Integrated Device Cloud Architecture for a Secure Cloud of Things Environment

V. K. Sanjeevi, Y. Sunil Raj, S. Albert Rabara

Abstract**: *Though IoT could impart intelligence to the environment, without cloud it could not do wonders in real world in the present cloud of things era. Numerous applications including scientific, engineering and financial applications, were developed and architectures framed, where most of which always depend on cloud and internet of things for better effectiveness. Therefore blending IoT with Cloud is essential and would change the way internet is used presently. Deployment of smart devices on smart environment in colossal scale will be future more challenging. Lacking of scalable architecture will tremendously affect the management of sensors/devices, leading to inefficiency in applications. Realising this a secure device cloud architecture is proposed as cloud provides anything as a service, which is also depicted as cross cloud federation management. As devices are equipped with intelligence that is IoT enabled, and are hosted as clouds. Focus is on providing end-to-end security while delivering more reliable services in CoT environment.***

Keywords **: *CoT, Cloud Security, IoT, Sensor Cloud, Cloud of Things, Device Agent.***

I. INTRODUCTION

IoT tends improving quality by enhancing awareness among pool of resources in the environment, and enrich user experience through sensors and devices. Wanting of scalable design, it would be quite tricky to manage expanding level of resources. Internet of Things blooms day by day, as a result there is a sudden increase in usage of sensors and actuators in fields of health, industrial technologies, agriculture, and so on [1]. Interconnection of intelligence embedded devices through internet designates IoT. It enables things to make remote access easy. Effective use of intelligent things affluence human life in various facets [2]. As resources being energized with sensors and protocol suites leads resources to remain connected keeping devices organized and more functional [3].

Devices embedding sensors among them enables interaction among physical and virtual world [6]. Each object is linked through making data transfer without any manual intervention of triggering the devices as depicted in Fig.1. IoT can be applied in multiple scenarios such as smart monitoring, waste management, autonomous driving and so on [3]. It provides devices easiness in broadcasting data while controlled by other devices or applications. Sensor networks (SNs) play a key protagonist on communication and networking aspects between similar objects [15].

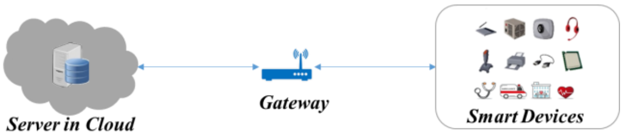

Fig. 1. General Scenario of IoT Based Computing

Cloud facilitates using configurable pool of computing assets, in a shared environment. With a trifling management exertion, Platforms, Infrastructure, and Services can be rapidly provided access. Foremost essential characteristics are elasticity, access of broad network, pooling resource, metered provisioning of resources etc. Cloud comes provisioning users with various service models like PaaS, IaaS and SaaS, and deployment models such as public, private, community and hybrid. Infrastructure capabilities to deploy and run software is provided by IaaS. Capabilities to develop and deploy applications on Cloud is rented by PaaS. Resources to use software's via thin-client interfaces like Web Browsers or API's are rented by SaaS [20].

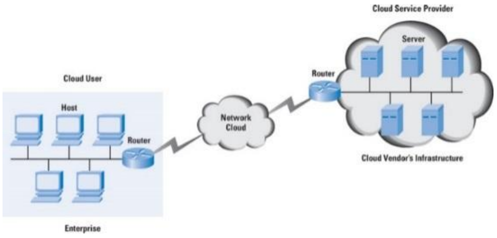

Fig. 2. Cloud in Real Applications

Fig. 2. Shows Cloud as a technology and a business model allowing users allocate resources on-demand, resulting in CSP's profiting by leveraging services to clients. Initiated with sharing of physical resources like processors and now physical machines are rented in a secure way.

Manuscript published on November 30, 2019.
* Correspondence Author

Mr. V. K. Sanjeevi*, Research Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, India. Email: vksanvi@gmail.com

Prof. Y. Sunil Raj, Assistant Professor and Research Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, Tamilnadu, India, Email: ysrsjccs@gmail.com.

Dr. S. Albert Rabara, Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous), Affiliated to Bharathidasan University, Tiruchirappalli, Tamilnadu, India. Email: a_rabara@yahoo.com

Cloud environment is able to provide numerous operational benefits with and without IoT to industries like, costs reduction, provision hardware and software, ease of expansion of infrastructure.

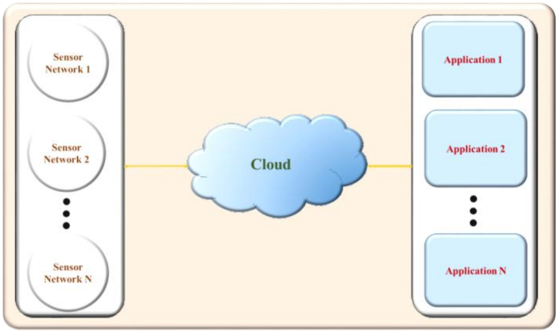

Fig. 3. General Architecture of Sensor Cloud Network

Combination of numerous sensors form WSN [9]. The sensor/device cloud constitutes WSN resulting into cloud managing IT resources as shown in Fig. 3. Sensors on cloud ought to be energy efficient as it requires more energy to run on live environment communicating constantly with server. As requests from users would be more frequent and as the requests are transmitted to network often, could exhaust the energy of sensor.

The capabilities of IoT enabled devices/ sensors/ actuators are high sensitivity, processing power, and networking functionalities. Cloud adoption leads to increase in reliability by providing self-healing mechanisms and enables mutual operation and participation of the users. Numerous trials have been tolerably analyzed to recognize the true prospective of applications on IoT.

II. LITERATURE REVIEW

[1] Has made an attempt solving problems such as attendance management and monitoring. Reducing the time consumption, system replaces manual and unreliable system while making the process faster and efficient. Security, confidentiality are the major advantages, while enhancing the staff and students ethically. Also proposes the inclusion of additional devices including biometric, web cam and retina scanner for the automation and effective management of the whole process.

[2] Proposes IoT enabled parking environment and uses cloud for handling parking spaces related information and process it real-time. The system facilitates reserving of parking slot from distant location. Authentication of valid booking is done for validating the users. The work proposed, reduces traffic, also provides cost effectiveness also helps reducing carbon footprint.

[3] Discuss the interface between smart cities and IoT. Achieving such objectives requires a tremendous amount of connected objects. The connected objects could make cities smart, opening up risks and privacy issues. The number of connected objects are growing exponentially.

[4] Provides IoT based solution to control the fleet remotely in secure way. Devices like sensors and GPS are used to continuously monitor the vehicle. The system controls the vehicle from remote and provide protective actions for sustaining the vehicle in reliable state. This is done by monitoring the distance travelled by vehicle and fuel consumed at a particular interval of time.

[5] Proposed an intelligent system to protect users from superfluous demises happened by road mishaps because of drunken drive. The system uses intelligent sensors for alcohol concentration detection, touch, face recognition and heartbeat recognizing to safeguard drowsy drivers. Also introduces mechanisms for safeguarding GPS module and automatic ignition off.

[6] Smart farm irrigation system is based on IoT for remote monitoring and controlling of drips through WSN. Wireless monitoring of irrigation system allows remote monitoring and controlling replacing human interference. Cloud based wireless system monitors and controls sensors and actuators to assess the plants. System is able to manage irrigation more effectively, while optimizing water consumption as moisture sensor is involved for the purpose.

[7] IoT enabled waste management system determine the status of trash container. The data acquisition module updates server as the level of garbage touches the limit. MQTT communication protocol links coordinator and server. User friendly and inexpensive method of communication is provided by Telegram bot between server and truck.

[8] As IoT delivers chance to healthcare, for bed-bound patients Lateral Rotation Mattress is introduced. Sensors embedded recognizes patients discomfort and alleviate it intelligently. PPG sensors eliminates the availability of care takers for certain petty actions. The intelligent lateral rotation system assuages the risks of pressure blisters caused of long stretch stasis.

[9] Cloud systems could forecast upcoming sensor data. The load-balanced routing could use different lanes to route data from node to gateway. Also enforces that usage of prediction in cloud and load-balancing routing in WSN would make the future to minimize energy consumption in the environment. It is found to be energy efficient as the requests, in large number are retorted at cloud level.

[10] Addresses personalized consumption demands in smart manufacturing by building cyber-physical production systems. The smart factory contains devices, cloud deployed privately, client machines, and all connected to a network integrates the system employed in production. Work presents an intra-layered negotiation and interaction for implement reconfiguration dynamically.

[11] Proposes an architecture provisioning medical services in cloud, where the cloud leverages medical services and techniques. The assessment is presented through the layered architecture. Test case and results are discussed along with performance measurement of service.

[12] Discusses the usage of infrastructure from several providers and benefit of decentralizing computing. The trend results in new computing architectures that satisfies a variety of services offered by cloud. Also impact areas of such cloud would be data-intensive computing, connectivity between people and devices and self-learning.

[13] Proposes a cloud based IoT platform to develop applications where new generation services interacts with surrounding environment, collecting data and applying to management strategies on integrating the two major technologies. Also have developed hardware for smart home scenario enabling connections with smart things using cloud services.

Retrieval Number: D8726118419/2019©BEIESP
DOI:10.35940/ijrte.D8726.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

[14] Presents CEB and validation scheme while signifying the scaling behavior of IoT extension and in dynamically growing loads. Also CEB architecture is used as a platform for employing optimization.

[15] Designs a gateway for CoT, which manages semantic-like stuffs, also performing as end-point for exhibition of data. Using virtual software's presents trivial effect in enactment. It is inferred that gateway facilitates slight and thick service deployments.

[20] Cloud enabled design for IoT, improves the deployment of intelligent systems in industry. The style comprises of layers for data gathering, data transformation, real-time analysis of data, reporting and dynamic control. Above all devices are monitored, controlled by sensors and actuators coupled to motor remotely.

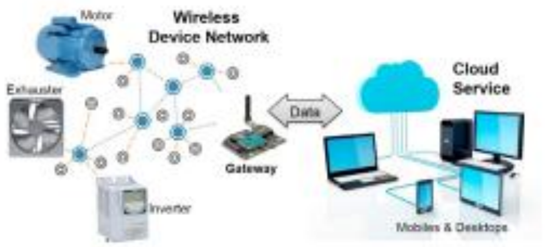

Fig. 4. Appliances Connected to the cloud for Control and Analysis [20]

As described Fig. 4, shows the adoption of real-time maintenance routines, implements abnormal behavior detection, failure of equipment's and industrial plant control. Benefits includes easiness of IoT prototyping using PaaS and IaaS service models. The architecture could be stretched to a variety of applications. The aspects such as privacy and security could be addressed by cloud systems and protocols.

[22] Cloud, IoT bore a new set of smart services that impacts everyday events. Numerous applications benefit M2M communications, which also may open certain security issues.

III. CLOUD IOT INTEGRATION

As integration of CC with IoT, major computing concepts are more workable, important aspects related to CoT are discussed in this section.

Paradigm IoT transforms Internet into interconnection of real world objects. As heterogeneous objects participates, storage, processing capabilities and key role is played by a number of middleware's lying between things and applications.

Cloud architecture could be split into four layers, each seen as a service for users. Cloud services grouped in three main categories: i) provisioning applications accessible through thin clients, ii) facilitation platform based resources, iii) providing storage, processing, and other such resources, letting user the control.

Cloud model is pretty as it carries itself the burden of investment in infrastructure. Outsourcing infrastructures to Cloud could shift business risk to provider. Also permit getting space for devices to be accessed in a consistent way. In order to face high number of devices/sensors and volume of data, administration and control of devices also be leveraged. This could be done by deploying mediators for mitigating regularity of data transfer. Cloud also guarantees optimization in resource utilization, energy efficiency, elasticity, and flexibility.

Espousal of CloudIoT paradigm assist daily lives of users. Common challenges are lack of trust, unpredictable performance, and other issues. It could lead to generation of opportunities for contextualization and geo-awareness. The result lead to better decision-making, acquiring information from heterogeneous infrastructures, accessing geo-location.

As this joint adoption enables the automation of activities, merging things with computing, enables transformation. Adoption allows automation in flow of services or goods, from source to destination, to meet time, cost efficiency. This blending acquaint with new management requirements for resources like sensors. It also deploy a prompt IS, between monitoring and sensors/actuators deployed in the environments.

These could provide services to user real-time, on-demand through different types of clouds in secure and cost effective manner. This could include temporary Clouds designed expanding the conventional Clouds to increase the whole processing capabilities.

Table 1. Efficiency Sharing between IoT and Cloud

Parameters	*IoT*	*Cloud*	*CoT*
Displacement	*Pervasive*	*Central*	*Pervasive & Central*
Reachability	*Limited*	*Cannot be Defined*	*Unlimited*
Computational capability	*Limited*	*Virtual*	*Unlimited*
Components	*Objects*	*Virtual*	*Virtual Objects*
Storage	*Limited*	*Virtual*	*Virtual*
Data	*Source*	*Managing*	*Virtual Management*

The analysis of efficiency that could be shared while blending two different technologies can be understood form Table. 1. As IoT has its own limitations, Cloud being a partner and giving hands together could take it to an unlimited nature. Which obviously could be serving the end users with its own capability and limits.

IV. PREPARE YOUR PAPER BEFORE STYLING

IoT integrated with Cloud makes a driving technology for evolution of high level processing such as analytics. Though presenting a high heterogeneity in devices, protocols, and technologies, it lacks security, reliability and flexibility. Looking to Cloud which not only proves providing them, also adding easy use and cost reduction to users, and making complexity analyses and data-driven decision possible.

As data are managed using cloud technology, it is possible to manage infrastructure such as storage, memory etc. Now it is time to think of using cloud to manage day to today usage devices. It is one of the duties of this architecture to propose such an environment where intelligent devices namely sensors, actuators and other appliances put together as cloud called as Device/ Sensor Cloud (DSC).

As cloud enables user with sensors/actuators interaction, satisfying crucial requirements like interconnection and control while automating activities. It allows sets - up space for sensors or intelligent devices for access in a reliably. In order to face large number of intelligent devices and large volume of data, administration and control of devices also be leveraged. This is possible by deploying powerful devices as mediators for mitigating incidence of data transfer.

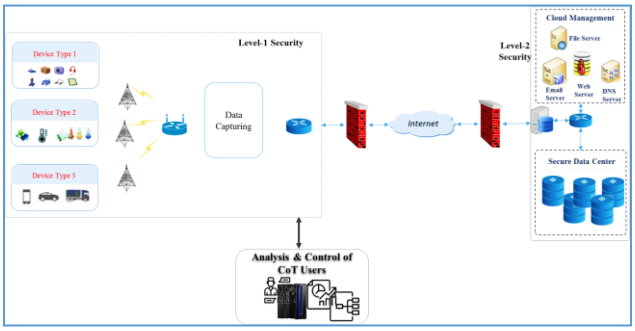

Fig. 5. Cross-Cloud Federation Management Architecture for Secure CoT Environment

From the above Fig. 5, partitioning whole architecture in to five major components can visualize the presence of, user, DSC, reader (Data Capturing), cloud processing and services.

a) DSC

Device/Sensor Cloud is a group of sensor enabled, appliances and devices. It can also contain a group of sensors, integrated together. Here to provide better service device id is assigned to each device/ sensor. That is done as follows:

$$\text{sd-> } C_iDSO_jS_k \text{ ------------------ } 1$$

Sensor/ devices are enumerated as ‘sd’, which represents device id generated by device agent. C_i represents the ‘i’th cloud that is created by an owner. DSOj representing the device/sensor owner, who may register their device on the cloud C_i. Finally, Sk is a sensor identity which is specific to a device/ sensor. This may be the name and model of device that registers on the device cloud C_i.

As devices respond to any request through intended cloud provider device identity can be recorded. This also enables us to monitor kind of access made and duration of access to a specific device. The device/ sensor is embedded with an encryption/ decryption module, so as to protect the device from the unauthorized access, of device.

The main actors of the CoT environment may be the users, categorized as owners and users. The device/ sensor owner is a cloud user who will enable their device for global usage. Thus making their resource shared by a remote user on the cloud. Here the geographical location of the user using the device is not known by the DSO. Also the device cloud user will not be aware of the owners.

b) Data Capturing

Data capturing involves a major security constraint, therefore data is read from the device with the knowledge of the device owner. As the device ID easily identifies the device owner. As data is received form intelligent device the data is controlled by the cloud modules that enables quick analysis and processing of requests. As the data originates from the source, data transferred through the mobile station will be let to pass through IoT gateway. The actual communication will take place between gateway and reader, while receiving the data acquired by the selected device.

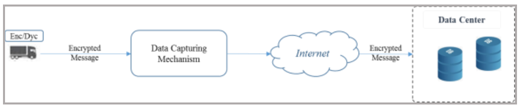

Fig. 6. Secure Data Transfer – Data Capturing

Fig.6, describes that the encrypted data received form node is transferred to the data centre through cloud server thereby reducing the security risk in data on transit and providing more security to data.

c) Cloud Processing& Services

The major part in cloud environment is processing mechanism. This enables a secure communication processing mechanism and also a secure data processing mechanism. As the initial job of this processing end is to register every new device cloud that is created, and provide the id as in the above section, i.e.

$$\text{sid ->} \textstyle\sum_{i,j,k}^{n} C_iDSO_jS_k \quad \text{------------- } 2$$

Apart from various services like data storage, services related to device can be provided, based on the device type. As directed for use DSC effectively, it requires proper management of resources. Therefore device agent is a major component here, which is a monitoring unit.

At any point of time device may be requested by user, while the DSC should wait for device agent’s direction. This DAgent is assigned to device cloud, who accesses the user log, device log and cloud log, will maintain its own log to regulate the usage of registered devices/ sensors on registered cloud. This is to enhance availability of devices/ sensors over the internet for remote users. As the device is allotted by the agent, usage can be metered and the bill can be generated basing on duration of time and the type of device. This also enhances the security to the device/ sensor by restricting unauthorized access.

Unauthorized access can be eliminated with the help of Device Agents, who directly communicates to the device clouds and provides access to the end users with a random device id. There by actual id of devices could be hidden for security of the devise, thereby putting intruders at the edge of risk.

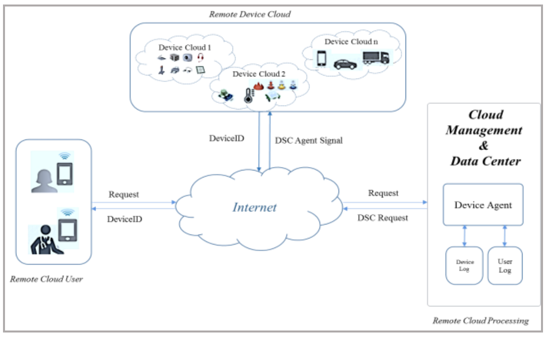

Fig. 7. Device Agent & CoT for Remote Cloud Users

Though the architecture proposed is novel, it doesn’t lose security it provides throughout the cycle of communication. Starting with the device registry each and every end security is being provided. Proper device authentication is provided and user authentication is provided.

As depicted in *Fig. 7*, the data received form node is encrypted using an encryption module embedded with device/sensor node. Hence security risk in data on transit is reduced, providing more security to data.

Retrieval Number: D8726118419/2019©BEIESP
DOI:10.35940/ijrte.D8726.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The key used in encryption mechanism is a resultant of cloud id, device id generated by device agent, device owner id and user id which is specific to the current user.

key ->sd+dso_id+loc_id+curr_uid

The key thus generated is used to encrypt data that is generated by device/ sensor on the device cloud and the message transmitted over network. Thus eavesdropping is made riskier, while protecting the data. Here in the above defined key generation mechanism, *sd* represents device identity, *dso_id* will hold the unique identity of a device owner, *loc_id* holds the geo-location of the device and *curr_uid* holding the identity of the valid user who is using the device/sensor. The key generated is of 32 characters, where 8 characters is meant for holding device id, 8 characters are intended for handling device owner id, 8 characters specific to location id and 8 characters specific to current user.

d) Analysis and Control

Control to any user on the network leads to reliable system. Enhancing the quality of service provided by the system will mostly depend on the type of access and control mechanism it uses. As the proposed system is monitored by the device agent, it also requires additional supporting module to enhance the capability of the system. In order to avoid the unnecessary access, otherwise possibly wrong access this analysis and control unit tempts to be a supporting component.

The major duty of this module is to keep communicating with the DAgent, in-order to assist it in decision making process. It classifies the nodes as well as the users as it receives entry on the logs. As the new device enters into network trying to be used inside the network, the control module enables the analysis module. Thereby verifying it with DAgent, new device will be granted permission. If device is found to be unauthorized, analysis module transfers signal, x=0 to control module. Control module rejects the request and prevents device form entering into the device cloud.

Supposing that, if a device after predicting that it is authorized by DAgent, analysis module returns x=1, such devices will be let to communicate with the device agent as the control module transfers its control to DAgent. While coming to the device cloud users, the overhead of validating the user and kind of request they make will be monitored. If the device is not meant for such user or if the user doesn’t have proper access permission, the control module stops the used form accessing the device cloud server.

e) End Users

Everything is present and if there doesn’t exist user for any service provided by CoT, it may not be able to present a better system to the environment. The users at using end will be allowing to use the devices/ sensors as other services are leveraged on the device cloud. The device used will not be seen or known by the users. Also the very owner of the device is not necessarily to be known by the user for using it.

It is a known fact that users must be authorized ones, for using any device/sensor that is available over the globe. The users will directly communicate with the control unit, where the valid user will be identified with the help of cloud server. The valid users will be directed to the DAgent and invalid users will be not be not let into the network. Thereby protecting the devices and data on device cloud.

V. RESULT AND DISCUSSION

Cloud of Things can play a vital role in day-to-day life and can be integrated together for getting better service. Such an architecture is proposed and analysis is shown as follows:

Device/ Sensor Cloud

As the initial task of cloud registration is handled using the registration module, where provider could check for the existing one with same request entries. If no such entries are found to be existing the log will be updated with the new data finally providing a cloud_id, for uniquely identifying a device/ sensor cloud.

```
Algorithm: Device Cloud Registration
BEGIN
  current_cloud:=Request_Registration
  IF (Existing == current_cloud)
      cloud_already_registered
  ELSE
    Update CloudLog (current_cloud)
      Create DeviceLog;
      Provide cloud_id;
  END IF;
End Service_Provider;
```

After assigning a unique identifier, service provider register the cloud and new device log will be assigned to created cloud. This log is intended to hold details related to devices on the cloud.

Begin the device registration a major task, in handling the devices on the cloud. The mandatory details are device name, device/ sensor owner id, cloud id and current location of the device. These are requested and as received for the device on its first access to the cloud through network (wired/ wireless).

```
Algorithm: Device Registration
BEGIN
  cur_dev:=Device_Name
  loc_dev:=current_location
  dev_ow:= owner_name
  IF(cloud_id) THEN
    IF (cur_dev & loc_dev & dev_ow) THEN
        IF (add_another_device) THEN
          Update (cur_dev)
        Provide sd
         Create accLog(cur_dev);
        ELSE
          Abort;
        /* Invalid Request*/
        END IF;
    ELSE
    Update Mal_Device_Log
            (cur_dev, loc_dev, dev_ow)
    END IF;
  ELSE
      Abort;
            // Invalid – Cloud ID – Detected
  END IF;
```

```
End Device_Registration;
```

To become part of device cloud, it is necessary to be registered on the cloud. Irrespective of the Selected Cloud and available device type registration could be done. Device *sd*$_i$ could be registered under any existing cloud (c_1, $c_{2,}$. . . c_n), or by creating a new private or public cloud by requesting CSP. Therefore in-order to do this it requires device specific details, owner details and location, as the device is GPS enabled.

As a device enters the network, cloud id should be verified and if the cloud id is not valid, device registration is not possible. If the provided cloud id is valid, check for the existence of same device and if not so proceed registration by updating the log. Otherwise pass existence intimation and exit. If the cloud id is not valid, or device owner name is not valid update the malicious log for further analytics.

```
Algorithm: DSO_id
Begin
  cid:= cloud_id;
  IF (cloud_id) THEN
     Static Count i;
        dsoid:=cidDSOi
     END LOOP;
  ELSE
     Abort;
     // Wrong Cloud ID
                 //invalid – owner request
  END IF;
END DSO_id;
```

DSO is a device cloud user who enables devices for global usage, sharing their resources to remote users on cloud. Here the geographical location of the user using the device is not known by the DSO. To provide such service, dso registration is mandated so as to enhance the security. If not considered malicious intruders who pretend to be DSO may break the network, leading to a great risk.

Therefor DSO is provided with a unique identifier, with which devices can be registered on the specified device cloud. Here cloud id is the input along with the DSO request. A unique id will be generated for each and every DSO request, if the cloud id is a valid device cloud id. Otherwise assuming intruder the request will be aborted.

```
Algorithm: SID
BEGIN
      IF(cloud_id) THEN
       cid:= cloud_id;
               IF (DSO) THEN
                  IF( gps & Crypt) THEN
                        Static Count i:
                                  sid=cidDSOSi
                        End Loop
                  ELSE
                 // Location not identified
                 // No Crypt Module Found
                 Abort;
                  END IF;
               ELSE
                   // Invalid Device Owner
                  Abort;
                  END IF;
      Else
  //invalid cloud id – Detected
                  Abort;
      END IF;
      RETURN;
End SID;
```

Device or Sensor are identified uniquely by their *sid* generated. Before generating the device id, the cloud id is verified for validity and also the device/ sensor owner is verified for validity. Only if the cloud and owner are authorised and valid, the device id will be generated. As the inputs are cid which represent a specific cloud, DSO which is specific cloud along with the device details.

While providing sid, the module checks for the presence of GPS and Crypt which is an cryptographic module which is expected to be embedded with the device. If any of the above two is not present the device id request will be neglected. There by removing the device from every existing entries.

The functioning of the entire system can be depicted in a simple form as follows:

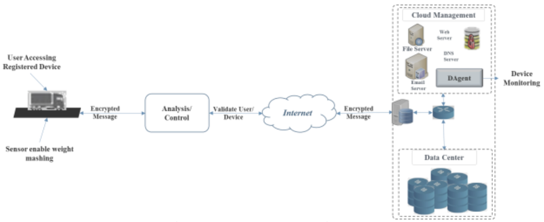

Fig. 8. Overall functioning of CoT Architecture

As depicted in Fig. 8, the user who is driving may require a device which is sensor enabled. As requested by the user the control module sends the data to DAgent, who have control on logs. Also the device is checked by DAgent, and as both the device and user are validated by DAgent. The response provided by DAgent based on the log will be valid or invalid. And for valid users the service will be enabled as the device is activated with the help of the secure id generated. Now as the data is transferred to the data storage, after analysis the results will be handled to the user's mobile device as response. Once the Weight detected is intimated to the user, the device is deactivated as the user sends feedback for the usage of device. This being considered validation of the whole system.

VI. CONCLUSION

CoT is expected to lead daily use applications for better usage. As it was found in day to day life, things being rented from anywhere, including vehicles, books, and construction materials. Renting of sensor/ devices over the internet is ideologically possible in this IoT enable world. As cloud being a better half provides strength to IoT. As this work presents a detailed view on the security architecture, security can be provided in a better way, while providing better service. Maintenance cost gets reduced for deployment and for complex data processing. Also it is energy efficient as every requests from user is responded at cloud level. The analysis proves that the architecture performs well with a large number of nodes and users on the cloud.

This can be implemented in live solutions for the betterment of environment and socio economic world.

REFERENCES

1. Madhu B.M, Kavya Kanagotagi, IoT based Automatic Attendance Management System, International Conference on Current Trends in Computer, Electrical, Electronics and Communication (ICCTCEEC-2017), IEEE, pp83 -86, 2017.
2. Mahendra, Dr Savita Sonoli, Nagaraj bhat , Raju, Raghu, IoT Based Sensor Enabled Smart Car Parking for Advanced Driver Assistance System, 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), 2017.
3. Badis Hammi, Rida Khatoun, Sherali Zeadally, Achraf Fayad , Lyes Khoukhi, IoT technologies for smart cities, The Institution of Engineering and Technology, 2017, pp. 1 -13.
4. Mahaveer, Dr. Shivashankar, Arjun, Goutham, Lohith, Sanjay, Smart Fleet Monitoring System using Internet of Things(IoT), 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), 2017.
5. Koneti Sandeep, Ponnam Ravikumar, Sura Ranjith, "Novel drunken driving detection and prevention models using Internet of things", International Conference on Recent Trends in Electrical, Electronics and Computing Technologies, IEEE, 2017, pp. 145-150.
6. Shweta B. Saraf, Dhanashri H. Gawali, "IoT Based Smart Irrigation Monitoring And Controlling System", 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology, 2017, pp. 815-819.
7. Karthikeyan, Sheela Rani, Sridevi, Bhuvaneswari, "IoT enabled Waste Management System using ZigBee Network", 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), 2017, pp. 2182 – 2187.
8. Shubangi Nataraja, Dr. Poornima Nataraja, IoT Based Application for E-Health An Improvisation for Lateral Rotation, 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), IEEE, 2017, pp. 1018 – 1021.
9. Kalyan Das, Dr Satyabrata Das, Rabi K. Darji, Ananya Mishra, "Energy Efficient Model for the Sensor Cloud Systems", 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), IEEE 2017, pp. 373 – 375.
10. Shiyong Wang, Jiafu Wan, Muhammad Imran, Di Li, Chunhua Zhang, "Cloud-based smart manufacturing for personalized candy packing application", Springer Science & Business Media New York, 2016.
11. Mridul Paul, Ajanta Das, "Provisioning of Healthcare Service in Cloud", Springer, Nature Singapore Pte Ltd., 2018. Pp. 259 – 268.
12. Blesson Varghese, Rajkumar Buyya, "Next generation cloud computing: New trends and research directions", Future Generation Computer Systems, Elsevier, 2018, pp.849–861.
13. Jadidyaneal, Bijeesh, "Cloud of Things Architecture with Application to Smart Home Scenario, International Conference on Emerging Technologies", Networking and Computational Intelligence, 2016.
14. Yi Xu, Sumi Helal, "Scalable Cloud-Sensor Architecture for the Internet of Things", IEEE Internet of Things Journal, IEEE, pp. 1-14.
15. Riccardo Petrolo, Roberto Morabito, Valeria Loscr, Nathalie Mitton, "The design of the gateway for the Cloud of Things", Mines-Tel´ ecom and Springer, Springer, 2016.
16. Bonomi F, Milito R, Zhu J, Addepalli S, "Fog computing and its role in the internet of things", Proceedings of MCC, 1st workshop on mobile cloud computing, vol 13, 2012.
17. Morabito R, Kjallman J, Komu M, "Hypervisors vs. lightweight virtualization: a performance comparison", Proceedings of IC2E - International IEEE conference on cloud engineering, 2015.
18. Petrolo R, Loscr`ı V, Mitton N, "Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms", Trans Emerg Telecommun Technol, 2015.
19. Sachs J, Beijar N, Elmdahl P, Melen J, Militano F, Salmela P, "Capillary networks — a smart way to get things connected", Ericsson. Tech. rep, 2014.
20. Ademir F. da Silva, Ricardo L. Ohta, Marcelo N. dos Santos, Alecio P. D. Binotto, "A Cloud-based Architecture for the Internet of Things targeting Industrial Devices Remote Monitoring and Control", International Federation of Automatic Control Hosting by Elsevier Ltd, Science Direct, 2016, pp. 108-113.
21. Mukhtar M.E. Mahmoud, Joel J.P.C. Rodrigues, Kashif Saleem, Jalal Al-Muhtadi, Neeraj Kumar, Valery Korotaev, "Towards energy-aware fog-enabled cloud of things for healthcare", Computers and Electrical Engineering 67, 2018, pp. 58–69.
22. Alessio Botta, Walter de Donato, Valerio Persico, Antonio Pescape, "Integration of cloud computing and Internet of Things: A survey", Future Generation Computer Systems, 2015.
23. Kalyan Das, Satyabrata Das, Rabi K. Darji, Ananya Mishra. "Energy efficient model for the sensor cloud systems", 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technologys, 2017.

AUTHORS PROFILE

Mr. V. K. Sanjeevi, is a graduate in Electronics & Communication Engineering from the College of Engineering Guindy, Anna University Chennai. Did MS in information Technology from Bharathidasan University, Trichy. And completed MBA in HRM from IGNOU, New Delhi. Entered Indian Telecom Service through UPSC. Held many positions in Department of Telecommunication and BSNL. Presently holding the position of Principal General Manager Southern Telecom Project under BSNL. Had the working experience of installation, operation & maintenance of varied Telecom services utilizing various technologies for 32 years. Having served as Chief General Manager of BSNL, Andaman & Nicobar Circle, he is currently involved in Installation and commissioning of Optical Fiber Cable systems, Satellite Communication for the Islands and Submarine Cable System for connecting the Andaman & Nicobar Islands to the main land. Being Involved in upgradation of BSNL core transmission network which carries the traffic of voice, data and video contents of landline, mobile, broadband and leased circuits. He is also involved in establishment of exclusive defense communication network in southern part of the country.

Mr. Y. Sunil Raj working as an Assistant Professor in the Department of Computer Science, St. Joseph's College (Autonomous) (Bharathidasan University), Tiruchirappalli. Have working experience of about 8 years in teaching. Have attended a number of Faculty development programs, workshops and seminars. He is also a research scholar and pursuing his research in cloud computing. Have published articles in international journals and conferences.

Dr. S. Albert Rabara is working as an Associate Professor in the Department of Computer Science, St. Joseph's College (Autonomous), (BDU) Tiruchirappalli. He obtained his Ph.D in Computer Science from Bharathidasan University. An expert in the field of Information and Communication Technology and Security, he is a consultant for several colleges in Tamilnadu. He has 30 years of teaching and research experience and guided nine Ph.D Scholars. Published more than 90 papers in Journals, International and National Conference Proceedings, his research contribution is significant in IEEE, ACM and Springer Science publications and DBLP library catalogues. He is a member of editorial board of several International Journals and life time member Computer Society of India (CSI) Elliptic Curve Cryptography based Security Framework for Internet of Things and Cloud Computing.

Retrieval Number: D8726118419/2019©BEIESP
DOI:10.35940/ijrte.D8726.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication