Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 2 (2017) pp. 295-307
© Research India Publications
http://www.ripublication.com

An Efficient Architecture for Handling IoT in Trusted Environment

E. Padma
Research Scholar
SCSVMV University, Enathur
Kanchipuram, Tamil Nadu, India.

Prof. Dr. S. Rajalakshmi
Director, SJCAC
SCSVMV University, Enathur
Kanchipuram, Tamil Nadu

Abstract

All the information and activities are automated these days systematically in order to provide better and faster performance. With the growth of Internet, wireless communication has become more popular. In such cases, it requires more and more secure features to maintain the information safe and secure. When developing new research technologies, various metrics have been implemented to provide such secure trusted platform and to inspect the performance. TPM (Trusted Platform Module) plays a major role in today’s computer technologies to facilitate the secure mechanisms.

IoT (Internet of Things) has evolved from the convergence of wireless technologies and the Internet. The IoT links smart objects to the Internet, for handling the objects via Internet and mobile devices. IoT is being used in many aspects of day to day life. When the IoT have great extent in our daily life, it is necessary to provide security on the things to be handled via IoT. In order to provide such kind of security, we merge the TPM on IoT to trust the users handling the things. Thus, we have proposed a methodology to trust the users for handling the things via the Internet (i.e.,) IoT. Also, we have built an architecture to validate the users to handle the IoT.

Keywords: Internet, Internet of Things (IoT), Secure, Trusted Platform, Wireless Communication.

I. INTRODUCTION

Recently, the way we go about our daily lives has been fundamentally transformed by the growth and development of Internet and Smart Connected Devices. Each and every action of our daily life has been integrated with the computer and the Internet which paves the way to access all the things from anywhere and anytime. The main advantage of all the things being computerized is to store the information electronically without loss of data. This added richness and connectivity which also poses problem with security due to increased intrusion. There is a need to provide more security on our data to avoid unwanted access by unauthorized users.

A. Trusted Platform Module (TPM):

In order to provide security on information, we must be able to implement some advanced technology to safeguard the stored information. One such security technology has emerged from Trusted Computing Group which addresses the increasing set of software threats, called Trusted Platform Module (TPM). The TPM can work on any device to provide security and enhanced services to users. The idea of trusted computing was introduced in order to respond to the users' concern on whether their data is protected and secured while they are connected to a network.. TPM provides three various aspects such as:

- Protection on data
- Ensure the platform is trustworthy
- Allow the users to decide if it is reasonable to trust other networks.

TPM provides three main roots of trust which are:

- Root of Trust for Storage (RTS)
- Root of Trust for Administration (RTA)
- Root of Trust for Validation (RTV)

RTS stores the data safe and secure. RTA maintains and manages the stored data and RTV trust the users those who access the data. Thus the TPM provides the trusted platform to secure the data.

B. Internet-of-Things (IoT):

Now-a-days, we almost have been adapted with Internet Infrastructure to access any things from wherever and whenever needed. The Internet-of-Things (IoT) provides architecture for connecting the potential objects to interact with each other on the Internet. IoT takes all precautions for securing the devices which are connected together.

The IoT is built on many different objects to provide better performance and security requirements. The performance and security requirements vary considerably from one application to another. The usage of the IoT has some limitations such as Data Assurance, Robustness, Ease of use, Security and Reliability.

The greater volume of confidential data transferred over the IoT, has greater risk in securing the same from theft and device manipulation.

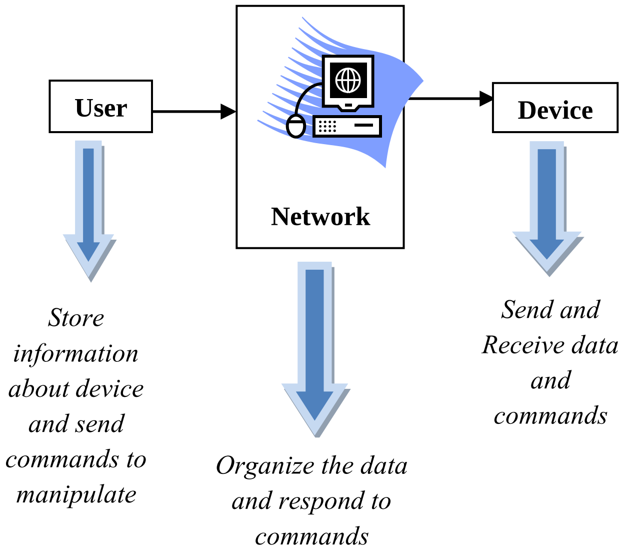
User
Network
Device
Store information about device and send commands to manipulate
Organize the data and respond to commands
Send and Receive data and commands

Fig-1: Data Manipulation through IoT

Sometimes, there may be some data leakage while handling things on IoT. This may happen due to accessing of devices by some unauthorized users. To avoid this kind of problems, we have proposed a new methodology with TPM on IoT in this paper.

C. Handling IoT with Trusted Platform:

TPM provides secure platform to access the data where as IoT allows the user to handle the device through Internet from anywhere and anytime. Thus, the proposed methodology integrates two technologies such as: TPM and IoT to handle the things on Internet in trusted platform, in order to provide more secure features and to maintain the data confidentially. The device on the Internet can be accessed only by the trusted users which can be authenticated through number of ways which will be discussed in our proposed method.

II. RELATED WORK

Han-Chuan Hsieh et al, in paper [1], discussed that the recent advances in sensing and wireless technologies exploited the Internet-of-Things (IoT) in various fields. The scale of IoT systems and the number of devices that they included had become huge and the construction of IoT applications is, therefore increasingly challenging. The paper proposed a script framework as a convenient development interface for Service Oriented Architecture (SOA) scheduling of web-based information of IoT applications, called ScriptIoT, which is composed of the IoT fundamental in case of all type of devices integration and a scriptable agent. The framework offers both polling an event-driven mechanism for delegating IoT applications to the agent and reporting event of the specified device and contributes to large-scale applications.

Jin Liu et al, in paper [2], stated about the Web of Things (WoT) environment and the web traffic logs which contain valuable information of how people interact with smart devices and web servers. Mining the wealth of information available in the web access logs has theoretical and practical significance for many important applications like network optimization and security management. They proposed a methodology to establish a graph by mining the temporal and casual information among aggregated HTTP requests.

Zhiyuan Li et al, in their paper [3] discussed the wide range deployment of disconnected delay-tolerant social Internet of Things (SIoT). They considered the preference similarity which is not determined in the existing search mechanisms and are designed in Cartesian Coordinates without sufficient consideration of real-world network deployment environments. They proposed a novel resource discovery mechanism in a 3-D Cartesian coordinate system with the aim of enhancing the search efficiency over the SIoT.

Qiang Tang, in his paper [4] considered a smart power model, where some subscribe share several energy providers and there are some malicious users in this power grid. The energy providers are managed by a power market scheduling center (PMSC), which broadcasts electricity price to subscribers and energy providers. In order to identify the malicious users and the unstable energy providers, the mechanism of identification and processing (MIP) for the malicious users and unstable energy providers was proposed. By integrating the MIP, they proposed a heuristic algorithm called the dynamic pricing algorithm with malicious users and unstable energy providers (DPAMU) to get the optimal electricity price as well as the optimal power requirement and the load capacity.

Ray et al, in paper [5] proposed a secure object tracking protocol to ensure the visibility and traceability of an object along the travel path to support the Internet of Things (IoT). The proposed protocol is based on radio frequency identification system for global unique identification of IoT objects. They evaluated the proposed protocol both quantitatively and qualitatively. They modeled the protocol using security protocol description language (SPDL) and simulated SPDL model using automated claim verification tool Scyther.

Ahmed Bader et al, in paper [6] promoted the use of multihop networking in the context of large-scale Internet of Things (IoT). Recognizing concerns related to the scalability of classical multihop routing and medium access techniques, they advocated the use of blind cooperation in conjunction with multihop communications.

They proposed an uncoordinated power control mechanism whereby each device in a blind cooperative cluster randomly adjusts its transmit power level.

Qie Sun et al, in paper [7] discussed about the significant increase in energy consumption and the rapid development of renewable energy such as solar power and wind power, have brought huge challenges to energy security and the environment, which in the meantime, stimulate the development of energy networks toward a more intelligent direction. They systematically reviewed the development and deployment of smart energy meters, including smart electricity meters, smart heat meters, and smart gas meters. The paper provided the insights and guidelines regarding the future development of smart meters.

KeshavSood et al, in their paper [8] considered the emergence of IoT which is a very challenging task, comprising information acquisition, information analysis, decision-making, and action implementation on large scale IoT networks. They started with the emergence of SDN and then highlight recent significant developments in the wireless and optical domains with the aim of integrating SDN and IoT. Challenges in SDN and IoT Integration are also discussed from both security and scalability perspectives.

Liang Liu et al, in their paper [9] analyzed and pointed out the key problem of IoT from the perspective of networking namely how to interconnect large-scale heterogeneous network elements and exchange data efficiently. They also presented some research progresses on three main aspects such as the basic model of IoT architecture, the internetworking mode and the sensor networking model.

III. PROPOSED METHODOLOGY

3.1 Proposed Method

The rapid development of the Internet technologies makes everything as computer-oriented. Each and every action in our day-to-day life has been computerized and can be accessible from anywhere. In such a way, IoT (Internet-of-Things) is a newly emerged computing concept which handles and manages the physical objects through Internet. In short, using IoT anything can be connected and communicated in an intelligent fashion via Internet. The physical object includes electronics devices, vehicles, buildings, and other items embedded with software and sensors. Through IoT, we can monitor and control the objects remotely across the Internet.

In our paper, we have proposed a methodology for implementing the concept of IoT in a much improved way. We have to sense the objects through the Internet along with the Mobile Phone, in order to provide improved user access with more security. While accessing the objects through mobile devices, if any interruption occurs, then there is a chance of loss of data. To overcome this kind of problems, we have to provide a solution by the way of sensing objects as web-based or cloud-based accessibility.

The aim of the paper is to propose an architecture to connect and communicate with the physical objects through mobile devices via the cloud with improved quality. The way how to implement the desired features can be explained below with suitable algorithm.

1. Applications of IoT:

IoT is a device connected via the Internet. Integration with the Internet implies that the devices will use an IP Address as a unique identifier. IoT can handle both sensory objects and actuation objects (e.g., bulbs or locks).

A. Auto Key Management:

A car can be handled remotely through sensor key to lock or unlock it. We have to extend this feature by adding security into it. That is, when we want to lock or open the car using the sensor key, it sends a message to the owner and waits for their acceptance. Only upon the owner accepts the message, the car will be opened or locked. Otherwise, the process has not been executed.

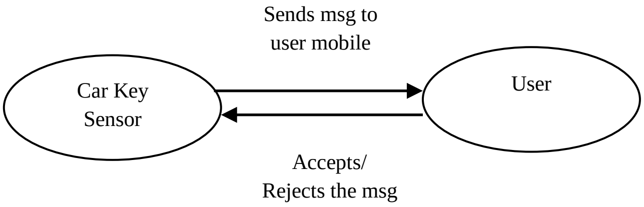

Fig-2: Auto Key Management

B. Health Care Management:

The health of a person can be continuously monitored by implementing a chip into their body. They can give the reports to one or more hospitals as per their wish. When the sensor detects a problem, it has to be reported to the hospital and the doctors can send emergency help to the person by identifying the location through their mobile phone. All medical information of the individual person such as BP, Heart Beat rate are all monitored by means of a chip. The chip may also be fixed in the watch of the person. Through this chip, the information is obtained remotely.

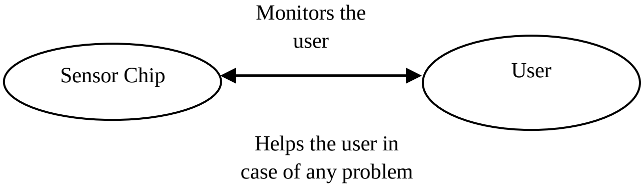

Fig-3: Health Care Management

C. *Managing Electronic Equipments:*

If a person in office wants to switch on the electric heater before he reaches home. He/she can do this by sending a message through the Internet by using the ID.

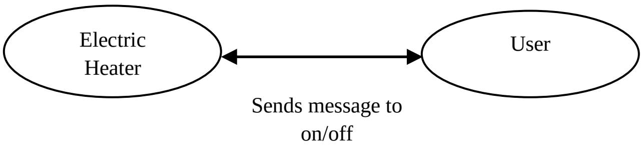

Fig-4: Electronic Equipment Management

2. Cloud-Based IoT:

We are proposing to implement the cloud-based accessibility into our methodology.

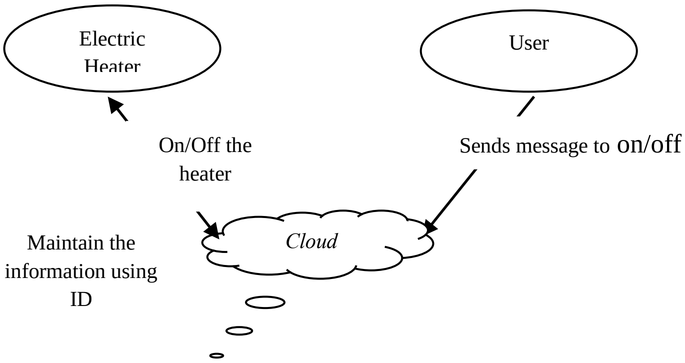

Fig-5: Electronic Equipment Management through Cloud

While we manage the things through encrypted user details in the cloud storage, we can have more advantages such as follows:

- All the things can be globally accessed
- Easier to access
- Handle the application either by mobile or by using web.

The information about the heater can be maintained in the cloud along with the user details and the heater Id. When the particular user sends message to switch on the heater, the cloud receives the message and checks the status of the heater. If the heater is already in the 'on' state, then the cloud drops the messages. Otherwise, the cloud turns on the heater.

Similarly, the auto key management and the health care management can be maintained as cloud-based in order to provide better performance.

3. Implementing Security Features:

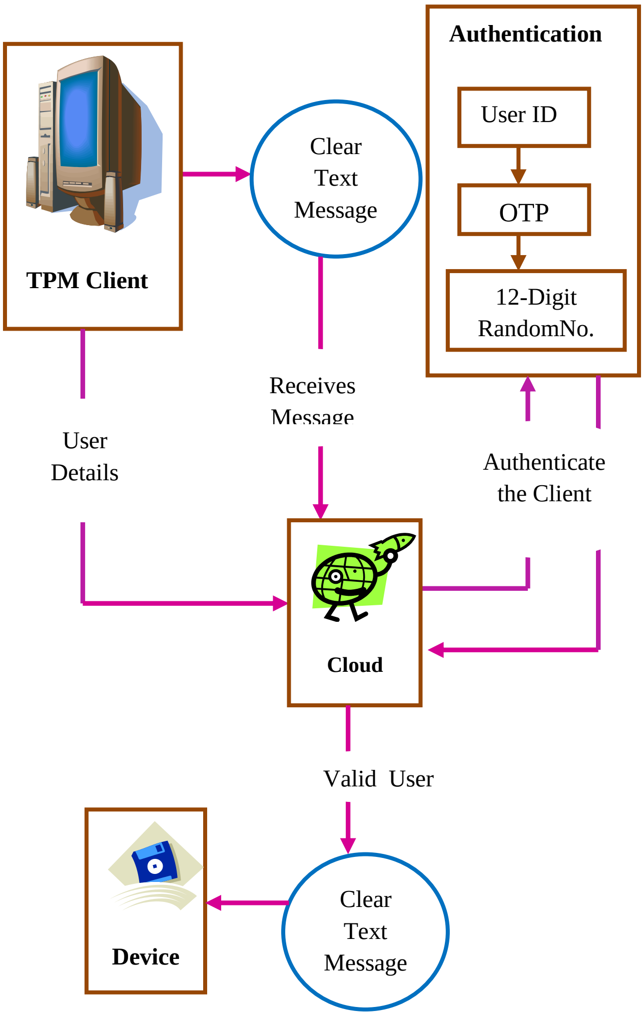

Fig-6: Architecture of our Proposed TPM

As the things can be globally accessible, it must be more securable and confidential. This can also be handled in our proposed methodology as follows:

Handling IoT is through downloading and installing software provided by the appropriate company of that particular device, which is similar to the application used in mobile devices. In our methodology, we can add a cloud-based environment with security features to provide better results. In this case, the application which is to be installed into our device consists of two phases:

- IoT Application
- Cloud Application

The first phase "IoT Application" is the one which is provided in the company along with the things, such as water heater or car key or a chip and so on. This application has been downloaded and installed into our device. The second phase "Cloud Application" is the one which provides cloud-based environment and security metrics. The steps involved in this application are discussed below:

1. Install the application into the device (either mobile phone or PC)
2. When we start to login into that website, we have to authenticate by providing valid username and password.
3. Upon providing those details, the cloud validates the detail and sends an OTP (One Time Password) to our mobile number.
4. Next step is to provide that OTP into the site for second authentication.
5. Then the cloud sends a 12-digit random number as an authentication code to validate the user.
6. Only by providing that random number, the cloud can provide permit to access the device. Otherwise, the user can be blocked.

Thus, our proposed TPM provides security to the devices and the information by validating the user and to prohibit the unauthenticated access.

The fig-6 clearly explains the architecture of our proposed TPM. In this architecture, the registered TPM Clients are connected with the cloud and can send message to operate the device. The message is received by the cloud and validates the client through a three-step security system. First the user details are encrypted and stored in the cloud. If the user wants to access the device, the encrypted details of the registered user must be matched with the cloud storage. Then the cloud sends an OTP to the user mobile. By providing the OTP correctly, the user clears the second step of authentication process. Finally, the user is provided with 12-digit random number which is like the randomly generated secret code to authenticate the user. Only if the user clears all the three step of validation process, he/she can able to be an 'Authenticated User' and their message has been forwarded to the device and operation starts to be executed.

3.2 Proposed Algorithm:

```
Start
Register the TPM Clients, Tn
Register the Devices, Dn
Store Encrypted Details in Cloud, C
If Tn wants to access Dn then
```

```
  Get the User Details, TUser, TPass
  If Encrypted(TUser and TPass matched C.Tn) then
    Generate the OTP by the Cloud, C.OTP
    Send the C.OTP to Tn.Mobile
    Get the OTP from Tn
    If Tn.OTP matched with C.OTP then
      Generate a 12-digit Random Number by the Cloud, C.Rn
      Send the C.Rn to Tn.Mobile
      Get the Rn from Tn
      If Tn.Rn matched with C.Rn then
        Allow the Tn to handle Dn
      Else
        Message "Random Number does not Match"
      End If
    Else
      Message "Invalid OTP"
    End If
  Else
    Message "Invalid User"
End If
End If
Update the Records in Cloud
End
```

3.3 Process-Flow Chart of our Proposed Method:

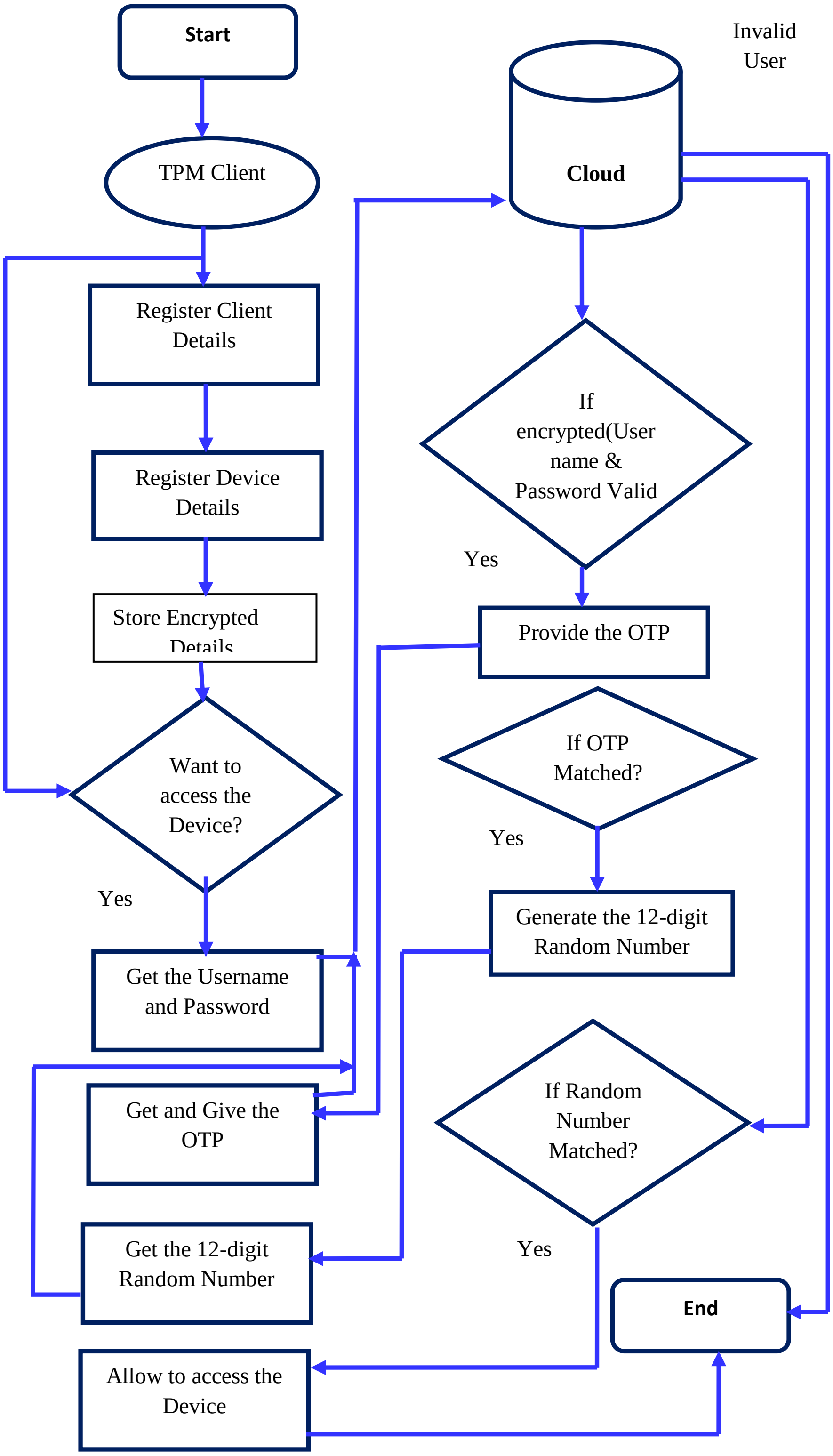
Start
TPM Client
Register Client Details
Register Device Details
Store Encrypted Details
Want to access the Device?
Yes
Get the Username and Password
Get and Give the OTP
Get the 12-digit Random Number
Allow to access the Device
Invalid User
Cloud
If encrypted(User name & Password Valid
Yes
Provide the OTP
If OTP Matched?
Yes
Generate the 12-digit Random Number
If Random Number Matched?
Yes
End

Fig-7: Flow of our Proposed TPM

IV. EXPERIMENTAL DATA

TPM plays a major role in many areas in order to provide security and better performance. In our paper, we implemented TPM to provide secure platform for handling things through Internet. While handling such things, our proposed methodology validates the user with proper authentication and to allow only the trusted user to handle the devices. Our methodology provides three-way secure mechanisms to trust the user and it is experimentally verified by handling different things in different ways. One such experiment is carried out by handling the car through Internet. The Cloud maintains the details about the user and their device such as car. When the user wants to access the car, then the user has to be trusted by providing their username and password. If the username and password gets authenticated, then the cloud sends an OTP to the user's mobile. The user has to enter that OTP for second authentication. If it is also be valid, then the cloud sends the 12-digit random number to the user. The user has to receive that random number and provide it for third authentication. Only if all the three process validates the user, the user is accepted as a 'Trusted User' and allows them to access the car. Otherwise, the user has to be treated as 'Unauthenticated User' and blocks him for further access.

Thus our proposed method supports TPM to trust the user and provide secure access on IoT with better performance.

V. CONCLUSION

In this study, we have presented a cloud-based architecture, which benefits to handle the devices on Internet IoT by using trusted platform TPM. The methodology has been experimentally verified and the result shows the better performance. Using the cloud-based methodology, the user will get enhanced performance feature, security features and ease of deployment through three-step authentication process. The explosion of devices with communicating capabilities is bring closer to the vision of IoT, in which the devices can be actuated through sensing functions and new capabilities are made to access the new information sources in a secure manner. IoT is an ideal emerging technology to provide the new evolving data and the required resources through the Internet. By examining all these things, the proposed methodology meets all the necessary requirements and security features to access the IoT in a trusted way by using TPM.

REFERENCES

[1] Han-Chuan Hsieh, Jiann-Liang Chen, "ScriptIoT: A Script Framework for and Internet-of-Things Applications", IEEE Internet of Things Journal, Volume: 3, Issue: 4, Sep 2015.

[2] Jun Liu, Cheng Fang, Nirwan Ansari, "Request Dependency Graph: A Model for Web Usage Mining in Large-Scale Web of Things", IEEE Internet of Things Journal, July 2015.

[3] Zhiyuan Li, Rulong Chen, Lu Liu, Geyong Min, “Dynamic Resource Discovery Based on Preference and Movement Pattern Similarity for Large-Scale Social Internet of Things”, IEEE Internet of Things Journal, June 2015.

[4] Qiang Tang, Kun Yang, Dongdai Zhou, YuanshengLuo, “A Real-Time Dynamic Pricing Algorithm for Smart Grid with Unstable Energy Providers and Malicious Users”, IEEE Internet of Things Journal, July 2015.

[5] BiplobR.Ray, Morshed U. Chowdhury, Jemal H. Abawajy, “Secure Object Tracking Protocol for the Internet of Things”, IEEE Internet of Things Journal, May 2016.

[6] Ahmed Bader, Mohamed Slim Alouini, “Localized Power Control for Multihop Large-Scale Internet of Things”, IEEE Internet of Things Journal, Aug 2015.

[7] Qie Sun, Hailong Li, Zhanyu Ma, Chao Wang, “ A Comprehensive Review of Smart Energy Meters in Intelligent Energy Networks“,IEEE Internet of Things Journal, Dec 2015.

[8] KeshavSood, Shul Yu, Yong Xiang, “Software-Defined Wireless Networking Opportunities and Challenges for Internet-of-Things: A Review”, IEEE Internet of Things Journal, Sep 2015.

[9] Liang Liu, Huadong Ma, AnfuZheu, Dong Zhao, “On Networking of Internet of Things: Explorations and Challenges”, IEEE Internet of Things Journal, Oct 2015.