International Journal of Multidisciplinary Research and Modern Education (IJMRME)
ISSN (Online): 2454 - 6119
(www.rdmodernresearch.org) Volume I, Issue II, 2015

HYBRID CLOUD ARCHITECTURE FOR INTERNET OF THINGS

Vijayamala S Yakri* & Priya Thomas**
Krupanidhi Group of Institutions,
Bangalore, Karnataka

Abstract:

Significant progress in the field of digitization, Internet and the worldwide web makes it possible to communicate between two computer host systems worldwide. Pervasive or omnipresent computation enhances it to a degree which can be conveyed by two erudite physical objects, anywhere. The Internet of Things (IoT) is a new paradigm which emerges from omnipresent computing which in conjunction with different technology, enables contact between several real objects. Integrating IoT into cloud storage provides various benefits when storing and manipulating big data from heterogeneous devices. Since both innovations have a tremendous influence on many fields of use, including smart house, smart agriculture, health care etc. Protection is one of IoT Cloud architecture's most critical problems. We suggest a stable hybrid, cloud-enabled IoT architecture (SHCEI) in this article (both public and private cloud). This architecture guarantees intra-domain data protection and also tackles scalability and interoperability problems. We also illustrate some of the research problems in the application of the combined Cloud and IoT architecture.

Key Words: IoT; Hybrid Cloud; Social IoT; Security; Scalability; Interoperability

Introduction:

World Wide Web's third generation, i.e. Web 3.0 of Universal and Widespread Computing has proliferated [1]. The modern age of Web 3.0 stresses the relation of actual objects and people to the internet through ever-present communication technologies. The Internet of Things (IoT) is a new Web 3.0 technology which brings about a new revolution in all-round communication. IoT was initiated in 1999 with the idea of incorporation of radio frequency identifiers (RFID) and sensors at the Auto-ID Center by the Kevin Ashton from the Massachusetts Institute of Technology (MIT) [2]. The IoT offers Machine-to-Machine (M2M) connectivity with transmit intelligence and decision-making capabilities between intelligent objects by combining a range of techniques, such as sensor, actuator, ID, monitoring and enhanced communication protocols [3-4]. IoT equipment has low power consumption, small battery weight, powered batteries, and minimal computing and storage capacity characteristics. IoT system resource limitations hinder effective IoT implementation in different emerging areas such as medical, transportation, logistics, and where the processing of large volumes of data and high power computing is needed. Effective IoT implementation in these areas requires adequate means of storage for heterogeneous data produced from numerous sources.

Cloud infrastructure [5] is one of the architectures to support the IoT architecture in terms of its device and resource specifications. The main factor behind Cloud computing is its configurable tools and facilities that can be supplied in the form of the Software as a Service [5], [6], Platform as a Service [6]. Even though many benefits can be obtained from the cloud-enabled IoT phase, the incorporation of cloud in the IoT ecosystem is complicated by wireless mobile tools such as large scaling, entity recognition, object labeling, heterogeneous nets, support to mobility, reliance on architectures, protection and privacy, mapping of protocols, robustness and so on [7]. Security is a critical problem for effective and secure data exchange in the IoT world.

Heterogeneous IoT system network enforced by distinct homogeneous networks has numerous security risks. Various architectures that incorporate IoT in a cloud were suggested in literature, but none considered intra-level information and services security. Users should be given such access privileges to a certain domain for creating a protected contact framework. To facilitate this feature a hybrid cloud structure can be used. This paper proposes an architecture that is stable, hybrid, cloud-enabled, i.e. SHCEI that uses public and private cloud to guarantee confidentiality and connectivity to a single domain. We propose the SHCEI adaptation layer which uses a private cloud to facilitate protection through intra-networking details. It also tackles the challenges in the heterogeneous IoT world of scalability and interoperability. Adaptation Layer also catches the benefits of federated cloud by sending / receiving information, resources and functionalities through various private clouds over the internet.

Literature Survey:

IoT and Cloud are different and separately tested systems. Cloud integration with IoT is important for data storage and energy-related solutions [8] to be supported with sensing devices. In this section, we will address the scope and shortcomings of many of the current architectures.

In IoT Cloud [9], sensors and messages can be handled online with various modules such as Controller, Message Broker, Sensors, Client, and GPS. The system elements are controlled by the controller. Message Broker maintains the low message routing information. In order to sensor clients, objects, targets and their availability, sensors are used by intelligent objects. To use a particular feature, customer subscribes to sensor data. The GPS Module connects sensors, M2M modules and IoT Cloud controllers to each other. Instead of GAE, Amazon EC2 and Microsoft Azure, this architecture uses Future Grid Cloud services [10].

Cloud Thing [11] provides online applications and services infrastructure for development, implementation, operation and composition. The IaaS, PaaS and SaaS services cloud services provide a service platform, a developer suite and a work portal. It uses the Restricted Application Protocol (CoAP) to provide an interface application / response model between application end points. It works on the Low Power WLAN (6LoWPAN) IPv6 based message frame format definition, fragmentation method and header compression techniques, which have to be fitted to IPv6/UDP datagrams in the very small IEEE 802.15.4 frame size.

Open IoT [12] is an open-source architecture based on SaaS. The sensors communicate directly with the M2M devices in this architecture and the cloud only contains databases. For any data, sensors must communicate with the Cloud via the Web portal.

In research, health, management, awareness, security etc the above architectures can be implemented. The sensor can be connected directly to M2M devices and the M2M devices can communicate via protocols such as CoAP, SOAP and REST ful Web Services to the cloud server. All of the architectures discussed use the public cloud only (GAE, Microsoft Azure, Amazon EC2, Future Grid, etc.). It is not possible to manage things jointly between the private and the public hybrid cloud. In the initial stage of deployment, these architectures implement all resources and features on their own. If there is a new resource requirement, the user must change and re-deploy the entire system. There is still no concept of sharing resources among clouds. In our suggested SHCEI architecture, the issues in the current architectures are discussed in a certain way.

Integration Issues in IOT and Cloud:

Although it provides many advantages, integration of Cloud with IOT has many issues [7]. Some of these issues are discussed here.

A. Communication:

- The flow of data from massive IoT objects into the cloud in order to cache, device and sustain the desired performance latency. In multi-hop contact, this delay can be caused by excessive processing on IoT computers.
- Extremely dense data are available from both required and redundant IoT devices. Unnecessary data transfer should not always be necessary. This data influx leads to insufficient use of capital on IoT's cloud side.

B. Security and Privacy:

- The security is one of the key problems to be solved in cloud IoT communication. IoT's wireless nature makes them vulnerable to various forms of security threats from insiders and externals. The continuing contact between IoT devices, or between IoT network and cloud interface may be disrupted by an attacker. The corrupted IoT/cloud connectivity negatively impacts secure and effective cloud data storage.
- Consumers use a wide array of public methods to reach the modern world with new computer types and heterogeneous networks. The adapted global method which captures user personal information cannot be managed by individuals. Through better access to servers, the publicly identified user information is retained for a long time, which encourages sensitive information to be revealed. Cloud use for IoT data management makes secrecy impossible by allowing all users to access information worldwide.

C. Management:

- The Cloud environment resource management is necessary to prioritize and satisfy the requests dynamically in real time. Cloud administrator finds it incredibly difficult to assess how much of basic resources a system requires.
- It's a daunting job to handle large volumes of data composed of highly regarded data combined with inaccurate data.
- Tracking mobile objects in the cloud-IoT environment to monitor their identity and location is a challenge. In order for clouds to provide omnibus connectivity between objects, information about objects relating to their location must be modified.

D. Services:

- The cloud manager (broker) in the IoT powered cloud is in charge of finding new customer resources. IoT functions, including the link or node leave of the network, create obstacles to explore new services for cloud administrators.
- Artifacts in IoT vary in several respects, e.g. computing capacity, band width demand, network interface and coverage (IP and Non-IP). To ensure smooth connectivity between artifacts in order to achieve an accurate service definition, publication and discovery process, interoperability solution should be maintained.

E. Architecture:

- The device-level protocol framework supporting cloud interface is important for proper IoT cloud realization. For low power energy, energy-reduced IoT net works, current protocols do not work well. A typical cloud-based architecture is required to support IoT with the cloud.

- Using IPv6 to classify the large number of IoT users. Cloud-IoT architecture needs an appropriate framework for facilitating IPv4-IPv6 coexistence.
- It is a challenge that needs to be overcome to manage distributed objects on a single network (i.e. in the cloud). Clouds must enforce an interoperability protocol for heterogeneous and distributed devices to allow interface for multiple devices to scalable the network.

F. Commercial Aspects:

- From the business perspective, IoT cloud integration involves price services issues. The estimation of tools available in the cloud relies on the cloud providers picked. While private cloud usage eliminates security risks, connectivity costs can increase communication costs. An optimized solution that blends public cloud with private cloud can be used to cope with such a trade in cost-security.

Proposed Architecture SHCEI:

In this section, we offer SHCEI, hybrid cloud architecture for deploying IoT while maintaining security. The SHCEI architecture is divided into four different levels – Device Layer, Adaptation Layer, Internet Layer and Service Layer. We talk briefly about each of these layers in the following paragraphs.

A. Device Layer:

The SHCEI architecture is founded on the Device Layer, where different smart objects communicate to each other to share information, according to IEEE802.15.4 and IETF IoT Specifications. Various technologies (i.e. smart objects) may be implemented to allow connectivity between nodes on the basis of domain criteria such as:

- Low power, low cost sensor motors for Wireless Sensor Networks (WSN).
- Smooth access to Mobile networks.
- For secure communication, connectivity-oriented Ethernet.

The most suitable technology for communication between physical objects is WSN [14] and Radio Frequency Identification (RFID) [15]. RFID system consists of several RFID tags (single identity attachments) and few RFID readers RFID systems (to read identity of objects). The 64- or 96-bit RFID tag can be used to store the unique EPC global ID of objects. Wireline sensor nodes equipped with several sensors acquire data, whether direct or via multi-hop communication in different forms (text, signal, image and video). These objects form clusters of various applications-based domains. Each cluster has one or more coordinating nodes, which have been designated to control the work and communication of other nodes. Compared to the other nodes or slave nodes, master nodes have more power and resources. Either through the master node or ad hoc, the slave nodes communicate. Every master node in a cluster sends data through a particular gateway to the adaption layer that allows heterogeneous networks to develop. Various latest micro controllers for IoT development with various sensors, such as Arduino, Raspberry pi, Beagle Bone Blacks etc [16], are available in the market.

The devices communicate with each other through mobile networks supplied by different carriers worldwide during mobile communication. These devices can then travel smoothly around coverage areas and connect through mobile gates.

Ethernet can also be used for certain sensing devices in situations where the node does not need to be transferred from locations and stable communication is required, but it is primarily used for communication from a gateway to the top layers. For example, some master nodes may need safe and stable connections to the gateway.

B. Adaption Layer:

The confidentiality of information can be breached from the outside with a shared cloud for access to data and resources. Private clouds have such rules that are outlined by a particular storage agency to discourage consumers from receiving all sorts of resources. Data obtained from the System Layer was first stored in a private cloud through gateways to ensure the protection of data within a single domain. In a business in which clouds can provide services like SaaS, Paas and IaaS for its internal customers, this layer offers data storage in private cloud.

In order to deliver a low weight infrastructure, online cloud providers use the REST ful [17] and the SOAP architecture [18]. REST implements operations of the GET, POST, PUT, CRUD (Creation, Reading, Update and Delete) protocol, and DELETE. SOAP administers the data of the sensor and its geographical position. Users will use the HTTP [19], CoAP [20] or MQTT protocols for use on the Web server. Constrained Application Protocol (CoAP) is a Web transfer protocol used between low power wireless networks integrated with HTTP interfaces. The application layer is a RESTful web transfer protocol. CoAP is less difficult to parse, has less overhead and operates on the User Datagram Protocol (UDP). The HTTP is a simple text-based protocol which supports many libraries. HTTP is a simple text code. The HTTP client in IoT-drives operates for half-duplex mode and extremely complex TCP (small eight-bit micro-controller devices).The MQTT is primarily configured to serve loss networks with minimal overheads of around two bytes in each post. It is used to publish and subscribe efficient bandwidth for data transportation, but does not provide device-to-device transmission or multi-cast.

Incorporating REST / CoAP into the Web and WSN with web applications (REST / HTTP) via CoAP / HTTP proxy enables visualization of WSN measurements in the CoAP-based HTTP web browser. The Datagram Transport Layer Security (DTLS) protocol guarantees data security. The use of private cloud on each domain reduces access to information from external users, which in essence, guarantees data protection within a particular domain.

SHCEI architecture allows for the use of internet on the concept, conceptual and procedural levels to exchange data, resources and functionalities with other private clouds and is known as the Cloud Federation. One company will in future be able to expand its working area to one more location with emerging technology and protocols. There is no need to update old setup to exchange data and services from different places. Adaptation Layer ensures safety not only through private cloud but also takes into account the problems of scalability and interoperability in a heterogeneous IoT setting. With the heterogeneous data obtained from various IoT devices stored in distinct private cloud, heterogeneous data on the same cloud eliminates complications. The collection and access of enormous data through standard protocols on the same platform solves interoperability problems. Although there are major benefits in implementing adjustment layer in the Cloud-IoT environment, additional overhead data problems may be present in SHCEI.

C. Internet Layer:

Internet Layer provides global connectivity between various private clouds for sharing of information. Then data can be stored and downloaded from these private clouds into a public cloud for global consumer access. This layer also includes tools and functionalities for communication between shared and private clouds through the Internet. In this layer, as the cloud communication mechanism is given, the principle of cloud federation, discussed in the previous paragraph. Both protocols and hardware

used in this layer must support IPv6 for Internet operation, in order to allow a wide number of devices in IoT.

D. Service Layer:

Users connect services or data via a shared cloud through multiple organizations. The SaaS and pooled resources are accessible worldwide through the public cloud. CoAP/HTTP/MQTT protocols can be used to consult different web resources that help to envision the details gathered by WSN embedded in RESTful and SOAP architecture.

Applications of SHCEI:

SHCEI can be helpful in different fields where safe data sharing such as healthcare and social IoT is required (SIoT). The collection and storing of information on patients, physicians and other personnel is a central element in the area of healthcare. Diagnosis of patients allows the corresponding doctor to have knowledge of their disease and different medical history. Some of them are classified and confidential. This is possible with the SHCEI adaptation plate.

SIOT incorporating the social networking idea with IoT is another field in which SHCEI can be applied. To allow social networking between various organizations, institutes or domains, SIoT requires safe communication of information. Social IoT autonomously creates social links to the individuals who are connected to it in order to improve contact and cooperation between human beings and objects. However, intelligence would be limited to local optima if a particular manufacturer's domain is used. By using knowledge from many collaborative social networks, the question can be solved. In addition to the gains obtained by this partnership, privacy is still a big concern. Information exchange within these social networks should take into account the sensitivity of users and protect people's privacy. Similar to the previous example, the SHCEI adaptation layer can also handle the privacy requirement in this situation.

Research Challenges:

While our proposed SHCEI architecture offers a modern structure for deploying IoT with the cloud, certain SHCEI architecture integration problems need to be resolved. Here we discuss some of the big issues:

- Overheads: The use of SHCEI architecture's private public cloud infrastructure gives rise to overheads. Data transmission between private and public clouds creates needless overheads that in turn impact the time, memory, bandwidth and other cloud resources.
- Data Transmission: Cloud-IoT data transmission requires powerful IoT devices recognition management to provide underlying service efficiency. The IPv6 addressing can be used to recognize large number of IoT artifacts. A coexistence IPv4-IPv6 mechanism must have been introduced by SHCEI architecture.
- Data integrity: Use of public-private cloud structure produces SHCEI architecture data integrity issues. Besides this the transmitted data generates redundant information among numerous clouds. In order to ensure efficient and consistent service delivery to customers, an effective framework for handling redundant data and for data security is important in the proposed architecture.
- Resource Management: Resource management and scheduling are essential for safe and productive usage of cloud services. Where and how many services are required is hard to decide. There is a need in the private and public clouds of the proposed system to incorporate an effective resource management algorithm and scheduling process.

- Protocol Mapping: Whilst SHCEI architecture uses a standard IEEE and IETF-compliant protocol structure, protocol mapping for different device types and at a different cloud level is an important problem. An effective mapping mechanism is required for the proposed architecture in order to maintain interoperability between IoT devices.
- Federated Cloud: Different challenges are involved in sharing resources and technologies between different SHCEI network clouds. Private clouds are imposed by the organization that uses the cloud with certain policies and laws. Some protocols should be followed to allow access to cloud services for the use of services of another cloud. A logical and conceptual level Architecture is needed which uses list of resources available on each cloud and signs SLA between clouds.
- Pricing: The cost of implementation is one of the most important aspects of any architecture. SHCEI deployment is subject to price issues because both private and public data storage clouds are implemented. The use of intra-domain private clouds leads to high costs that cannot be achieved in an application environment which is costly.

Conclusion:

SHCEI, an architecture that ensures security for the heterogeneous network data in IoT environment while ensuring scalability and interoperability, is proposed. While bringing the two all-embracing technologies together to speak, we discussed various integration issues and derived mutual benefits from their strengths and offer great services to users. In the proposed architecture, we added an adaptation layer that implements private clouds, which provides safe and seamless network and sensor communication. In addressing the security issue and the communication between private clouds, we used the Cloud Federation. There are also some of the research challenges facing the proposed architecture.

We would like to take on the challenges of research in the future and develop an IoT Cloud prototype model that secures both inter and intra-level data. To ensure its applicability, we will attempt to apply the proposed architecture in real time. We expect to use fewer resources, expand on most effective protocols and to have sufficient service level agreements in place for data exchange and resource sharing for our future strategy.

References:

1. J. Hendler, “Web 3.0 Emerging,” Computer, vol. 42, no. 1, pp. 111-113, 2009.
2. http://postscapes.com/internet-of-things-history.
3. 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.
4. L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787-2805, June 2010.
5. P. Mell and T. Grance, “The NIST definition of cloud computing,” 2011.
6. B. B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, “Cloud computing for Internet of Things & sensing based applications,” in 6th International Conference on Sensing Technology (ICST), 2012, pp. 374-380.
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. A. Botta, W. de Donato, V. Persico, and A. Pescape, "On the Integration of Cloud Computing and Internet of Things," in International Conference on Future Internet of Things and Cloud (FiCloud), 2014, pp. 23-30.
9. https://sites.google.com/site/opensourceiotcloud/.
10. G. C. Fox, S. Kamburugamuve, and R. D. Hartman, "Architecture and measured characteristics of a cloud based internet of things," in International Conference on Collaboration Technologies and Systems (CTS), 2012, pp. 6-12.
11. J. Zhou, T. Leppanen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, H. Jin, and L. T. Yang, "Cloud things: A common architecture for integrating the internet of things with cloud computing," in 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), IEEE,2013, pp. 651-657.
12. J. Mineraud, O. Mazhelis, X. Su, and S. Tarkoma, "Contemporary Internet of Things platforms," arXiv preprintar Xiv:1501.07438, 2015.
13. N. Mitton, S. Papavassiliou, A. Puliafito, and K. S. Trivedi, "Combining Cloud and sensors in a smart city environment", EURASIP Journal on Wireless Communications and Networking, Vol. 2012, no. 1, pp. 1-10, 2012.
14. I. F. Akyildiz, W. Su, Y. Sankara Subramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer networks, vol.38, no. 4, pp. 393-422, 2002.
15. S. Hodges and D. McFarlane, "Radio frequency identification: technology, applications and impact," Auto-ID Labs WhitePaper Series, vol. 1, 2005.
16. http://postscapes.com/internet-of-things-hardware.
17. A. Rodriguez, "Restful web services: The basics," IBM developer Works, 2008.
18. G. Alonso and F. Casati, "Web services and service-oriented architectures," in 21st International Conference on Data Engineering, ICDE, p. 1147.
19. U. Hunkeler, H. L. Truong, and A. Stanford-Clark, "MQTTS–A publish/subscribe protocol for Wireless Sensor Networks," in 3rd International conference on communication systems software and middleware and workshops, comsware, 2008, pp.791-798.
20. Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," 2014.