IoT-based Efficient Tamper Detection Mechanism for Healthcare Application

Ahmed A. Elngar
(Corresponding author: Ahmed A. Elngar)
Faculty of Computer and Information, Beni-Suef University, Egypt
62511, Beni Suef, Salah Salem Str., Egypt
(Email: elngar_7@yahoo.co.uk)
(Received Apr. 28, 2017; revised and accepted Aug. 26 & Sept. 2, 2017)

Abstract

Security of networks is the most important challenge of the Internet of Things (IoT) that need smarter security mechanisms. Therefore, a tamper detection (TD) is an efficient security mechanism based on networks of IoT for healthcare applications, which used to deal with security violations. In this paper, a new TD mechanism based IoT for real data of healthcare application called (IOT-TD) model has been proposed. This paper effectively proposed (ANN-GA) tamper detection mechanism. Where, Genetic Algorithm (GA) is used to optimize weight and bias values of artificial neural networks (ANN) which lead to maximize the ANN detection accuracy, minimize the timing detection and efficiency energy saving. The experimental results showed that the tamper detection performance of (ANN-GA) is 98.51%. In addition, the proposed model showed that the (ANN-GA) enhances the timing to 0.03 sec which is important for real time of (IOT-TD) model healthcare application and the efficiency energy saving transmission is 1980 times better than full transmission. Also, the proposed Model relies on the certificate-based DTLS handshake protocol as it is the main security for (IoT-TD) model.

Keywords: Artificial Neural Network; Genetic Algorithm; Healthcare Applications; Internet of Things; Tamper Detection

1 Introduction

Nowadays, IoT is becoming one of the hottest research topics. IoT describes the future, where every day physical objects will connect to the Internet and be able to identify themselves to each others [19]. Hence, the IOT realizing smart environments such as: smart living, smart home, smart manufacturing, and smart healthcare applications. Due to the spread of chronic diseases and rising the cost of traditional healthcare application around the world; so it urgently demand transform the healthcare from hospital centered systems to remote personal healthcare systems [12]. Sensors, equipments and detectors around us have a significant impact on our everyday activities. Which It is becoming more pervasive for attempting to fulfill end users' need and provide easy of usability, specially in healthcare applications [14]. Therefore, one of the most important challenges of IoT based healthcare is a data security [9]. Where security is a major issue concerned of the most devices and their communications in nature [6]. These devices have a capability to send / receive data between each others using different communication protocols. The communication protocols must allowed low energy consumption and sufficient data security. Therefore, communication protocols are very important to secure the networks of IoT [17]. Hence, different types of communication protocols such as $CoAP$, $IEEE$ 802.15.4, $ZigBee$, $6LOWPAN$ and $Ethernet$ are used [13, 15]. The following Figure 1 shows some of security and management protocols for IoT.

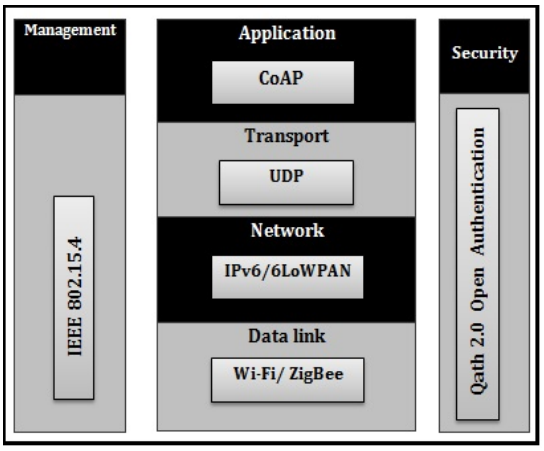

Figure 1: The framework protocols for IoT based healthcare

The main objective of internet of things based healthcare application is enhancing the interaction of device-to-

device, as well as the interaction of device-to-human via Internet. [14]. Although the collected data from harmless wearable sensors, such data is vulnerable to top privacy concerns. Where as the networks of IoT is secured based encryption and authentication mechanisms, but it so vulnerable against cyber-attacks [18]. So, this paper aims to secure data for digital communication in healthcare application [9, 21].

This paper, present a secure and efficient model for IoT-based healthcare using TD mechanism that monitor the malicious traffic in IOT-networks. Which it can defend the IOT-networks from intruders [1]. Intrusions are malicious activities that harmful to sensor nodes. Therefore, tTD can be used to inspect and investigate devices, user actions, and identifies the malicious activities for IOT-networks [11]. The TD works as IOT-networks observer, which avoids the damage of data by generating an alert before the attackers begin to attack. Also, TD can detect both external and internal attacks. An external attacks are launched by third party who is initiated by outside IOT-networks, whereas internal attacks are launched by nodes that belong to the IoT-networks.

There are mainly three components of TD: monitoring, detection and alarm [10]. The monitoring component monitors the network traffics, patterns and resources, detection is a core component of TD which detects the intrusions according to specified algorithm and alarm component raised an alarm if intrusion is detected [10].

In this paper, $IOT-TD$ model employs the ANN which have been used to solve classification problems. The performance of a ANN depends directly on the design of the hidden layers, and in the calculation of the weights that connect the different nodes [20]. In order to obtain a feasible results, the weights of ANN are calculated using a GA [4]. The GA is a meta-heuristic algorithm based on the concept of evolution processes. So, from all the search spaces of possible weights, the GA will generate new points of possible solutions to ANN.

Also, this paper employs $DTLS$ handshake protocol as it is a main security solution for the $IoT-TD$ model. To the best of our knowledge, $IoT-TD$ model is the first effort for proposing a secure and efficient model for IoT-based healthcare application using $(ANN-GA)\,TD$ mechanism. The elaboration of proposed model from the viewpoint of security as well as performance analysis is conducted. Also, the results reveal that the proposed $IOT-TD$ model based healthcare application increases the detection accuracy, speed up the detection time and the efficiency of energy saving compared to other well-known approaches.

Table 1 is the nomenclature of the paper.

The rest of this paper is organized as follows: Section 2 gives a literature survey. Section 3 presents a concept of the tamper detection mechanism. Section 4 gives the problem formulation. Section 5 introduces the proposed $IOT-TD$ model for healthcare application. Section 6 gives the implementation results and analysis. Finally, Section 7 contains the conclusion remarks.

Table 1: Nomenclature

IOT	Internet of Things
TD	Tamper Detection
ANN	Artificial Neural Network
GA	Genetic Algorithm
$DTLS$	Datagram Transport Layer Security
IDS	Intrusion Detection System
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
$COAP$	Constrained Application Protocol

2 Literature Survey

The IOT performs the complicated functions in a simple way, which lead to structure more intelligent environments to make it a safe places for live in. Many researchers have been working on IoT-based healthcare applications and wireless sensor areas to provide the best mechanisms for data security. This section describes a variant contributions which are proposed in recent years.

Jun in [7] proposes event processing based IDS. Which solves the problem of real time of IDS in IoT-networks. Authors claimed a design of IDS approach based on the basis of Event Processing Model EPM. It is rule-based IDS in which rules are stored in Rule Pattern Repository and takes SQL and EPL of Epser as a reference. According to the results, this proposed consumed more CPU resources, less memory and took less processing time than traditional IDS for IoT-networks.

Alsadhan in [2] proposed an optimized IDS for IoT-networks using soft computing mechanisms. The objective of this proposed is increasing the performance of the system and identify each activities in a robust way. Where authors implemented the soft computing mechanisms like PCA, PSO and Greedy Search in IDS. In this proposed, the number of features are reduced with increasing of detection rate.

In [5], is proposed an IoT-based health monitoring system architecture which uses star-based $6LoWPAN$ motes that are integrated with an AFE device. The system uses a gateway which collects the data from the motes and transmits them to server, so they can provide many services for the connectivity conservation and the reinforcement of the system.

In [8], Kasinathan proposed IoT-networks based DoS detection IDS architecture within the EU FP7 project ebbits network framework. In this approach, IDS can listen or monitor $6LoWPAN$ traffic by using IDS probe. They used hybrid approach for placement of IDS. DoS protection manager is core component of proposed system which raised an alert by using information available on network manager component.

3 Tamper Detection Mechanism (TD)

TD mechanism is an ability of a device to sense with an active attempt which compromised the device or the data associated with that device. Hence, it enables this device to start appropriate defensive actions against any attacks [22]. The methods used for TD are typically designed as a suite of sensors each specialized for a single threat type. Also, TD mechanism enables the device to be aware of tampering and typically fall into one of three groups:

- **Switches**: to detect the opening of a device.
- **Sensors**: to detect environmental changes, voltage and power sensors to detect glitch attacks.
- **Circuitry**: to detect drilling or penetrating the device boundary.

The idea behind of a TD mechanism is to be a sensitive enough to detect the presence of a tangible threats. Also, it be able to distinguish from "false alarms" situations. There are several methods for applying TD mechanism; such as ANN and $C4.5$ methods [16].

4 Problem Formulation

Let z_t be set of patient sensors values acquired at time t.

$$z_t(a) = D_t[b_t](a),\ \forall\ a\ \in A \tag{1}$$

Where, D_t denoted as an operator transforming the original record b_t, and $a \in z^2$ indicates the sensors values that belonging to the regular record $A \subset z^2$. As far as there are no tampering attacks/events.

$$D_t[b_t](a) = b_t(a) + \eta_t(a),\ \forall\ a\ \in A \tag{2}$$

Where, η_t is a random variable accounting for record noise values, and b_t are acquired from the same sensor even though typically $b_t \neq b_t - 1$; because values of patient record are changed.

When, at time τ^* an external disturbance introduces a tampering, the record b_t is degraded by an unknown tamper attack and z_t becomes:

$$D_t[b_t](a) = \int b(e)h_t(a,j)d_j + \eta_t(a),\ \forall\ a\ \in A, t \succeq \tau^* \tag{3}$$

Where, $h_t(a,j)$ is the value-spread function at value $a \in A$.

The proposed $ANN - GA\ TD$ mechanism analyzes a sequence of $\{z_t, t = 1, ...,\ number\ of\ sensors\}$ to detect the time instant τ^* when tampering like 3 occur. We assume that T_0 tampering-free values are provided for training.

5 The Proposed $IOT - TD$ Model for Healthcare Application

This section contains the description for the proposed model $IOT - TD$. So, the main aim of the proposed model is to detect the tampering and ensure authentication of the biomedical information in IoT based healthcare application. Our proposed model designed to detect a huge types of attacks, which compromise the security of the biomedical information. These attacks such as: imitating and alteration. In which intruder can interfere and send an altered data that causes the tampering, bugging, and interruption of the biomedical information. The proposed model have a combination of IoT technologies, and communication protocols to design an efficient healthcare application.

5.1 Model Architecture

The architecture of the proposed $IOT - TD$ model shown in Figure 2 consists of three main modules: the digital environment module, local data processing environment module and remote doctor workstation module.

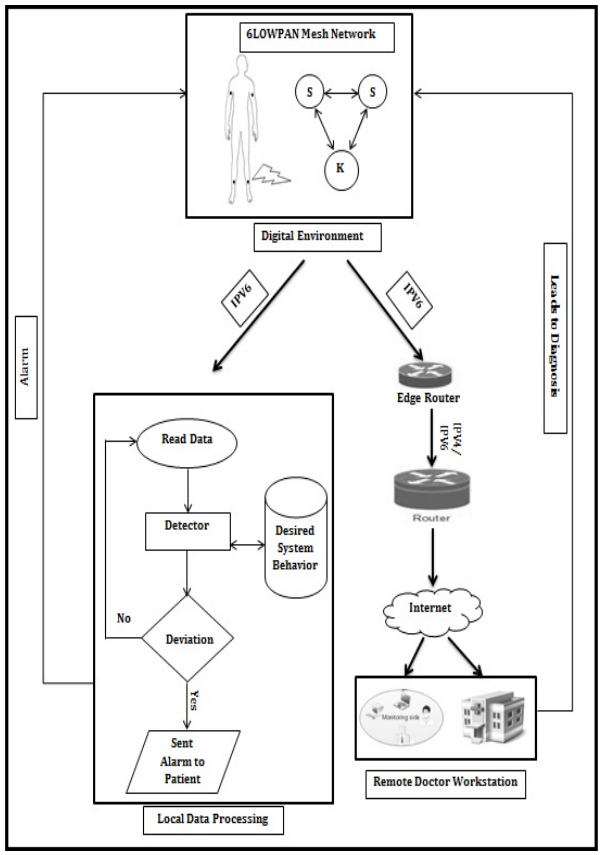

Figure 2: Structure $IOT - TD$ for healthcare model

5.1.1 Digital Environment Module

The digital environment module represented by the Arduino UNO Board and some medical sensors such as: Body temperature sensor, and pulse sensor, etc., which measure some variables, such as: blood pressure, temperature, and heart rate, etc.. Then the values will gathered to create a database as shown in Figure 3.

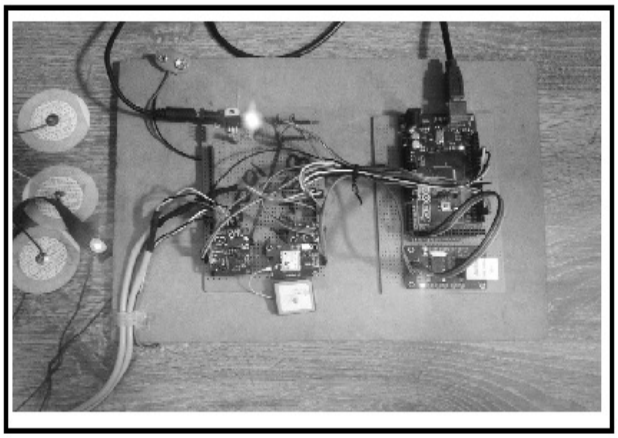

Figure 3: $IOT - TD$ hardware architecture

5.1.2 Local Data Processing Module

The local data processing module which consists of the TD component. Which it will receive the data (i.e., temperature, etc.) transmitted from user monitoring sensors in real-time. Then will be analyzing these values using $ANN - GA$ TD mechanism and compared it with the normal values of same patient. Where, ANN composed of digital nodes explained in subsection 5.1.1 module (equivalent to neurons of a human brain) which are interconnected by weighted links (equivalent to synapses between neurons) as shown in Figure 4.

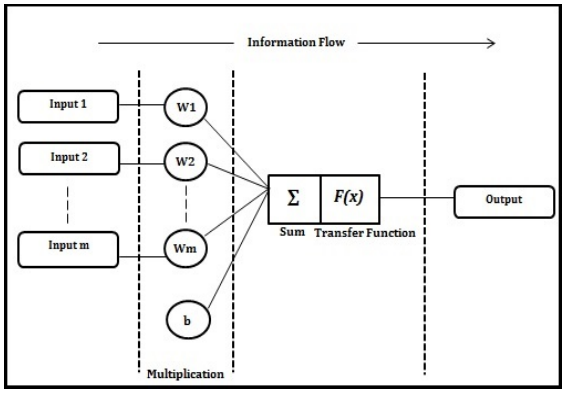

Figure 4: Design of ANN-GA

Hence, the outcome of the ANN is altered by changes of the weights of links. So, the weights of the ANN are calculated using GA approach. Such that from all the search hypothesis space of all the possible weights, the GA will generate new points of the possible solutions. Therefore, The mathematical description of $ANN - GA$ as follows:

$$Y_i = F(\Sigma_{i=0}^{m} W_i \times X_i + b) \quad (4)$$

Where,

- X_i: is input variable associated with each node.
- W_i: is connections' weights between inputs x_i estimated by GA.
- b: is the bias of the node.
- F: is the transfer function.
- Y_i: is the desired output of ANN.

If the output of $ANN - GA$ within the normal range; which indicates that the patient values observed is normal, then the data processing module will continue read the data from patient' medical sensors. While, if these values are not within the normal range; it indicating that the user's values monitor is abnormal, then the TD will send a reminder of warning to the patient.

5.1.3 Remote Doctor Workstation Module

Also, the remote doctor workstation module consists of the same TD mechanism component which observe the data for patient medical sensors in the real-time , then set up a personal database for each patient. Hence, TD will send an alert to patients when sense with abnormal values at any time then gives disposal proposals.

5.2 Model Topology

In this section, we focuses on the topology of the connections between the sensors and the actuators; which all nodes are connected to each other by links. In which it can used to communicate for the data and the signals transferring. The proposed model' network is consisting of $IEEE$802.15.4 which used in the physical layer. So, it can provide a wireless communications, where the bits of data after they have been converted into signals can be transmitted and received. Moreover, in the data link layer, 6$LoWPAN$ is used as (adaptation layer) where; the adjustment from $IPv6$ to $IEEE$ 802.15.4 is done. In the addressing and routing of data the Internet Protocol IP is used. So, we assign to every node a unique $IPv6$ address. The next layer is a transport layer, where UDP is used for the carriage of the data. The UDP is supplying lower latency and it is faster than TCP. The application layer is last layer, where it uses the $CoAP$. The proposed model' network also connects to other networks via $Wi - Fi$.

The notations used throughout this work which describes the proposed model shown in Table 2.

Suppose that the proposed network involves a set of sensors $\{S_1, S_2, ..., S_n\}$ and set of actuators

Table 2: Notations

Notation	Description
S_n	Total set of sensors
K_m	Total set of actuators
L_{node}	total set of links
S_{data}	Total sensor data
K_{sig}	Total actuator signals
P_{loss}	packet/signal loss
D_{rec}	Total data received
D_{sent}	Total data sent
N_{nf}	Number of nodes fails to transmit
A_{nodes}	Number of nodes succeeded

$\{K_1, K_2, ..., K_m\}$ which connected with each other. This situation is described by the two equations below:

$$(S_n + K_m) - N_{nf} = A_{nodes} \quad (5)$$

$$(S_{data} + K_{sig}) - P_{loss} = D_{sent} \quad (6)$$

The proposed model used the duplex mesh communications, which means if nodes failed to transmit data/signal; it doesn't affect the transmission from other nodes. This is shown below:

$$[(S_n + K_m) \times \frac{(S_n + K_m - 1)}{2}] = L_{nodes} \quad (7)$$

6 Implementation Results and Security Analysis

The proposed $IOT - TD$ model is evaluated for the 36 normal and 36 abnormal patients. All experiments have been performed using Intel Core i3 2.13 GHz processor with 2 GB of RAM. The experiments have been implemented using Java language environment with C, Eclipse, Cloud Interface Linux Operating System 64-bit, and Windows Operating System 64-bit.

6.1 Performance Measurements

The detection effectiveness of the proposed $IOT - TD$ model is measured in term of TP Rate, FP Rate and $F - measure$; which are calculated based on the confusion matrix (CM). The CM is square matrix where columns correspond to the predicted class, whereas, rows correspond to the real classes. Table 3 presents the CM, which shows the four possible prediction outcomes. Here,

True negatives (TN): indicates the number of normal events are successfully labeled as normal.

False positives (FP): refer to the number of normal events being predicted as abnormal.

False negatives (FN): The number of abnormal events are incorrectly predicted as normal.

True positives (TP): The number of abnormal events are correctly predicted as abnormal.

$$TPRate = \frac{TP}{TP + FN}$$

$$FPRate = \frac{FP}{FP + TN}$$

$$F - measure = \frac{2 * TP}{(2 * TP) + FP + FN}.$$

Table 3: Confusion matrix

	Predicted Class	
Real Class	Normal	Abnormal
Normal	TN	FP
Abnormal	FN	TP

6.2 Experiment Results

The detection performance measurements by $ANN - GA$ TD are shown in Tables 4 and 5. Table 4 shows the accuracy measurements achieved for $C4.5$ method. While, Table 5 gives the accuracy measurements of $ANN - GA$ TD for the proposed $IOT - TD$ model.

Table 4: C4.5 tamper detection

Class name	TP Rate	FP Rate	F-Measure
Normal	0.793	0.267	0.791
Abnormal	0.733	0.207	0.736

Table 5: $ANN - GA$ tamper detection

Class name	TP Rate	FP Rate	F-Measure
Normal	1	0.033	0.987
Abnormal	0.967	0.0	0.983

From Tables 4 and 5, it is clear that the detection accuracy achieved using $ANN - GA$ as TD method is better than using $C4.5$.

Table 6 compares the TD accuracy and timing speed of $C4.5$ and proposed $ANN - GA$. Table 6 illustrate that the propose gives better detection performance (98.51%) than the $C4.5$.

Also, the proposed enhances the timing speed to 0.03 sec which is important for real time $IOT - TD$ model in healthcare application.

The performance comparison of the proposed model over two other approaches based on several features are listed in Table 7.

6.3 Energy-Saving Transmission Efficiency Analysis

The nodes in the $IoT - TD$ base healthcare application are usually battery energy hence; energy is a scarce re-

Table 6: Testing accuracy and timing comparison

System	Test accuracy	Model building Time
IOT-C4.5	76.66%	0.06 sec.
Proposed IOT-ANN-GA	98.51%	0.03 sec.

Table 7: Comparative analysis between the proposed model and other approaches

Feature	[3]	[5]	Proposed
IoT-based	✓	✓	✓
TD-based	×	×	✓
Coap	×	×	✓
Topology	Star	Mesh	Full Duplex Mesh
Security	Basic	AES Block	AES-128, DTLS, WPA2
Energy Efficiency	×	✓	✓
802.15.4	×	✓	✓
Scalability	High	Low	High
Adaptability	High	High	High

source. Here, this paper compared the transmission efficiency every 5-minutes according to different abnormal patient ratios with "full transmission" and "energy-saving transmission". In the energy-saving transmission mode, data is transmitted to the remote doctor workstation module in a 32- byte package at a 5-minute interval. In the full transmission mode, data is transmitted continuously at a 1-second interval. In total, the size of continuous data transmitted over 5-minutes is 57,652 bytes ($12\ bits * 128/sec * 300s + 20\ bytes\ of\ package\ field + 32\ bytes\ of\ ANN - GA\ result$). A twenty-four hour of data-set is emulated using 288 every five-minute data sets. The normal ratio is defined as the percentage of normal $ANN-GA$ results analyzed by the multi-pattern abnormal disease matching in the remote doctor workstation module. Once the $ANN - GA$ parameters are transmitted to the remote doctor workstation module, they are analyzed to decide whether to transmit the raw data. For instance, if the normal ratio is 80%, the twenty-four hour energy-saving transmission transmits $288 * 32\ bytes + 57652\ bytes * 288 * (1 - 80\%) = 3.176\ Mb$, and the efficacy is $15.84\ Mb/3.176Mb = 4.99$. Suppose that 100% normal patterns can be detected from the patients; the transmission efficiency is then 1980 times. It is useful when analysis a huge amount of data such in healthcare application as shown in Table 8.

6.4 Security Analysis

The security of the proposed model "$IoT - TD$" is an important issue for healthcare application. Where as the healthcare information is very sensitive and the internet will never be safe. So, this section is going to discuss the security architecture of the proposed model in each layer.

This paper propose $(ANN - GA)\ TD$ efficient mechanism at both local data processing and remote doctor workstation. Where, GA with ANN will produce a hybrid neural network. So, the weights of ANN are calculated using GA algorithm. From all possible weights of search space, the GA will generate new points of possible solutions. Which implies that, it possible to optimize the ANN by modifying the structure of weights calculation. Hence, $(ANN - GA)\ TD$ mechanism leads to maximize the TD accuracy, minimize the detection timing and efficiency energy saving.

Also, $6LoWPAN$ in data link layer security which is responsible for the encryption and authentication of the links. $6LOWPAN$ provides secure data packets delivery. besides, in the transport layer the proposed model use UDP over $DTLS$ mechanisms that could also be used for $CoAP$ security, in order to save the communications between the objects. Furthermore, the $IEEE$ 802.15.4 standard has many security protocols, such as the $Wi-Fi$ Protected Access $WPA2$ which provides data integrity, confidentiality and authentication.

7 Conclusions

This paper proposed a new $IOT - TD$ model which employs $(ANN - GA)\ TD$ mechanism for secure the sensitive information in healthcare applications. Therefore, $ANN - GA$ can be used to satisfy the security requirements of IoT-networks environment. According to the primary and earlier experiments, the proposed $ANN - GA$ mechanism achieved 98.51% TD rate, which can be considered as the best tamper detection rate compared with the $C4.5$ algorithm which achieved 76.66%. Also, the proposed $ANN-GA$ mechanism enhances the timing detection to 0.03 sec compared with the $C4.5$ algorithm which achieved 0.06 sec and efficiency energy saving which is important for the real-time $IOT - TD$ model of healthcare applications.

Acknowledgments

The author gratefully acknowledge the editor and the anonymous reviewers for their valuable comments.

References

[1] R. Aarthi, A. R. Renold, "Coap based acute parking lot monitoring system using sensor networks," *ICTACT Journal On Communication Technology: Special Issue on Advances In Wireless Sensor Networks*, vol. 5, no. 2, pp. 923–928, 2014.

[2] A. Alsadhan, N. Khan, "A proposed optimized and efficient intrusion detection system for wireless sensor network," *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, vol. 7, no. 12, 2013.

Table 8: Energy-saving transmission efficiency results

Normal ration	0%	20%	40%	60%	80%	100%
Full transmission (Mb/24-hour)	15.84	15.84	15.84	15.84	15.84	15.84
Energy-saving transmission (Mb/24-hour)	15.84	12.67	9.54	6.33	3.176	0.008.
Efficiency (times)	1	1.25	1.66	2.50	4.99	1980

[3] S. R. Anurag, A. M. Rahmani, T. Westerlund, G. Yang, P. Liljeberg, H. Tenhunen, "Pervasive health monitoring based on internet of things: Two case studies," in *EAI 4th International Conference omn Wireless Mobile Communication and Healthcare (Mobihealth'14)*, pp. 275-278, 2014.

[4] A. A. Elngar, D. A. El A. Mohamed, F. M. Ghaleb, "A fast accurate network intrusion detection system," *International Journal of Computer Science and Information Security*, vol. 10, no. 9, Sept. 2012.

[5] T. N. Gia, A. M. Rahmani, T. Westerlund, P. Liljeberg, H. Tenhunen, "Fault tolerant and scalable IoT-based architecture for health monitoring," in *IEEE Sensors Applications Symposium (SAS'15)*, pp. 1-6, 2015.

[6] J. He, C. Hu,, and X. Wang, "A smart device enabled system for autonomous fall detection and alert," *International Journal of Distributed Sensor Networks*, vol. 1, 2016.

[7] C. Jun, C. Chi, "Design of complex event-processing IDS in internet of things," in *IEEE Sixth International Conference on Measuring Technology and Mechatronics Automation*, 2014.

[8] P. Kasinathan, *et al.*, "Denial-of-service detection in 6LoWPAN based internet of things," in *IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'13)*, 2013.

[9] H. Kayarkar, "Classification of various security techniques in databases and their comparative analysis," *ACTA Technica Corviniensis*, vol. 5, pp. 135-138, 2012.

[10] M. Kovatsch, "CoAP for the web of things: From tiny resource-constrained devices to the web browser," in *Proceedings of ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication*, pp. 1495-1504, 2013.

[11] Y. Ma, "NFC communications-based mutual authentication scheme for the internet of things," *International Journal of Network Security*, vol. 19, no. 4, pp. 631-638, 2017.

[12] S. R. Maynard, H. Thapliyal, and A. Caban-Holt, "Smart home system for patients with mild cognitive impairment," in *Proceedings of the 2015 International Conference on Computational Science and Computational Intelligence*, pp. 738-742, 2015.

[13] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based internet of things," *International Journal of Network Security*, vol. 18, no. 3, pp. 459-473, May 2016.

[14] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities," in *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60-70, 2016.

[15] P. Pongle, G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," in *IEEE International Conference on Pervasive Computing (ICPC'15)*, 2015.

[16] J. R. Quinlan, *C4.5 Programs for Machine Learning*, Morgan Kaufmann San Mateo Ca, 1993.

[17] E. Raptopoulou, *CoAP Enabled Sensors for the Internet of Things*, Department of Applied Informatics and Multimedia, Technological Educational Institute of Crete, 2014.

[18] W. L. Tai, Y. F. Chang, "Comments on a secure authentication scheme for IoT and cloud servers," *International Journal of Network Security*, vol. 19, no. 4, pp. 648-651, 2017.

[19] L.M.R. Tarouco, L.M. Bertholdo, L.Z. Granville, and L.M.R. Arbiza, "Internet of things in healthcare: Interoperatibility and security issues," in *IEEE International Conference on Communications*, pp. 621-6125, 2012.

[20] G. Wang, J. Hao, J. Ma and L. Huang , "A new approach to intrusion detection using artificial neural networks and fuzzy clustering," *Expert Systems with Applications*, vol. 37, pp. 6225-6232, 2010.

[21] D. Xu, Z. Wu, Z. Wu, Q. Zhang, L. Qin, J. Zhou, "Internet of things: Hotspot-based discovery service architecture with security mechanism," *International Journal of Network Security*, vol. 17, no. 2, pp. 208-216, 2015.

[22] Y. Ye, Y. He, Y. Wang, "SHVC, the scalable extensions of HEVC and its applications," *ZTE Communications*, vol. 14, no. 1, 2016.

Biography

Ahmed A. Elngar graduated with a B.Sc. in computer Science from computer science Department, Al-Azhar University, Master of computer science in Intrusion Detection System (IDS) from Ain Shanm university. He obtains his P.hD at computer science Department, Al-Azhar University. Also he is a member in Egyptian Mathematical Society (EMS) and International Rough Set Society(IRSS). Now he is a member of Scientific Research Group in Egypt (SRGE). He is Asst. Prof. of computer scienceat Faculty of Computer and Information, Beni-Suef University.