Farooq *et al. EURASIP Journal on Wireless Communications and Networking* (2019) 2019:210
https://doi.org/10.1186/s13638-019-1531-0

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Efficient adaptive framework for securing the Internet of Things devices

Umer Farooq*, Najam Ul Hasan, Imran Baig and Naeem Shehzad

Abstract

The research on the Internet of Things (IoT) has made huge strides forward in the past couple of years. IoT has its applications in almost every walk of life, and it is being regarded as the next big thing that can change the way humans perceive about their daily life. Smart IoT devices of heterogeneous nature make an essential part of modern day IoT-based systems. The security of these devices is of paramount importance as they handle an enormous amount of critical data and its breach can lead to potentially life-threatening situations. To secure the IoT devices of heterogeneous nature, we formulated a weighted optimization problem in this work. The objective function of this problem is to secure the IoT devices while finding the best trade-off between their resource usage and throughput. To achieve the objective, we consider a pool of five different implementations of Advanced Encryption Standard (AES) cryptographic schemes that offer varied resources and throughput numbers. These implementation schemes are mapped to IoT devices of heterogeneous nature. The mapping is performed through a novel adaptive framework that can consider different weights for resources and throughput to eventually find the best trade-off between the resources and throughput of an IoT-based system. This framework considers the resource and throughput requirements of different IoT devices and uses the Hungarian algorithm to adaptively map different AES implementations on them. Extensive experimentation is performed where the best trade-off is found through varying resource and throughput weight combinations. The comparison of the proposed framework with random and greedy approaches is also performed. Comparison results show that the proposed framework adaptively secures the IoT-based system while providing better resource usage and throughput results. The proposed framework provides, on average, 11% and 17% better throughput and 3% and 13% better resource usage results as compared to random and greedy approach, respectively.

Keywords: IoT, Security, Adaptive Framework, AES algorithm, Cryptography

1 Introduction

The Internet of Things (IoT) is a paradigm that has seen enormous popularity in last few years. A formal definition of IoT does not exist yet. However, a loose interpretation of IoT is that it provides internet-based services that involve human-to-thing, thing-to-thing, and thing-to-things communications [1]. Entities of varied nature can interact with each other through IoT. These entities include humans, sensors, computing devices, or potentially anything that can give/receive services [2]. The striking emergence of IoT is a result of the rapid advancement in various communication protocols which is further aided by ever improving design process and miniaturizing processing technologies [3]. The improved communication protocols and better design process have resulted in devices with increased computing capabilities, higher data rate, and more energy storage capacities. At the same time, the IoT devices are becoming smaller in size and more efficient in terms of performance. The technological advances in software as well as hardware have tremendously increased the number of smart devices connected to the internet, and this number is expected to grow exponentially in future with the advent of new communication technologies. The importance of these devices and the level of services that could be provided by them in the future is limited by human imagination only. Some of the possible applications of IoT are smart vehicles,

*Correspondence: ufarooq@du.edu.om
Department of Electrical and Computer Engineering, Dhofar University, Salalah, Oman

smart buildings, health monitoring systems, environmental monitoring, and food supply chain [3].

The aforementioned applications of IoTs indicate that IoT-based systems have to handle an enormous amount of data which includes information about smart cars, industrial plants, health monitoring systems, and smart buildings [4]. The amount and type of data handled by IoTs require efficient algorithms for data processing and analysis [5, 6]. Authors in [7] have proposed smart solutions for big data collection, processing, and analysis of IoT-based systems. Moreover, the simple data collection and analysis for IoT-based systems is not enough. This is because of the fact that the type of data usually handled by IoTs is of very critical nature and this makes IoT-based systems an interesting target for different kinds of adversaries. For example, potential attackers might be interested in stealing location information, financial information, or health-related records from IoT-based systems. Furthermore, they can compromise the IoT components to subsequently launch security attacks against third-party entities. The theft/compromise of any information may result in poor confidentiality, lower integrity, and smaller availability of IoT devices. This could eventually lead to even life-threatening situations [8–11]. Therefore, for safe and reliable operation of IoT-based systems, security becomes the fundamental enabler where the confidentiality, authenticity, and integrity of the IoT data is ensured [12].

There is no doubt that the security is of paramount importance in the IoT devices. However, the way to best implement the security in IoT-based systems is debatable [13]. IoT-based systems have normally multiple layers. The number of layers may vary depending upon the reference model under consideration. But, all of them usually have at least three common layers called the application layer, the network layer, and the edge side layer [14]. The application and network layers can be protected through firewalls and other well-established security protocols. But, the security of the deeply embedded edge side nodes is a challenging task. This situation is further aggravated because of the heterogeneous nature, varied resources, and different performance requirements of these nodes [15]. Edge side nodes are normally susceptible to different kinds of security attacks. Some examples of these attacks are hardware trojans [16], side-channel attacks [17], denial-of-service (DoS) attacks [18], and node replication attacks [19]. There are several countermeasures like side-channel analysis, isolation, blocking, and implementation of cryptographic schemes [14, 20, 21]. To secure the edge nodes, these countermeasures can be used against the security attacks. Among these countermeasures, cryptographic schemes are particularly popular. The cryptographic schemes are generic, hardware independent, and offer high-level robustness to the IoT-based systems. Advanced Encryption Standard (AES) is a commonly used cryptographic scheme that uses a symmetric cipher to achieve the highest possible security level. AES has robust security properties, and its implementation is simple both in software as well as hardware. It is an iterative, round-based, and symmetric algorithm that supports different key sizes. Standard implementation of AES requires a large number of hardware resources and is not normally recommended for resource-limited IoT edge nodes. However, nowadays, the logic capacity of the IoT devices is larger than ever before. This is because of the optimized design process and miniaturized processing technologies. Moreover, the efficient implementations of AES [22, 23] have made it a suitable candidate that can offer a solution to the security challenges of IoT-based systems. In this regard, authors in [24] have presented an efficient implementation of AES for IoT devices. Authors in [14] also proposed the use of AES for IoT devices. But, both aforementioned propositions are static in nature. Both propositions consider only single AES implementation and do not take into account the heterogeneous nature of IoT devices. This kind of approach can be unjustified owing to the varied constraints of the different IoT devices. Furthermore, these implementations neither consider any reference IoT system model and nor take into account any resource/throughput constraints of the IoT-based system.

Contrary to the aforecited work, in this work, we propose an adaptive framework that considers five different AES implementation schemes [22] for IoT devices. Based on their implementation, these schemes offer different resource and throughput values. In order to best exploit the diverse resource and throughput requirements of IoT devices, we propose an optimization model that finds the best scheme owing to a weighted distribution of resource and throughput numbers. To get the best trade-off between resource and throughput, we map the optimization problem to a bipartite graph which is solved using the Hungarian algorithm [25] subsequently. To validate our results, we compare our schemes to those obtained through the random and greedy approach as well. To the best of our knowledge, this is the first work of its kind in the context of IoT-based systems. Although some static implementations of AES algorithm can be found in literature [14, 24], they are very limited in their scope and they do not take into account the heterogeneous nature of IoT devices. In the context of security for IoT devices, Table 1 presents a summary of the comparison between the proposed framework and the existing state-of-the-art work. In this table, column 1 gives the reference number and year of publication of the reference work. Column 2 describes the objective of each reference work. Columns 3, 4, and 5 indicate the measures takes to achieve the objective of the work. It can be seen from this table that our proposed framework is the only work that

Table 1 Summary of related work

Reference	O[1]	E[2]	A[3]	H[4]	Remarks
[8], 2014	Identification of possible threats to wearable devices				Discussion without proposing any solution
[9], 2011	Mitigating passive attacks like eavesdropping and active attacks like control of wearable devices	✓			Rolling cryptographic protocol is used
[10], 2008	Alleviating software attacks on wearable devices				Zero power mitigation is used
[13], 2017	Highlighting security issues in architecture elements of IoTs				Discussion on possible architectural threats without any solutions
[15], 2013	Identification of security challenges to embedded platforms				Discussion without providing any solutions
[16], 2016	To reduce the susceptibility of a circuit layout to hardware trojan insertion				Vulnerability analysis of hardware circuit layout is carried out
[17], 2016	To cope with the information leakage in wearable devices				Identified the reasons for physiological information leakage and suggested countermeasures such as signal strength reduction, information reduction and noise addition
[18], 2013	To reduce the effect of DoS attacks				Proposed modification in network routing protocol by Parno et al [19]
[20], 2013	To increase the trojan detection sensitivity in ICs	✓	✓		Use thermal and power maps for trojan detection
[21], 2004	To provide secured authentication for RFID systems	✓	✓		Used AES algorithm as a cryptographic primitive
[22], 2017	Efficient implementation of AES for embedded devices	✓	✓		Comparison of different AES implementation techniques for embedded devices
This work, 2018	Efficient resource and area throughput based encryption scheme selection for heterogeneous IoT devices	✓	✓	✓	Used matching algorithm to find the encryption scheme

[1]Objective
[2]Encryption
[3]AES
[4]Hybrid

adaptively uses the AES cryptographic encryption scheme for the security of IoT devices of heterogeneous nature. The main contributions of this work are also summarized as follows:

- An adaptive framework is proposed that considers different AES implementation schemes for the security of heterogeneous IoT devices.
- The proposed framework finds the best trade-off between the resources and throughput of an IoT-based system through a mathematical optimization model and a modified bipartite matching algorithm.
- Extensive experimentation is done and comparison is performed with random and greedy approaches.

The rest of the paper is organized as follows. Section 2 details the different reference models in the state-of-the-art. This section also discusses the reference system model that we consider in this work. Section 3 discusses the mathematical equations that consider the weighted values of resource and throughput constraints of IoT devices in an IoT-based system. Section 4 discusses the proposed adaptive framework that uses the weighted equations and maps their values to a modified bipartite graph. In this section, details about the optimization equation, weighted distribution, and optimization algorithm are given. Section 5 presents the experimental setup and gives details about the five AES schemes that we consider for experimentation. This section also presents the comparison of proposed approach with random and greedy approaches. The paper is finally concluded in Section 6 with some discussion on the future work.

2 Reference IoT model

Different IoT models have been discussed in the past in various research publications but no standard model for IoTs exists yet. For example, authors in [26] present a three-layered IoT model which was an extension of wireless sensor networks (WSNs) and it was among the first reference models for IoT-based systems. A more detailed

model was presented in [2] which was comprehensively extended by CISCO in 2014 [27] and has the potential to be standardized for IoT-based systems. A three-layered fog-based detection system was presented by [28] that used a trust evaluation mechanism to detect internal attacks at data level. In this work, however, we consider a reference model similar to CISCO reference model and its pictorial presentation is given in Fig. 1. It can be seen from this figure that it is a multi-layered model. In this model, at the bottom level, we have sensors that are attached to different IoT devices. These devices are assumed to be heterogeneous in nature with different resource and performance requirements. In a secure IoT-based system, these devices are of critical importance as the integrity and authenticity of data starts from this level upwards. It can be seen from the figure that next we have a gateway that sends/receives data from a public or private cloud. At the gateway level, essential processing/computation of data is also performed so that load on the lower level is reduced and a high response rate is ensured. Next in the level, we have data accumulation and data abstraction points. At this level, data is stored and analyzed for upper level computing servers. At this level, the data is stored, analyzed, and formatted in such a way that the additional processing on the data becomes easier; hence, eventually making it more meaningful for the higher level applications and end users. Finally, we have applications that collect the analyzed data from a data center and provide the interpretation of that data which is then used by end users for specific purposes.

To have a secure IoT-based system, considering a reference IoT model is of pivotal importance. Without a reference IoT model it becomes quite difficult to have a global picture of an IoT-based system. Moreover, it becomes even more challenging to identify the levels where cryptographic schemes are required to be implemented. In the reference model of Fig. 1, security at the higher levels can be ensured through network firewalls and well-developed protocols. Moreover, the devices at higher levels normally operate in protected environments and they are well beyond the reach of malicious attackers. However, as we move towards the lower levels, the issue of security exacerbates and it becomes more challenging to secure IoT devices. Specially from the gateway level onwards, we have to take into account the heterogeneous nature of IoT devices which usually have different resource capacities and diverse throughput constraints. Furthermore, the lower level devices are usually in direct access of attackers which makes them an attractive target for all kinds of security attacks [16–19]. A few cryptographic countermeasures against these attacks have been proposed by [14, 24]. But these propositions are static

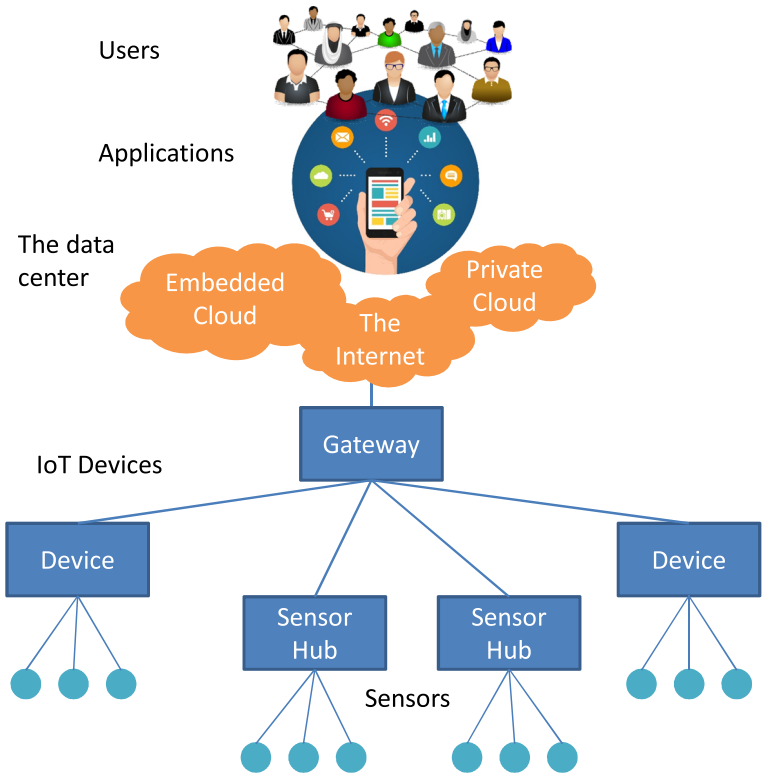

Fig. 1 Multi-layered reference IoT model

in nature as they do not adapt as per the target IoT device requirements. Furthermore, they do not consider any IoT reference model. The static nature of these propositions can not justify different resource and throughput requirements of various IoT nodes. In this work, we consider the reference model shown in Fig. 1 and propose to use five different implementations [22] of AES algorithm. These techniques use different hardware implementation optimizations. For example, we use optimizations like pipe-lining, loop unrolling, and serial implementation in different implementations. These techniques are applied from gateway level downwards. As a results of the implementation mechanism, these techniques give a variety of area and throughput results. We use a pool of five techniques as it gives us the choice to best satisfy the different resource and performance constraints of target IoT device. Because, a single technique would have either resulted in compromise of logical resources or throughput or even both.

In order to best utilize these techniques for reference IoT-based system, in this work, we first present a mathematical system model. Next, we propose an adaptive selection mechanism. This selection mechanism uses optimization equations of mathematical system model that consider weighted values of resource and throughput constraints of target IoT devices. Based on those constraints and available values of different AES implementation techniques, a selection of the technique for a particular device/gateway is made through the Hungarian algorithm. This process is applied on hundreds of IoT devices to improve the overall throughput of the IoT-based system while adaptively minimizing the resource usage of IoT devices. Further details about the mathematical system model, adaptive selection mechanism, and matching algorithm are given in the succeeding sections of the paper.

3 Mathematical system model

As stated in Section 1, the objective of this work is to adaptively secure an IoT-based system while finding the best trade-off between the resource and throughput constraints. For this purpose, it is important to first model the system mathematically and later do the optimization using matching algorithm. To mathematically model an IoT-based system, in this paper, we considered an IoT network with three main entities namely sensors, IoT devices, and IoT servers (i.e. gateway). Sensors interact with the physical environment and collect the environmental information. IoT devices acquire the data from these sensors and make it available to different applications via IoT servers. The IoT network is usually characterized as a dense network with a large number of IoT devices. These devices are generating massive amounts of data. To handle such a big amount of data, a significantly large number of IoT servers are needed to be deployed. Therefore, it can be assumed that each IoT device is associated with one of these servers. The communication between the IoT devices and servers takes place over the wireless link. To ensure a secure channel between the IoT device and the IoT server, the data must be encrypted. But the heterogeneous nature of IoT devices renders a uniform encryption for all these devices infeasible. Therefore, IoT servers are assigned with an additional task of selecting the appropriate encryption scheme. This selection is based on minimizing the resource and maximizing the throughput for an IoT-based system. There are a large number of IoT servers, and a large number of IoT devices are associated with each of them. However, for the sake of simplicity, we considered the case of just one IoT server without the loss of generality.

For mathematical model, let there be N IoT devices that are associated with an IoT server. After associating with an IoT server, each i^{th} IoT device sends its relevant information including its available resources R_i and the required demand in terms of its throughput T_i based on the running application. With the given information about available resources and required throughput for each IoT device associated with it, an IoT server assigns an encryption scheme to each IoT device. There are total M number of different encryption schemes. Each encryption scheme is also attributed with two parameters: first is the number of resources required to implement this scheme, and second is the maximum throughput it can provide to the IoT devices. From a pool of M different encryption schemes, the IoT server has to assign a certain scheme to each device that is associated with it. The assignment should be such that the overall throughput of the network is maximized and the resources being used are minimized while respecting the constraint of each individual IoT device. Since there are two objective functions of this problem, we designed a weighted multi-objective optimization problem, which can be mathematically written as follows:

$$\begin{aligned} &\max \textstyle\sum_{i=1}^{N} \sum_{k=1}^{M} \; (w_1 f_1 + (1-w_1) f_2) x_{ik} \\ &\text{s.t.} \\ &\qquad \mathbf{C1}: \textstyle\sum_{i=1}^{N} x_{ik} = 1 \\ &\qquad \mathbf{C2}: R_i^d > R_k^s x_{ik} \\ &\qquad \mathbf{C3}: T_i^d < T_k^s x_{ik} \end{aligned} \tag{1}$$

The utility function of Eq. 1 is a weighted sum of two functions i.e. f_1, f_2. The objective of f_1 is to maximize the throughput and that of f_2 is minimize the resource usage. The mathematical expression for the two functions is as follows:

$$f_1 = \frac{T_i - T_{\min}}{T_{\min}} \tag{2}$$

$$f_2 = \frac{R_{\max} - R_i}{R_{\max}} \tag{3}$$

The sum of the weights assigned to both f_1 and f_2 is equal to 1, where w_1 is the weight assigned to f_1 and $1 - w_1$ (also termed as w_2 in Section 5) is the weight assigned to f_2 and x_{ik} is the binary variable. The value of x_{ik} is 1 if the k^{th} scheme is assigned to the i^{th} IoT device and 0 otherwise. It can be seen from Eq. 1 that the optimization problem has also three constraints. The explanation of these constraints is as follows:

- *Constraint 1 (C1).* Constraint 1 states that each IoT device must be assigned only one encryption scheme.
- *Constraint 2 (C2).* This constraint states that the resource required for the selected scheme should be less than the resources available at the IoT device.
- *Constraint 3 (C3).* Constraint 3 states that the throughput for the selected scheme should be greater than the required throughput of the IoT device.

A description of symbols used in Eqs. 1, 2, and 3 is also given in Table 2.

4 Proposed adaptive framework

To solve the problem described in previous section, we opted a graph theory approach. We mapped this problem into a matching problem in the form of a weighted bipartite graph. A bipartite graph is a graph of two disjoint sets, i.e., X and Y such that $X \cap Y = \infty$. The bipartite graph is unidirectional graph, in which the edges always point in one direction that is $X \rightarrow Y$. Moreover, in a weighted bipartite graph, each edge is also assigned a weight based on a specific criteria. Usually in such a kind of problem where a weighted bipartite graph is involved, once a graph is formed, a matching algorithm is employed to find the matching solution consisting of edges in order to optimize certain objective function.

Table 2 Symbol Description

Symbol	Description
N	Number of IoT devices
M	Number of candidate encryption schemes
R_i^d	Resources available at i^{th} IoT device
R_k^s	Minimum resources required to implement k^{th} encryption scheme
T_i^d	Required throughput for the i^{th} IoT device
T_k^s	Throughput given by the k^{th} encryption scheme
f_1	Function to maximize the device throughput of an IoT device
f_2	Function to minimize the resources being used at an IoT device
T_{min}	Minimum throughput offered by any of the M encryption scheme
R_{max}	Maximum resources required by any of the M encryption scheme
w	Weight factor to set priority for f_1 and f_2.

For our problem, X and Y are considered to be the set of IoTs and the set of different encryption/implementation of the encryption schemes. A graph $G(X, Y, E)$ is formed by drawing the edges E_{ij} between X and Y. Each edge in this graph is drawn between the i_{th} device and j_{th} encryption scheme. The edge between i_{th} device and j_{th} encryption scheme is drawn if all the constraints mentioned in the mathematical model of Section 3 are satisfied. In the graph, $i \in X$ and $j \in Y$. Once the edges are drawn, each edge is assigned a weight based on the objective function defined for the optimization problem. For the sake of clarity, we take an example where X consists of four IoTs and Y consists of 2 encryption schemes. A graph $G(X, Y, E)$ is formed as shown in Fig. 2a. To solve the given optimization problem on the given graph, we have to apply a one to one matching algorithm. The outcome of this algorithm is that the IoT devices I_1 and I_3 are assigned encryption scheme S_1 and S_2, respectively. This is shown with the solid-lined edge on the graph of Fig. 2a. But the problem with this solution is that only two out of four IoT devices (i.e., I_1 and I_3) are assigned an encryption scheme, whereas I_2 and I_4 have not been assigned any of the encryption scheme. One solution to this problem is to modify the graph G and generate another graph G' in which we copy the schemes such that number of elements belonging to X and Y become equal. The modified graph G' for the aforementioned example is shown in Fig. 2b. Now, if one to one matching algorithm is applied to this problem, the outcome of this is that each IoT device is assigned at least one scheme. For example, I_1 and I_4 are assigned S_1, and I_2 and I_3 are assigned S_2 as shown with the solid-lined black edges of Fig. 2b. But there is still another problem given the same example which need to be addressed. For instance, if a scenario is encountered in which S_1 is the most efficient in terms of overall resource utilization and throughput provision for a given set of IoT devices. In such a case, all of the four IoT devices need to be assigned the S_1 encryption scheme. However, this is not possible by solving G', because two out of four IoT devices will still be assigned S_1 and the remaining two will be assigned S_2. To cope with this situation, the graph is modified to generate another graph G'' in which we have to copy all the schemes equal to the number of IoT devices as shown in Fig. 2c. Also, since one to one matching algorithms are applicable to only symmetric graph, we need to pad zeros as shown in Fig. 2c. Once we apply one to one matching on G'' both of the aforementioned problems in graphs G and G' are solved. Each IoT device can be assigned encryption scheme that suits best in terms of resource and throughput requirements. For instance in Fig. 2c, each of the four IoT devices have been assigned a scheme S_1 as shown with the solid-lined edges. A well

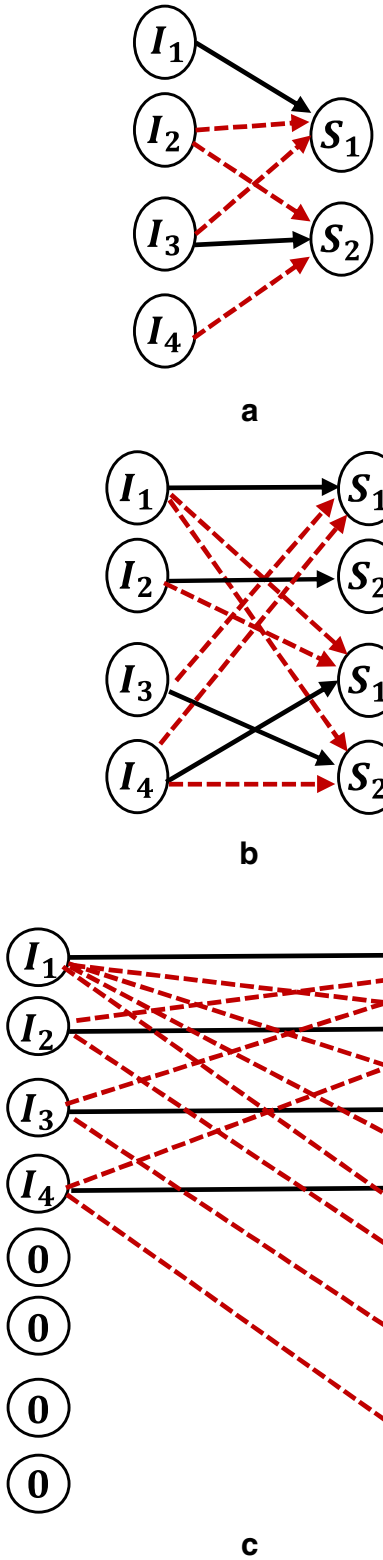

Fig. 2 Graphical representation of mapping between IoT devices and cryptographic schemes. **a** Initial bipartite graph, **b** Modified bipartite graph G', and **c** Final bipartite graph G'' to solve the assignment problem

known one to one matching algorithm named Hungarian is employed to solve the graph G''. The steps involved in the Hungarian algorithm are as follows:

1. Generate a square martrix Z of order $K \times K$ where $K = N \times M$. Each entry of Z is computed using $Z_{ij} = \sum_{i=1}^{N} \sum_{k=1}^{M} (w_1 f_1 + (1 - w_1) f_2)$.
2. The minimum value of each row of Z is subtracted from that row which results in another matrix Z'.
3. The minimum value of each column of Z' is subtracted from each entry in that column. This results in a new matrix Z''.
4. Cross out the rows and columns Z'' with all zeros entries. Terminate, if the number of crossed out rows and columns are equal to the number of sensors used in Step 2 and exit.
5. Find the minimal uncrossed entry of matrix Z'' and add to all the elements that crossed out both horizontally and vertically and subtract it from all uncrossed entries in Z'' and return to step 3 with this new updated coefficient matrix.

It is clear from the discussion presented in this section that an IoT-based system is first mathematically modeled. Next, the model is mapped to a modified bipartite graph. Finally, the objective function of the model is adaptively optimized using the Hungarian algorithm.

5 Experimentation and analysis

In this section, we present the experimental results that we have obtained through our proposed adaptive framework. For experimentation, we have considered the system model discussed in Section 3. For this model, we consider five different AES implementation schemes. These implementation schemes are considered for a number of IoT devices that are heterogeneous in nature and they have varying resource and throughput requirements. We use the adaptive framework discussed in Section 4 to optimize the overall resource and throughput of an IoT-based system. The current section is mainly divided into two parts. In the first part, a comprehensive overview of the five implementation schemes is given. In the second part, the results obtained through experimentation are presented and discussed.

5.1 Different AES schemes

In this section, we give a comprehensive overview of AES algorithm and the different AES implementation schemes that we have used in this work. An overview of standard AES implementation is given in Fig. 3. It can be seen from this figure that the implementation of AES algorithm is governed by two modules: one is cipher module and the other is key expansion module. The cipher module is an iterative process, and it can be optimized in the hardware

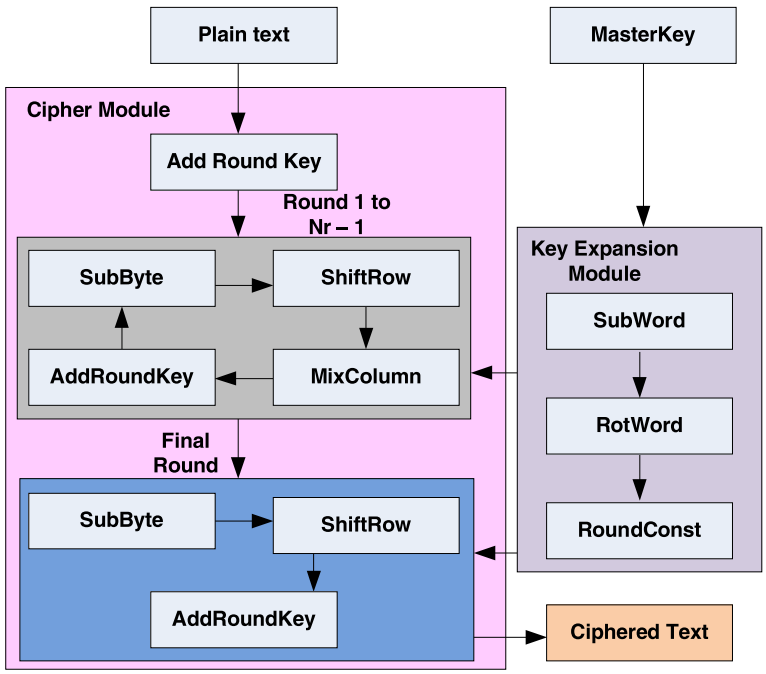

Fig. 3 An overview of standard AES implementation with different modules and sub-modules

using techniques like loop unrolling and pipe-lining. An unrolled cipher module can be coupled with a smaller key expansion module to increase the overall throughput of AES implementation. Similarly, the implementation of AES can also be improved by efficiently exploiting the resources of target architecture. By combining the aforementioned optimization techniques and hardware resource exploitation, we explore five different AES implementation schemes in this work. These schemes are used by the adaptive framework discussed in Section 4 to find the best trade-off between resource and throughput of a reference IoT system model. Further details on the five schemes are given next.

As discussed before, in this work, we use five different AES implementation techniques, and a summary of the resource and throughput metrics of the techniques under consideration is given in Table 3. These metrics are obtained through the implementation of these schemes on a Stratix V FPGA. The variation in the throughput and resource requirement of these techniques is because of different hardware implementations. A brief discussion on the optimizations applied on each technique is as follows:

Table 3 AES Schemes Overview

Name	Logic Resources	Throughput (Gbps)
Technique 1	3571	17.5
Technique 2	4789	28.5
Technique 3	4563	26.6
Technique 4	6066	27.5
Technique 5	9631	113.4

- *Technique 1.* It can be seen from Fig. 3 that both cipher module and key expansion module of the AES implementation have several sub-modules. In this technique, the sub-modules of cipher and key expansion module are implemented in the hardware in a serialized way. In serialized implementation, first, the key expansion module is implemented, and next, the cipher module is executed. The serialized implementation of this technique requires minimal logic resources while also giving the lowest throughput among the five techniques under consideration.
- *Technique 2.* In this technique loop unrolling is performed for the cipher module and key expansion is performed online. Online key expansion improves the execution speed. Because of the parallel implementation, this technique gives better throughput results as compared to technique 1. But at the same time, it requires more resources as well.
- *Technique 3.* In this technique, pipe-lining is introduced for the key expansion and cipher module is executed in a serialized manner. This results in comparatively less resources and smaller throughput as compared to technique 2.
- *Technique 4.* In this technique, loop unrolling is performed for key expansion and the cipher module

is executed in a pipe-lined manner. This results in a significant increase in terms of resource requirement. But, the throughput gain is not that much significant.

- *Technique 5.* Finally in technique 5, all the implementation of the AES is performed in such a way that the execution is totally parallel which eventually results in the highest logic resource requirement while giving the best throughput among the five implementation techniques under consideration.

5.2 Results and analysis

In this work, we consider a system model where our objective is to map the AES cryptographic scheme to heterogeneous IoT devices in such a way that the average throughput of the system is maximized while minimizing the number of resources used. For this purpose, we use a weighted function described in Eq. 1. In this equation, combinations of different weights are assigned to the throughput and resource metrics in order to determine the techniques that give the best results through our proposed adaptive framework described in Section 4.

A number of experiments are performed where the number of end users (i.e., IoT devices) are varied and along with that the weights of the throughput and resources of the devices are also varied. The main objective of this variation is to find the trade-off between throughput and resources that gives the best overall results. In this regard, the average throughput results with different weight combinations and varying number of users are shown in Fig. 4. In this figure the value of w_1 corresponds to the weight assigned to throughput parameter whereas the value of w_2 corresponds to the weight for resources. The value of w_2 is equal to $1 - w_1$. The values of w_1 and w_2 are varied from 0.2 to 0.8. As discussed in Section 3, the sum of w_1 and w_2 should always be equal to 1. It can be seen from Fig. 4 that when the value of w_1 is 0.2 and the value of w_2 is 0.8 then the average throughput is at the lowest point. It can also be seen from this figure that the average throughput increases as the number of users (i.e., IoT devices) increase and it stabilizes after the number of devices surpass a certain number. Furthermore, Fig. 4 shows that the average throughput of the system steadily increases as the value of w_1 is increased from 0.2 to 0.8. This is because of the fact that an increase in w_1 weight causes a decrease in w_2 value which eventually gives higher preference to throughput increase rather than resource curb.

As mentioned earlier, the objective of the proposed framework is to maximize the throughput while minimizing the resource usage of the system under consideration. In this regard, the average resource requirement results with different weight combinations and a varying number of users are shown in Fig. 5. It can be seen from Fig. 5 that when values of w_1 and w_2 are 0.2 and 0.8, respectively, then the average resources is at the lowest point and it steadily increases with the increase in the value of w_1. This is because of the fact that a bigger value of w_2 means more focus on resource optimization; hence, smaller resource requirement and vice versa. The results in Figs. 4 and 5 demonstrate that with the maximum value of either w_1 or w_2, we can achieve either best throughput or minimum resource usage. It is clear from these figures

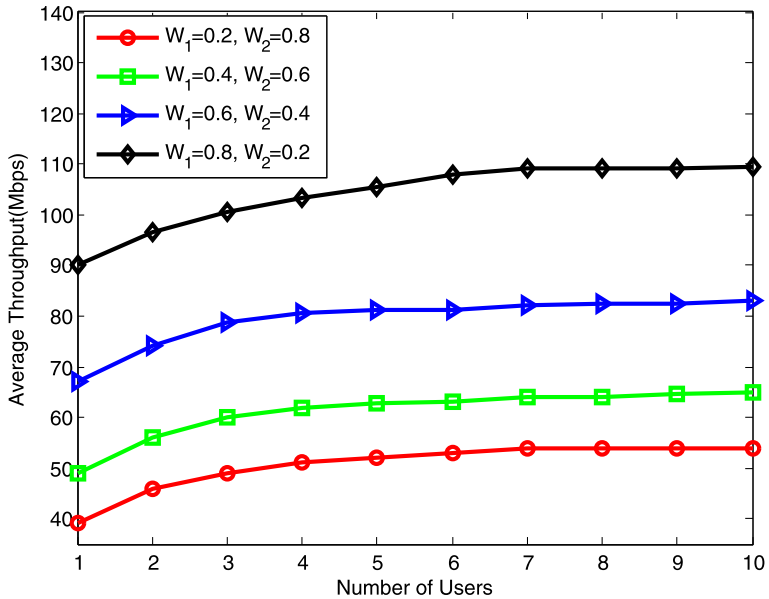

Fig. 4 Average throughput results with different weight combinations and number of devices

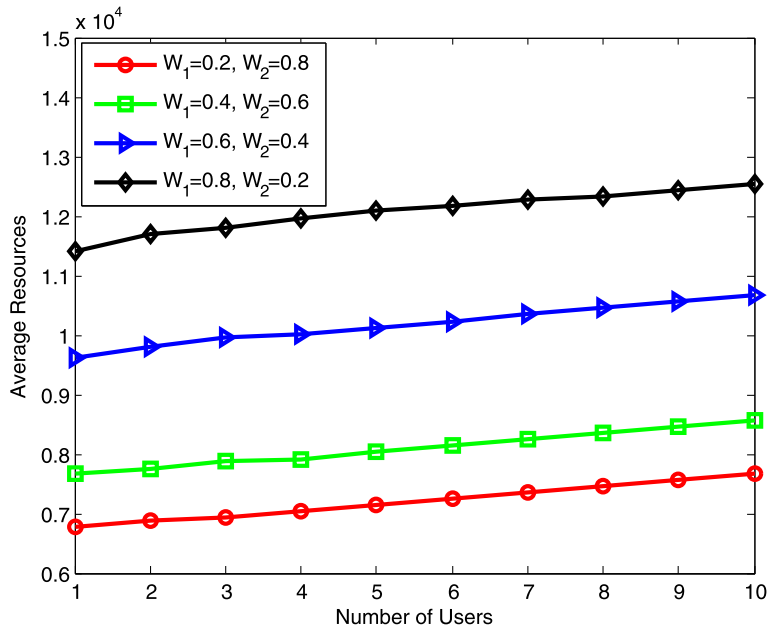

Fig. 5 Average resource requirement results with different weight combinations and number of devices

that both constraints cannot be satisfied simultaneously, and we have to find a trade-off between them. For this purpose, the average throughput and resource results for a fixed number of users are plotted in Fig. 6. In this figure, horizontal axis shows the values of w_1 and w_2, while primary and secondary Y-axis give the average throughput and resource results for varying values of w_1 and w_2. As stated earlier, the sum of values of w_1 and w_2 is always equal to 1. It can be seen from Fig. 6 that when the value of w_1 is 0.1 and the value of w_2 is 0.9 then the average throughput is at the lowest point and the average number of resources is also the smallest. This is because of the fact that when the value of w_1 is 0.1 and the value of w_2 is 0.9, the lowest priority is given to throughput and the highest priority is given to resource saving. On the other hand, when the value of w_1 is 0.9 and the value of w_2 is 0.1, then both the average throughput and average number of resources used by the system are at their peak. The

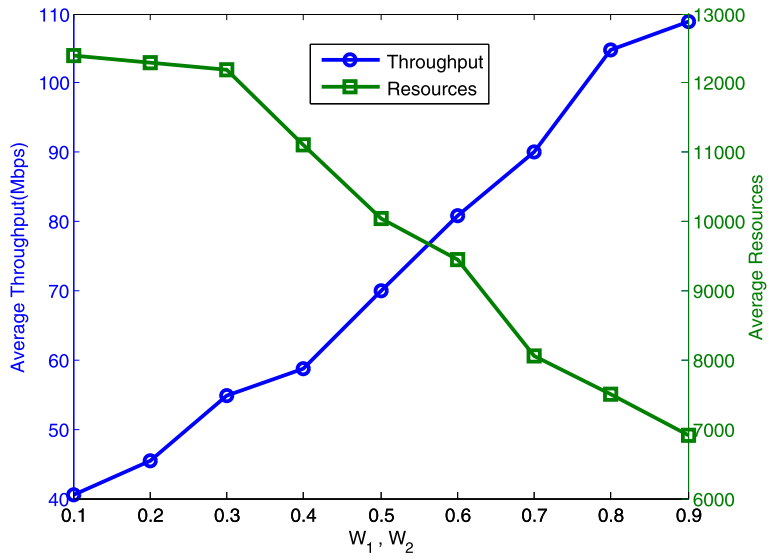

Fig. 6 Average throughput and resources for varying weights

aforementioned two cases are the extreme cases where in the first case the resources are given the highest priority while in the second case the average throughput is given the top priority. As stated earlier, the objective of the proposed framework is to find the best trade-off between average throughput and resource values. To achieve this objective when the value of w_1 is increased and value of w_2 is decreased, both average throughput and average resources start increasing and eventually the values of w_1 and w_2 between 0.5 and 0.6 give the best overall throughput and resource values for the reference system model under consideration. It is important to note that the results in this figure are generic in nature and they hold for any number of users/IoT devices.

In this work, we also perform average throughput and resource comparison between the proposed framework and random, greedy approaches. For this purpose, we fix the weights of throughput and resources at 0.5 each as this weight combination gives the best average throughput and resource results (see Fig. 6). Next, we vary the number of users (i.e., IoT devices) and observe the impact on overall throughput and resource of the system. We perform the experimentation for the proposed framework and compare the results against random and greedy approaches as well. The throughput and resource results are shown in Figs. 7 and 8, respectively.

The average throughput results in Fig. 7 show that initially the average throughput of the system under consideration increases with an increase in number of users. However, it stabilizes when the number of users are more than five. Furthermore, it can also be observed from this figure that the proposed framework gives better throughput results as compared to random and greedy approaches. This is because of the fact that the proposed framework considers all the possible combinations of schemes and devices and then selects the best possible combination using the Hungarian algorithm. On the other hand, the greedy approach either goes for the best throughput or resource value and does not look for the best trade-off. As a result the proposed framework gives, on average, 11% and 17% better throughput results as compared to the greedy and random approach respectively.

Average resource usage results for proposed framework versus random and greedy approach are shown in Fig. 8. It can be seen from this figure that the average number of resources increase with increase in number of users. Moreover, it can also be observed from this figure that the random approach requires, on average, the largest resources while the proposed framework requires the least number of resources while giving the overall throughput results. Results in Fig. 8 show that the proposed framework, on average, requires 3% and 13% fewer resources as compared to the greedy and random approach, respectively.

6 Conclusion

IoT is the next big thing in the domain of science and technology. Its role is increasing exponentially in human lives with each passing year, and this trend is not going to slow down any time soon. Because of the critical nature of the data handled by IoTs, an IoT-based system is an

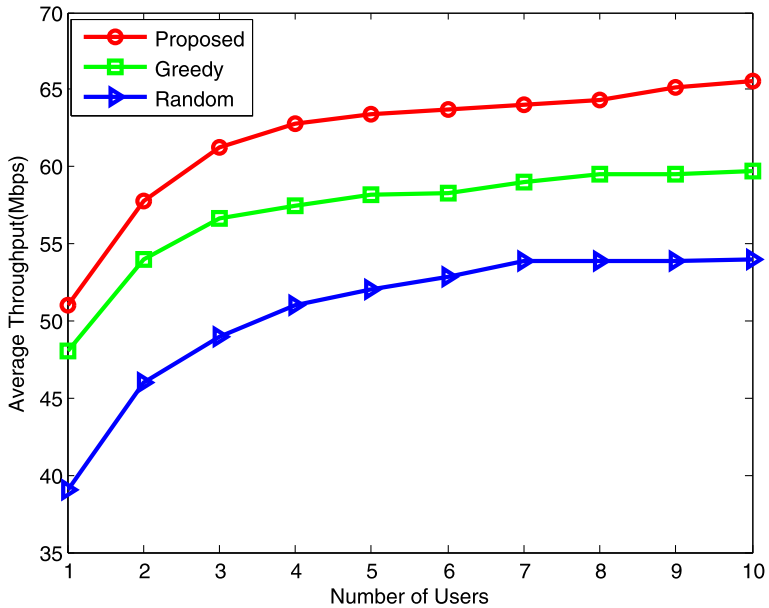

Fig. 7 Average throughput results for proposed framework versus greedy and random approach

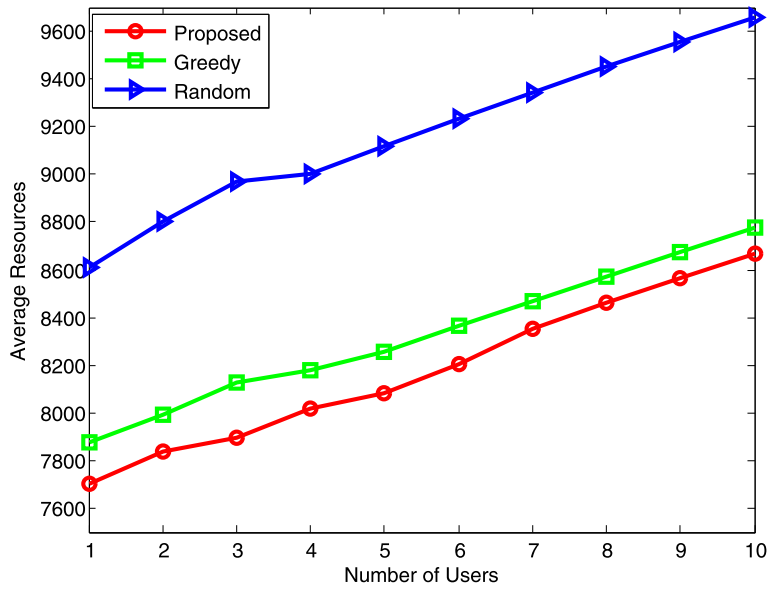

Fig. 8 Average resource results for proposed framework versus greedy and random approach

attractive target for malicious attackers. However, because of the limited resources of IoT devices, researchers face a difficult task of making an IoT-based system secure. In this work, we formulated a weighted optimization function to secure the IoT devices. Among a pool of available cryptographic implementation schemes of AES, this optimization function assigns values to them based on their weights. We next propose an adaptive framework that considers the heterogeneous nature of IoT devices and metrics of different implementation schemes. The adaptive function maps the AES implementation schemes to the IoT devices using a modified bipartite matching graph. During mapping, the core objective is to optimize the throughput of the IoT-based system while using the minimum resources. This mapping process is optimized using Hungarian algorithm. We perform extensive experimentation using the proposed framework. Comparison is also performed between the results of the proposed framework and those of the random and greedy approach. Analysis of the results shows that the proposed framework provides, on average, 11% and 17% better average throughput and 3% and 13% better resource usage results as compared to the random and greedy approach, respectively.

In this work, we consider two optimization parameters only. In the future, we would like to extend this work to multiple objectives like fairness and energy and power consumption parameters. Moreover, we would extend the current work from single network scenario to multi-network scenario as well.

Abbreviations

AES: Advanced Encryption Standard; DoS: Denial of service; IoT: Internet of Things; WSN: Wireless sensor networks

Acknowledgements

Not applicable.

Authors' contributions

UF worked on the overall writing of the paper. He also worked on the design and simulation part. NUH worked on the manuscript review, data gathering, and simulation analysis of the results. IB worked on the design part of the problem, the optimization of the techniques, and manuscript writing of the paper. NS worked on the analysis of the results, design and optimization of the problem, and overall manuscript improvement of the work. All authors read and approved the final manuscript.

Funding

No funding was received for this research work.

Availability of data and materials

It is not applicable to this article as it mandatory for biology and medical journals only.

Competing interests

The authors declare that they have no competing interests.

Received: 18 January 2019 Accepted: 7 August 2019
Published online: 27 August 2019

References

1. D. Singh, G. Tripathi, A. J. Jara, in *2014 IEEE World Forum on Internet of Things (WF-IoT)*. A survey of internet-of-things: Future vision, architecture, challenges and services, (2014), pp. 287–292
2. L. Atzori, A. Iera, G. Morabito, The internet of things: A survey. Comput. Netw. **15**, 2787–2805 (2010). http://doi.org/10.1016/j.comnet.2010.05.010
3. A. Mosenia, N. K. Jha, A comprehensive study of security of internet-of-things. IEEE Trans. Emerg. Top. Comput. **5**(4), 586–602 (2017)
4. A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, B. B. Gupta, Efficient iot-based sensor big data collection–processing and analysis in smart buildings. Futur. Gener. Comput. Syst. **82**, 349–357 (2018)
5. C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi, B.-G. Kim, et al., Algorithms for efficient digital media transmission over iot and cloud networking. J. Multimed. Inf. Syst. **5**(1), 27–34 (2018)
6. V. A. Memos, K. E. Psannis, Y. Ishibashi, B.-G. Kim, B. B. Gupta, An efficient algorithm for media-based surveillance system (eamsus) in iot smart city framework. Futur. Gener. Comput. Syst. **83**, 619–628 (2018)

7. K. E. Psannis, C. Stergiou, B. B. Gupta, Advanced media-based smart big data on intelligent cloud systems. IEEE Trans. Sustain. Comput. **4**(1), 77–87 (2018)
8. M. Zhang, A. Raghunathan, N. K. Jha, Trustworthiness of medical devices and body area networks. Proc. IEEE. **102**(8), 1174–1188 (2014)
9. C. Li, A. Raghunathan, N. K. Jha, in *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system, (2011), pp. 150–156
10. D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, W. H. Maisel, in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses, (2008), pp. 129–142
11. C. Stergiou, K. E. Psannis, B. B. Gupta, Y. Ishibashi, Security, privacy & efficiency of sustainable cloud computing for big data & iot. Sustain. Comput. Inform. Syst. **19**, 174–184 (2018)
12. Y. Cherdantseva, J. Hilton, in *2013 International Conference on Availability, Reliability and Security*. A reference model of information assurance & security, (2013), pp. 546–555
13. S. Vashi, J. Ram, J. Modi, S. Verma, C. Prakash, in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. Internet of Things (iot): A vision, architectural elements, and security issues, (2017), pp. 492–496
14. H. Suo, J. Wan, C. Zou, J. Liu, in *2012 International Conference on Computer Science and Electronics Engineering, vol. 3*. Security in the internet of things: A review, (2012), pp. 648–651
15. M. M. Kermani, M. Zhang, A. Raghunathan, N. K. Jha, in *2013 26th International Conference on VLSI Design and 2013 12th International Conference on Embedded Systems*. Emerging frontiers in embedded security, (2013), pp. 203–208
16. H. Salmani, M. M. Tehranipoor, Vulnerability analysis of a circuit layout to hardware trojan insertion. IEEE Trans. Inf. Forensic Secur. **11**(6), 1214–1225 (2016)
17. A. M. Nia, S. Sur-Kolay, A. Raghunathan, N. K. Jha, Physiological information leakage: A new frontier in health information security. IEEE Trans. Emerg. Top. Comput. **4**(3), 321–334 (2016)
18. E. Y. Vasserman, N. Hopper, Vampire attacks: Draining life from wireless ad hoc sensor networks. IEEE Trans. Mob. Comput. **12**(2), 318–332 (2013)
19. B. Parno, A. Perrig, V. Gligor, in *2005 IEEE Symposium on Security and Privacy (S P'05)*. Distributed detection of node replication attacks in sensor networks, (2005), pp. 49–63
20. K. Hu, A. N. Nowroz, S. Reda, F. Koushanfar, in *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*. High-sensitivity hardware trojan detection using multimodal characterization, (2013), pp. 1271–1276
21. M. Feldhofer, S. Dominikus, J. Wolkerstorfer, *Strong Authentication for RFID Systems Using the AES Algorithm*. (Springer Berlin Heidelberg, Berlin, Heidelberg, 2004), pp. 357–370
22. U. Farooq, M. F. Aslam, Comparative analysis of different aes implementation techniques for efficient resource usage and better performance of an fpga. J. King Saud Univ. Comput. Inf. Sci. **29**(3), 295–302 (2017)
23. M. Jung, H. Fiedler, R. Lerch, in *Ecrypt Workshop on RFID and Lightweight Crypto*. 8-bit microcontroller system with area efficient aes coprocessor for transponder applications, (2005), pp. 32–43
24. S. Kulkarni, S. Durg, N. Iyer, in *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*. Internet of things (iot) security (IEEE, 2016), pp. 821–824
25. G. A. Mills-Tettey, A. Stentz, M. B. Dias, The dynamic hungarian algorithm for the assignment problem with changing costs. Tech Report (2007)
26. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): A vision, architectural elements, and future directions. Future Generation Computer Systems. **29**(7), 1645–1660 (2013). Special sections: cyber-enabled distributed computing for ubiquitous cloud and network services & cloud computing and scientific applications, big data, scalable analytics, and beyond. http://www.sciencedirect.com/science/article/pii/S0167739X13000241
27. CISCO, The internet of things reference model. CISCO, Tech. Rep. (2014). Available: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf
28. G. Zhang, T. Wang, G. Wang, A. Liu, W. Jia, Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system. Concurr. Comput. Pract. Experience, e5109 (2018). https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.5109

Publisher's Note