Chapter

Embedded Devices Security Based on ICMetric Technology

Khattab M. Ali Alheeti, Duaa Al_Dosary and Salah Sleibi Al-Rawi

Abstract

An intelligent wheelchair application is required which is equipped with the MEMSs which are magnetometer, gyroscope, and accelerometer sensors. The generated process of ICMetrics number is heavily based on magnetometer, gyroscope, and accelerometer sensors. In addition, this number can be utilised to provide the identification of device. Our proposed system passed through three phases. The first phase is bias reading that was extracted from MEMSs (gyroscope, magnetometer, and accelerometers) sensors; whereas, in the second phase, ICMetric number is generated by using the sensor bias readings that was extracted in the first phase. Therefore, this number is non-stored and can be utilised to provide identification of device. In the third phase, the security system is tested/evaluated to measure its effectivity. In other words, it is tested with dataset that was extracted from the trace file of ns-2. In this phase, performance metrics are calculated, which are rate of error, confused metrics, and accuracy.

Keywords: ICMetric technology, security, intelligent wheelchair, application, MEMSs, magnetometer, gyroscope, accelerometer

1. Introduction

The increasing number of embedded systems is subjected to a growing number of threats as community of the hacker is beginning to exhibit interestingly to these systems. Moreover, the achievement of security is not easy consequent to resources constraints of these devices. In this chapter, we demonstrate the basic concepts of security and explain the role of applying identification in the promotion and development of embedded device security using ICMetric technology.

This chapter presents the following concepts:

- Define the basic concepts of security and attacks.
- Explain embedded devices security.
- Describe ICMetric technology and its phases.
- Describe the type of application and sensors utilised.
- Explain statistical analysis and how ICMetric number can be generated for identification of embedded devices.

- Explain how performance metrics of a system can be evaluated.
- Conclusion.
- Future works.
- References.

2. Security concept

Security aims for achieving the protection of system information in order to preserve the data from manipulation and theft and to attain the availability, confidentiality, and integrity. It includes protection of hardware, software, information, and telecommunications [1].

Security is a term used to describe different states, such as lack of risks and threats situation, prevention of risks, or achieve confidence. Achieving security is required in many areas at the level of individuals and organisations. Ensuring security requires individuals with competence and experience, so the level of security varies from one organisation to another. To ensure better security for organisations and individuals, it is important for network users to use the systematic approach, which involves analysing, designing, implementing, and maintaining a required network security system [2].

There are many goals of security as illustrated below:

- *Authentication*: means verifying the identity of a device or person.
- *Confidentiality*: means preserving the information confidential to prevent unauthorised access to the information. Confidentiality loss of information means disclosure of information which leads to loss of information.
- *Availability*: means the data is available when needed. Failure to access information in a timely manner causes a system malfunction.
- *Integrity*: means ensuring that the information is sound from manipulation and destruction. Lack of integration means that information is subject to modification or sabotage.
- *Non-repudiation*: Ensures that information can never deny ever sending or receiving the message.
- *Access control*: block illegitimate or unwanted access by restricting access only for authenticated entities.

In order to gain illegitimate access, adversaries are capable of exploiting system weaknesses. As systems move out from homes and offices security to more settings in every place, security importance cannot be denied. It is essential to guarantee the hardware and software security of any system.

3. Security attacks

In order to protect systems from attacks, security experts must assess and identify the risks and vulnerabilities of the system and define how to use mechanisms

that ensure security for the safety of the system. Section below presents a discussion of possible attacks of the system and their propagation in daily life.

3.1 Attacks types

Many types of attacks are described below with some detail:

1. Focused attack: this type of attack focuses on specific systems and does not restrict to money, resources, and time. The most practical examples of these type of attacks are targeting to defence installations and penetrating enemy communication lines.

2. Cryptanalytic attacks: cryptanalysis attacks have the ability to decrypt the ciphered text without accessing the encryption keys. These attacks are combined plain and cypher text attacks.

3. Network attacks: at present, systems are vulnerable to external attack through networks. This type of attack is done through monitoring, password hiding, and spoofing.

3.2 Targets of attacks

The system is exposed to different types of attacks; some of these attacks are presented in the following subsections. Generally, expected attacks are divided into three groups: attacks against availability, authenticity, and confidentiality :

1. Threats on availability: attacks' types on availability are the strongest, and we will mention two categories which are:

    a. Message suppression attack: packets are dropped by the attackers from the network, they exploit these packets in other time. This type of attack causes a lot of problems in the network.

    b. Drop the package**:** black hole attack is a dropping attack where the existence of this type of attack is the reason of package losing.

2. Threats to integrity: an example of this threat is alteration attack that happens when the attack changes message content. Re-send or delay of the message is considered as one of the forms of this attack.

3. Threats on authentication: fabrication attack is an example of this threat where attackers can gain their goals by broadcasting false messages in the network. These false messages are certificates, warnings, and identities.

4. Embedded devices security

An embedded system is a special-purpose computer system, which is fully encapsulated in the device it controls. These systems have special requirements and complete pre-defined tasks [3]. It consists of a combination of hardware and software; it is designed for dedicated functions. Embedded systems include several elements; each of them has a pre-defined task, and these differ from the typical desktop or laptop computer.

Figure 1.
Embedded system applications.

Embedded system spread in many devices, and the users of these devices are capable of performing almost all the network/internet applications that run on these devices. These devices are also involved in transport of secure data over public networks that require defence from unauthorised access.

As a result, security in embedded systems has spread every passing day in many fields like aerospace, telecom, healthcare, and wearable devices. **Figure 1** illustrates embedded systems applications such as railways, mobile phones, consumer electronics, tables, laptops, and healthcare application.

Embedded devices spread in a wide range of applications, and these devices handle critical information. For this reason, it is desirable to have some security mechanism deployed on embedded devices either in the form of software or hardware. However, embedded devices security is a challenging function and treated an open research case due to the resource-constrained nature of these devices. The security of embedded systems can become an issue, even bigger than the insufficiency of security of current desktop computers. The reason for this lack of security is hardware devices' constraints when performing measures of security and security cost. Manufacturers attempt to reduce costs of production to gain a market advantage for price critical products.

Many of application is heavily based on embedded systems that present in all our lives aspects. Embedded system devices are often networked via wireless communication links to accomplish advantageous tasks. However, the communication channel that is characterised by the wireless nature between the embedded devices makes them vulnerable to attacks and adversaries. Therefore, security of embedded systems is a main aspect of embedded systems design and is currently a major field of scientific research.

5. Problem definition

Many protection techniques have been proposed that try to provide security still do not interest on the most serious matter about who has access to the system. An alternate approach for providing the security of system from measurable properties of a target device is named ICMetric. In this chapter, ICMetric technology exploits the characteristic and behaviour of an embedded system to obtain a collection of properties and features, which aims to uniquely identify and secure an embedded system based on its own behavioural identity. The ICMetric technology allows a device to generate an identity which is used for authentication and a range of other cryptographic services.

In addition, some security techniques depend on the stored keys to enable secure information. Such techniques have a failure when the stored keys compromised the security of any data protected by these keys. Thus, it is important to employ security mechanisms to protect these systems from attackers. ICMetric technology has been designed as a method of deterring key theft by exploiting features of device to provide ICMetric number that will be utilised for identification of device. ICMetric number is not stored on the system and generated only when it is required by lightweight equation.

6. Objectives

In this chapter, the ICMetric technology is utilised to develop embedded devices security. This technology proposes using features of a device to generate ICMetric number used for device identification. The objectives behind using ICMetric were to overcome the problems related to accuracy rate, the failure to detect new attacks and the increased number of false alarms.

In this chapter, the objectives are as follows:

- Utilising ICMetric technology that depend on features that make each device different to generate a single and unique number called ICMetric number used for device identification.

- Demonstrating that it is possible to use the features of a device to create an identification that provides security of embedded devices. To achieve this, possible properties and features are investigated which can be used for the creation of an ICMetric of a device.

- Solving security problem presented in embedded device by applying device authentication.

- Proving that MEMS sensors can be used to improve security and apply identification of device. Bias reading generated by these sensors can be utilised to provide identification of device.

- Applying some statistical and mathematical analysis on bias readings extracted from MEMS sensors to provide ICMetric number used for identification and other security services.

- Training and testing dataset by using Support Vector Machine (SVM).

- Testing and evaluating system performance metrics, which are confused matrix, accuracy rate, and error rate.

- Evaluating additional performance metrics such as packet delivery rate, throughput rate, and end-to-end delay rate.

7. Integrated circuit metric technology

Encryption systems rely on the use of algorithms which in turn depend on the use of the secret key which is stored. Trying to increase the size of the key to stop

the brute force, but increasing the size of the key cannot always protect the security of the system and deter theft [4].

In order to eliminate the theft and by relying on the special features of each device, we can create an identification for each device, and this identification is called ICMetric. Other hardware techniques differ from the ICMetric technology in the selection of device characteristics. Traditional fingerprinting techniques depend on the characteristics that are easily exposed to capture, deception, or repetition by the attackers. ICMetric technology uses internal behaviour that increase the complexity of generated ICMetric and they are hard for an attacker to predict or spoof at runtime such as features that can be employed for creation an ICMetric are Media Access Control (MAC) addresses and serial numbers. Other features are utilised, which are application usage special task, such as browsing histories, camera resolutions, common user files, and system profiles [4].

ICMetric technology retains the idea of storing the key where there is no encryption key in the system; this will reduce the attackers. It uses hardware and software features of device to create ICMetric, which will be used in encryption services. There is a similarity between the biometric systems and the ICMetric, as these systems used features for identification of different persons. Similarly, ICMetric uses the characteristics of the device to identify each device uniquely and thus eliminates the idea of stored keys and deters theft of stored keys.

ICMetrics points to a new technique that can be employed to extract features from the hardware and software environment of a system. Every device is singular in its internal environment and then the features that make every device diverse can be employed to create a unique and single number for each device. It is based on the next concepts:

1. ICMetric number is not stored on the system and can be recreated when needed.

2. If the system is attacked, there will be no theft because the ICMetric is non-stored.

3. ICMetric number and any proceeding outcomes that are based on the ICMetric number will change if any adjusting has been done with the software, hardware, or environment.

4. There is no requirement to store any template that can serve the aim of device validating.

The generation of ICMetric system is comprised of two phases: calibration phase to collect detailed knowledge and operational phase to distribute each extracted features for typical sensors.

7.1 Calibration phase

At this phase, the characteristics are documented and analysed, normalisation distributions are utilised on feature values noticed in the system. A device ICMetric basis number can be created by applying statistical and mathematical operations on the extracted feature values. This phase is utilised once only when the system needs the ICMetric basis number. The features on which the ICMetric is based are unique; therefore, it is difficult for the attacker to detect or generate it. This is an important case to improve the ICMetric strength.

7.2 Operational phase

Operational phase follows the calibration phase where the unique number is generated depending on the extracted features. The preprocessing phase can be applied to generate unique features that distinguish it from others [5]. In this phase, an effort is made to generate a resulting device ICMetric basis number through either feature concatenation or feature addition.

8. Intelligent wheelchair application

Some companies produce different types of an intelligent wheelchair. An intelligent wheelchair can be defined as a uniquely modified powered wheelchair which is provided with a control system and variant sensors. Intelligent wheelchair is designed to provide several services to users in different ways. It eliminates the user's responsibility for moving the wheelchair. User types of intelligent wheelchairs are different according to their situations and disabilities. According to this, there will be different designs of intelligent wheelchair. The aim of intelligent wheelchair is to grant higher independence to people with lower mobility such as disabled or elderly individuals [6]. **Figure 2** states intelligent wheelchair.

In this chapter, ICMetric technology is integrated into an intelligent wheelchair. MEMS sensors embedded in intelligent wheelchair are utilised to ensure effective usage and to provide identification of intelligent wheelchair.

Figure 2.
Intelligent wheelchair.

9. Appling ICMetric technology in intelligent wheelchairs

In this chapter, ICMetric technology is integrated into an intelligent wheelchair. In order to ensure effective usage of the intelligent wheelchair and the need to protect the safety of each wheelchair, it is advantageous to provide identification of intelligent wheelchair to confirm the user's right to access the system and information and defend against identity theft and fraud. For achieving these aims, ICMetrics represents a new method for generating unique identifiers for embedded devices and improves security by reducing fraudulent activity.

ICMetric technology can improve secure communication between devices, reduce fraudulent activity, prevent unauthorised access to the systems and devices connected with the wheelchair, implicit detection of tampering of the software or hardware associated with the wheelchair, and prevent the fraudulent cloning or imitation of the electronics associated with the wheelchair.

While many security techniques are now developed, these cannot necessarily defend against unauthorised activity when the security and safety cannot be absolutely assured. The use of ICMetric technology to provide identification represents a new concept of controlling access to devices and is explicitly aimed at providing protection against attacks and improving security.

The ICMetric security system proposed in this chapter uses bias readings that have been extracted from sensor devices. These readings exploited to create ICMetric basis numbers that were working as identification for device.

In this chapter, suitable features can be gotten from the sensors to describe behaviour of intelligent wheelchair such as the gyroscope, magnetometer, and accelerometers. The offset is utilised in the sensor measurement to propose a security system that apply an ICMetric basis number using the sensor bias readings.

10. Intelligent wheelchair sensors

In order to apply features measuring of wheelchair, specific hardware circuits along with a software-based monitoring infrastructure are needed to be prepared and integrated in the system. Features can be read from various integrated sensors, and large origin of features is also the system's behaviour. For obstacles avoiding, intelligent wheelchairs need sensors to perceive their surroundings. Many sensors are used by intelligent wheelchairs as explained below:

- Ultrasonic sensors (i.e. sonar) and sonar sensors are very precise when the sound wave emitted by the sensor strikes an object at a right angle or head on.

- Infrared (IR) sensors emit light, rather than sound, and can be fooled by dark or light absorbent material rather than sound absorbent material.

- Laser Range Finders (LRFs) offer a 180°, two-dimensional scan within the plane of the obstacles in the environment. Another option is a 'laser striper', which contains a laser emitter and a charge-coupled device camera. The image of the laser stripe returned by the camera can be used to determine distances to obstacles and drop-offs based on breaks in the stripe.

In this chapter, MEMS sensors, which are magnetometer, accelerometer, and gyroscope, are used. MEMS sensors have many applications in measuring either acceleration or angular velocity about one or several axes as an input to control a system. Some details of accelerometer, gyroscope, and magnetometer sensors are presented below:

10.1 MEMS accelerometer in intelligent wheelchair

The MEMS accelerometer is a highly sensitive sensor and capable of detecting the tilt. This sensor changes the direction of the wheelchair depending on tilt. For example, if the tilt is to the right side, then the wheelchair moves in the right direction, and if the tilt is to the left side, then the wheel moves in the left direction. The wheelchair movement can be controlled in forward, reverse, left, and right direction

with obstacle detection using ultrasonic sensor. This wheelchair automatically senses the presence of an obstacle in its path and turns its direction of movement.

10.2 MEMS gyroscope in intelligent wheelchair

The MEMS gyroscope sensor provides an angular velocity of the wheelchair's wheel as compared to translating the acceleration values to rotation angles for calculating heel rotations. Angular velocities are used directly to estimate linear speeds and distances travelled, which allow us to provide wheelchair users with real-time feedback through smartphone applications.

10.3 MEMS magnetometer in intelligent wheelchair

Intelligent wheelchairs used MEMS magnetometer sensors for measuring and detecting magnetic fields. Hall effect, magneto-resistive effect, and fluxgate effect are the most popular principles in magnetometer sensors. Magnetometer sensor measures the magnetic fields based on Hall effect.

ICMetric technology presented here uses bias readings that have been generated from sensor devices. These readings are used to apply ICMetric basis numbers that were utilised as identification for device. Sensor-based identification field has proved that the use of sensory data is possible and that it is feasible to provide device identification.

11. The ICMetric security system

Current defensive mechanisms are not enough for preventing the internal attacks in device, since they require ICMetric security system as protection system to increase their security. ICMetric technology depends on measureable features, which have been achieved from the properties of a particular embedded system. Features are generated in the particular system that represents a unique feature for that system. The focus is on utilising a magnetometer, gyroscope, and accelerometer sensors that are provided in the new system.

In this chapter, an intelligent wheelchair is required where the bias readings extracted from sensors embedded in intelligent wheelchair are utilised in the ICMetric security system generation. These bias readings were employed to create an ICMetric basis that was used as identifications for device. In this chapter, ICMetric security system based on bias readings is extracted from gyroscope, accelerometer, and magnetometer sensors. The proposed algorithm is summarised in the following steps:

Algorithm (3.1): The Implement ICMetric
Input: Behaviour features that extracted from trace file of ns-2.
Output: Normal behaviour or abnormal behaviour.
Step 1: Establishing parameters for simulation. Step 2: Generating mobility and traffic model. Step 3: Extracting features from trace file. Step 4: Pre-processing of the extracting features. Step 5: Integrating of ICMetric number generated by MEMS sensors. Step 6: Dividing the extracted dataset into three groups which are training set, testing set, and validation set. Step 7: Training phase. Step 8: Testing phase. Step 9: Results.

12. Sensors bias measurement

In some cases, it is not feasible to collect the bias in the sensor. Sensors are required for generating the bias readings of a system which do not require user intervention and are not influenced by external factors. MEMS is a technology that combine mechanical and electrical components. There are many MEMS-based sensors that are being embedded into recent vehicles, wearable devices, laptops, and smartphones. The most commonly used and good examples of MEMS sensors are the accelerometer, the magnetometer, and the gyroscope. Accelerometers are intended to measure the acceleration of an object, whilst gyroscopes measure angular velocity. Magnetometer sensors are used for measuring and detecting magnetic fields.

MEMS sensors are used in this chapter because they are readily available and also the required stimulus is easy to create. Various numbers of bias reading are obtained from MEMS sensors to generate ICMetric number. The system needs to determine the optimal number of readings which are used in identification processes to control the stability of the statistical processes of the ICMetric generation. We need to calculate the population mean and compare the result with the mean value calculated for a smaller subset of readings to determine the best number of readings.

In order to extract reading from sensors, MEMS sensors are placed on the board, simulation is applied to produce a constant bias. The case is similar when a sensor is under operation where accuracy of sensor output is affected by unclear damages due to mistreating. For bias generation, the stimulus must be specified. One of the advantages of stimulus is that it does not need a specific device to evaluate it but is equipped by the user. The readings generated by the sensor must be equal to the stimulus applied to the sensor. Every axis owns a different bias, which is showed in the readings. Experiments prove that the bias in every sensor is unique and reproducible. These bias readings are utilised to provide identification of device and improve security.

13. Statistical analysis for ICMetrics

ICMetric is not stored but is created when needed this distinguishes the technology of ICMetric in protection from attacks. Since it is created when needed, it requires simple mathematical processes and a statistical analysis for the values of features. Below are some statistical analyses required for the generation process of the ICMetric number is utilising to apply identification of device.

If we assume that $\overline{X}$ represents mean, x represents particular sample reading from accelerometer, magnetometer, and gyroscope, and n is total number of reading, then [7]:

$$\overline{X} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{1}$$

In order to complete ICMetric generation process, we need to calculate σ^2 as explained below, where σ^2 is the standard deviation.

$$\sigma^2 = \sum_{i=1}^{n} p(x_i)\,(x_i - \overline{X})^2 \tag{2}$$

Furthermore, other statistical and mathematical functions are utilised to analyse the generated reading. For example, we need to calculate variance (s^2) as explained in the following equation:

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n} (x - \overline{X})^2 \tag{3}$$

where s^2 is a measure of dispersion for extracting readings.

The skewness distribution (S) is a measure of asymmetry of the probability distribution of bias readings. It can be negative or positive:

$$S = \frac{3\,(\overline{X} - m)}{s^2} \tag{4}$$

To prove the uniqueness of the bias generated from accelerometer, magnetometer, and gyroscope sensors, we use 95% confidence interval. If $\overline{x}$ is the mean, σ is the standard deviation, and n is the total number of observations, then the confidence interval CI is given in the Eq. (5) where the numeric value v here equals to 1.96.

$$CI = \overline{X} \pm v\,\frac{\sigma}{\sqrt{n}} \tag{5}$$

In addition, other statistical and mathematical functions are utilised to analyse the generated reading such as inter quartile range (IQR) that represents difference between the third and the first quartile in offset data. IQR can be calculated according to the Eq. (6), where $Q3$ represents upper quartile and $Q1$ represents lower quartile.

$$IQR = Q3 - Q1 \tag{6}$$

14. Performance metrics

ICMetric security system has been evaluated using a number of ways based on trace file evaluation. The ICMetric security system can be generally evaluated from two views [8]:

1. Accuracy: this portion also termed effectiveness classification characterises the ability of the system to separate between intrusive and non-intrusive activities.

2. Efficiency: this portion deals with the resources required to be allocated to the system including CPU cycles and main memory

System features can be evaluated in terms of performance, correctness, and usability. Researchers used metrics to assess the performance of the system. Many performance measures are used to evaluate the system, which are based on the dataset extracted from the trace file created by ns-2.

The identification rate and four alarms are utilised as performance metrics to test the system. To measure and evaluate the system performance, four types of alarms are needed to calculate: true positive (TP), false positive (FP), true negative (TN), and false negative (FN). The measures will be calculated as follows [5]: Let

TP = normal connection record classified as normal

TN = attack connection record classified as attack

FP = normal connection record classified as attack

FN = attack connection record classified as normal

Then,

$$TP_{Rate(\text{sensitivity})} = \frac{TP}{TP + FN} \tag{7}$$

$$TN_{Rate(\text{specificity})} = \frac{TN}{TN + FP} \tag{8}$$

$$FN_{Rate(1-\text{sensitivity})} = \frac{FN}{FN + TP} \tag{9}$$

$$FP_{Rate(1-\text{specificity})} = \frac{FP}{FP + TN} \tag{10}$$

In addition, some extra metrics are utilised to evaluate system performance such as packet delivery rate (PDR), throughput, and end-to-end delay.

- Packet Delivery Ratio (PDR): the ratio between the number of packets sent from the origin and the proportion of packets received at the destination.

$$\text{PDR} = \sum N_r / \sum N_s \tag{11}$$

where N_r = number of packets received and N_s = number of packets sent.

- Throughput: the total number of packets that are transferred in the system. Throughput of a system can be presented as shown in the following equation.

$$\text{Rate of throughput}(\text{kbps}) = N_r * S/ST \ (12) \tag{12}$$

where N_r = number of packets received and S = packet size and ST = simulation time.

- Average end-to-end delay: the average time for packets reaching from the origin to the destination. Average end-to-end delay is explained in the following equation:

$$\text{Rate end} - \text{to} - \text{end delay (ms)} = \left(\frac{\sum end_{time} - start_{time}}{\sum N}\right) \tag{13}$$

where N represents a number of connections.

15. Conclusions

The main contribution of the present chapter is to achieve an identification model for intelligent wheelchair application with high rate of accuracy and with low error rate. This was done through the design of an identification process by using ICMetric technology. From the given results, the following substantial remarks were obtained:

1. ICMetric technology can be used to apply identification and improve security of embedded devices.

2. ICMetric technology relies on the special internal features of device where each device is unique in its internal environment.

3. MEMS gyroscope, magnetometer, and accelerometer sensors embedded in intelligent wheelchair are utilised. Three axes readings achieved from every sensor where every sensor will have unique readings.

4. Readings generated from MEMS sensors are analysed statistically to generate ICMetric number utilised for device identification. A statistical study of the readings generated from sensor shows practical use of MEMS sensors for the generation of a device identification.

5. Support vector machine exploited in this chapter to evaluate and test system under certain conditions.

6. In order to evaluate system performance, we need to calculate the performance metrics, which are accuracy rate, error rate, and four types of alarms.

7. Additional performance metrics can be evaluated for system such as, PDR, throughput, end-to-end delay.

During the training and testing processes, the SVM with dataset is extracted from the trace file generated by ns-2; it was found that using ICMetric technology for embedded devices identification provides better rate of accuracy and low error rate.

16. Future work

1. This chapter has established the design of an ICMetric by using different features of device. Therefore, the aim of the future research is to discover more features which can strengthen the device ICMetric.

2. The ICMetric technology has not been researched in bitcoins and block chains. It can be integrated into bitcoins to provide secrecy of transactions.

Author details

Khattab M. Ali Alheeti[1*], Duaa Al_Dosary[2] and Salah Sleibi Al-Rawi[3]

1 Computer Networking Systems Department, College of Computer Sciences and Information Technology, University of Anbar, Iraq

2 Computer Sciences Department, College of Computer Sciences and Information Technology, University of Anbar, Iraq

3 Information Systems Department, College of Computer Sciences and Information Technology, University of Anbar, Iraq

*Address all correspondence to: co.khattab.alheeti@uoanbar.edu.iq

References

[1] Stallings W. Cryptography and Network Security: Principles and Practice. 5th ed. Prentice Hall; 2011

[2] Alshahrani M, Teymourlouei H. Network security: Threats and vulnerabilities. In: International Conference on Security and Management. CSREA Press; 2016. pp. 115-121

[3] Lizarraga J, et al. Security in embedded systems. In: IADIS International Conference Applied Computing; 2006. pp. 697-699

[4] Tahir H, Mcdonald-maier K. Securing health sensing using integrated circuit metric. Sensors. 2015;**2015**(15):26621-26642

[5] Ali KM. Intrusion detection system in external communication for self-driving vehicles [PHD thesis]. School of Computer Science and Electronic Engineering, University of Essex; 2017

[6] Faria B, Mónica S, Vasconcelos L, Reis P, Lau N. A methodology for creating intelligent wheelchair users' profiles. In: ICAART 2012—Proceedings of the 4th International Conference on Agents and Artificial Intelligence. 2012 SCITEPRESS (Science and Technology Publications). Vol. 1. 2012. pp. 171-179

[7] Tahir H, Tahir R, Mcdonald-maier K. Securing MEMS based sensor nodes in the internet of things. In: 2015 Sixth International Conference on Emerging Security Technologies Securing; 2015. pp. 44-49

[8] Kumar G. Evaluation metrics for intrusion detection systems—A study. International Journal of Computer Science and Mobile Applications. 2014;**2**:11-17