

# A Systematic Review of Information Security Frameworks in the Internet of Things

Mohammad Irshad  
Lead Architect System/Security  
Singtel Cyber Security Institute  
Singapore  
[irshad@ncs.com.sg](mailto:irshad@ncs.com.sg)

**Abstract** -- By 2020, it is estimated that the number of connected devices is expected to grow exponentially to 50 billion. Internet of things has gained extensive attention, the deployment of sensors, actuators are increasing at a rapid pace around the world. There is tremendous scope for more streamlined living through an increase of smart services, but this coincides with an increase in security and privacy concerns. There is a need to perform a systematic review of Information security governance frameworks in the Internet of things (IoT).

**Objective** -- The aim of this paper to evaluate systematic review of information security management frameworks which are related to the Internet of things (IoT). It will also discuss different information security frameworks that cover IoT models and deployments across different verticals. These frameworks are classified according to the area of the framework, the security executives and senior management of any enterprise that plans to start using smart services needs to define a clear governance strategy concerning the security of their assets, this system review will help them to make a better decision for their investment for secure IoT deployments.

**Method** -- A set of standard criteria has been established to analyze which security framework will be the best fit among these classified security structures in particularly for Internet of Things (IoT). The first step to evaluate security framework by using standard criteria methodology is to identify resources, the security framework for IoT is selected to be assessed according to CCS. The second step is to develop a set of Security Targets (ST). The ST is the set of criteria to apply for the target of evaluation (TOE). The third step is data extraction; fourth step data synthesis; and final step is to write-up study as a report.

**Conclusion**-- After reviewing four information security risk frameworks, this study makes some suggestions related to information security risk governance in Internet of Things (IoT). The organizations that have decided to move to smart devices have to define the benefits and risks and deployment processes to manage security risk. The information security risk policies should comply with an organization's IT policies and standards to protect the confidentiality, integrity and availability of information security. The study observes some of the main processes that are needed to manage security risks. Moreover, the paper also drew attention on some suggestions that may assist companies which are associated with the information security framework in Internet of things (IoT).

**Keywords**-- Information Security; Internet of Things; Systematic Review; Risk Management Framework; IoT Architecture

## I. INTRODUCTION:

The concept of Internet of stuff embraces several definitions depending on the meanings of the word The

Internet of things (IoT) define as a network of networks which enables the identifications of digital entities and physical objects. Today we see a shift in our conception of Internet of things a global network of “smart objects” which can be called “the Internet of things” (IoT). There is now a growing realization that this trend will continue as increasing numbers of even simpler, more constrained devices (sensors, actuators, home appliances, personal medical equipment) get connected to the Internet. The term “embedded Internet” is often used to refer to the part of the Internet that is invisibly and tightly woven into our daily lives [1].

Many of these applications have security requirements; for example, health information must only be made available to authorized personnel (authentication) and be protected from modification (data integrity) or disclosure (confidentiality) in transit. Even seemingly innocuous data such as temperature and pressure readings may need to be secured [2]. Consider the case of a chemical plant where sensors are used to monitor the reactions used in manufacturing the final product continuously without adequate security, an attacker could feed highly abnormal readings into the monitoring system ([2]-[3]), and trigger catastrophic result the areas that are expected to be directly affected initially includes healthcare ([3]-[4]), Supply chain management [5], transport system [6], agriculture and environmental monitoring[7]; life at home and more as we move towards “smart homes” and the next generation of smarter cities” [8].

## A. Growth of the IoT:

An important inflection point occurred in 2008 when the number of things connected to the Internet surpassed the human population. The adoption rate of the IoT is trending to be at least five times faster than the adoption of electricity and telephony.

\$4.6 trillion in government spending over the next decade, as IoT takes off, it will lead to lots of variabilities regarding network traffic, processing, and storage needs. For example, an unanticipated refrigerator defect could start a flood of log data that would need to be distributed and analyzed by manufacturers, parts suppliers, and distributors simultaneously, the same scenario would be true for other events like a global pandemic, active hurricane season, or a water shortage; but despite this variability, network-based sensors will also enhance capabilities for capacity planning by collecting vast amounts of data for analysis. This review will result in pattern recognition that can help predict impending utilization spikes.

The evolution of Internet of things leads to a need for the proper assurance security framework which deals with the different levels of safety and against which the smart devices can be secured [Sloan (2009 [8]), Subashini (2011). S. Raza et al. [7], has provided end-to-end (E2E) secure communication between IP enabled sensor networks and the traditional Internet. This is the first compressed lightweight design, implementation, and evaluation of 6LoWPAN extension for IPsec. Their extension supports both IPsec's Authentication Header (AH) and Encapsulation Security Payload (ESP). Thus, communication endpoints can authenticate, encrypt and check the integrity of messages use standardized and established IPv6 mechanisms.

Former Google CEO Eric Schmidt (2010 technology conference) declared that we now create as many data every two days as we did from the dawn of civilization until 2003, since it is an issue that cannot be tackled unilaterally [Ponemon Institute (2011)]. The ever-changing environment of IoT leads to a need for a suitable assurance framework which deals with different levels of security and against which IoT model can be secured [Sloan (2009,[8]); Subashini (2011)].Where there is less consensus is how best to implement security in IoT at the device, network, and system levels. Network firewalls and protocols can manage the high-level traffic coursing through the Internet.

Wang studied [10] A standards-based end-to-end security architecture for the embedded internet are predicting that the amount of global data generated will increase by a factor of 10x between now and 2020 as a result of IoT technology proliferation.

#### B. Overview of Internet of Things and its Features:

Zhang et al. [17] explained IoT (the Internet of things) means the network, which contains radio frequency identification (RFID) [14], [15], [16] infrared sensors, global positioning systems, laser scanners and other information sensing device. All things in IOT can be connected to the internet according to the agreement, and exchange the information, thus to achieve quick identification, location, tracking, monitoring, and management of a network. IOT is known as "the sensor system" in the international area, which is the concept of sensor networks in an expansion of things. IOT was proposed in 1999, and the traditional concept of IOT is "connected to the Internet of Things": firstly, all core and foundation things in IOT are based on Internet and IOT is the expansion and extension of Internet; secondly, IOT develops broader and deeper than that of Internet, it can make things exchange information between themselves anytime and anywhere. IOT represents the new direction of informatics.

#### C. The Architecture of the Internet of Things:

Many people [3], including myself [4] hold the view that cities and the world itself will be overlaid with sensing and actuation, many embedded in "things" creating what is referred to as a smart world, [Barbara Kitchenham 2007] carried out search for existing security Frameworks for IoT and their reviews showed a lack of publications dealing with these issues.

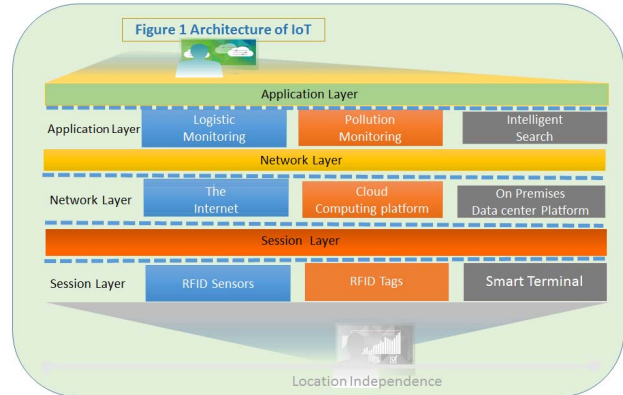


Figure 1: Architecture of IoT:

Figure1 illustrates the IoT reference architecture which can be considered as a three layers system consist of Session, Network and Application layer enabling IoT technologies. A description about these smart devices technologies while more details about reference architecture can presented by Atzori et al. [13].

Key information technologies such as middleware and sensor networking are now available and expected to become widely applied. The core technologies of The IOT includes radio frequency identification (RFID) devices, WSN(wireless sensors network) networks, infrared sensors, global positioning systems, Internet and mobile networks, network services, industry applications.

The IOT is composed of millions of different devices, such as sensors, smart cards and so on. These devices will not only directly convey information but also process the information in transition. IOT should have three characteristics, firstly, IOT is easy to fully aware, using RFID and sensors technology, such as two-dimensional code to catch the information about the access to objects at anytime and anywhere.

Secondly, IOT is reliable delivery, through the integration of telecommunications networks and the internet, real-time information about the object is accurately passed on.

Thirdly IOT is the kind of intelligent process, IOT makes use of cloud computing and fuzzy recognition and other intelligent computing technology, using the massive data and information analysis to achieve the intelligent control.

## II. RESEARCH AGENDA:

The objective of this papers is to propose comprehensive guidelines for systematic literature reviews appropriate for researchers. A systematic literature review is a means of evaluating and interpreting all available research relevant to a particular research question, topic area, or phenomenon of interest. Systematic reviews aim to present a fair evaluation of a research topic by using a trustworthy, rigorous, and auditable methodology multiple Security frameworks exist, but few of them specify differentiating procedures for IoT environments.

The recent emergence of IoT deployment signifies that more in-depth research must be undertaken to identify both the differentiating security framework of IoT and to rectify vulnerabilities and mitigate risks. Specifying the research question, which drives the systematic review methodology, is a critical step in the process.

In this paper, the research question focuses on identifying existing Security frameworks, initiatives that have been designed to be applied in IoT. The scope defined is, therefore, twofold, the review is aimed at comprehensive frameworks that deal with all the security aspects that may arise, from operational measures to management aspects, but particularly with the governance of information security. The approaches must consider the particular characteristics of IoT; only those initiatives that have been designed for the IoT model have been taken into account.

The structure of this paper is as follows: the following section 2 describes the systematic literature review process that has been conducted, detailing the steps involved; Section 3 presents a comparative framework in which a set of criteria related to the IoT is defined; Section 4 shows the main contributions of each Security framework in relation to the relative criteria; Section 5 contains the analysis results of the comparison performed; and finally, the review concludes in Section 6.

### III. METHODS: SEARCH STRATEGY FOR SYSTEMATIC LITERATURE REVIEW:

This section describes the process followed to perform a systematic review using a reliable methodology [Barbara Kitchenham (2004)]. The basic aim of a systematic review is to compile and evaluate the available research related to a question of interest, thus achieving unbiased, auditable and repeatable results. The review method presented in [Barbara Kitchenham (2007)] has been adapted to allow us to conduct our research in the field of IOT security governance. Although it might appear that the process is executed in a linear chain, it, in fact, produces its results through a sequence of iterations. Each cycle helps to refine each step in the process until appropriate results are attained.

A bibliographic reference has been used to keep track of each iteration and to record the whole process. The first step of evaluating a security framework by using common criteria methodology is to identify resources, the security framework for IoT is selected to be assessed according to CC standards. The second step is to develop a set of Security Targets (ST). The ST is the set of criteria to apply for the evaluation of the TOE, followed by data extraction; data structure; and data report.

#### A. Definition of Review Scope:

A precise procedure was needed to avoid biased results in the systematic review. In this section, we define the protocol followed in the literature review. Once the research question had been settled, a set of search terms was extracted from it. These terms, or keywords, were used in the review to identify all the relevant initiatives that were related to the research question and to attempt to answer it. A precise definition of the research terms is vital if comprehensive results are to be achieved without overlooking important approaches. The proposed research question embraces characteristics from different research areas; it was necessary to define the search terms in a way that all of them were included.

Some synonyms of the terms were also included to avoid the situation of a proposal being avoided because of the

different use of language. The proposed keywords that were used in the systematic literature review were the following:

IoT Security Framework  
IoT Security  
IoT Information Security Governance

This set of keywords was used to attempt to compile all the initiatives related to Security frameworks in the deployment of smart devices or IOT, selecting the sources in which the research will be developed is another crucial step.

We, therefore, chose a group of databases, some of which provide their engines to perform the searches. This choice was made by considering the general prestige of certain publications within the academic community, our previous knowledge of publications containing contents related to our research question, and sources suggested by authorities in the field.

The review was therefore executed on a variety of sources, including electronic databases, search engines, journals, magazines and conference proceedings. The sources chose to perform the systematic review are listed below.

- Application layer protection
- System Layer Protection
- Secure boot & secure firmware updates
- Secure communication
- Data at rest protection
- Embedded firewall & intrusion detection
- Key and certificate management
- Authentication & Authorization
- Integration with security management systems
  - a. Security policy management
  - b. Security event reporting
- Security framework must comply the following security policies and standards across the domain.
  - a. IT Security Policy
  - b. Network Security Policy
  - c. Access Control Policy
  - d. ICT Security Standards
  - e. Multi-tier IoT security (MTCS)
  - f. In cases where policy and procedures requirements cannot be complied with, the security framework, it must address the security risk assessment and an alternate control to mitigate the risk.
- Security framework must address the System security.

### IV. COMPARISON OF SECURITY FRAMEWORKS:

In this section, we introduce a comparative framework of security frameworks/security governance and provides a review of four different security frameworks for IoT and this paper will summarize the main contributions of each Security Frameworks analyzed in our systematic review in the light of the proposed common criteria standards (CCS).

The differentiating characteristics of each Security frameworks are therefore highlighted so that both clients and providers may easily distinguish which one suits their necessities for successful security framework.

The summary of the comparison of IoT has been explain in the summary table later section, security frameworks with defined criteria and the main concepts included in each Security Framework concerning the IoT related comparative criteria (Policies and Processes Adaptation, Control and Audit, security risk assessment and their applicability). In addition to presenting the main contributions, the table also shows an 'X' whenever a criterion is insufficiently developed, and lacks are evident. An '(\*)' is used to indicate the cases in which the subjects are dealt with in an external source that is different to the reference analyzed in our systematic review, but belongs to or is related to the same Security framework.

Generally speaking, a first glance at the table shows that most of the Security framework approaches offer recommendations or advice to cover the fields of the proposed criteria. The authors follow the widely known Plan-Do-Check-Act (PDCA) cycle suggested in popular security standards such as ISO/IEC 27001 [ISO/IEC (2005)].

#### A. Cisco Security Framework:

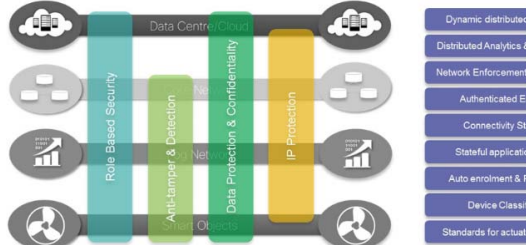


Figure 2: Cisco proposed Model for IoT:

Above figure shows the Cisco proposed security implications for IoT/M2M constructs are vast, deconstructing a viable IoT/M2M security framework which can be the foundation for the execution of security in IoT environments. The authors have proposed such a framework that may be used in protocol and product development, in addition to, policy enforcement in operational environments which suitable both for application and infrastructure.

The embedded endpoint layer is comprised of highly constrained devices, and so far, has limited the growth of malware to this layer. The growth of IP-based sensors corresponds to attack surface growth. This highlights the fact that new security protocols and identification techniques are required, and IoT endpoint security needs to correlate to its enhanced capabilities, clearly, IoT presents new challenges to network and security architects. Smarter security systems that include managed threat detection, anomaly detection and predictive analysis need to evolve. Windows and Linux based solutions are too big, power hungry and slow to support low-end IoT devices, this framework review will help to protect from physical attacks, such as DAR (data at rest protection) and Intrusion detection/prevention system (IDS/IPS).

#### B. Floodgate Security Framework:

This Security framework also fully comply with the ISA/IEC 62443 Compliance, ISA99 is an international standards organization defining the ISA/IEC 62443 cybersecurity standards for Industrial Automation and Control

Systems (IACS). A framework such as Icon Labs' Floodgate Security Framework, integrated with the MCU, provides IoT developers with the tools needed to secure their devices as per below figure3 illustrates in detail.

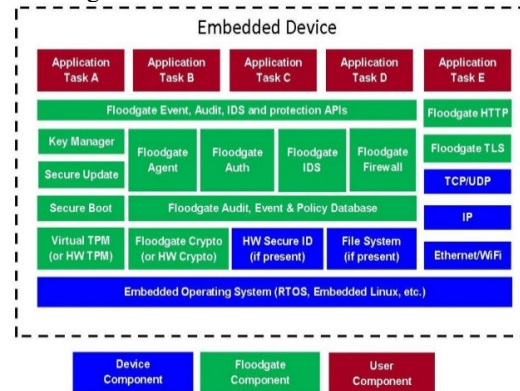


Figure 3: Floodgate Security Framework:

This security framework help securing IoT devices against today's cyber threats as well as future threats that will emerge during the lifetime of the device is a critical challenge for embedded developers. Low-end IoT devices require a custom solution, designed to meet the memory and performance requirements of these resource constrained environments.

#### C. CoAP Constrained Application Protocol Frameworks:

The framework consists of various modules to handle security and trust issues of IoT environments. The CoAP, the Constrained Application Protocol, Frameworks works at application layers first, Research efforts towards securing the IoT have thus mostly concerned designing lightweight variants and porting them to constrained devices, which led to a situation where the nearly standardized Constrained Application Protocol (CoAP) fully supports the application requirements. devices, due to their severe energy and memory constraints, heavily rely on group communication, asynchronous traffic, and caching billions of smart, but constrained objects wirelessly connected to the global.

#### D. OSCAR: Object Security Framework for Internet of Thing:

OSCAR security framework, analyzed by both Tanimoto et al. [17] and Alhomidi and Reed Tanenbaum, Bogdan, Maarten et al. [17] explores a novel approach to the problem of E2E security in IoT. This framework is based on the concept of object security that introduces security within the application payload. It was however considered separate confidentiality and authenticity trust domains.

Privacy is used as a means to provide capability-based access control and protection against eavesdropping during the communication. This security framework protects from replay attacks by coupling the content encryption key with the duplicate detection. Moreover, there is a need to specify the structure requirements based on the core framework. OSCAR also demonstrated the feasibility of the concept by evaluating

the proposal in the M2M communication scenario where all parties are resource constrained. Author believe that billions of smart, but constrained objects, encompassing IoT are the best argument for a scalable solution such as OSCAR

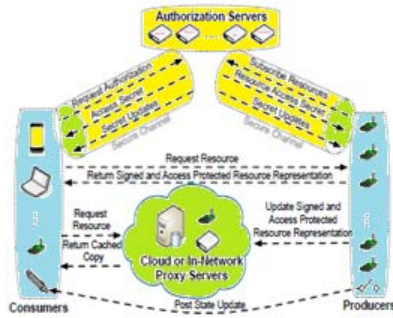


Figure 4: OSCAR Security Framework

OSCAR is particularly useful in Smart City deployments where energy constrained servers are expected to have a large number of clients. Moreover, there is a need to specify the structure requirements based on the core framework requirements: policies, standards, guidelines and procedures.

Moreover, leveraging the access right confidentiality domain and the concept of object security, our proposal intrinsically supports multicast. We take off the burden of a security handshake with every client from constrained servers. Instead, authors rely on secure communication channels with Authorization Servers that are in charge of resource access right key management. Cryptographic burden is then shifted to clients that need to perform signature verifications for the content they are interested in.

Table 1: Summary of the Comparison of IOT Security Frameworks with Defined Criteria

| Security Framework                                             | Policies, Standards, Process Adaption & Secure IOT Components                                                                                                          | Audit and Control                                                                                | Service Level Agreement                                                                                       | Applicability                                                               |
|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| <b>Cisco Security Framework</b>                                | Authentication<br>Authorization<br>Network Enforced Policy<br>Secure Analytics:<br>Risk and Assurance                                                                  | Threat Detection,<br>Anomaly Detection,<br>Predictive Analysis<br>contextual- Awareness          | X                                                                                                             | Infrastructure Framework                                                    |
| <b>Floodgate Security Framework</b>                            | Software APIs to enable secure boot<br>Hardware root of trust integration<br>Software based vTPM for legacy systems<br>Integration for secure remote firmware updates. | Runtime Integrity Validation (RTIV)<br><br>Application Guarding APIs<br>Internet security (DDOS) | Identify the threats and Floodgate firewall IDS Support<br><br>Compliance support<br>Security Evaluation      | Best Fit in Infrastructure Security Framework                               |
| <b>COAP (Constrained Application Protocol Framework)</b>       | IoT Smart Objects<br>Protocol suites.<br>CoAP, UDP, 6LoWPAN<br>IEEE 802.15.4e<br>provide the easy mapping to HTTP at the gateway                                       | X                                                                                                | X                                                                                                             | Best Fit in Application Security Framework                                  |
| <b>OSCAR: Object Security Framework for Internet of Things</b> | Technological Trends and Design Goals<br>Producer-Consumer Model<br>Fitting the Concept with the REST Architecture and CoAP<br>Object Security Approaches              | Access Control<br>Confidentiality<br>Authenticity<br>Availability                                | Analyzed and extracted risks of utilizing cloud computing by using the Risk Breakdown Structure (RBS) method. | Based on Object Security Approaches<br><br>Best Fit in application Security |

## V. RESULT

After reviewing four security frameworks, this study makes some suggestions related to information security frameworks in IoT. The organizations that have decided to move to IoT to define the benefits and risks of IoT and implement processes to manage security risk.

The information security risk management policies should comply with an organization's IT policies and standards to protect the confidentiality, integrity, and availability of security frameworks. The assessment of the IoT to evaluate the IoT plans and analyze the historical security status. The second step entails a risk analysis of IoT by identifying the assets, threats, and vulnerabilities.

Risk assessment is the third process in the implementation of risk management. Risk assessment means assessing security incidents from two dimensions, i.e., the likelihood and the adverse impact of an incident. After the risk management plans are implemented, there is a need for follow-on actions as part of a comprehensive assessment and continuous.

It is also suggested that OSCAR explores a novel approach to the problem of E2E security in IoT. It is based on the concept of object security that introduces security within the application payload. In this Frameworks confidentiality is used as a modes to provide capability-based access control and protection against eavesdropping during communications, authorization and authentication challenges for constrained environments which tackled separately.

## VI. CONCLUSION

IoT has the advantages of high efficiency and low costs, as well as scalability. As the march of IoT continues, security

issues have appeared. Indeed, the investigations in the IoT environment have mainly focused on the service side, while the security side has not been sufficiently looked at. Presented and compared four different Security frameworks that covered all of IoT deployment models. The comparison was undertaken according to the framework requirements as per ISO 27001 standard and the coverage area of the frameworks that were presented in this study, the paper sheds light on some suggestions related to the information security risk management in IoT.

Moreover, the study acquires different recommendations that may help enterprises with choosing between the existing Security frameworks. It is crucial to specifying the IoT deployment models, the purpose of the structure, and whether there is a need for one or more Security frameworks.

## REFERENCES

- [1] Jayavardhana Gubbia, Rajkumar Buyyab,\*, Slaven Marusic a, Marimuthu Palaniswamil., "IoT: A vision, architectural elements, and future directions," Future. Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013.
- [2] Andrea Zanella, Lorenzo Vangelista., "Internet of Things for smart cities," IEEE Internet Things J. , vol. 1, no. 1, pp. 22–32, Feb. 2014
- [3] Gang Zhao, "Holistic framework of security management for cloud service providers," in Industrial Informatics (INDIN), 2012 10th IEEE. (references).
- [4] John A. Stankovic, "Research directions for the Internet of Things," IEEE Internet Things J., vol. 1, no. 1, pp. 3–9, Feb. 2014
- [5] P. Johnson, "What are Policies, Standards, Guidelines and Procedures? | MindfulSecurity.com – The Information Security Awareness Resource." accessed in 20/4/2014
- [6] Malisa Vucinic, Bernard Touran cheau, Franck Rousseau, Andrzej Duda, Laurent Damon, et al. "OSCAR: Object Security Architecture for the Internet of Things" 2014 IEEE 15th International Symposium on, Jun 2014, Sydney, Australia. 2014".
- [7] S. Raza, S. Dequenne, T. Chung, T. Voigt, U. Roedig et al., "Securing Communication in with compressed IPsec," in DCOSS. IEEE, 2011, , pp. 1–8.
- [8] Sloan K (2009) "Security in a Virtualised Work" Network Security 2009; 15-18.
- [9] Barbara Kitchenham "Procedures for Performing Systematic Reviews" Keele University Technical Report TR/SE-0401 ISSN:1353-777.
- [9] Malisa Vucinic, Bernard Touran cheau, Franck Rousseau, Andrzej Duda, Laurent Damon, et al. "OSCAR: Object Security Architecture for the Internet of Things: IEEE 15th International Symposium on, Jun 2014, Sydney, Australia. 2014".
- [10] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, "SecureCloud: Towards a Comprehensive Security Framework for Cloud Computing" IEEE 34th Annual, pp. 393–398. 2010.
- [11] C. Wang, M. Daneshmand, M. Dohler, X. Mao, R. Q. Hu, and H. Wang, "Guest Editorial—special issue on the internet of things (IoT): architecture, protocols, and services," IEEE Sensors Journal, vol. 13, no. 10, pp. 3505–3508
- [12] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, 2009, pp. 50–55.
- [13] A. J. Stankovic, "Research directions for the internet of things," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3–9, 2014.
- [14] L. Atzori, et al. "The internet of things: A survey," in Computer networks, vol. 54 no.15, pp. 2787-2805, 2010.
- [15] A. M. Ortiz et al., "The cluster between Internet of Things and social networks: Review and research challenges," IEEE Internet Things J., vol., no. 3, pp. 206–215, Jun. 2014.
- [16] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework for creating a smart city through the internet of things," IEEE Internet of Things Journal, vol. 1, no. 2, pp. 112–121, 2014.
- [17] H. Zhou, et al., "A Cognitive Adopted Framework for IoT Big-Data Management and Knowledge discovery Prospective," in Proceedings of the IEEE.
- [18] T. Wiechert et al., "Connecting Mobile Phones to the Internet of Things", AMCIS' 07, Keystone, Colorado, USA, 2007.
- [19] T. Kriplean et al., "Physical Access Control for Captured RFID Data", IEEE Pervasive Computing, vol. 6, no. 4, pp. 48-55, 2007.
- [20] A. Juels, "RFID Security and Privacy: A Research Survey," IEEE Journal on Selected Areas in Communications, vol.24, pp. 381- 394, 2006.
- [21] Bogdan, Maarten et al, "A Security Architecture for Object-Based Distributed Systems" 18th Annual Conference (ACSACi02).
- [22] M. Ma, P. Wang, and C.-H. Chu, "Data management for an internet of things: challenges, IEEE International Conference on and IEEE Cyber, IEEE, 2013.