A Survey Paper on Secure Integration of IoT and Cloud Computing using Agent Mechanism

Shwetal M. Sathavara
Department of Computer Engineering
LDRP College, Gandhinagar

Dr. Sanjay G. Patel
Assistant Professor
Department of Computer Engineering
LDRP College, Gandhinagar

Dr. Hiren Patel
Head of the Computer Department
Department of Computer Engineering
LDRP College, Gandhinagar

Abstract

Cloud computing integrating with Iot is a new technology which refers to an infrastructure where both data storage and data processing operate outside of the mobile device. Another recent technology is Internet of Things. Internet of Things is a new technology. The IoT Agent Platform mechanism to separate IoT functions from physical devices and to run isolated IoT functions on cloud environment. This is a transparent programming framework for IoT devices where we don't care about communication, server side programming or database.

Keywords- Internet of Things, Cloud Computing, IoT Security, Agent Mechanism

I. Introduction

The best definition for the Internet of Things would be defined by ITU-T Y.2060:
"Global infrastructure for the society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies."
IoT is such a system that supplies connectivity and interactive communication. A thing at this moment in the IoT environment can be a man-made object, a person with a heart monitor implant, any animal with a biochip transponder and any vehicle with sensor. All these things are assigned with one unique IP address and have the ability to transfer data over the Internet. So far, IoT closely related to Machine-to-Machine (M2M) communication in manufacturing, oil, and gas, power industries.

Internet of Things (IoT) hypothesis is that the objects or things interact and exchange large scale information. Organizations use IoT devices to collect real time and continuous data and make better business decisions to increase customer satisfaction. An operation has to store data generated from the Internet of Things and this data grows exponentially, it forces to think about cloud storage for storing IoT data.

The cloud was an adorable choice for IoT data storage, various organizations store this information on site considering it is either costly or sensitive to store on the cloud. The cloud has more advantages to store IoT data than on-premises storage. First, a direct connection is provided between the devices and the public cloud provider. This direct link allow storing data faster therefore, it need less storage and lower per-device cost. Second, data management and storage management is the cloud provider problem therefore organization has to use the service only. Cloud becomes an absolute storage location for storing and processing IoT data but there are some problems to use the cloud for IoT data Storage. The main and major issue is security of cloud storage. In many situation data collected from IoT devices is more sensitive or very relevant for the organization. When cloud storage is used, then organizations worried about the cloud security issues.

We focus on protecting physical devices from illegal access by intruder. It avoids the risk of being infected by malware and being abuse as well as revealing data from physical devices. To think of IoT security, in particular protecting physical devices from illegal access by intruder, we have to understand some fundamental gaps between physical devices and embedded IoT software in terms of features, lifecycle, ownership, maintenance, user attention, developer skills and so on. we summarize and give basic analysis for such fundamental gaps between physical devices and embedded IoT software. We can specify that the critical difficulty in IoT security is implementing both of device functions and IoT. we can protect physical devices from illegal access by intruder, we have to understand some fundamental gaps between physical devices and embedded IoT software in terms of features, lifecycle, ownership, maintenance, user attention, developer skills.

We summarize and give basic analysis for such fundamental gaps between physical devices and embedded IoT software. We also clarify that the critical difficulty in IoT security is implementing both of device functions and IoT functions on a same physical device. We could minimize the cost to protect such devices. We describe the concept and the basic architecture of IoT Agent Platform.

A big challenge of this paper is proposing transparent development model for designing and implementing IoT functions on cloud environment. This makes it possible to separate IoT functions from physical devices. We introduce the Cloudsim which is a transparent programming framework for IoT devices. The framework makes it simple and easy to develop IoT functions without special knowledge of communication, server-side programming or database.

II. Objectives

Our Main Objective was bridging Fundamental gap between physical devices and embedded IoT software. We also resolve that the difficulty in IoT security is implementing both of device functions and IoT functions on a same physical device. Analyzing deep analysis for IoT devices another objective of this paper is explaining the architecture of IoT Agent Platform where we have virtual clones of physical devices on cloud environment. A leading concept of the platform is that we would separate IoT functions from physical devices and run such isolated IoT functions on cloud environment.

The Internet of Things is composed of three key parts:

1) The ‘‘things’’ (objects).
2) The communication networks that connect them.
3) The computer systems via data streaming from and to objects.

The main intense of the interaction and cooperation between things and objects sent through the wireless networks is to fulfill the objective set to them as a combined entity. In addition, based on the technology of wireless networks, both the technologies of Cloud Computing and Internet of Things grow rapidly. In this survey paper, we represent a survey of integration of IoT and Cloud Computing with a focus on the security issues of both technologies. Specifically, we combine the two aforementioned technologies (i.e. Cloud Computing and IoT) in order to review the common features, and in order to describe the major characteristics of their integration.

A. IoT and IoT Security Issues

The Internet of Things is a network of devices that transmit, share, and use data from the physical environment to provide services to individuals, corporations, and society. Also, the Internet of Things has different applications in health, transport, environment, energy or types of devices: sensors, devices worn/carried (wearable), e.g. watch, glasses, home automation.

Some examples of IoT sectors are listed below:

1) Smart solution in the bucket of transport
2) Smart power grids incorporating more renewable
3) Remote monitoring of patients
4) Sensors in homes and airports
5) Engine observing sensors that identify & predict maintenance issues

1) IoT Security Issues

IoT security is the area of protecting safeguard with connected devices and networks in the Internet of things. The Internet of Things involves the quick acknowledgment of objects and entities – known, in this context as things – provided with distinctive identifiers and the ability to repeatedly transfer data over a network. Significant escalation in IoT communication originate from computing equipments and embedded sensor systems used in industrial machine-to-machine (M2M) communication, smart energy grids, home and building automation, vehicle to vehicle communication and adjustable computing devices. The main problem is that because the idea of networking instruments and other objects are relatively new, security has not always been considered in product design. IoT products are often wholesaled with ancient and unpatched embedded operating systems and software. Moreover, consumers often flop to shift the default passwords on smart devices—or if they do change them, lose to select sufficiently strong passwords. To develop security, an IoT device that demand to be instantly accessible over the Internet, should be segmented into its own network and have network access restricted. The network segment should then be examined to distinguish potential anomalous traffic, and operation should be taken if there is a problem. Security experts have warned of the potential risk of huge numbers of unsecured instruments connecting to the Internet since the IoT concept was first proposed in the According to Proof point, more than 25% of the botnet was made up of devices other than computers, including smart TVs, baby monitors and other household appliances.

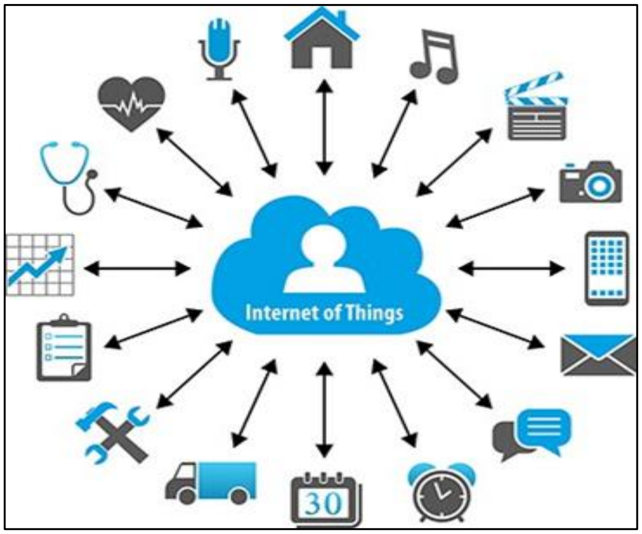

Fig. 1: Internet of things Technology

B. Cloud Computing and Cloud Computing Security Issues

Cloud computing offers computing, storage, services, and applications over the Internet. In general, to restore smartphones energy efficient and computationally efficient, major revolution to the hardware and software levels are required. This associates the cooperation of developers and manufacturers. Mobile cloud computing is well-defined as an combination of cloud computing technology with mobile devices in order to sort the mobile devices resource-full in terms of computational power, memory, storage, energy, and context awareness. The technology of Mobile Cloud computing is the outcome of interdisciplinary procedure for combining mobile computing with cloud computing. Thus, this disciplinary domain is also referred as mobile cloud computing. There are two aspects in which the term Mobile Cloud refers: (a) infrastructure based, and (b) ad-hoc mobile cloud. In the infrastructure based mobile cloud, the hardware infrastructure persists static and also provides services to the mobile users. (see Fig. 2).

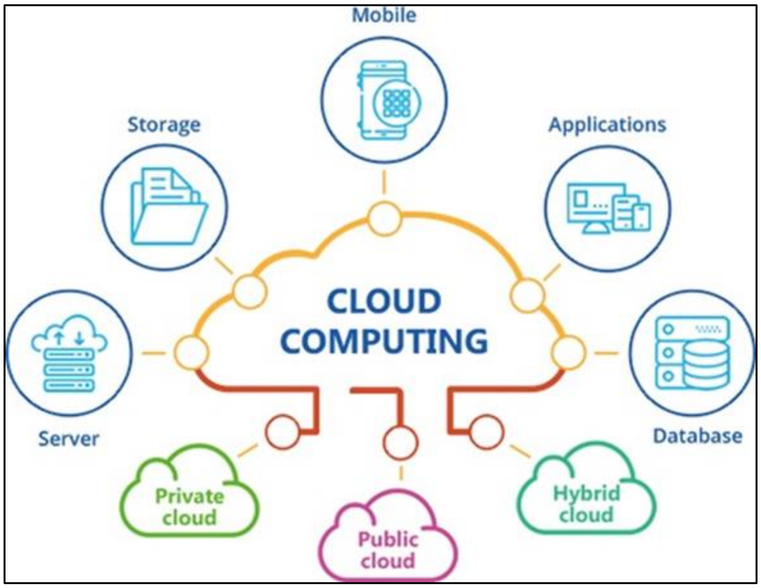

Fig. 2: Cloud computing Technology

Cloud Computing technology has some characteristics which conclude its function.
(a)Storage over Internet(b)Service over Internet(c)Applications over Internet(d)Energy Efficiency(e)Computationally Capable.

1) Cloud Computing Security

Cloud security is an advanced sub-domain of computer security, network security, and, more broadly, information security. It assigns to a wider set of policies, technologies, and controls deployed to secure data, applications, and the related infrastructure of cloud computing. Cloud computing and storage solutions produce users and enterprises with various potentiality to store and process their data in third-party data centers. Organizations use the Cloud in a variety of numerous service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community). There are a number of safekeeping regards connected with cloud computing.

These consequences fall into two wide-ranging categories -Security concerns faced by cloud providers (organizations providing software, platform, or infrastructure-as-a-service via the cloud) and security outcomes challenged by their customers. The burden is shared, however. The provider need guarantee that their infrastructure is secure and that their clients' data and applications are secured while the user must take measures to support their application and use robust passwords and authentication measures.

C. IoT and Cloud Computing Integration

'Cloud Computing', has created its appearance in the last few years with the aim of providing approach to the information and the data from any place at any time, thus limiting or eliminating the need for hardware tools. The term 'cloud computation' is defined as the use of computing logistical assets, as well as the software level, through the use of services transported over the Internet.

Cloud computing services comprise one of the world's largest areas of contest between huge companies in the IT sector and software. Cloud Computing is a technology which can be set as a ground technology in the use of IoT. More specifically, Mobile Cloud Computing is defined as consolidation of cloud computing technology with mobile devices so as to make the mobile devices resourceful in terms of computational power, memory, storage, energy, and context awareness.

Mobile Cloud Computing is the result of interdisciplinary approaches, joining mobile computing and cloud computing. Cloud computing provides computing, storage, services, and applications over the Internet. The innovation in Mobile Cloud computing is the results of inter disciplinary method, combining mobile computing with cloud computing.

Some of the main features of the Cloud Computing technology which relate to the characteristics of both Internet of Things are: (a) Storage over Internet, (b) Service over Internet, (c) Applications over internet, (d) Energy efficiency and (e) Computationally capable.

III. IOT AGENT PLATFORM

There are wider unsafe gaps between device functions and IoT functions. A forthright idea to advance IoT security of IoT devices is splitting IoT functions from physical devices, that is, it seems reasonable to divide device functions and IoT functions and preserve both functions independently. In this section, we recommend IoT Agent Platform on cloud environment where virtual clones be existent for physical devices is that we would separate IoT functions from physical devices and run such solitary IoT functions on cloud environment. To furnish these objective, we have some hypothesis for communication model of IoT devices. Existing IoT devices are physical devices incorporated with embedded IoT software. Thus, IoT devices have both of device functions and IoT functions in a same physical device and communicate with IoT service systems or users. IoT service system runs on cloud to provide IoT application service. Users also synchronize and may communicate with the IoT service system or physical devices.

We focus to protect physical devices from evil intruders on the Internet, which is, securing IoT functions for IoT devices. Note that protecting IoT service systems, users, and securing communication between users and IoT service systems are out of scope in this paper.

A. Analysis of Fundamental Gaps

The fundamental gaps caused by having two functions in a same physical device, Now, we clarify gaps between device functions and IoT functions.

1) Scope

Scope of physical device is very tiny. For example, environment sensors may get air conditions, temperature or humidity in very small area. On the other hand, aim of embedded IoT software is universal. It must interconnect with IoT service system on cloud it might be somewhere on the Internet. It is enough to think of conditions in a very minor space to improve device functions, while we have to think of universal trend and prominent edge security technologies to change IoT functions.

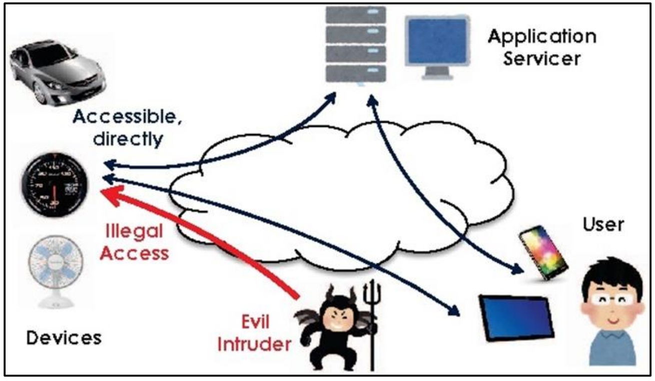

Fig. 3: Iot Agent Platform

2) Lifecycle

Lifecycle of physical devices and embedded IoT software is diverse. It is acute for IoT security issues, in particular the chance of fix or renew. Talking about physical devices, a user repairs a physical device when the device would be broken and the user still needs use the device. In other words, the user would not renovate the device if device function works or the user has no need to custom the device any more. On the other hand, IoT functions communicate with IoT service systems, continuously. We keep informed (that means, repair) such software as soon as probable when any IoT security problem would be found in the software, even if device function works or user has no need to use the device at all.

3) Identification

In the past, device dealers did not recognize device users, in many cases. Dealers change mass products, that is, common, standardized, designed for unknown users and sold such devices via distribution channel. Users bought such products at retail shops but there is no need for dealers to know who use such products. On the other hand, embedded IoT software's need to communicate with IoT service systems, and such systems always identified individual devices or users, by nature. The gap of unknown or identified user model causes big difference not only for service monitoring or maintenance but also for correspondence in the case of security accident.

4) Monitoring

It was not important for device dealers to know or to understand who use their products. It is not important to notice their products, as well. Maintenance of their products would be operated based on user report or user wish. On the other hand, embedded IoT software is connected to the public Internet. Of course real-time (or semi real-time) service monitoring and rapid maintenance on any security accident is very important from security point of view.

5) Consciousness

The most important gap between physical devices and embedded IoT software is consciousness. Historically, vendors developed physical devices as isolated products described in later. It is difficult for vendors to understand characteristics of connected embedded IoT software and to get the skill to design and implement such software especially from security point of view. Users also have consciousness of physical devices same as vendors. Users take care such devices only when they need to use. They don't have any interest on such devices, in most cases, even if there is a security incident.

B. Concept of IoT Agent Platform

Fig.4 shows the basic concept of IoT Agent Platform.

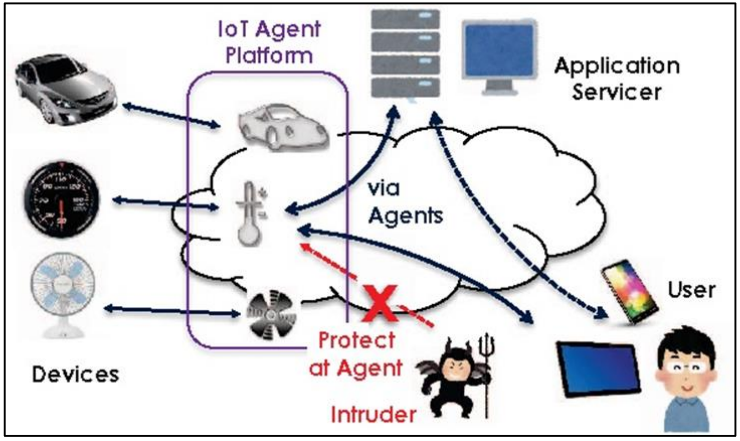

Fig. 4: Iot Agent Platform

Purple dotted oval means the platform on cloud environment. Any physical device has its virtual clone on the platform. The clone has riposte of the physical device status. The clone also has all functions to communicate with IoT service system, as well, and the physical device is restricted to communication with anybody other than the clone. The architecture insulates physical devices from the public Internet. Virtual clones act as gateways for physical devices to communicate with IoT service system. Of course, only way for exterior nodes (including evil intruders) to communicate with the physical device is admitted the clone.

C. Benefits of IoT Agent Platform

In the IoT Agent Platform model, we assume third party service operator would deliver cloud service and monitor or Sustain IoT software for virtual clones. The model separate not only IoT functions from physical devices but also operation and management roles from device vendors. The separation of device functions and IoT functions have lots of benefits, as described below.

1) Separated Scope

Vendors and users may have interest about small restricted area to use device functions, while the service provider watch global behavior of IoT functions and follow global trend, as well.

2) Separated Identification

Vendors do not need to identify users who use physical devices, while the service provider identify who and what devices are connected via IoT functions.

3) Separated lifecycle

Users may repair physical devices only when device functions has problems and users want use such functions, while the service provider keep IoT functions up to date and maintain whenever they found security issues.

4) Separated Monitoring

Vendors and users need NOT to monitor device functions by 7x24, while the service provider monitors any incident on IoT functions by 7x24.

5) Separated Consciousness

Vendors have interest about physical devices when they sell such devices. Users have interest about physical devices when they use such devices. Both vendors and users need NOT have interest about IoT functions when users don't use such devices. The service provider always takes care IoT functions, instead.

IV. TRANSPARENT DEVELOPMENT MODEL

To realize the IoT Agent Platform, it is very important to provide simple and easy mechanism to develop IoT functions outside physical devices, e.g., as a software component on cloud environment. In this section, we propose to apply the Dripcast. Which is a transparent programming framework for IoT devices, for implementing IoT functions on cloud environment.

A. *Dripcast Architecture*

The Dripcast is a framework for storing and processing Java objects. Any object has the world unique ID represented as UUID. The Dripcast framework always recognizes ID (explicitly or even implicitly) to identify the object on the cloud. The Dripcast framework consists of four components which are Client, Relay, Engine and Store.

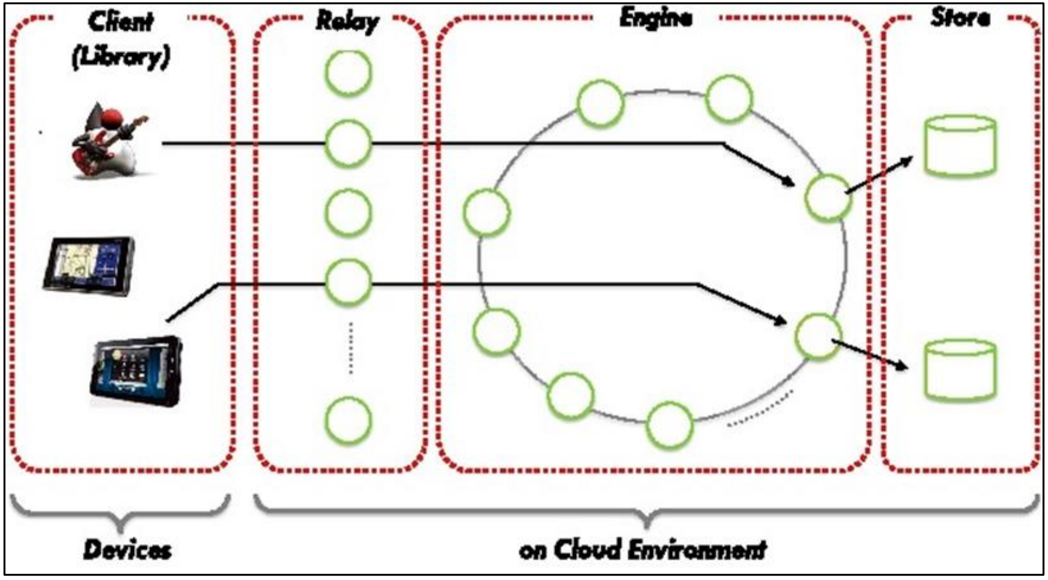

Fig. 5: Dripcast Architecture

1) Client

Client is a small Java library which works on user devices such as smartphones, tablets, and home gateways and so on. There are two major roles: (1) managing transparent Java objects in client devices, and (2) sending remote procedure call requests to the Relay.

2) Relay

Relay is a set of relay servers. A relay server is a distribution gateway, which receives requests (Job instances) from Client and delivers such requests to engine servers described in the next subsection. A relay server knows the association of ID and engine servers. The association is managed by Distributed Hash Table (DHT). There is only one engine server for an ID at the same time so that the distribution gateway can select the unique engine server for a request. Relay servers also deliver very simple operations such as create and remove data in the same manner. Relay servers are stateless so that the Relay mechanism would be highly scalable. Since the Relay is a only one entrance to access virtual objects on cloud environment, we design and implement strict access control on that. Any connection to the Relay from outside world would be encapsulated and required user/password (or authenticate key) access to establish the session.

3) Engine

Engine is a set of engine servers. Each engine server has its own key space assigned by DHT, so that it would read, write and process Java objects in a consistent environment for authorized key space. Each engine server runs JavaVM. In other words, the engine is the distribute JavaVM for parallel and distributed processing environment, managed by DHT. The most important role of an engine server is executing the Java method for remote procedure call requests encapsulated in Job instances when an engine server receives a Job instance which contains ID, method-name, argument-classe and arguments. The server loads the Java object with ID as the key from the Store, and tries to invoke the method of the object specified by the method-name and argument-classes with given arguments. If there is any change in the object, the engine server stores it back into the Store. Finally, the engine server returns the result back to the relay server that sent the request. Engine servers are not connected to the public Internet at all so that the servers are accessible only from Relay servers. Engine servers also have strict access control for virtual objects. When the servers would access objects, access permission based on user ID and access mode of READONLY, READWRITE.

4) Store

The Dripcast assumes there are highly scalable data store in backend. Any scale-out distributed No SQL might be applicable. Store should provide mechanisms for replication management and automatic failover for resiliency. The Dripcast may call the following methods with ID:
1) GET – get a serialized Java object.
2) PUT – put (update) a serialized Java object.
3) REMOVE – remove existing data.
Store servers are not connected to the public Internet as well so that the servers are accessible only from Engine Servers.

V. CONCLUSIONS

The Cloud Computing technology offers many opportunities, but also places distinct limitations as well. Cloud Computing apply to an infrastructure where both the data storage and the data processing happen outside of the mobile device. In this paper, we introduce a survey of Internet of Things Technology, with an explanation of its operation and use. Moreover, we present the main features of the Cloud Computing and its tradeoffs. Cloud Computing bring up to an infrastructure where both data storage and data processing happen outside of the mobile device. Also, the Internet of Things is a new technology which is growing rapidly in the field of telecommunications, and especially in the modern field of wireless telecommunications.

In this paper, we summarize the IoT security issues, in particular for protecting IoT devices. We clarify the gaps of physical devices and embedded IoT software that is gaps between device functions and IoT functions, from various points of view. Then, we proposed IoT Agent Platform so that we would improve IoT security in IoT devices. The basic concept of IoT Agent Platform is separating IoT functions from physical devices so that it isolates IoT security risk from the devices. In the IoT Agent Platform mechanism, a physical device has its virtual clone on cloud environment and any IoT functions would be implemented and provided by the clone. One of key challenge of this paper is proposing transparent development model for such virtual clones on IoT Agent Platform mechanism. In the development model, by applying the Dripcast framework, virtual clones are accessible transparently from physical devices (or others), while there is no need of taking care of server-side programming, database nor communication at all, Transparent development model enables very simple and easy development for device vendors to develop physical devices. The research of IoT Agent Platform mechanism with transparent development model gets started recently and we have a lot of research topics, such as variety of accessing and updating methods for virtual clones, detailed security model of virtual clones reducing the risk of revealing privacy information from virtual clones and so on. We will describe these topics in future research papers.

REFERENCES

[1] Ikuo Nakagawa, Shinji Shimojo Intec Inc., Japan Osaka University, Japan (2017) 'IoT Agent Platform mechanism with Transparent Cloud Computing Framework for improving IoT Security', IEEE 41st Annual Computer Software and Applications Conference,

[2] Christos Stergiou a, Kostas E. Psannis a, Byung-Gyu Kimb, Brij Guptac a Department of Applied Informatics, School of Information Sciences, University of Macedonia, Thessaloniki, Greece b Department of Information Technology (IT) Engineering at Sookmyung Women's University, Republic of Korea c National Institute of Technology Kurukshetra, India (December 2016) ' secure integration of iot and cloud computing', www.elsevier.com, (311338093),

[3] (https://en.wikipedia.org/wiki/Science_Publishing_Group)

[4] Engin Leloglu R&D Department, Vestel Electronic Inc., Manisa, Turkey (2017) ' A Review of Security Concerns in Internet of Things', Journal of Computer and Communications, 2017, 5,, (121-136),

[5] Jayant D. Bokefodea, Avdhut S. Bhiseb, Prajakta A. Satarkara and Dattatray G. Modanic (2016) ' Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption', International Multi-Conference on Information Processing-2016 (IMCIP-2016), 12th(121-136),

[6] Available at: www.sciencedirect.com

[7] Vageesh Mishra1, Prof. Pooja Kadam2 1,2Bharati Vidyapeeth Institute of Management and Information Technology (june- 2017) ' Security in Internet of Things', International Journal of Current Trends in Engineering & Research (IJCTER), 7th(Issue 06).

[8] Available at: http://www.ijcter.com

[9] Ikuo Nakagawa, Shinji Shimojo Intec Inc., Japan Osaka University, Japan (2018) ' Secure IoT Agent Platform with m-cloud Distributed Statistical Computation Mechanism', IEEE International Conference on Computer Software & Applications, 42nd( ), pp. [Online].

[10] Ikuo Nakagawa, Masahiro Hiji and Hiroshi Esaki Intec Inc., Japan Osaka University, Japan Tohoku University, Japan University of Tokyo, Japan (2016) ' Design and implementation of global reference and indirect method invocation mechanisms in the Dripcast', IEEE 40th Annual Computer Software and Applications Conference, 40th

[11] Sebastien Ziegler Mandat International Geneva, Switzerland University of Murcia Eunsook Eunah Kim Stefano Bianchi Softeco Sismat Genova, Italy (2017) 'ANASTACIA: Advanced Networked Agents for Security and Trust Assessment in CPS IoT Architectures', IEEE Annual Computer Software and Applications Conference

[12] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers (2017) 'Twenty security considerations for cloud-supported Internet of Things', IEEE INTERNET OF THINGS JOURNAL, ( ), pp. [Online]. Available at: http://www.ncr.nhs.uk/

[13] Shinsuke Tanaka Kenzaburo Fujishima Nodoka Mimura, Dr. Eng. Tetsuya Ohashi Mayuko Tanaka (2016) ' IoT System Security Issues and Solution Approach', IEEE INTERNET OF THINGS JOURNAL, 65(8)

[14] Bogdan Manat,e, Teodor-Florin Fortis, West University of Timis¸oara, Faculty of Mathematics and Informatics Viorel Negru Institute e-Austria Timis¸oara (2014) 'Infrastructure Management Support in a Multi-Agent Architecture for Internet of Things', European Modelling Symposium, 8th(),

[15] Philippe Massonet∗, Laurent Deru∗, Amel Achour∗, Sebastien Dupont∗, Louis-Marie Croisez∗, Anna Levin†, Massimo Villari‡, (2017) 'Security in Lightweight Network Function Virtualisation for Federated Cloud and IoT', International Conference on Future Internet of Things and Cloud, 5th(),

[16] Jaejin Jang, Im.Y Jung, Jong Hyuk Park,AnEffective Handling of Secure Data Stream in IoT, <![CDATA[Applied Soft Computing Journal]]> (2017), http://dx.doi.org/10.1016/j.asoc.2017.05.020

[17] Munindar P. Singh Department of Computer Science North Carolina State University Amit K. Chopra School of Computing and Communications Lancaster University (2017) 'The Internet of Things and Multiagent Systems: Decentralized Intelligence in Distributed Computing', IEEE International Conference on Distributed Computing Systems, 37th()