jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2019, VOL. 65, NO.3 , PP. 397-405
Manuscript received April 15, 2019; revised August, 2019. DOI: 10.24425/ijet.2019.129791

A New Trust Framework for E-Government in Cloud of Things

Hasan Abualese, Thamer Al-Rousan, and Bassam Al-Shargabi

Abstract— **The idea of using the Cloud of Things is becoming more critical for e-government, as it is considered to be a useful mechanism of facilitating the government's work. The most important benefit of using the Cloud of Things concept is the increased productivity that the e-governments would achieve; which eventually would lead to significant cost savings; which in turn would have a highly anticipated future impact on e-governments. E-government's diversity goals face many challenges; trust is one of the major challenges that it is facing when deploying the Cloud of Things. In this study, a new trust framework is proposed which supports trust with the Internet of Things devices interconnected to the cloud; to support the services that are provided by e-government to be delivered in a trusted manner. The proposed framework has been applied to a use case study to ensure its trustworthiness in a real mission. The results show that the proposed trust framework is useful to ensure achieving a trusted environment for the Cloud of Things for it to continue providing and gathering the data needed for the services that are offered by users through E-government.**

Keywords—**Cloud of Things, E-Government, Fuzzy Logic, Trust**

I. INTRODUCTION

E GOVERNMENT is considered nowadays as one of the vital fields in modern information technology. It facilitates the government's processes and enabling citizens and the public sector agencies to have easier access to government services. E-democracy services are characterized by being simple, aid in reducing the cost of operations and in saving time, and enhancing the effectiveness of services and increasing business productivity [1]. E-government enhances the transparency of the services that the government offers, as it enables the public to be aware of what the government is working on, in addition to the policies that it is attempting to implement [2]. The complexity and expansion of e-governments are increasing daily; therefore, the amount of their computational data is increasing as well. The increased demand for data and services by the citizens and the continuous progress in technology put the governments under a great deal of pressure to become more innovative .[3]

One of the new inventions is the Internet of Things (IoT). The IoT offers various opportunities for the e-governments to ease costs, boost citizen services, and to operate more efficiently and effectively. Internet of Things is becoming an adoptable technology for e-government systems. Projections for the impact of the Internet of Things on our daily lives are impressive; as some estimates indicate that by the year 2025, about a 100 billion of connected objects and devices will be in service, while the total global economic impact of IoT is expected to be more than $10 trillion [4].

IoT offers many applications in different domains, by being connected to everyday objects. IoT applications could be organized into three primary groups depend on their interests: "environment, society, and industry." Its application in the industry includes aviation and transportation, while healthcare and smart building are examples of the social aspects where IoT can be used. Some of the benefits that can be gained from its environmental applications include monitoring accessible drinking water and having the ability to control dangerous waste [5].

Cloud computing provides a platform for system resources, especially processing power and storage, available on-demand from anywhere and at any time [6]. So, we can use Cloud and IoT in the combine, in a way that would enable both features to complement each other; to have the Cloud of Things (CoT) as an outcome of their combination. Cloud computing and IoT are two different paradigms. By using both aspects in the combine, they complement each other by utilizing each other's characteristics [7]. Cloud computing can offer IoT a wide range of resources and competences while benefiting from IoT in terms of widening its own range.

The outcome would be the ability to apply this new technology in numerous lifetime scenarios. Some countries have already started using the Cloud of Things; as it has been used by the public sector in different aspects, with a notable benefit being achieved from its use. However, most countries are not harvesting the opportunities that Cloud of Things offers as described by [8]. The reason for not utilizing the Cloud of Things with the expected fruit is the vast number of challenges that e-government is facing; as these challenges slow its adoption by the public sector. One of the key challenges facing e-governments across the world is minimizing the uncertainty and risks which are related to security, privacy, trust, and the return of investment, as presented by [3].

Cloud of Things is a popular research field that not only brings opportunities to e-governments but also raises challenges. The security and trust concerns are critical issues that prevent e-government from adopting the IoT along with Cloud computing. In this study, we primarily focus on the importance of security and trust as critical issues that prevent e-government from adopting the Cloud of Things. We also attempt to propose a new trust framework to tackle the challenges which are related to trust. The framework composed of four layers. The trust layer providing a way to validate and authenticate IoT devices before connecting to Cloud to ensuring a trusted environment for Cloud of Things to continue providing and gathering data needed to provide services to users through the E-government services.

Hasan Abualese is with Faculty of Information Technology, Ajloun, National University, Jordan (e-mail: homouch@yahoo.com).

Thamer Al-Rousanis with Faculty of Information Technology, Isra University, Amman-Jordan (e-mail: thamer.rousan@iu.edu.jo)

Bassam Al-Shargabi is with Faculty of Information Technology, Middle East University, Amman-Jordan (e-mail: bassam_shargaabi@meu.edu.jo).

The rest of the study is organized as follows: Section 2 focuses on providing an overview of the Cloud of Things. Section 3 providing the related work. Section 4 describing the recent Cloud of Things and trust issues. Section 5 providing detail about the proposed framework. Section 6 includes experimental results. Lastly, a conclusion is presented in Section 7.

II. CLOUD OF THINGS

The World has witnessed a tremendous revolutionary change by introducing IoT and its applications, as that influenced every aspect of our lives. The year 1999 was when the idea of IoT was introduced, with a future vision of depending on computer-aided objects, rather than people, in data gathering and organization [9]. A vast number of technological applications can be incorporated by using IoT. Those technologies vary from personal devices to applications and servers, in addition to sensors or actuators. In other words, we can use this technology in collecting data from different sources, with the ability to aggregate, merge, analyze and process the collected data to obtain important actionable information to provide intelligent and complicated services. The future outlook of communications and computing will be reshaped by the revolution created by IoT [10]. IoT is a technology that is seen as a tool that would provide creative solutions for different existing systems. Among the systems that would benefit from this technology are the manufacturing systems, healthcare, smart systems to be used in street lighting and different home uses, besides its use in other applications, as described by [11].

The internet infrastructure is affected by the huge amount of data collected by the Internet of Things combined with the other big data already available. So, to ease that pressure, corporations are working to find solutions that would resolve the data obstacle, with the main part of these solutions being Cloud computing. Cloud computing possesses the ability of processing, managing and storing huge data; which in turn enables the utilization of these abilities to share and distribute the data generated by IoT devices and other sensors [12]. The way Cloud had become an essential part of the architecture of IoT is by enabling a convenient, scalable and on-demand access of the networks, to different devices and sensors, or other computing resources that are IoT configurable.

Two of the most important features of the upcoming internet are Cloud and IoT, as their combination creates what is known as the Cloud of Things. Cloud computing paradigm is inspired by the IoT paradigms where everything, specifically ‘smart things’, are completely connected to the internet and is integrated with Cloud computing. Cloud of Things facilitates the communication with all the services offered by Cloud computing which include the SaaS, IaaS and PaaS [11]. A cheap and guaranteed access to smart things has become achievable through CoT, in addition to being user-friendly and doable in a cost-effective manner. Although Cloud computing is a different paradigm from IoT, combining them bears the benefit of facilitating several advantages as reported in the literature [12],[13]. Figure 1 shows the way Cloud Computing interacts with the Internet of Things.

There is a complementary relationship between IoT and Cloud computing, as the two of them work to enhance efficiency in our daily life. The Internet of Things is generating an unmatched quantity of data, while Cloud computing offers paths for that data to move to its destination. Cloud can offer IoT the following advantages and benefits: Big data analysis and aggregation, availability, cost-saving “Pay for what you use”, effective management and the ability to control and supervise a variety of systems and services, and the ability to offer a solution which would assure an efficient method of implementation of IoT services, while guaranteeing resource management.

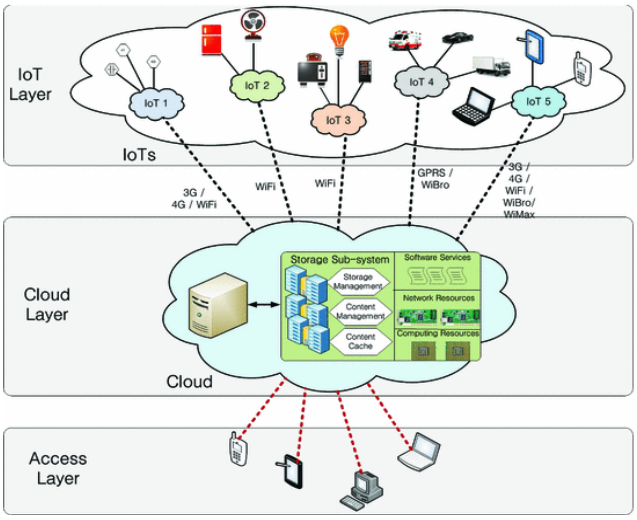

Fig.1.The interactions within Cloud of Things

The increased popularity of CoT, especially in e-government, is associated with several problems. The main problem which hurdles the incorporation of IoT with Cloud computing is trust, especially regarding security and privacy. Whereas, IoT includes a wide range of devices; which in turn would render these devices weak in the face of attacks, and leave them more susceptible to threats. Also, in most situations, sensitive data such as personal information and crucial infrastructures are stored by IoT devices, thus security and privacy within CoT are the two key challenges that shall be tackled [14].

Security and privacy are two highly related terms. Privacy is concerned with informational self-determination, which means that the information shall not be disclosed without its owner’s authorization. Alternatively, security is mainly concerned with confidentiality, integrity and the availability of the required information. Trust is a term closely related to security and privacy. Trust is concerned with the confidence that the information or the processes will be processed in the expected ways. Trust could be viewed as a result of progress towards security or privacy goals [15].

The widespread use of the internet, with a large number of users accessing the Cloud via IoT devices, has dramatically increased. CoT technology has become more prevalent and integrated into our daily life tasks. In e-government, users need to have the trust that CoT devices and associated data are protected. Weakly secured CoT devices can serve as a possible way in for cyber-attacks; which in turn would disclose the users’ data. Although literature had proposed many means to achieve security and privacy, none of them has comprehensively discussed these vital issues and the current practices which are used in CoT deployment [16]. So, collaborative security and privacy frameworks will be needed to develop effective and suitable solutions for the challenges facing CoT security and privacy, which will be well suited to e-government.

III. RELATED WORK

Literature provides different definitions of trust. According to a study by Girau and Atzori [17], trust identifies the degree of belief from the trusting party’s (trustor’s) point of view, taking into account a trusted party (trustee). This belief is recognized based on a certain trust feature which probably involves a risk or benefit. Therefore, trust is a direct link between two sides, among the giver (trustor), and the receiver (trustee).

The structure of CoT is foreseen to comprise billions of devices and users. This environment represents a dynamic where devices interact among each other and/or with the Cloud to access, manipulate, or communicate data. In this regard, trust is a critical feature that ensures that only authorized users and devices take part in these interactions. Also, the trust protects the CoT from physical attacks and any malfunctions of the devices [5]. As a result, the success of CoT highly depends on resolving the associated challenges with trust and reducing the uncertainties which affect CoT.

Several methods are proposed in the literature for calculating trust for CoT frameworks. For example, Kohlas et al. [18] present a trust evaluation method which is based on the theory of logic and probability. The reliability of a device is logically argued by applying the qualitative part of the mentioned method. Another method is proposed for computing the trust directly for the wireless sensor nodes based on the confidence interval concept [19]. In this method, the behavior of an adjacent node is observed over a considerable time; after which the trust value is determined. In [20], table-based trust storage criteria are utilized for each adjacent node, where it uses fussy logic to quantify the trust by depending on the honesty of recommendation provided by a sensor node, or by depending on the evaluation of past experiences.

A trust in service-oriented CoT systems presented by Guo and Chen [21]. They discussed the malicious attacks threaten CoT. They also proposed a model for facing these threats based on trust classification and trust aggregation for several attributes of social trust. The challenges related to protecting the privacy of the user discussed by [22]. The study investigated the privacy challenges between CoT and regular networks. The asymmetric encryption model proposes by [23]. He used encryption procedures to classify the shared authentication to protect data within the CoT environment.

Another approach is suggested by Zhang et al. [24] for trust-based control. The three layers which form the base of the proposed trust model include the device and request, in addition to the access control. The request layer is where the calculation of a trust score value of one device or more takes place, as that calculation is based on three attributes; knowledge, experience, and recommendation. A membership function is specified for the semantic values of these attributes over the set of all possible values. Also, fuzzy values are transformed into a crisp value using the concept of Center-of-Gravity (COG), which is one of the most popular methods for defuzzification. Compared with traditional access control, the proposed framework attains better results regarding lower energy consumption. Another trust model is proposed by Mai et al. [26], which is established upon subjective logic. The proposed model offers a series of particular operators for computing the value of trust. Nevertheless, the delegation of authorization has made a wrong choice due to the absence of a centralized server, and due to its restricted resources.

Entropy function represented a new trust model between two nodes [26]. This model helps compute the trust dynamically, although many studies consider this model slow. In Kauchak and Leroy [27], the authors discussed the relationship between user privacy and trust, but the practical implantation is missing. Another Theoretical trust model represented by Sriram et al. [28], discussed the trust control in CoT without performance measures. Also, an approach presented by [29], where the trust score is computed based on validating the monitored attribute before altering the trust score. Their approach relies on the hysteresis-based algorithm.

IV. CLOUD OF THINGS AND TRUST

Trust can be looked at as a relation between the so-called trustor and trustee. In CoT, trust is commonly referred to in terms of identification and authentication [12]. The process of claiming the identity by a device or an object takes place in the identification process; while checking the claim and the daily life activities happen in the authentication process. Validating the user's identity is the major goal of both processes; "identification and authentication" [30]. Cloud's resources are useful for confirming the user's identity by using the authentication process, which is achieved by confirming some of the user's unique features. Among the helpful features is the recognition of the user's voice and face, in addition to the secret codes, and drawing patterns. The user authentication permits which are organized into various groups by Chang et al. [9] are described below:

- **Something is known by the user or by you.** This kind of authentication approach is to deal with shared data among the interconnected devices. It is commonly approached by authenticating a password, confirming drawing patterns on devices with screens, and by recognizing graphical images. The mentioned methods are inefficient to exchange the use of usual password identification; because there is no sufficient security benefit achieved by using these approaches [13].
- **A thing a user is or what you are.** An identification approach which uses modern biometric information. It includes fingerprints, a scan of the face, and the voice. The risks of the use of biometric data are among the disadvantages of such an approach. Along with the possibility of information theft, copying or exploiting; to be used for counterfeiting; due to the uniqueness of the biometric data when used as a password [31].
- **Something a user or you have.** Information from the user as a true item (token) is another identification method. This approach uses a Universal Serial Bus (USB) stick, a smart card, or a serial tap; which are means that are used to store the secret of the user. Memorizing a secret (as in the case of The Password) is not required to grant authorization to the right person [32]. The disadvantage of such a method is the difficulty of y of identifying the real user; because of the number of things that are shared amongst users. Besides the fact that those things could be stolen or lost.

The authentication of devices represents another essential aspect in CoT; since they have a big role in the interactions which take place within the CoT technology. Device authentication is a security procedure that is applied to assure that just "IoT authorized" devices can connect to, or communicate with CoT [30]. As the device is defined by a unique value, it does not require to be changed through the life of a product, and the value can be added through device production. Device's authentication approaches can be classified into different groups as suggested by Boatwright and Luo [33]. Those approaches are described below:

- **Something which is distinctive to a device.** The IoT device identity is approved or determined in this procedure by relying on credentials, or by physical contact. These credentials are thought of as being based on context, rather than on identity [20].

- **Something which the device possesses.** The IoT device is used in this approach to storing a secret key; as the secret key needs to be provided to identify the user's identity (same term as "something which a user has"). The IoT device, in this case, is automatically used, without the need for the user's presence. So, the secret which is saved in the IoT devices is required for the identification of both the user and the device [34].

E-government benefits a lot by employing the Cloud of Things to enhance its services and make them more efficient. In e-government, the user's security, in addition to the privacy's expectations and rights, is essential to guarantee the user's trust in the e-government services and its related devices. Several studies emphasize the importance of trust in e-government. Literature has several interpretations of trust. CoT deals with a big number of loosely connected things and devices that are scattered in an uneven pattern over a specific area. The number of communication devices is constantly growing, users, especially in e-governments, need proper trust methods to interconnect different objects and identify them.

V. PROPOSED CLOUD OF THINGS TRUST FRAMEWORK

In this section, the proposed CoT trust framework for e-government is presented, which mainly focuses on tackling the issues that relate to the IoT device or sensor identification and authentication process with CoT in e-government; by introducing a trust layer as illustrated in Figure 2. In the proposed layer, authorized users and devices are identified and given access to the cloud. Authenticating users and devices can be performed in this layer via several methods. The first function is performed in the authentication layer which focuses on checking the IP address or Mac address of any device connected to IoT. Then match it with the address which is previously defined in the Cloud domain. The function of user identification is performed as soon as the two addresses match.

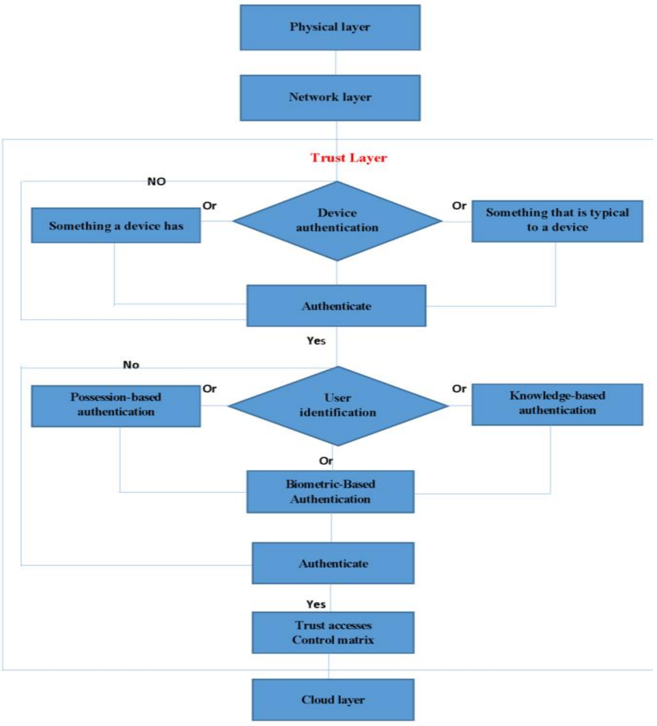
Physical layer
Network layer
Trust Layer
NO
Or
Something a device has
Device authentication
Or
Something that is typical to a device
Authenticate
Yes
No
Or
Possession-based authentication
User identification
Or
Knowledge-based authentication
Or
Biometric-Based Authentication
Authenticate
Yes
Trust accesses Control matrix
Cloud layer

Fig.2. E-government trust framework for Cloud of Things

The main four components of the proposed framework are described below:

A. The Physical Layer

The vision of the Internet of Things is to connect each object which possesses communication, computing, and sensing capabilities, to the Internet [35]. The first layer as demonstrated in figure 2 is the things layer which holds a diverse range of devices; from Radio Frequency Identification (RFID) tags, cars, sensor nodes, and even shoes. The primary goal of this layer is information collection, and to deliver the collected information to the above layer. Its role is crucial; as it is considered to be the proposed framework's ears [31].

B. The Network Layer

The network layer's main purpose is collecting the information from "the physical layer"; then delivering it to the next layer. The network layer backbone is the wireless sensor networks, where the data is transmitted to the host after connecting with IoT devices or sensors. It works by assigning a specific Internet Protocol (IP) for every object in IoT, which is applied later to authenticate the data.

C. The Trust Layer

Trust layer in the proposed framework acts as an intermediate layer, where the IoT devices and additionally people who are linked to the "IoT network," become able to access the information which is saved in Cloud. There are two consecutive stages to get the authorization, as follows:

1) Devices authentication

This security technique is applied to assure that just the authorized devices are able to connect with the Cloud of Things. It needs certification or physical connection (IP or Mac address), which signals for authenticating or distinguishing the devices, as explained before. Therefore, whenever an IoT device or sensor attempts accessing the data saved in the Cloud, a test of validation is carried out. An IP or Mac address is assigned to each device in the trust layer. Accordingly, the IoT objects will be granted authorization; provided that the address assigned to the object in the Cloud is identical to its counterpart from the incoming object. Several threats may take place by only relying on the authentication of devices, such as in the cases of device theft or if it gets lost. If any of these cases happen, the unauthorized person who possesses the device will have full access to the account and the information which is related to it. In our model, this issue is resolved by relying on another authentication technique, which is called the "Identification Method", as described below.

2) The Identification method

This stage requires validating the user to guarantee that the rightful user is granted the authorization. Unique personal features are used to guarantee that he/she is granted access. Among such features is recognizing the face or voice, secret codes and drawing patterns, in addition to the graphical pictures feature. A process of validating the user is applied to identify the user; depending on comparing the user's input, with what had been previously registered in the Cloud domain. If both have the same patterns, the authorization is granted. When biometric information is used as an identifying pattern; then the chances of a possible threat through theft and "copy making" would vanish. Precise results are secured when biometric features are used; because these features are incomparable and non-replicable. Accordingly, trustworthiness and privacy are assured. The data in the Cloud will be accessible to the user or devices after the trust test is successfully passed, or after identifying the user or authenticating the device. After performing the function, access to the trust matrix is authorized via the Access Control Matrix (ACM); as it is formed by "user-role pair matrix," where the privileges to gain access are related to roles [36]. Depending on the device classification, different users have different rights; where some users have elaborated review, while others get fewer details.

3) Device classification

Cloud of Things holds a diverse range of devices in virtue of the slogan "everything has to connect to the Internet", so the environmental parameters in terms of context information play a significant role in clarifying what is significant regarding the interaction between devices, or between users and devices. Context information could be given by a single parameter or more. The parameter is a specific common feature like the type of the device or its IP address. These parameters are very crucial to distribute the CoT network to a huge sum of devices. Device classification is the parameter which is used by our trust framework to determine the trust, and then achieve access control to the cloud layer.

The proposed trust framework is implemented to ensure that only trusted data could enter the Cloud layer; which is why the CoT devices were classified in the trust layer according to the trust authentication. The classification methods are used in this framework along with the following authentication methods:

- **In first dimensions,** three user authentication methods are used which are based on three different features; knowledge, possession, and biometrics.
- **In the second dimension**, device authentication is achieved depending on something characteristic to the device (something the device is) or depending on something the device has.

By this trust authentication classification, six classes are introduced: A, B, C, D, E and Class F. For example, Class A follows: knowledge-based authentication in the first dimension for the user's authentication, in addition to following the second dimension for device authentication; which is something characteristic to the device. Figure 3 shows the result of CoT devices classification according to trust authentication.

.

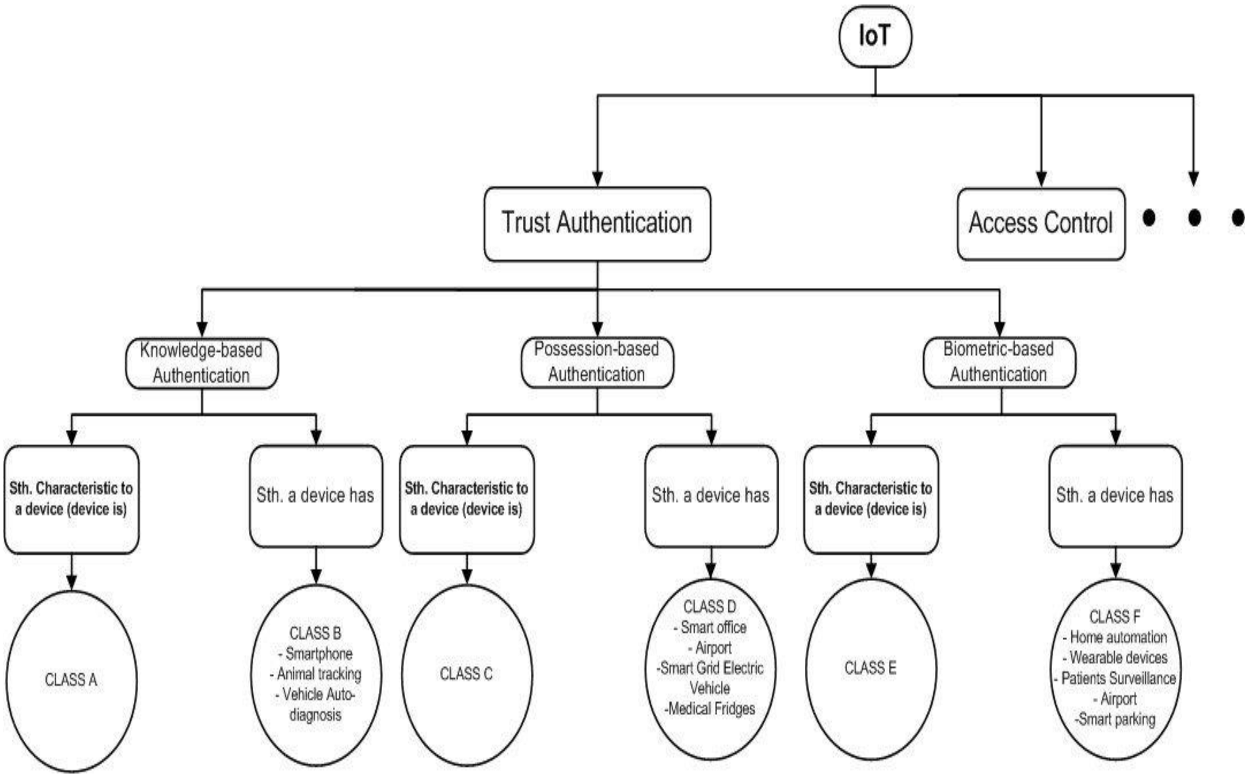
IoT
Trust Authentication
Access Control
Knowledge-based Authentication
Possession-based Authentication
Biometric-based Authentication
Sth. Characteristic to a device (device is)
Sth. a device has
Sth. Characteristic to a device (device is)
Sth. a device has
Sth. Characteristic to a device (device is)
Sth. a device has
CLASS A
CLASS B - Smartphone - Animal tracking - Vehicle Auto-diagnosis
CLASS C
CLASS D - Smart office - Airport -Smart Grid Electric Vehicle -Medical Fridges
CLASS E
CLASS F - Home automation - Wearable devices - Patients Surveillance - Airport -Smart parking

Fig. 3. CoT devices classification according to trust authentication

There is adversity in the range of devices which are communicating with each other in the CoT network, the number of these devices is unknown; therefore, the resulting uncertain environment requires achieving the device classification as the first step which would enable accomplishing access control. The user's life and daily activities are enhanced and simplified by an important role which is played by the relation between trust and cloud. So, the Cloud will need to assign a privilege to each class before any service is delivered. Adequate privilege of devices in CoT is critical to provide complete trust [37], [38]. Such cases could be handled by a trust calculation of the CoT devices, which is fuzzy-based.

The second step defining the trust value is for each of these classes. Cloud will assign a privilege to each class by comparing its calculated trust value and the predefined trust threshold for each type of the given privileges. Figure 4 shows the proposed classification strategy in addition to the use of fuzzy logic to calculate the trust values for each class.

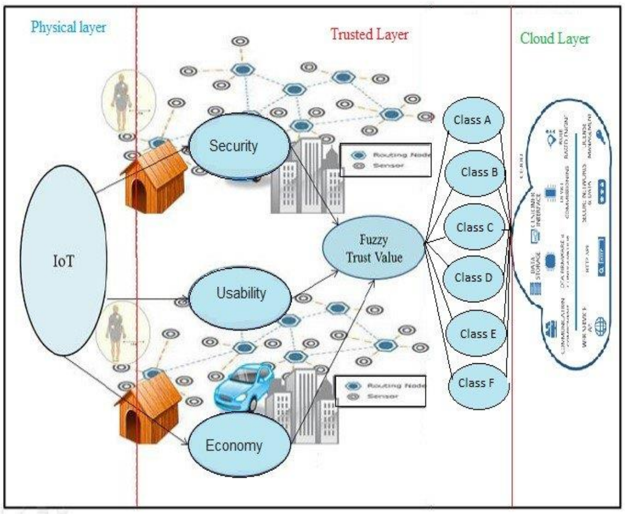

Fig. 4 An augmented fuzzy-based trust calculation model for the trustworthy framework

The linguistic variables are used to quantify the trust for each class based on the membership functions specified for these variables. Each class is evaluated against attributes that contribute to the overall trustworthiness of that class. These attributes are the security, usability, and economy, which are described in experimental results.

This device classification is helpful to design an efficient policy in e-governments. Based on the devices' classification, it is simple to apply suitable services to the users in e-governments and to design an efficient policy for each class of devices resulting in an efficient solution for e-governments.

D. Cloud Layer

The Cloud layer is the final layer of the projected framework, where the data is stored and manipulated. Depending on the end product of the trust layer, initiation, control, and command are considered as the main objective of this layer. It is where computing the network layer's data takes place. It plays the role of the service provider's platform, as it also plays the role of being the portal web where the users can join, in addition to its role of removing and observing people's things. Cloud is the location where numerous devices can join through registration in that layer; it is also where the devices will be granted identification by device authentication (IP address), and via user authentication; as it was previously revealed in the trust section. The purpose of all these authentication techniques is ensuring trust and secure authentication.

VI. EXPERIMENTAL RESULTS

A common scenario for CoT (actuators, sensors, RFID, etc.) is to be used in e-government space and to be applied in E-Health. Its main goal is to simplify life activities; including "health services efficiency" in terms of both geographic and time obstacles. Smart health care is an important aspect. Health sensors could be worn on the body or in our living environments; which would gather information related to our mental and physical health. This information makes a positive modification in the aspect of health care.

Patient surveillance is presented here in terms of a case study to validate and evaluate the proposed framework. The devices which are wearable by the patients; consist of sensors, detectors, and actuators; as they enable the doctors to monitor the patient's health state, including skin temperature, respiratory rate, and blood pressure. The wearable device is considered as an equivalent to the physical layer of the trustworthy framework. The devices are linked to the Internet via Wi-Fi as authenticated users are allowed access to them to perform a set of activities which are shown in Table I. For instance, access code (001) as privileges; means this device can gain full access to Cloud; to read and write data in that layer. Therefore, the access control which is permitted to the device is based on access level privileges given to each device; and is divided into six classes (A-F).

The CoT device connection starts by establishing the setting in which; data from the device is collected and communicated to the trust layer through the network layer. The trust layer in this framework ensures that only authorized people can enter and check the patient's state; such as the patient's doctor, one of his family members or the patient himself; by authenticating both the devices and the users. For this scenario, doctors or physicians generate a request message to check the patient's state via an application installed on the device. The device is authenticated by matching its characteristic with the one stored in Cloud. If the device's identity is approved, access is authorized to that device. The second stage is set thereafter for user authentication. Users are authenticated by asking them to first provide credentials in the form of fingerprint recognition. This initiates a call to the authenticator which matches the supplied credentials against the list of authorized users. As a result, another call is sent back to either accept or reject the access request. In the trust layer, classification is carried out according to calculated trust value and the predefined trust threshold for each type of the given privileges. In the e-Health scenario, six classes are obtained which are based on the access level. As described in Table I; the six classes are A, B, C, D, E and F. The privileges for each class are granted according to the trust level values for each class.

TABLE I-

PRIVILEGE CONTROL ACCESS MATRIX

"Access Level"	**"Access Code (bits)"**	**"Privileges of Device"**	**"Privileges Of Users"**
1	001	"Read, write and complete access"	Physicians
2	010	"Read, write and limited server(s) access"	Nurses
3	011	"Read, write access"	Specialist
4	100	"Read, Write Access"	Pharmacist
5	101	"Read, Write Access"	Laboratory
6	110	"Read, Access"	Patients

In the aforementioned scenarios of use for Patients Surveillance in public Hospitals, the proposed framework was implemented and evaluated using the fuzzy-logic toolbox in MATLAB to calculate the trust for each class based on a set of rules; which identify the relationship among the performance indicators. The obtained classes are to be evaluated against a set of performance measures that reflect how well these attributes are satisfied by a class in reality. In this paper, security, economy, and usability are used to evaluate a specific class and are given linguistic values such as poor, fair and good. The linguistic variables are used to quantify the trust for each class based on the membership functions specified for these variables. Table II shows the linguistic value of usability, security, and economy; as L is denoted for the linguistic variable. A membership degree in the interval [0, 1] is introduced in this study; where 0 confirms that there is no membership, and 1 reveals to full membership.

TABLE II
LINGUISTIC VALUE OF USABILITY, SECURITY, AND ECONOMY

L(Usability)	L(Economy)	L(Security)	Crisp Range	Fuzzy Numbers
Poor	Poor	Poor	Below 0.2	(0,0,0.2,0.4)
Fair	Fair	Fair	0.4-0.6	(0.3,0.4,0.6,0.8)
Good	Good	Good	Above 0.8	(0.7,0.8,1,1)

Each class is evaluated against those attributes which contribute to the overall trustworthiness of that class as presented below:

Security: This attribute is required to represent the safeguarding of the connected users and devices to CoT, ensuring that only authorized users and devices are given access to the CoT network. The security of a specific class is assessed based on its ability to prevent impersonation by an attacker and to prevent theft. The crisp range and the fuzzy numbers of security are defined in Table II.

Usability: Assessing the usability of the authentication methods which are proposed in this framework is based on the ease of operation and the need for special hardware. The crisp range and fuzzy numbers of Usability are defined in Table II.

Economy: It is often regarded that the most expensive authentication methods should be more secure. However, the cost of deploying an authentication method depends on several factors as in this framework. The cost of implementing each class is assessed based on the initial capital cost and the running cost. The crisp range and fuzzy numbers of the economy are defined in Table II. Based on these linguistic variables, trust is defined in Table III and its corresponding membership function is presented in Figure 5.

TABLE III
FUZZY TRUST VALUE

Linguistic Trust	Range	Fuzzy numbers
Poor	Below 0.2	(0,0,0.2,0.4)
Fair	0.4-0.6	(0.3,0.4,0.6,0.8)
Good	Above 0.8	(0.7,0.8,1,1)

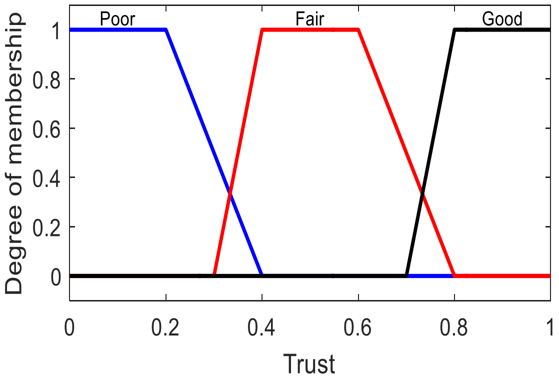

Fig. 5. Membership Function for Trust

The Mamdani-type fuzzy rule-based model is used which deals with the linguistic values of security, usability, and economy where vagueness is inherent. The output of this model is conveyed as a fuzzy set. The defuzzification process is used to convert the fuzzy value of the trust to a crisp value. The Mamdani scheme represents a type of fuzzy relational model where an If-Then relationship is used to represent each rule. For each of the linguistic variables (i.e. security, usability and economy), three linguistic terms have been assigned (i.e. Good, Fair, Poor). As a result, 27 rules are induced to thoroughly investigate the performance of trust across all possible combinations of these variables. These rules are summarized in Table IV.

The input and output variables are defined using the fuzzy logic toolbox in MATLAB. The Mamdani trust model used in this experiments is shown in Figure 6. The representation of the membership function for each interval of the linguistic variables is used as shown in Table III. The rules are also specified as described previously in Table IV. The crisp values of security, usability, and economy for each class are used to calculate the crisp value of the trust. Table V shows the results as shown below the calculated crisp value of the trust for each class.

TABLE IV
TRUST RULES

Rule	Security	Usability	Economy	Result
1	Poor	Poor	Poor	Poor
2	Poor	Poor	Fair	Poor
3	Poor	Poor	Good	Poor
4	Poor	Fair	Poor	Poor
5	Poor	Fair	Fair	Fair
6	Poor	Fair	Good	Fair
7	Poor	Good	Poor	Poor
8	Poor	Good	Fair	Fair
9	Poor	Good	Good	Good
10	Fair	Poor	Poor	Poor
11	Fair	Poor	Fair	Fair
12	Fair	Poor	Good	Fair
13	Fair	Fair	Poor	Fair
14	Fair	Fair	Fair	Fair
15	Fair	Fair	Good	Fair
16	Fair	Good	Poor	Fair
17	Fair	Good	Fair	Fair
18	Fair	Good	Good	Good
19	Good	Poor	Poor	Poor
20	Good	Poor	Fair	Fair
21	Good	Poor	Good	Good
22	Good	Fair	Poor	Fair
23	Good	Fair	Fair	Fair
24	Good	Fair	Good	Good
25	Good	Good	Poor	Good
26	Good	Good	Fair	Good
27	Good	Good	Good	Good

In Table V, column 2 represents fuzzified trust value based on the defined 27 rules. These fuzzy trust values are mapped to privileges for each devices within each class , and as Table V shows that the devices within classes F and E has the higher trust values, which is related to the higher values of linguistic terms that is based on devices trustworthiness with reference to security, economy and usability as linguistic variable. Moreover, as the trust value influenced by devices crisp and fuzzy value assigned to each linguistic variable. We may set more linguistic terms like Very Bad, Very Good, and Below Average etc. As we are dealing with linguistic terms, the growing number devices does not impact on the performance of devices which making the proposed framework more flexible.

The fuzzy logic toolbox is used to define the input and output variables in MATLAB. The Mamdani trust model used in this experiment is shown in Figure 6. The representation of the membership function for each interval of the linguistic variables is used as shown in Table III. The rules are also specified as described previously in Table IV. The crisp values of security, usability, and economy for each class are used to calculate the crisp value of trust. Table V shows the results with the calculated crisp value of the trust; for each class.

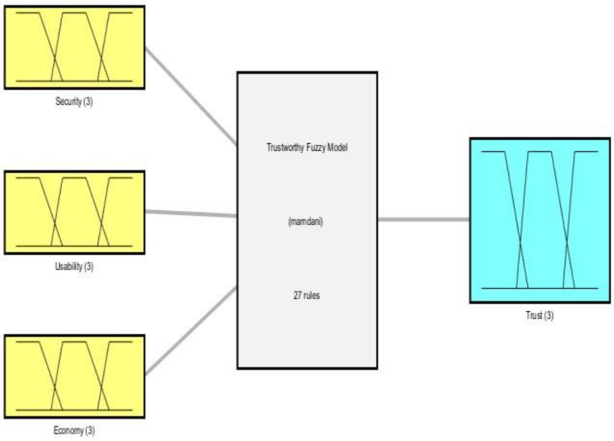

Fig. 6. Mamdani Fuzzy Trust Model

TABLE V
TRUST VALUE IN CLASSES

Class	Trusted Value
Class A	0.258
Class B	0.32
Class C	0.538
Class D	0.684
Class E	0.813
Class F	0.876

In table V, column 2 shows the fuzzy trust values; based on the outlined 27 rules. These values are then translated to privileges for each device within each class, and as table V shows, the devices within classes F and E have the higher trust values, which is related to the higher values of linguistic terms that are based on the devices trustworthiness with reference to security, economy, and usability as linguistic variable. Moreover, the trust value is influenced by the crisp and fuzzy values of the devices which are assigned to each linguistic variable. More linguistic phrases could also be set, like Very Bad, Very Good, Below Average, etc.; making the proposed framework more flexible

VII. CONCLUSION

With the fast-growing pace of technology, the future seems to hold a big role for The Cloud of Things in supporting many e-government systems. Governments, businesses, and citizens can achieve great benefits from the Cloud of Things. Simultaneously, the Cloud of Things raises important challenges that may well stand in the way of achieving its possible benefits. Trust is a major challenge when deploying a Cloud of Things in e-government. In this paper, a new framework is proposed that supports trust communication amongst the Internet of Things devices and cloud; in order to support e-government services to be delivered in a trusted manner. The framework is composed of four layers. The trust layer provides a way to validate and authenticate IoT devices before connecting to Cloud; to ensure a trusted environment for the Cloud of Things; which will enable it to continue providing and gathering data that are needed to provide services to users through E-government services.

In the trust layer, the CoT devices are first authenticated using different methods to guarantee that the data is transferred in a secure and trusted manner between the devices and the cloud. The authentication process as proposed in this framework is divided into different classes, and each class has its own authentication method to differentiate the access control for each device based on its classes. The obtained classes are to be evaluated against a set of performance measures that reflect how well these attributes are satisfied by a class in reality. The security, economy, and usability are used to evaluate a specific class and are given linguistic values such as poor, fair and good. The linguistic variables are used to quantify the trust for each class based on the membership functions specified for these variables. Accordingly, to evaluate the trust of each device based on its class, the Mamdani-type fuzzy rule-based model is used to calculate the trust for each class based on a set of rules which are used to identify the relationship among the performance indicators. To validate and ensure the feasibility of the proposed framework, the e-health use case has been applied to ensure the trustworthiness of the proposed framework in a real mission.

REFERENCES

[1] B.Al-Shargabi, “Security Engineering for E-Government Web Services: A Trust Model,” *in Proceedings of the Information Systems Engineering (ICISE)*, 2016,pp.33-45.

[2] D.Miorandi and S. Sicari, “Internet of Things: Vision, Applications and Research Challenges,” *Ad Hoc Networks*, vol.10, no.7, pp.1497-1516, 2012.

[3] S. Nirmala, and S. Sachchidanand, “Internet of Things (IoT): Security Challenges, Business Opportunities & Reference Architecture for E-commerce,” *in Proceedings International Conference on Green Computing and Internet of Things (ICGCIoT)*, Noida, India, 2016, pp.223-229.

[4] T.Al-Rousan, “*Cloud Computing for Global Software Development: Opportunities and Challenges*,” in Transportation Systems and Engineering: Concepts, Methodologies, Tools, and Applications IGI Global, 2015, pp. 877-908.

[5] R.Khan, S. Zaheer and F.Khan, “Future Internet: The Internet of Things Architecture, Possible Applications and key challenges,” *in Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT)*, 2015, pp.256-259.

[6] C. Buzduga and C. Ciufudean, “Internet of Things for Flexible Manufacturing Systems Diagnosis,” *in Proceedings of the 5th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*, Rome, Italy, 2017, pp.119-125.

[7] A.Serbanati, A. Segura, O. Oliverau, A. Saied and y. Gruschka, “*Internet of Things Architecture, Concept and Solutions for Privacy and Security in the Resolution Infrastructure*,” EU project IoT-A, Project report D4 ., pp. 2012, 346-391.

[8] D.Chen, d. Chang, l. Jin and J.Ren, “A Novel Secure Architecture for the Internet of Things,” *in Proceedings of the International Conference on Genetic and Evolutionary Computing (ICGEC)*, 2016, pp.78-85.

[9] K. Chang, C. Chen, J. Chen and H. Chao, “Internet of Things and Cloud Computing for future Internet,” *in Proceedings of the Security-Enriched Urban Computing and Smart Grid, Berlin Heidelberg*, 2017,pp.189-191.

[10] J. Zhou, T. Leppanen, E. Harjula, M. Ylianttila and T. Ojala, “Yang, “Cloud things: A Common Architecture for Integrating the Internet of Things with Cloud Computing,” *in Proceedings of the Computer Supported Cooperative Work in Design (CSCWD)*, 2015, pp.201-208.

[11] M. Shahzad and M. Singh, “Continuous Authentication and Authorization for the Internet of Things,” *IEEE Internet Computing*, vol 21, no.2, pp.86 - 90, 2017.

[12] C. Sarkar, R. Prasad, A. Rahim, R. Neisse and G. Baldini, “A Scalable Distributed Architecture for IoT,” *IEEE Internet of Things Journal*, vol 5, no.3 10, pp. 230-239, 2018.

[13] M. Ahlgren, M. Hidell and E. Ngai, ‘Internet of Things for Smart Cities: Interoperability and Open Data,” *IEEE Internet Computing*, vol 20, no.6, pp.52 - 56, 2016.

[14] A. Sheth, “Internet of Things to Smart IoT Through Semantic, Cognitive, and Perceptual Computing,” *IEEE Intelligent Systems*, vol 31, no.2, pp.108 - 112, 2017.

[15] T.AL-Rousan, A. AL-Zobadi and O. AL-Haj Hassan, “The Roles of Decisions Making and Empowerment in Jordanian web-based," *Journal of Web Engineering*, vol 15, no.(5&6), pp.469-482, 2014.

[16] R. Roman, J. Zhou and L. Lopez, “The Features and Challenges of Security and Privacy in Distributed Internet of Things,” *Computer Networks*, vol 60, no. 10, pp. 2266-2279, 2016.

[17] R. Girau and L. Atzori, “Trustworthiness Management in the Social Internet of things,” *IEEE Transactions on knowledge and Data Engineering*, vol 28, no. 5, pp. 1253-1266, 2016.

[18] Kohlas, J. Jonczy and R. Haenni, “A trust Evaluation Method Based on Logic and Probability Theory," *in Proceedings of the International Conference on Trust Management*, 2017, pp. 17-32.

[19] J. Mai, X. Shuai and Z. Wang, “Access Control Mechanism Based on Trust Quantification,” *in Proceedings of the Second International Conference on Social Computing*, 2016, pp.411-419.

[20] R. Roman, P. Najera and J, Lopez, “Securing the internet of things,” *Computer*, vol 49, no. 9, pp. 51-58, 2016.

[21] J. Guo and R. Chen, “A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems,” *in Proceedings of the IEEE International Conference on Services Cloud Computing (SCC),2016, Kiev, Ukraine*, pp. 324-331.

[22] D. Rotondi, and S. Piccione, “Managing access control for things: A capability based approach.,” *in Proceedings of the 7th International Conference on Body Area Network* , 2018, pp.192-201.

[23] Y. Sun, Z. Han and K. Ray, “Information Theoretic Framework of Trust Modeling and Evaluation for Ad-hoc Networks,” *IEEE Journal of Selected Areas in Communications*, vol 24, no. 2, pp.305-319, 2013.

[24] R. Zhang, Y. Zhang and K. Ren, “Distributed Privacy-Preserving Access Control in Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol 27, no. 1, pp.1427-1438, 2016.

[25] J. Mai, X. Shuai and Z, Wang, “Access control mechanism based on trust quantification,” *in Proceedings of the Second International Conference on Social Computing*, 2017, Dallas, USA, pp.411-419.

[26] M. Weyrich and E.Ebert, “Reference Architectures for the Internet of Things,” *IEEE Software*, vol 33, no. 1, pp.112 - 116, 2016.

[27] D. Kauchak and G. Leroy, “Moving Beyond Readability Metrics for Health-Related Text Simplification,” *IEEE Journals & Magazines*, vol 31, no. 4, pp. 41-51, 2016.

[28] N. Sriram, A. Premnat and J. Zygmunt, “Security and Privacy in the Internet of Things under Time-and-Budget-Limited Adversary Model,” *IEEE Wireless Communications Letters*, vol 14, no.3, pp. 571-583, 2018.

[29] Q. Hassan, “An Overview of Enabling Technologies for the Internet of Things,” in Proceedings of the Internet of Things A to Z:Technologies and Applications,Wiley-IEEE Press, 2018, pp148-173.

[30] M. Thiyagarajan and C. Raveendra, “Role of Web Service in Internet of Things,” *in Proceedings of the 3rd International Conference on Applied and Theoretical Computing and* Communication Technology (iCATccT), Tumkur, India, 2017, pp.35-42.

[31] T. Al-Rousan, H. Abualese, B. Al-Shargabi, “A New Security Model for Web Browser Local Storage,” International Journal of Advanced Computer Science and Applications (IJACSA), vol.10, no.8, 2019.

[32] H. Virdi and B. Singh, “Analysis of the Software Code based upon Coupling in the Software,” *in Proceedings of the 7th International Conference on Computing Communication & Networking Technologies (ICCCNT'18)*,Houston, USA 2018, pp.518-527.

[33] D.Singh, G. Tripathi and A, Jara, “A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Services,” *in Proceedings of the World forum on nternet of things (WF-IoT)*, 2017, pp.57-62.

[34] B. Al-Shargabi and O. Sabri, “Internet of Things an Exploration Study of Opportunities and Challenges,” *in Proceedings of the International Conference of Engineering and MIS* , Monastir-Tunisa, 2017, pp.263-269.

[35] E.Chowdary and D. Yakobu, “Cloud of Things (CoT) Integration Challenges," *in Proceedings of the Computational Intelligence and Computing Research (ICCIC)*, Roma. Italy, 2016, pp. 457-464.

[36] W. Karunianto and A. Saputro, “Design and implementation remote laboratory based on Internet of Things: Study case in diffraction grating experiment," *in Proceedings of the International Conference on Computer*, Keiv, Ukraine,2017, pp.398-408.

[37] T. Al-Rousan, “An Investigation of User Privacy and Data Protection on User-Side Storage,” *International Journal of Online and Biomedical Engineering (iJOE)*, vol.15, no.9,2019

[38] H. Takabi, J. Joshi and G. Ahn, “Security and privacy challenges in Cloud Computing environments,” *IEEE Security & Privacy*, vol 15, no. 6, pp.24-31, 2017.