2, 3 \ldots \ldots \ldots \ldots 31$
TEA = Yarrow
$V_i = \mathrm{h}(V_{i-1} \mid V_o \mid i)$ *for* $i = 1, 2 \ldots \ldots \ldots \ldots N_i$
$K' = h'(h(V_{Ni} \mid K), K)$
Initiate cipher for encryption.
Generate cipher text

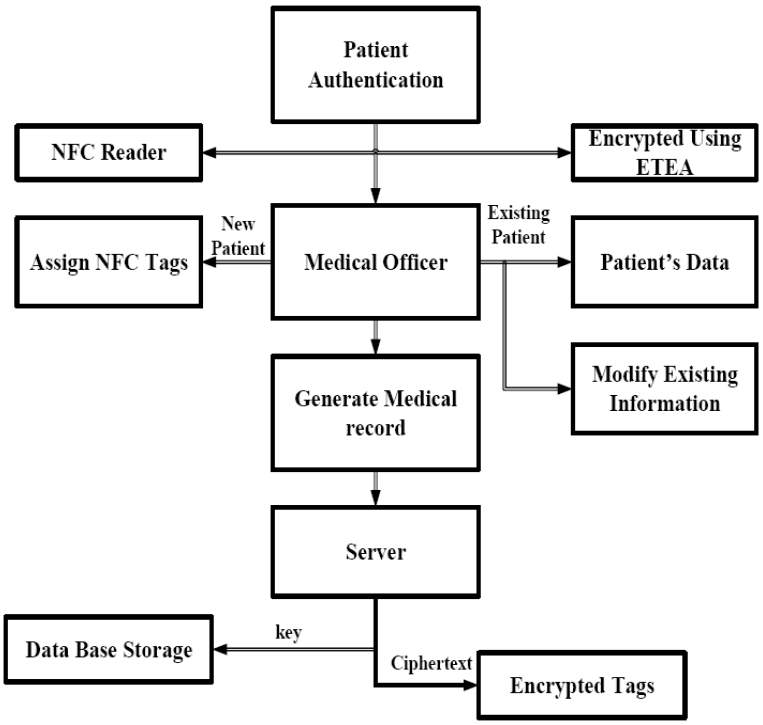
Decryption process
Input: Cipher text
Output: Plaintext
Initiate Cipher text
$K' = h'(h(V_{Ni} \mid K), K)$
$delta = K'$
Extract data
Generate plaintext.

3.4 Patient NFC tag authentication using eTEA

As highlighted from literature, the need to design a secure system for efficient healthcare delivery with key emphasis on patient's authentication using NFC tags becomes imminent. NFC is one of the most recent remote correspondence innovations. NFC is an evolution of radio frequency identification technology (RFID), which operates on very low power and a frequency of 13.56 MHz (Pirrone and Huerta, 2015). The process of trying to identify or determine patient access is referred to as legal authentication. Figure 4 is the detailed diagram of the system, depicting the working principles and sequence to be followed for proper authentication and encryption of patient data. It comprises of tag assignment, tag encryption/authentication, retrieving and generating reports. Also, it provides detailed history of patient's access. Figure 5 depicts the flow chat of the tag modification interface. The tag modification interface involves establishing a connection between the reader and the tag, given establishment of a successful connection, the data from the tag is been decrypted. If at any point the NFC tag did not establish a connection, a waiting period is exercised till the tag and the reader is synced. At the decryption stage, the system notifies an invalid tag when the data is not

properly decrypted to access the contained information. For valid tags, the information is securely decrypted to end the connection.

Figure 4 Patients NFC tag authentication



3.5 NFC module hardware design considerations

The NFC reader (Module PN532) in the NFC hardware was interfaced with Arduino Nano and NFC Mifire 4kB tags were used for authentication of valid patient, as depicted in Figures 6 and 7 respectively. These tags have read/write supported functions. The application programming interface (API) used was a SmartCard API, these provided the functions of read and write process, nevertheless, during operation the device may only be in one particular mode: either read or write mode. Procedure for authentication was supported through uniquely assigned patients tag. For instance, when legitimate tags are in the NFC reader's vicinity, its able to detects tags and also checks its content for user's identification stored in the database, after proper decryption. In the off chance that the user has not been authenticated, then the administrator assigns him/her a new identification, which is now been written to the tag's content, otherwise, the tag is invalid. When this same patient visits again, the reader determines the ID kept in the provided tag and patient is automatically authenticated. This way the system proves to be more efficient and reliable.

Figure 5 NFC tag read/write modification

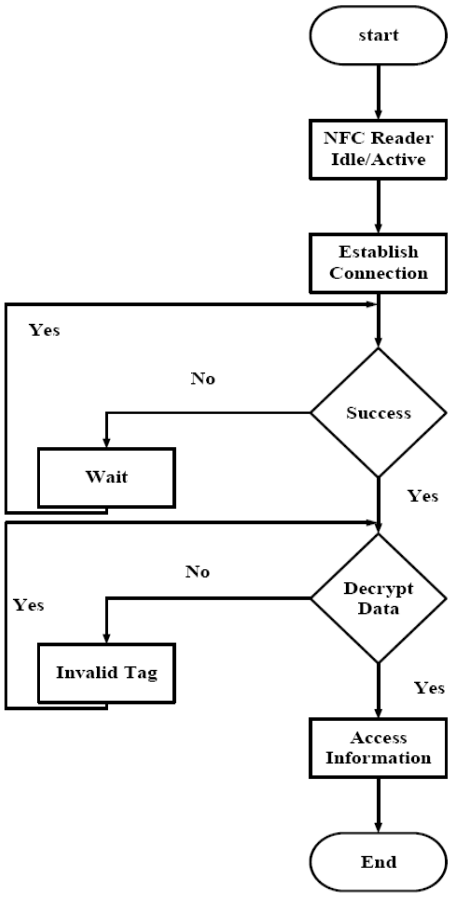


Figure 6 Transmission and receiving connection of the Arduino Nano interfaced with PN532 (see online version for colours)

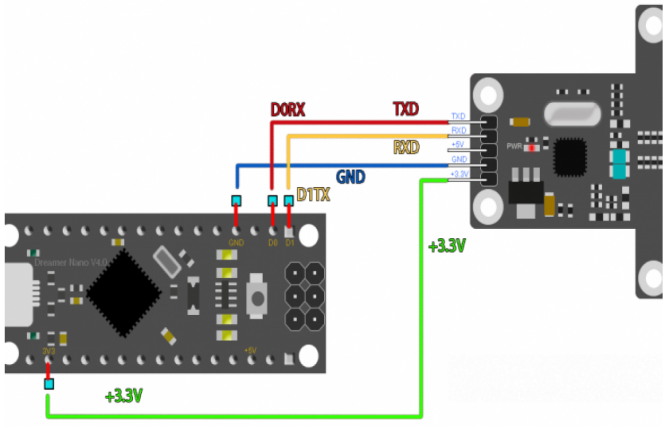
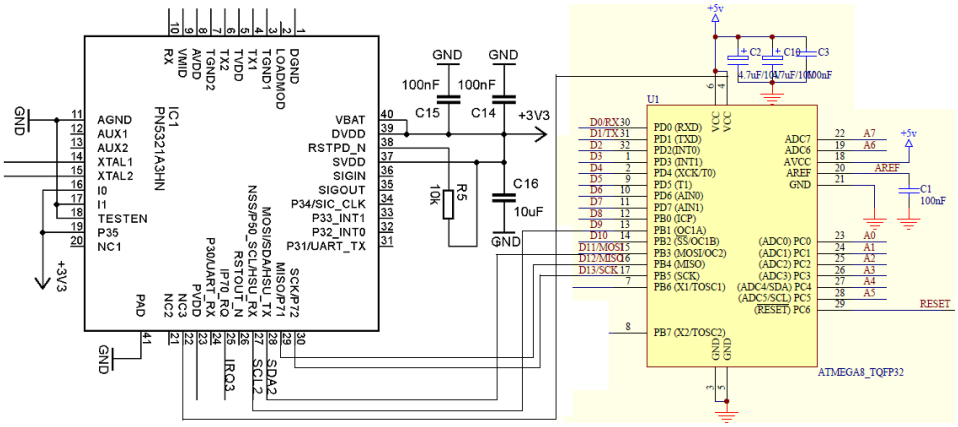


Figure 7 Circuit diagram of NFC based EHR authentication system (see online version for colours)



4 Results and discussion

4.1 System experimental and performance evaluation procedures

Figure 8 is a pictorial view of the Arduino with a serial USB 2.0 and a PN532 for NFC tag read/write modification. Figure 9(a) shows the NFC module interfaced to the computer ready to be detected, while Figure 9(b) shows the NFC tag modification page for establishing connection. The developed eTEA was implemented in Java for easy interfacing with the web application. The developed algorithm was then tested. Figure 10 shows the encryption and decryption stage of the developed algorithm. As explained in Section 3.3 using Figure 4, after EHR is been encrypted using eTEA, the cyphered text is then written to the tags through the serial ports of the NFC module.

Figure 8 Pictorial view of the coupled PN532 with Arduino Nano (see online version for colours)

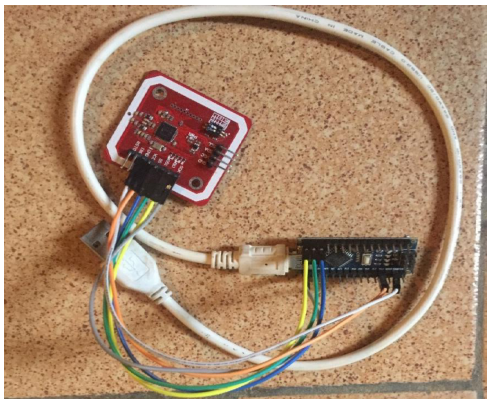
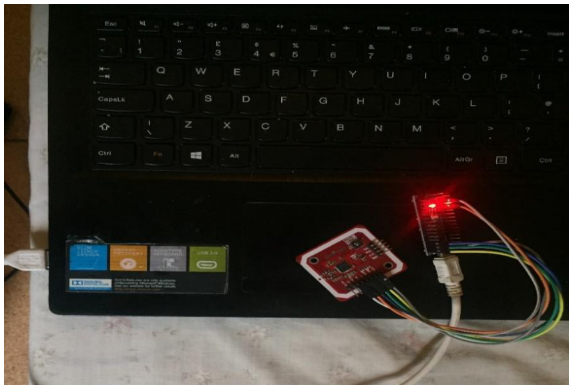
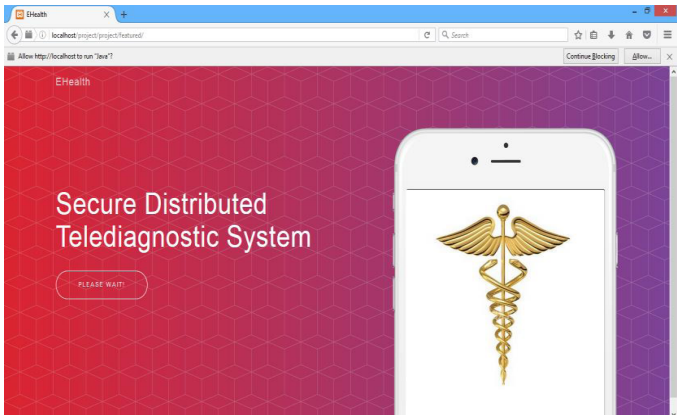


Figure 9 (a) Arduino interfaced with EHR system application (b) System NFC tag interface for modification (see online version for colours)



(a)



(b)

Figure 10 Encryption and decryption stage for authentication

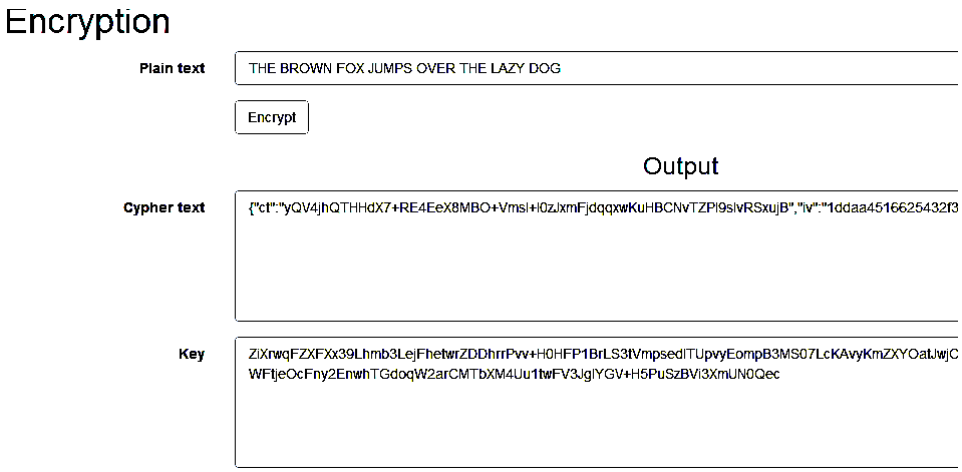
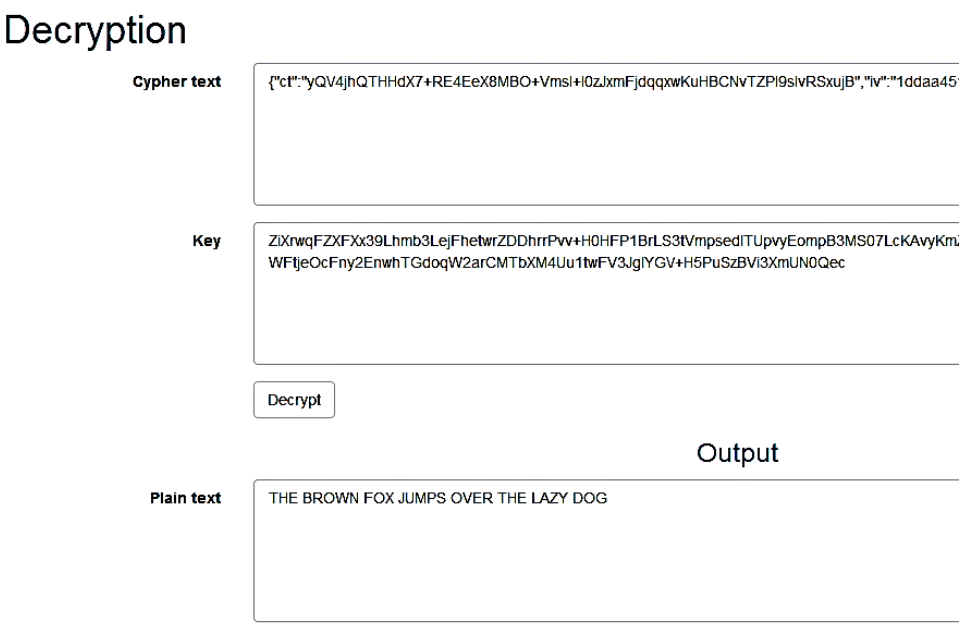


Figure 10 Encryption and decryption stage for authentication (continued)



4.2 Performance evaluation of the developed eTEA

The developed eTEA was tested for its security strength using two important performance analysis criteria developed for block cipher algorithms; Avalanche effect and completeness tests. Applying a suitable algorithm to a specific area of application requires proper knowledge of its limitation and strength. Subsequently, the performance evaluation of the developed algorithms, keeping in mind its strength and weakness.

4.2.1 Avalanche effect of the developed eTEA

A required assessment for all encryption algorithm is that a little variation in the key or plaintext should generate substantial variation in cipher text (Abdelhalim et al., 2012). Nevertheless, a variation in one bit of key or plaintext should generate a significant change in nearly all the bits of cipher texts. This desired property is termed avalanche effect. This can be computed from equation (3):

$$Avalanche\ effect = \frac{Number\ of\ \ filled\ bits\ in\ cypheredtext}{Number\ of\ \ bits\ in\ cypered\ text} \tag{3}$$

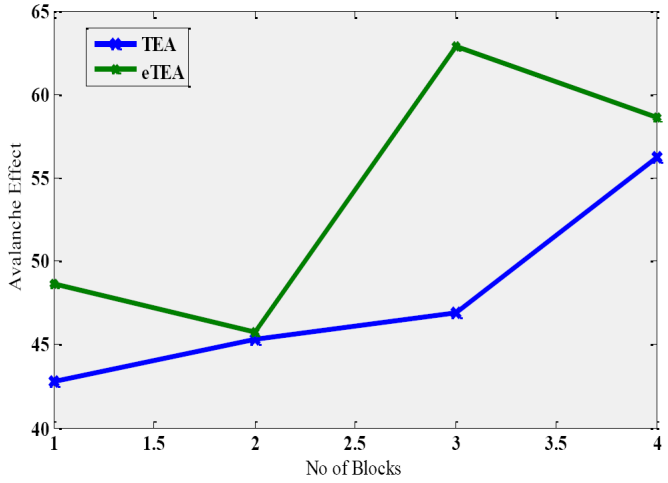
Avalanche effect performance was carried out by encrypting 4 plaintexts that results in 4 cipher texts; this same 4 plaintexts were encrypted again with a bit difference in the plaintext used in previous test. Each two generated cipher texts resulting from the different plaintext with a bit difference were XORed. The number of ones from this XORing was computed and percentage average of each result was obtained. Finally, the percentage average for all 4 results was calculated in other to properly evaluate the

avalanche effect of the algorithm when the input/key was changed slightly, the output changed significantly. This test was done for the standard TEA and enhanced TEA. The results are shown in Table 2. The result shown in Table 2 implies that, for every plaintext that's been encrypted, the probability of bit reoccurrence in the cypher text is very low as compared to the traditional TEA. For example, in block 4, avalanche effect for TEA was recorded 56.25 and 58.75 for eTEA, with a margin of 2.05, this implies that there's 0.02 probability reoccurrence of bits in the TEA compared to the eTEA. Figure 11 is a plot of the avalanche effect of eTEA as compared with the traditional TEA. The graph shows a considerable difference in margin when the effect is rendered. In other words, proves a greater strength.

Table 2 Avalanche effect results of the developed eTEA

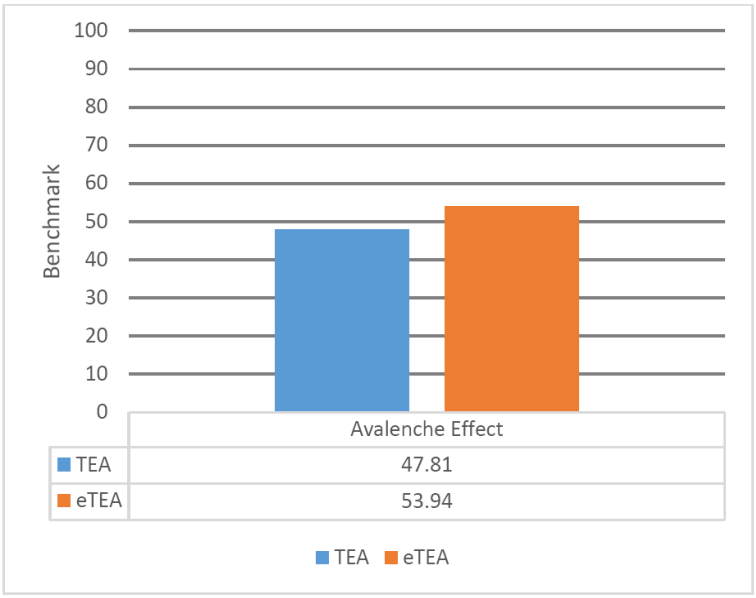
Block #	*TEA*	*Enhanced TEA*	*Difference margin*
1	42.81	48.61	5.80
2	45.31	45.71	0.4
3	46.87	62.85	15.98
4	56.25	58.57	2.32
Ave total	47.81	53.94	6.13

Figure 11 Avalanche effect of eTEA when compared to TEA (see online version for colours)



A graph of avalanche effect was plotted for different blocks as in Figure 11. The experimental results show no instance of lower avalanche effect on the cipher text created by the enhanced TEA as compared to the traditional TEA. The least margin recorded for four different blocks was 0.4 and the highest was 15.98. It can be inferred that, as multiple encryptions are being encountered, all instances of the generated cipher text prove to be stronger than the traditional TEA. Figure 12 goes further to differentiate and create the benchmark of the developed algorithm to the traditional algorithm. It can be seen that the developed algorithm clearly crossed the 50% average mark for an avalanche effect process.

Figure 12 Benchmarking avalanche effect of eTEA and TEA (see online version for colours)



4.2.2 Completeness test of the developed eTEA

Performance for completeness test was carried out using a matrix of (8 × 9) elements with 72 ciphered text of length 64 bits, each plaintext differed from the next by only a bit, after which they were encrypted and its output – cipher text – were XORed with previous output from the previous plaintext. Finally, the results were entered in a matrix format. The number of generated ones were added and the percentage average value of was taken, this determined how the algorithm achieved percentage of completeness that each bit of the cipher text needs to depend on many bits on the plaintext, using the equation in (4)–(6). This test was performed for the standard TEA as well as enhanced TEA. The results are shown in Table 3.

1	0	1	0	1	1	0	1		1	0	1	0	0	1	0	1	0	1
0	1	0	1	0	1	1	0		0	1	1	0	1	0	0	1	0	1
0	1	0	0	1	0	1	1		1	0	1	1	0	1	1	0	1	0
1	0	1	1	0	0	1	1		0	1	0	0	1	0	1	0	0	1
0	0	1	0	0	1	0	1		0	0	1	0	0	1	0	1	0	1
1	1	0	0	1	0	1	0		1	0	0	1	0	0	1	0	1	0
0	0	1	1	1	0	1	0		0	1	0	1	1	0	1	0	1	0
1	0	0	1	0	1	1	0											
0	0	1	1	0	1	0	1											

Matrix A Matrix B

let

X Number of 1 s in the matrix.

X' Number of 0 s in the matrix.

Y Total number of 1 s and 0 s in the matrix.

Z Probability of X.

Z' Probability of X'.

J Probability of 1 s and 0 s

$$J = \frac{Y}{X + X'} \tag{4}$$

$$Z = \frac{X}{Y} \tag{5}$$

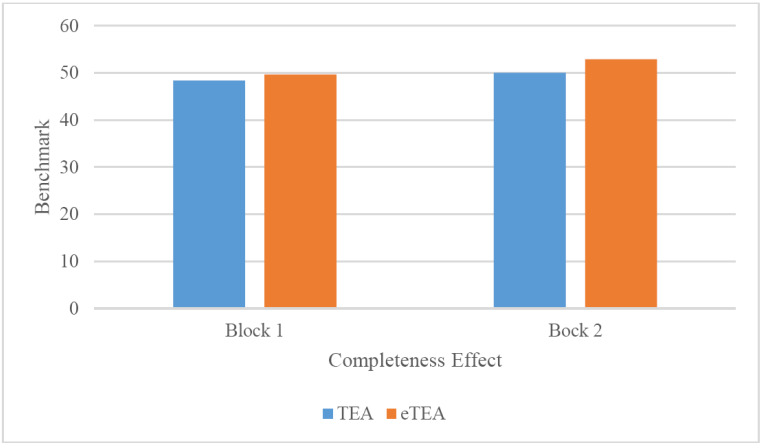
$$Z' = \frac{X}{Y'} \tag{6}$$

Table 3 Completeness test evaluation of the developed eTEA

	TEA	*Enhanced TEA*
Matrix A	0.4836	$Z' = 0.5004$
Matrix B	0.4964	$Z' = 0.5291$

As defined in equation (4)–(6), X represents number of 1 s that will appear in the matrix and X' represents number of 0 s. After computing Z' as the probability of X'. A value of 0.5004 was gotten from Matrix A, implying that there's more than 50% probability when comparing the first and the second cypher text as clearly shown in Figure 13. This proves the completeness effect of an algorithm.

Figure 13 Benchmarking completeness effect eTEA and TEA (see online version for colours)



4.3 Simulation results

Table 4 represents the simulation analysis for different data sizes represented in text format and equivalent encryption time for the developed enhanced TEA. Also, the corresponding CPU utilisation and memory usage of the developed algorithm were also recorded. The simulated result reveals that the execution time for the developed enhanced TEA is shorter when compared to the traditional TEA. Figure 14 denotes the execution time for different text data sizes for eTEA. Execution time was used to compute throughput of the encryption system in Figure 15. From Figure 15, it can be clearly inferred that the speed of execution produced a better throughput when comparing the developed algorithm to the traditional algorithm. Furthermore, this indicates that as the throughput increases, the rate of power consumption of the developed encryption performance increases. The throughput further explains that the encryption speed of the developed eTEA is faster and better than the traditional TEA.

Table 4 Simulation analysis for the developed eTEA

Data size (KB)	*Encryption time (milliseconds)*	*CPU utilisation (%)*	*Memory (KB/sec)*
11	50	0.3	22
17	68	0.4	25
22	80	0.7	27.5
58	94	2.0	61.7
Average time (milliseconds)	73		
Throughput (KB/sec)	36.99		

Figure 14 Encryption time for different data sizes when using eTEA and TEA (see online version for colours)

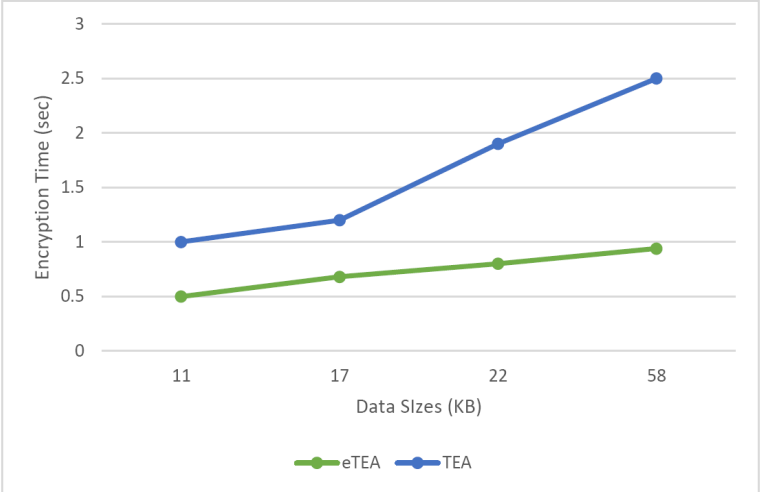


Figure 15 Encryption throughput of eTEA and TEA (see online version for colours)

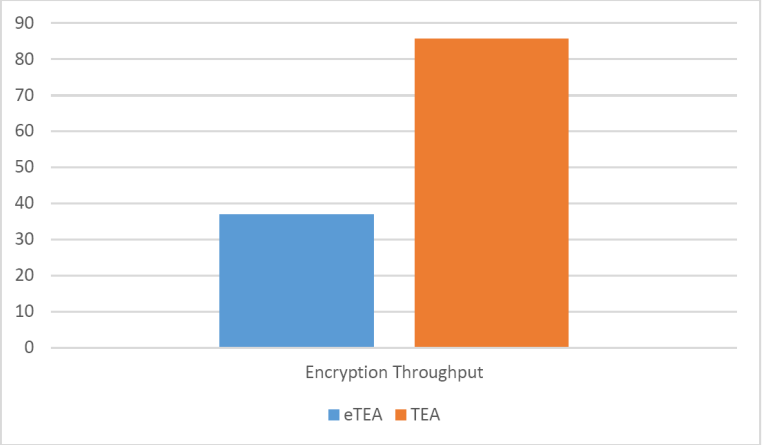


Table 5 Simulation analysis for the traditional TEA

Data size (KB)	*Encryption time (milliseconds)*	*CPU utilisation (%)*	*Memory(KB/sec)*
11	100	1.2	11
17	120	1.7	14.17
22	190	2.9	11.58
58	250	5.4	23.2
Average time (milliseconds)	315		
Throughput (KB/sec)	85.71		

Figure 16 Memory usage of eTEA and TEA (see online version for colours)

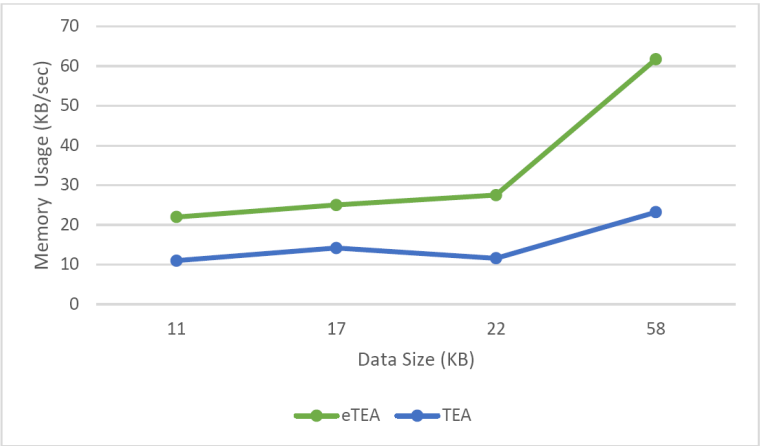


Table 5 represents the simulation analysis for different data sizes represented in text format and equivalent encryption time for the traditional TEA. Also, the corresponding CPU utilisation and memory usage of the developed algorithm were also recorded. The simulated result reveals that the execution time for the developed enhanced TEA is shorter when compared to the traditional TEA. Figure 16 represents the memory consumption rate of the developed eTEA and TEA. It can also be clearly inferred that the memory consumption of the traditional TEA is greater and the transfer rate in KB/sec is slower.

5 Conclusions and plan for future research endeavour

The development of an eTEA to secure patient authentication was successfully designed around NFC environment. The TEA is appropriate for lightweight cryptographic algorithm utilised in secured embedded systems like NFC and RFID systems. The TEA is a Feistel structure utilised to soothe the diffusion and confusion properties in other to appropriately hide statistical data. Conversely, TEA proves to be weak in terms of key generation, key scheduling and related-key attacks. therefore, an enhanced TEA algorithm was designed to overcome the security weaknesses of the TEA algorithm. The eTEA proves to be stronger when tested with the avalanche effect, an average of 53.94 was recorded for the enhanced TEA and 47.81 for the traditional TEA, in which the enhanced TEA proves to be stronger. Completeness test was also performed on the two algorithm, a margin of 0.0168 and 0.0327 was recorded between the eTEA and TEA, implying that the eTEA proves to be stronger for addressing issues of privacy and eavesdropping attack in tele-consultation.

In future, efforts to create electromagnetic induction jamming of signals for illegitimate tags shall be intensified upon as open issue. Since Yarrow algorithm independently defends cryptanalytic attack, but lacks proper strength to entropy generation, efforts would also be made to increase the strength, by properly managing generated entropy.

References

Abdelhalim, M., El-Mahallawy, M., Ayyad, M. and Elhennawy, A. (2012) 'Design and implementation of an encryption algorithm for use in RFID system', *International Journal of RFID Security and Cryptography (IJRFIDSC)*, Vol. 1, Nos. 1/2, pp.15–22.

Aboelfotoh, M.H., Martin, P. and Hassanein, H.S. (2014) 'A mobile-based architecture for integrating personal health record data', Paper presented at *2014 IEEE 16th International Conference the e-Health Networking, Applications and Services (Healthcom)*.

Acharya, D. et al. (2011) 'Security in pervasive healthcare networks: current R&D and future challenges', Paper presented at the *11th International Conference on Mobile Data Management*.

Alizadeh, M., Shayan, J., Zamani, M. and Khodadadi, T. (2012) 'Code analysis of lightweight encryption algorithms using in RFID systems to improve cipher performance', Paper presented at the *2012 IEEE Conference Open Systems (ICOS)*.

Blobel, B. (2004) 'Authorisation and access control for electronic health record systems', *International Journal of Medical Informatics*, Vol. 73, No. 3, pp.251–257.

Chao, W.C., Hu, H., Ung, C.O.L. and Cai, Y. (2013) 'Benefits and challenges of electronic health record system on stakeholders: a qualitative study of outpatient physicians', *Journal of Medical Systems*, Vol. 37, No. 4, pp.1–6.

Devendran, A., Jayam, R. and Sindhuja, P. (2015) 'Electronic medical records using NFC technology', *ARPN Journals*, Vol. 10, No. 3, pp.3–15.

Dunnebeil, S., Kobler, F., Koene, P., Leimeister, J.M. and Krcmar, H. (2011) 'Encrypted NFC emergency tags based on the German telematics infrastructure', Paper presented at the *2011 3rd International Workshop Near Field Communication (NFC)*.

Ebrahim, M., Khan, S. and Khalid, U.B. (2014) *Symmetric Algorithm Survey: A Comparative Analysis*, arXiv preprint arXiv: 1405.0398.

Ertl, J., Plos, T., Feldhofer, M., Felber, N. and Henzen, L. (2013) 'A security-enhanced UHF RFID tag chip', Paper presented at the *2013 Euromicro Conference Digital System Design (DSD)*.

Femi, E., Temitope, O., Foluso, A., Vekima, N., Carole, D. and Victor, M. (2017) 'Telemedicine diffusion in a developing country: a case of Nigeria', *Science Journal of Public Health*, Vol. 5, No. 4, pp.341–346, DOI: 10.11648/j.sjph.20170504.20.

Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O. and Toval, A. (2013) 'Security and privacy in electronic health records: a systematic literature review', *Journal of Biomedical Informatics*, Vol. 46, No. 3, pp.541–562.

Hameed, S., Hameed, B., Hussain, S.A. and Khalid, W. (2014) 'Lightweight security middleware to detect malicious content in NFC tags or smart posters', Paper presented at the *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*.

Hameed, S., Jamali, U.M. and Samad, A. (2015) 'Integrity protection of NDEF message with flexible and enhanced NFC signature records', in *Trustcom/BigDataSE/ISPA*, IEEE, Vol. 1, pp.368–375.

Hameed, S., Jamali, U.M. and Samad, A. (2016) 'Protecting NFC data exchange against eavesdropping with encryption record type definition', in *Network Operations and Management Symposium (NOMS)*, IEEE/IFIP, pp.577–583.

Huang, C-H. and Huang S-C. (2013) 'RFID systems integrated OTP security authentication design', Paper presented at the *2013 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*.

Jeddi, Z., Amini, E. and Bayoumi, M. (2013) 'A novel authenticated encryption algorithm for RFID systems', Paper presented at the *2013 Euromicro Conference Digital System Design (DSD)*.

Kartik, B., Bhargav, J., Mahajan, M. and Rathod, S. (2015) 'Near field communication based android API healthcare system', *Multidisciplinary Journal of Research in Engineering and Technology*, Vol. 2, No. 4, pp.681–686.

Kinoshita, S., Ohkubo, M., Hoshino, F., Morohashi, G., Shionoiri, O. and Kanai, A. (2005) 'Privacy enhanced active RFID tag', *Cognitive Science*, Research Paper-University of Sussex CSRP, Vol. 577, p.100.

Malin, B.A., El Emam, K. and O'Keefe, C.M. (2013) 'Biomedical data privacy: problems, perspectives, and recent advances', *Journal of the American Medical Informatics Association*, Vol. 20, No. 1, pp.2–6.

Mars, M. (2013) 'Telemedicine and advances in urban and rural healthcare delivery in Africa', *Progress in Cardiovascular Diseases*, Vol. 56, No. 3, pp.326–335.

Neubauer, T. and Heurix, J. (2011) 'A methodology for the pseudonymization of medical data', *International Journal of Medical Informatics*, Vol. 80, No. 3, pp.190–204.

Olaniyi, O.M., Arulogun, O.T., Omotosho, A. and Onuh, O.V. (2017) 'Securing clinic tele-diagnostic system using enhanced tiny encrypted radio frequency identification and image steganographic technique', *International Journal of Telemedicine and Clinical Practice (IJTMCP)*, Vol. 2, No. 3, pp.242–266, DOI: 10.1504/IJTMCP.2017.10008683.

Özcanhan, M.H., Dalkılıç, G. and Utku, S. (2014) 'Cryptographically supported NFC tags in medication for better inpatient safety', *Journal of Medical Systems*, Vol. 38, No. 8, pp.1–15.

Pirrone, J. and Huerta, M. (2015) 'Hippocratic protocol design to improve security and privacy in healthcare applications for NFC smartphone', Paper presented at the *World Congress on Medical Physics and Biomedical Engineering*, 7–12 June, Toronto, Canada.

Razmi, N.N.K. and Sangar, A.B. (2016) 'The use of NFC technology to record medical information in order to improve the quality of medical and treatment services', *Modern Applied Science*, Vol. 10, No. 6, pp.136–142.

Saeed, M.Q. and Walter, C.D. (2012) 'Off-line NFC tag authentication', Paper presented at the *International Conference for Internet Technology and Secured Transactions*.

Saito, J., Ryou, J-C. and Sakurai, K. (2004) 'Enhancing privacy of universal re-encryption scheme for RFID tags', Paper presented at the *International Conference on Embedded and Ubiquitous Computing*.

Wamala, D.S. and Augustine, K. (2016) 'A meta-analysis of telemedicine success in Africa', *JPatholInform* [online] http://www.jpathinformatics.org/text.asp?2013/4/1/6/112686.