Hybrid Cloud – Intra Domain Data Security and to Address the Issues of Interoperability

Suma M.R, Madhumathy P

Abstract*: Cloud computing is a major computing paradigm which has drawn widespread attention in recent days. Various objects surrounding human tend to be on the network in one form or another in the cloud computing and IoT framework. Though both cloud computing and Internet of Things together has profound applications, integrating them involves many challenges. Any cloud worker can access the information from the cloud hence, sustaining the security and interoperability of the information becomes difficult. In this paper, a Secure Hybrid cloud-enabled architecture for the Internet of Things (SHCEI) has been proposed. This involves a hybrid cloud- Private cloud and Public cloud. The main purpose of this paper is to ensure intra domain data security and to address the issues of interoperability.

Index Terms*: Amazon Web Services, Cloud computing, Internet of Things, Net Beans, SOAP.

I. INTRODUCTION

The new era of Web 3.0 with the proliferation of ubiquitous and pervasive computing; emphases on creating a communication link between real objects and people via the internet. One of the major technologies which ensure ubiquitous communication is the Internet of Things which provides machine to machine communication. Deploying IoT efficiently in various fields must ensure larger storage capacity and data security.

Cloud computing provides the IoT architecture with the resources and computational requirements. The driving force behind using cloud computing is its configurable resources. Cloud computing includes three main services Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). These models make computing easy in various environments. Although integration of cloud computing with IoT has numerous advantages, it faces many issues with respect to massive scaling, object identification, the naming of objects, mobility support, mapping of different protocols, architectural dependency, interoperability, security, and privacy etc. The proposed architecture ensures the security of data. It also addresses the issues of interoperability along with issues regarding scalability.

The paper is organized as follows. Section I presents Introduction. Section II presents a literature survey. Section III explains the existing architecture for hybrid cloud architecture and their work in general. Section IV describes the issues involved in the integration of cloud and IOT. Section V gives a brief about the proposed architecture and its explanation. Section VI gives the flowchart of the project with logic. Section VII shows the test results. Section VIII outlines the conclusion of the architecture.

.

II. LITERATURE SURVEY

Cloud-integrated IoT is not a newly introduced concept. Developing new technologies for increasing the security and interoperability was the subject on which maximum effort was made on. This section summarizes the various related studies.

In SHCEI architecture, users can also share data, resources and functionalities with other private cloud by using internet on the conceptual, logical, and procedural level and this technology is known as Cloud Federation [1]. The author has presented an architecture which is supposed to solve the technical issues involved with the IoT such as the deployment, discovery, management, and interoperability of many varieties of smart objects deployed in large quantities. To this end, a sensor-centric framework called the 'IoT Cloud' [2] was developed which supports an extensible set of sensor-types and large numbers of possibly, geographically distributed smart objects. The author suggested that the cloud-based embedded system programming is the integration of cloud computing with Wireless Sensor Networks which resulted in another architecture called "Cloud of Things" [3]. A brief about the various major and minor architectural changes made through the period, research projects employed, issues and future direction of Cloud IoT [4] which gave us a better idea regarding where we are heading is provided. An extensible Apian a cloud-compatible open source controller, known as '**IoT Cloud**' [5], enabled the developers to create scalable sensor-centric applications using public cloud and high-performance IoT. Due to their short ranges, sensor networks have limited communication to the external world. Gateways are usually used to export WSN data to other devices connected to the Internet. Also, WSNs have to be characterized by high heterogeneity because of the number of propriety and non-proprietary solutions. There is then a need for complex application specific conversions to be implemented on the gateways

Revised Manuscript Received on May 30, 2019.

Suma M.R, Electronics and Communication Engineering, DSCE, Bengaluru, India.

Dr. Madhumathy P, Electronics and Communication Engineering, DSCE, Bengaluru, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

for communication between different standards [6]. When Iota's of entirely different and unexpected things would be asking for resources on a cloud, resource allocation would be a challenge. Because it would be very difficult to decide how much a particular resource may be required by an entity or a particular IoT. Depending upon the sensor and the purpose for which sensor is being used, the type, amount, and frequency of data generation, resource allocation has to be mapped. Sending a sample packet from the newly added node can also be useful. [7]. The average recognition rate of a single electronic appliance can reach 96.14%, where the parallel electronic appliance recognition is carried out without presenting any power usage conditions, and the recognition rate can be higher than 84.14%, thus, validating the feasibility of a lightweight electronic [8]. Apart from increasing workload, decreasing idle time of servers and improving the overall cost-efficiency ratio, the approach eases software updates for manufacturers inside the legally non-relevant section [9]. The author has proposed an Open IoT [10] based open service framework to clear the way into IoT related mass market. The sensor communicates with the M2M devices directly and with the public cloud through a web portal for any data.

III. EXISTING SOLUTIONS

IoT and Cloud are different technologies that are assessed separately. IoT and Cloud integration is provided with data storage facility for the data sensed from the sensing devices and the solution for energy-related issues.

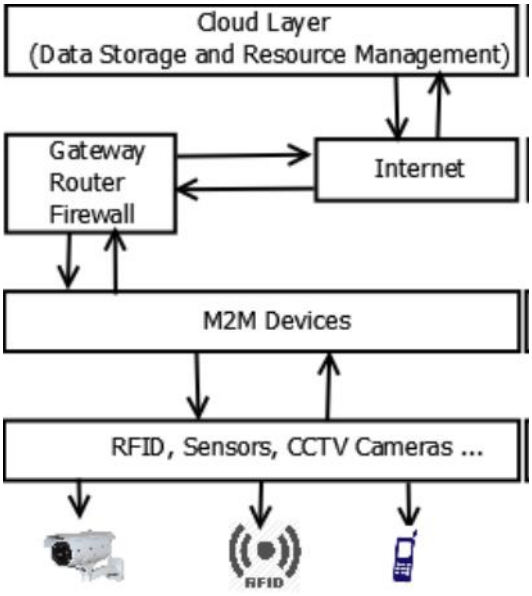


Figure 1: Basic architecture of Cloud-IoT integration

The sensory data collected from different sensors is sent to the M2M devices as shown in f Figure 1. The data from the machine to machine devices is sent through the gateway which routes the traffic from the device to the network serving the web page and blocks the traffic for a particular IP addresses or server ports that are not authenticated. The huge data coming from the gateway are pushed to the public cloud through the internet. Constrained Application Protocol (CoAP) along with SOAP and RESTful Web Services were used to provide a request/response interaction model between application end-points. This architecture uses Future Grid Cloud services instead of GAE, Amazon EC2 and Microsoft Azure platforms.

IV. PROBLEM STATEMENT

The previously proposed architecture was all aimed at specific objectives which were being fulfilled perfectly fine. However, they all had major flaws which cannot be overlooked.

The architecture on OPENIOT required the devices to communicate with the public cloud through web portals for any data. Also, data management becomes very difficult due to the availability of a large amount of data. In case of the IoT Cloud architecture, the issues are the security breach and minor jitters due to the presence of message brokers. The Cloud-integrated IoT architecture using sensor clouds have issues like tampering/stealing sensor data in raw/processed form. The communication channel between client, sensors, and cloud are vulnerable to side channel information leak.

Accessing public cloud infrastructure is nothing but utilizing the internet for transport. But this model is filled with risk of an attack, hack, or data loss. If public cloud model cannot offer effective separation and segregation of customer data, then it is likely to even come to market. Also accessing the public cloud involves a lack of visibility into the rented infrastructure that is enjoyed by an enterprise within its own environment. This could pose risk and compliance obstacles for companies that must adhere to certain industry-specific standards.

The sensitive data and business pertinent environments which have to be moved to the public cloud can require authorization and nightmare levels of bureaucratic red tape. Ironically, an environment that is more secure, easier to manage, and better backed-up than ones hosted on premise can be created by implementing and following AWS best practices. With the emergence of large companies like Microsoft and Amazon entering the public cloud marketplace, many major companies have felt more comfortable moving to the cloud.

Protocols may also present challenges to businesses in moving their IT structure to a public cloud. It is impractical to run apps in the public cloud for certain high-speed functions. When a number of networks are accessing the public cloud, there is a need forcontinuous updating of the networks regarding their entry and exit from the node, which otherwise will lead to chaos.

Our project aims at integrating both private and public cloud which gives rise to a Hybrid cloud. The

proposed architecture improves security by storing confidential and sensitive information in the private cloud. The private cloud is provided with authentication mechanism which provides additional security. This sensitive information can be accessed only by the respective organization or user. The non-sensitive information will be stored in the public cloud and is publicly accessible. While using a single public cloud and few private clouds, there is a need for interaction with one another to get faster and accurate services. Hybrid cloud provides the opportunity to shift the heavy lifting of the network off-premises and, in doing so, improves the availability, scalability, and reliability of the connection by leveraging the provider's network investment. The extra cost of purchasing exclusive server hardware can be saved by using the Hybrid cloud. Hybrid clouds can be operated at any time and from any part of the world. This gives them a global reach for businesses that want to spread their reach beyond geographic boundaries. Also, in case of outages, fair reliable connectivity is provided by this architecture.

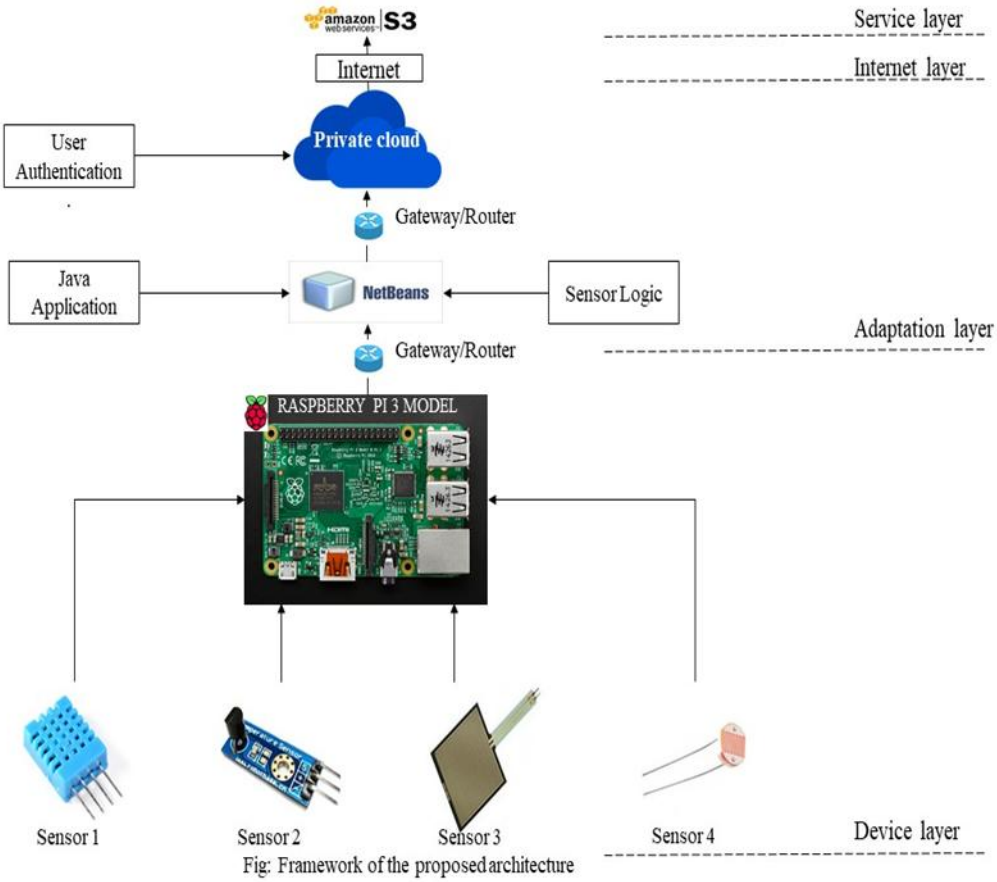


Fig: Framework of the proposed architecture

V. PROPOSED ARCHITECTURE

In this section, we propose an architecture using a hybrid cloud for deploying IoT with security as the crucial requirement. The architecture has four layers which interact with each other via gateway/router.

The fundamental layer is the device layer which accommodates the IoT smart objects such as sensors which interacts not only with humans but also with each other to share information. Sensors sense the variations of phenomenon such as change in temperature, humidity, pressure. This data is obtained in various forms such as text, image, and signal and are used to interact among them. Different sensors are integrated using microcontroller and theIoT/device layer is formed. Most popular choices of microcontrollers, in the present days, are Raspberry Pi, BeagleBone Black, Arduino, MSP 430 etc.

Public clouds are services provided by cloud service providers on the internet for web servers or applications where security is not paramount concern. The resources are shared between multiple users publicly and the data is accessed by anyone who can access the cloud. In contrary, private clouds are deployed inside firewalls and are used by organizations that have security and data privacy as their top priority. To ensure this security, data collected from the IoT is stored in the public cloud which is present in the Adaptation layer. User can use web application through protocols namely HTTP, CoAP or MQTT. However, these protocols are constrained to specific applications and cannot be used for ubiquitous computing. In order to solve this, a service-oriented protocol called Simple Object Access Protocol (SOAP) can be used. With the help of Cloud federation, users can also share data, resources, and functionalities with other private cloud over the internet. By encouraging distinct private cloud to process disparate data collected from the IoT devices, adaptation layer helps enhance interoperability.

Worldwide communication for exchange of information

between different private clouds and uploading of the processed data from private to a public cloud for global access is carried out by the Internet layer. Cloud Federation can also be implemented here.

The service layer contains public cloud which provides SaaS. Information stored in the public cloud is available to be utilized by all users. Data acquired from the sensors are visualized by accessing various web services with the aid of SOAP architecture.

A. WORKING

The client sends the data gathered by the sensors in the device layer to the private cloud. The introduction of private cloud is the first point of security in the architecture. This also upgrades the scalability and interoperability issues faced in the previous architectures. The data is processed in the private cloud according to the user's wish. The private cloud can only be accessed by the users who are authenticated with user id and password. This is the second point of security. In the private cloud, a logic is instituted which enables users to decide which data needs to be pushed to the public cloud and which needs to remain back in the private cloud. This is the third and the final point of security.

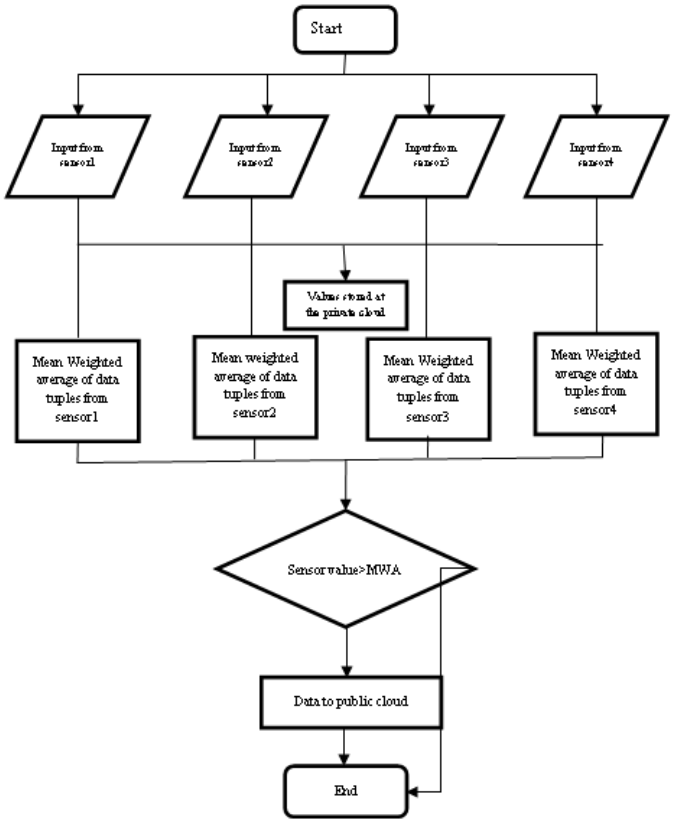
Cloud computation takes place in a heterogeneous environment. Hence in order to facilitate easy interaction of these clouds, it is very essential to develop generality, simplicity and flexible usability among them. For this purpose, the client and service should be supportive of extensible markup language (XML). XML acts as a translator for both sides.

In the above diagram shown, the IoT device i.e. sensors along with Raspberry Pi is the client. NetBeans is an integrated development environment for Java which permits application development. NetBeans has a default web server called Glassfish which helps in creating the web service in which the logic of the architecture is written. Web service is written on top of the Glassfish server. Public cloud service used for storing the populated data from the private cloud is S3 (simple storage service) of Amazon web service (AWS).

When the web service wants the client to dispatch the gathered data, it signals the client with its location in the form of a WSDL (web service descriptive language) URL. At this point, a stub is created at the server side which converts the URL into XML format. The client senses the arrival of the signal from the service and hence creates a skeleton layer. The skeleton converts the URL present in XML format into a format understood by the client. The data is then sent to the web service after being interpreted by the skeleton and then the stub. The collected data is subjected to the logic given in the web service by the user which allows the required data to be sent to the public cloud. The entire set of data (including the one pushed to the public cloud) is also retained in the private cloud.

VI. FLOWCHART

The logic followed in our project is meaning weighted average of the values obtained from the IoT smart devices i.e. sensors. The values collected from each of these sensors are arranged as separate packets. These packets in the form of documents are stored in the private cloud along with the specific time of upload. Data from each of these sensors are grouped as tuples containing 10 data at a time and are subjected to the main logic of the program. This logic decided whether the data should be retained in the private cloud or pushed to the public cloud for third-party usage. Mean weighted average of the data in the form of tuples from each individual sensor is obtained. Now individual sensor values are compared with their corresponding mean weighted average value. If the individual sensor value is less than the mean weight average (or vice versa depending on the need of the application), then it is retained in the private cloud else it is pushed to the aws (public cloud). Data from aws can be used by the third party for various applications.

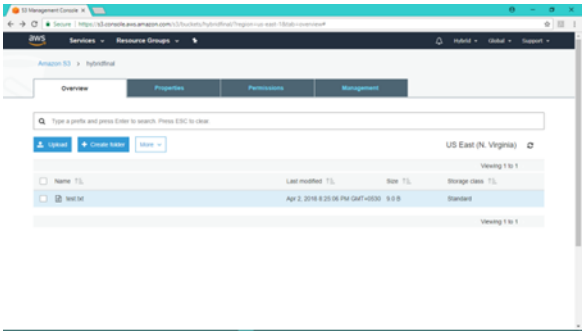


VII. TEST RESULTS

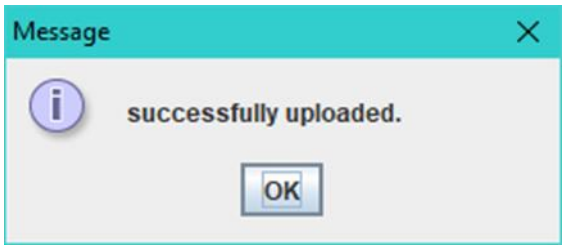
The test results of the proposed architecture are shown in snapshots below.

A) Start of a new web service.

B) Amazon Bucket



C) Response of successful Amazon uploads



VIII. CONCLUSION

Cloud Computing and IoT have given rise to easy data access from remote locations. Due to the surge in Smart devices in the present days, securing the data has become a priority. Security breach has given rise to a number of architectures which intend at resolving the issue in hand. The proposed architecture aims at eliminating the problems regarding user authentication and data security by the implementation of a private cloud in the form of a web service to provide secure and seamless communication between the network and the sensors. In order to address the issue of security and communication between distinct private clouds Cloud Federation is used.

REFERENCES

1. AVANI SHARMA_,TARUN GOYALY, EMMANUEL S. PILLI_, ARKA P. MAZUMDAR_, M. C. GOVIL_, R.C. JOSHI "A SECURE HYBRID CLOUD ENABLED ARCHITECTURE FOR INTERNET OF THINGS" 2015 IEEE 2ND WORLD FORUM ON INTERNET OF THINGS (WF-IOT) YEAR: 2015,PAGES: 274 - 279
2. PRAHLADA RAO B.B, PAYAL SALUJA, NEETU SHARMA, ANKIT MITTAL, SHIVAY VEER SHARMA, "CLOUD COMPUTING FOR INTERNET OF THINGS & SENSING BASED APPLICATIONS,"2012 SIXTH INTERNATIONAL CONFERENCE ON SENSING TECHNOLOGY (ICST).
3. TJ. ZHOU, T. LEPPANEN, E. HARJULA, M. YLIANTTILA, T. OJALA, C. YU, H. JIN, L. T. YANG "CLOUD THINGS: A COMMON ARCHITECTURE FOR INTEGRATING THE INTERNET OF THINGS WITH CLOUD COMPUTING".
4. A. BOTTA, W. DE DONATO, V. PERSICO, A. PESCAPE, "ON THE INTEGRATION OF CLOUD COMPUTING AND INTERNET OF THINGS," INTERNATIONAL CONFERENCE ON FUTURE INTERNET OF THINGS AND CLOUD (FICLOUD), 2014.
5. GEOFFREY C. FOX, SUPUNKAMBURUGAMUVE, RYAN D. HARTMAN",ARCHITECTURE AND MEASURED CHARACTERISTICS OF A CLOUD-BASED INTERNET OF THINGS," INTERNATIONAL CONFERENCE ON COLLABORATION TECHNOLOGIES & SYSTEMS (CTS), IEEE, 2012.
6. J. TAN AND S. G. M. KOO, "A SURVEY OF TECHNOLOGIES IN INTERNET OF THINGS," IN IEEE INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING IN SENSOR SYSTEMS (DCOSS), 2014, PP. 269-274.
7. .M. AAZAM, I. KHAN, A. A. ALSAFFAR, AND E.-N. HUH, "CLOUD OF THINGS: INTEGRATING INTERNET OF THINGS AND CLOUD COMPUTING AND THE ISSUES INVOLVED," IN 11TH INTERNATIONAL BHURBAN CONFERENCE ON APPLIED SCIENCES AND TECHNOLOGY (IBCAST), 2014, PP. 414-419.
8. S.Y. CHEN, C.-F. LAI, Y.-M. HUANG, AND Y.-L. JENG. "INTELLIGENT HOME-APPLIANCE RECOGNITION OVER IOT CLOUD NETWORK". IN WIRELESS COMMUNICATIONS AND MOBILE COMPUTING CONFERENCE (IWCMC), 2013 9TH INTERNATIONAL, PAGES 639–643. IEEE, 2014
9. ALEXANDER OPPERMANN; FEDERICO GRASSO TORO; FLORIAN THIEL; JEAN-PIERRE SEIFERT "SECURE CLOUD COMPUTING: CONTINUOUS ANOMALY DETECTION APPROACH IN LEGAL METROLOGY", 2018 IEEE INTERNATIONAL INSTRUMENTATION AND MEASUREMENT TECHNOLOGY CONFERENCE (I2MTC), YEAR: 2018, PAGES: 1 – 6
10. JAEHO KIM, JANG-WON LEE, OPENIOT: AN OPEN SERVICE FRAMEWORK FOR THE INTERNET OF THINGS, 2014 IEEE WORLD FORUM ON INTERNET OF THINGS (WF-IOT).

AUTHORS PROFILE

Suma M R

Suma M R is working as Assistant Professor at Dayananda Sagar College of Engineering Bengaluru, Karnataka, India. She completed her engineering from Mysore University, M.Tech from VTU and Pursuing Ph.D. from VTU University .She has rich experience in teaching for about 20 years. Her area of interests includes Embedded Systems, Wireless communication, Internet of Things, Computer Networks .She has published 10 papers in international, national journals and conferences.

Dr.Madhumathy P

Dr.Madhumathy P is working as Associate Professor at Dayananda Sagar Academy of Technology and Management, Bengaluru, Karnataka, India. She completed her engineering from Anna University in 2006, M.E (gold medallist) from VMU in 2009 and Ph.D. from Anna University in 2016.She has rich experience in teaching for about 12 years. Her area of interests includes Computer networks, Wireless communication, wireless sensor networks, Internet of Things, Wireless Channel Modelling, Mobile communication and topics related to networks and wireless Communication Domains. She has published more than 60 papers in international, national journals and conferences. She is a life member in ISTE. She serves as a reviewer for IEEE, IET, Springer, Inderscience and Elsevier journals. She has registered and published one Indian Patent.