International Journal of Applied Research 2017; 3(9): 587-592

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2017; 3(9): 587-592
www.allresearchjournal.com
Received: 27-07-2017
Accepted: 28-08-2017

Dr. Syed Nisar Ahmed
Associate Professor of Physics, Osmania College, Kurnool, Andhra Pradesh, India

Correspondence
Dr. Syed Nisar Ahmed
Associate Professor of Physics, Osmania College, Kurnool, Andhra Pradesh, India

Analysis of security services in cloud based internet of things

Dr. Syed Nisar Ahmed

Abstract
Cloud computing technology is enabling IT to do more with the infrastructure that already exists, as well as adding new ways to expand capacity quickly and economically by using external cloud computing resources. Given the benefits of cloud computing, its broad appeal is not surprising. However, this new approach does raise some concerns. Chief among them is securing data in the cloud. Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Cloud Computing leverages many technologies (SOA, virtualization, Web 2.0). Cloud computing promises to make the billions of low-profile "things" in the IoT resource rich by enhancing their processing and storage capabilities, but it also brings forth security and privacy concerns. Smart devices have become an intricate part of our everyday lives. The development of these devices has also led to numerous notable innovations in communication technologies, which aim to improve connectivity and accelerate traffic flow. Information and communication technologies (ICT) are now moving toward the Internet of Things (IoT), a new paradigm in which smart objects or "things" interact with each other and with humans to achieve objectives. Conventional infrastructure security controls designed for dedicated hardware do not always map well to the cloud environment. Nonetheless, the concept of cloud computing for IoT brings forth security and privacy concerns. The comprehensive connectivity topographies of these technologies leave them open to malicious attacks and destabilization of normal processes and trust. In this article, we present an IoT cloud architecture that allows connection of users, their devices and the cloud system in a modular way.

Keywords: IoT, Cloud Computing, Sensors, Security

1. Introduction
Different parts of an application might be in different place in the cloud that can have an adverse impact on the performance of the application. Complying with regulations may be difficult especially when talking about cross-border issues – it should also be noted that regulations still need to be developed to take all aspects of cloud computing into account. It is quite natural that monitoring and maintenance is not as simple a task as compared to what it is for PCs sitting in the Intranet. Second, the cloud customers may risk losing data by having them locked into proprietary formats and may lose control over their data since the tools for monitoring who is using them or who can view them are not always provided to the customers [1]. In parallel, the emergence of the Internet of Things (IoT) that involves sensors embedded to every day devices promotes monitoring data produced by humans or by the environment in an automatic way. The concept of cloud computing gets significant attention during the latest years and many companies recognized the advantages and the impact can have in people's life. Today, it is evolved to an important technology for application developers and end users by allowing on demand and remote resource access. In a nutshell, cloud computing has enabled operations of large-scale data centers which has led to significant decrease in operational costs of those data centers. On the consumer side, there are some obvious benefits provided by cloud computing. Data loss is, therefore, a potentially real risk in some specific deployments.

1.1 Architecture of Cloud Computing

In this section, we present a top-level architecture of cloud computing that depicts various cloud service delivery models [2]. Cloud computing enhances collaboration, agility, scale, availability and provides the potential for cost reduction through optimized and efficient computing. More specifically, Fig.1. shows cloud describes the use of a collection of distributed services, applications, information and infrastructure comprised of pools of compute, network, information and storage resources Their methodology considers deduplication of encrypted data to save cloud storage space, reduce storage costs, and provide green cloud storage services by using the hash values of previously generated data. Different keys are used to provide different cryptographic services. If the storage request is from the data owner and the same data is already present on the cloud (verified by comparing hash values of stored and incoming data), the owner is notified and data isn't stored again [3]. If the storage request is from some other user, a request is sent to the data owner for verification. If the other user is allowed to access the data, it's reencrypted by the owner with a new set of policies and sent to the cloud. The cloud service deletes the old copy, saving the new one. Data from the requesting user isn't stored on the cloud. However, a new set of policies allows the user to download and decrypt the owner's copy of the data.

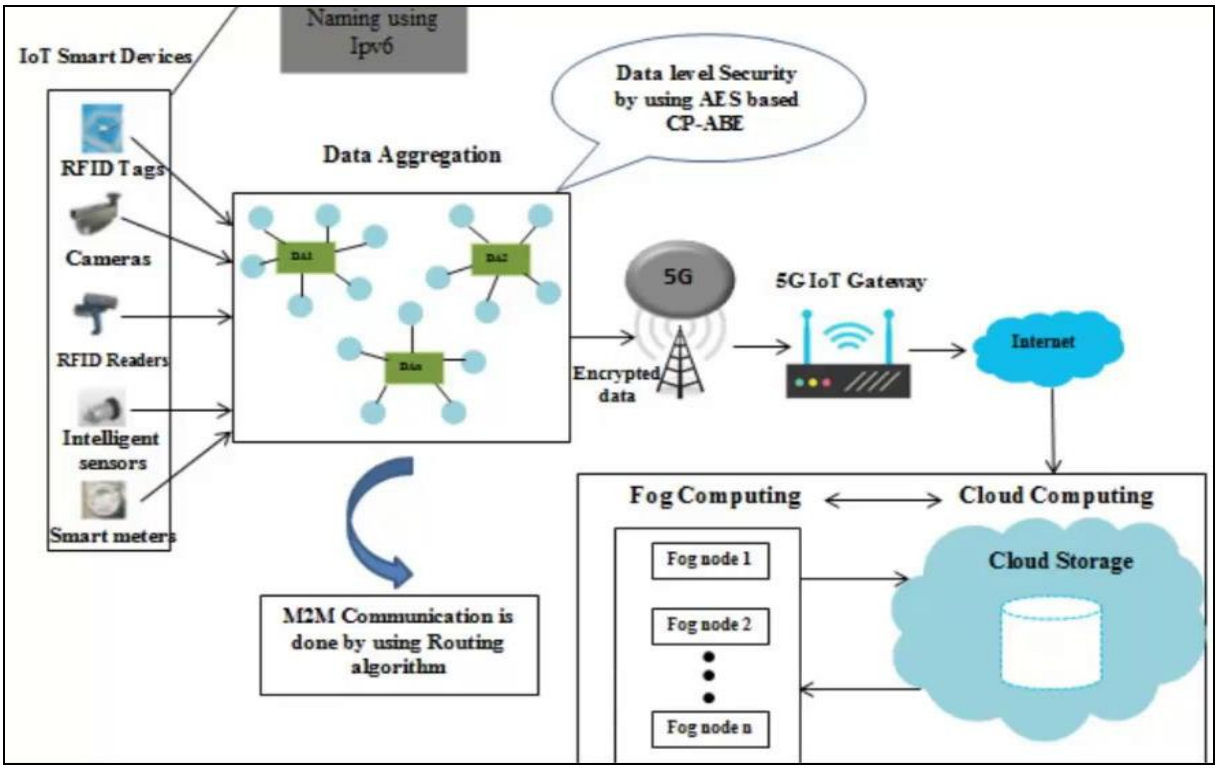

Fig 1: Architecture of Cloud Computing with IoT

These components can be rapidly orchestrated, provisioned, implemented and decommissioned using an on demand utility-like model of allocation and consumption. Cloud services are most often, but not always utilized in conjunction with an enabled by virtualization technologies to provide dynamic integration, provisioning, orchestration, mobility and scale.

2. Cloud Burst Security

There are many models available today which attempt to address cloud from the perspective of academicians, architects, engineers, developers, managers and even consumers. The architecture that we will focus on this chapter is specifically tailored to the unique perspectives of IT network deployment and service delivery [3, 4]. Cloud services are based upon five principal characteristics that demonstrate their relation to, and differences from, traditional computing approaches. These characteristics are: (i) abstraction of infrastructure, (ii) resource democratization, (iii) service oriented architecture, (iv) elasticity/dynamism, (v) utility model of consumption and allocation. One of the primary advantages of cloud computing is that enterprises can move applications that consist of several virtual machines to the cloud provider when the physical environment requires additional processor or compute resources. These bursting virtual machines need security policies and baseline histories to move with them. When a virtual machines moves, if the security policy does not accompany it, that virtual machines becomes vulnerable [5]. In addition, when virtual machines move, they lose their performance histories and administrators must re-evaluate the virtual machine performance baselines.

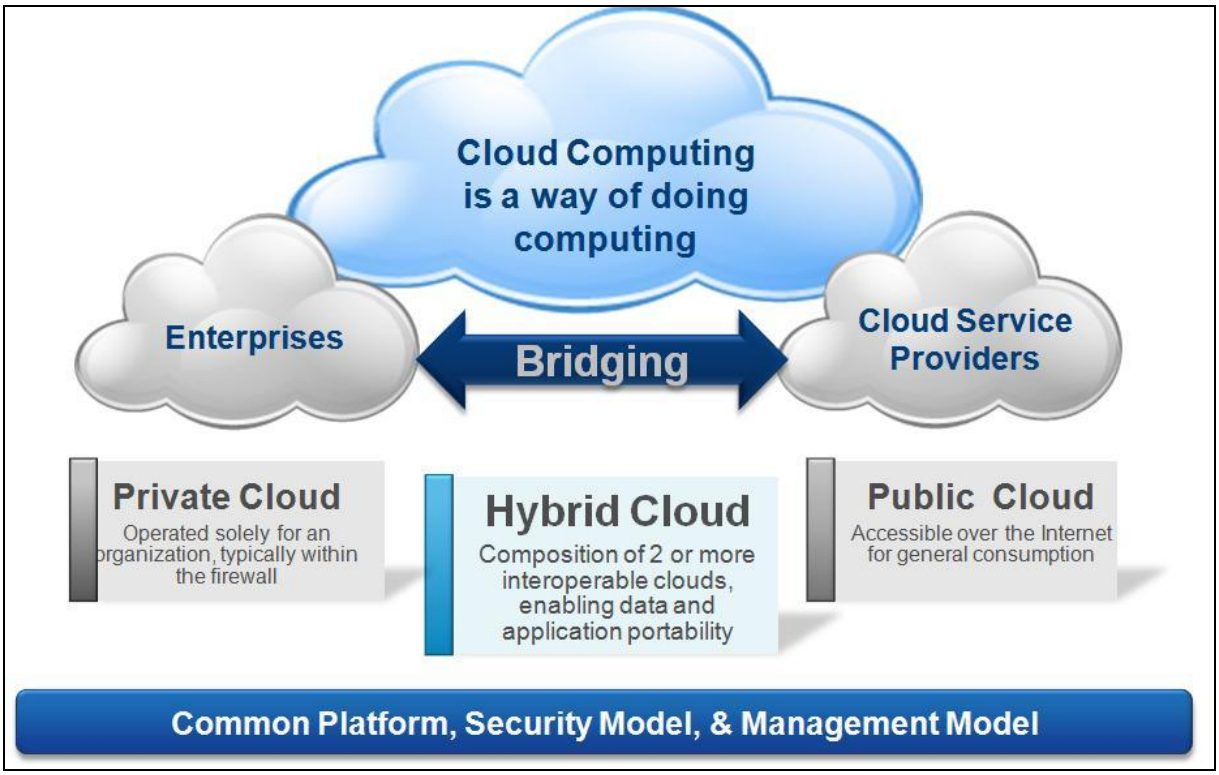

Fig 2: An architecture of the layer model of cloud computing

2.1 Public cloud: As shown in Fig.2 Public clouds are provided by a designated service provider and may offer either a singletenant (dedicated) or multi-tenant (shared) operating environment with all the benefits and functionality of elasticity and the accountability/utility model of cloud. In this article we propose a generic IoT architecture and we present a motion sensing cloud service to assist patients, derived from it. The fundamental idea is that placing such sensors in in enhanced living environments (ELE) will provide patient protection from accidents (i.e. elderly falls) and monitoring performed by caregiving staff without requiring their presence [6]. In particular, they can monitor and create predefined movements for patients that are in a rehabilitation phase. One of the advantages of a public cloud is that they may be larger than an enterprise cloud, and hence they provide the ability to scale seamlessly on demand.

2.2 Private cloud: Private clouds are provided by an organization or their designated services and offer a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity and accountability/utility model of cloud. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variants of private clouds:

1. on-premise private clouds and (ii) externally hosted private clouds.
2. The on-premise private clouds.

2.3 Hybrid cloud: Hybrid clouds are a combination of public and private cloud offerings that allow for transitive information exchange and possibly application compatibility and portability across disparate cloud service offerings and providers utilizing standard or proprietary methodologies regardless of ownership or location [7].

3. Secure, consistent backups and restoration of cloud-based resources

The service provider needs to validate the patch level and security level prior to bringing a vApp into the production environment. The VMware vCloud reference architecture should include a DMZ area for validating the vApp and mitigating any security violations according to each enterprise's security profile. Security in the cloud is achieved, in part, through third party controls and assurance much like in

traditional outsourcing arrangements. But since there is no common cloud computing security standard, there are additional challenges associated with this. Many cloud vendors implement their own proprietary standards and security technologies, and implement differing security models, which need to be evaluated on their own merits. In a vendor cloud model, it is ultimately down to adopting customer organizations to ensure that security in the cloud meets their own security polices through requirements gathering provider risk assessments, due diligence, and assurance activities. The physical infrastructure is owned by and/or physically located in the organizations' data centers with an extension of management and security control planes controlled by the designated service provider [8, 9]. The notion of public, private, managed and hybrid when describing cloud services really denotes the attribution of management and the availability of service to specific consumers of the services. The service provider should be able to supply the customer with a transparent and secure backup mechanism to allow the customer's cloud-based resources to be backed up on a consistent basis and enable fast restoration in the event of downtime. Snapshot and cloning capabilities of VMware virtualization technology make it possible to backup and restore data, and also complete operating systems and applications running within those operating systems.

- Generally, SaaS provides a large amount of integrated features built directly into the offering with the least amount of extensibility and in general a high level of security (or at least a responsibility for security on the part of the service provider).
- PaaS offers less integrated features since it is designed to enable developers to build their own applications on top of the platform, and it is, therefore, more extensible than SaaS by nature.

4. Strong Authentication, Authorization and Auditing Mechanisms:

These self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact. Although software encryption can also be used for protecting data, it makes the process slower and less secure since it may be possible for an adversary to steal the encryption key from the machine without being detected. Encryption is the best option for securing data in transit as well [10]. In addition, authentication and integrity protection mechanisms ensure that data only goes where the customer wants it to go and it is not modified in transit. Strong authentication is a mandatory requirement for any cloud deployment. It is very important in this type of shared environment to properly and securely authenticate system users and administrators, and provide them with access to only the resources they need to do their jobs or the resources that they own within the system. It is also very important in a cloud environment to know who is doing what within the system, when they did it, and what exactly they did. Separating duties and enforcing least privilege applies for both the cloud provider and the customer.

5. Encrypt critical data

The *trusted computing group's* (TCG's) IF-MAP standard allows for real-time communication between a cloud service provider and the customer about authorized users and other security issues. When a user's access privilege is revoked or reassigned, the customer's identity management system can notify the cloud provider in real-time so that the user's cloud access can be modified or revoked within a very short span of time. One of the more obvious cloud concerns is separation between a cloud provider's users (who may be competing companies or even hackers) to avoid inadvertent or intentional access to sensitive information. Typically a cloud provider would use *virtual machines* (VMs) and a hypervisor to separate customers. Technologies are currently available that can provide significant security improvements for VMs and virtual network separation. In addition, the *trusted platform module* (TPM) can provide hardware-based verification of hypervisor and VM integrity and thereby ensure strong network separation and security [11]. Data encryption adds a layer of protection, even if a system is compromised. Encrypting data in transit is especially important, as that traffic will be traversing a shared network and could potentially be intercepted if an attacker gains access at a critical point in the network. Encrypting the data as it traverses the network makes it much more difficult for an attacker to do anything with intercepted traffic. Encrypting critical data "at rest" within the virtual disk file is also very important. This will protect critical data from "walking off," and will make it much more difficult for an attacker to compromise data, even if they are able to compromise an endpoint [12]. The cloud provider should ensure that only authorized administrators have access to resources. They should also provide the customer with a mechanism for giving internal administrators access to necessary resources.

5.1 Cloud Security Threats

The threats to information assets residing in the cloud can vary according to the cloud delivery models used by cloud user organizations. There are several types of security threats to which cloud computing is vulnerable.

5.2 Privileged User Access

The cloud provider must have demonstrable security access control policies and technical solutions in place that prevent privilege escalation by standard users, enable auditing of user actions, and support the segregation of duties principle for privileged users in order to prevent and detect malicious insider activity. Encryption of data prior to entry into the cloud poses two challenges [13]. For encryption of data to be effective means of maintaining data confidentiality, decryption keys must be segregated securely from the cloud environment to ensure that only an authorized party can decrypt data. Once data is stored in the cloud, the provider has access to that data and also controls access to that data by other entities (including other users of the cloud and other third party suppliers). Maintaining confidentiality of data in the cloud and limiting privileged user access can be achieved by at least one of two approaches by the data owner: first, encryption of the data prior to entry into the cloud to separate the ability to store the data from the ability to make use of it; and second, legally enforcing the requirements of the cloud provider through contractual obligations and assurance mechanisms to ensure that confidentiality of the data is maintained to required standards [14]. This could be achieved by storing keys on segregated systems in house or by storing keys with a second provider. An additional challenge around encryption in the cloud is to prevent manipulations of encrypted data such that plain text, or any other meaningful data, can be recovered and be used to break the cipher. This constraint in encryption technology means that cloud providers must not be granted unlimited ability to store and archive encrypted data. If the cloud user organization permits the cloud service provider to handle unencrypted data, then the cloud service provider must provide assurance that the data will be protected from unauthorized access, both internally and externally. Within the cloud, the generation and use of cryptographic keys for each cloud customer could be used to provide another level of protection above and beyond data segregation controls. Cloud customers should ensure that they understand their obligations within all of the jurisdictions used by the cloud provider, and have policies and procedures in place to deal with specific external enquiries with respect to encrypted data.

6. Data Location and Segregation

Data location and data segregation are of particular importance in the cloud, given the disparate physical location of data and shared computing resources [15]. Cloud users may be under statutory, regulatory or contractual obligations to ensure that data is held, processed and managed in a certain way. There are a number of associated security risks in this situation:

- The cloud provider being required to disclose data (and potentially decryption keys) or hand over physical media to a third party or statutory authority.
- Development of liabilities to pay tax to local authorities as a result of processing sales or other
- transactions within their jurisdictions.
- Environmental hazards such as earthquakes, flooding, and extreme weather affecting the security of customer data, and Macro-economic hazards such as hyper-inflation or deep recession affecting the providers' services and personnel conditions. Central storage arrangements in cloud computing also provide attackers with a far richer target of information. In a single attack, attackers could potentially gain access to confidential information belonging to several customer organizations. If adequate segregation of data isn't applied many customers may find themselves suffering a security breach due to an incident that should have been limited to a single customer.

6.1 Data Disposal

Cloud services that offer data storage typically provide either guarantees or service-level objectives around high availability of that data. Cloud providers achieve this by keeping multiple copies of the data. Where the cloud customer has a requirement to delete data, cloud-based storage may be inappropriate for that data at all points in its lifecycle. Depending on the type of data hosted in the cloud, customers may require providers to delete data in accordance with industry standards. Unless the cloud architecture specifically limits the media on which data may be stored and the data owner can mandate use of media sanitization techniques on that media in line with the required standards, customers may need to preclude their data from being transmitted in the cloud.

6.2 e-Investigations and Protective Monitoring

In the following, we discuss some additional security threats that are relevant in cloud computing and are being detected and researched by academia, security organization and both cloud service providers and the cloud customers [16]. Implementing protective as shown in Fig.3, monitoring in the cloud presents challenges for both cloud customers and providers given the disparate location of physical data and the high number of providers involved. While cloud enabling technologies are designed to place a security perimeter between the cloud service systems and the cloud users, vulnerabilities in this layer of security cannot be ruled out altogether. There is a risk of insider threats and attacks on the cloud and this is likely to require expertise in e-investigations and protective monitoring. Effective protective monitoring of cloud-based information assets is likely to require integration between monitoring tools employed by the cloud provider as well as tools employed by the cloud user.

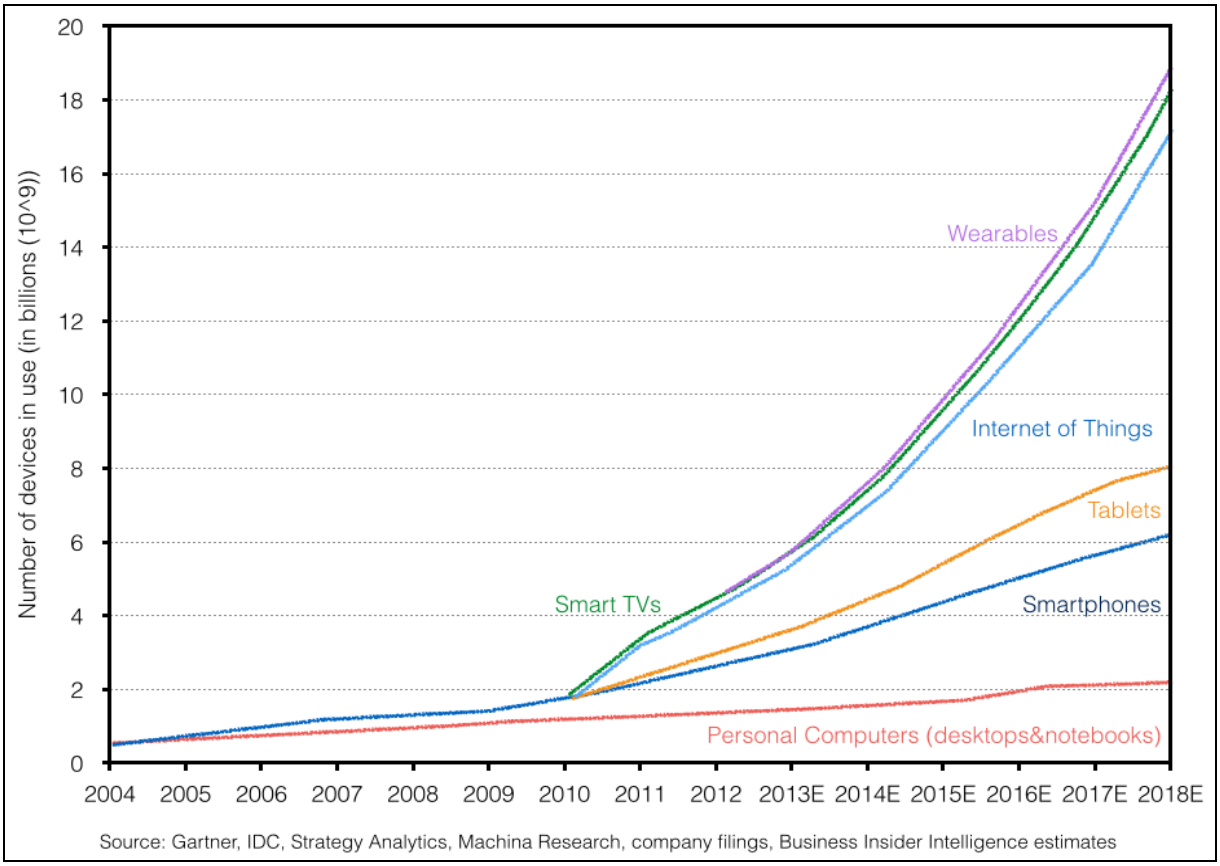

Fig 3: Result analysis of monitoring in the cloud, IoT based Systems

Tracing actions back to accountable users and administrators in the cloud may require an integrated or federated (mutual trust) identity management and associated logging system which permits unambiguous identification of all authorized individual with access to the cloud resources.

7. Conclusion

The proliferation of devices with communicating-actuating capabilities is bringing closer the vision of an Internet of Things, where the sensing and actuation functions seamlessly blend into the background and new capabilities

are made possible through access of rich new information sources. The evolution of the next generation mobile system will depend on the creativity of the users in designing new applications. IoT is an ideal emerging technology to influence this domain by providing new evolving data and the required computational resources for creating revolutionary apps. The proposed Cloud centric vision comprises of a flexible and open architecture that is user centric and enables different players to interact in the IoT framework. It allows interaction in a manner suitable for their own requirements, rather than the IoT being thrust upon them. In this way, the framework includes provisions to meet different requirements for data ownership, security, privacy, and sharing of information. Some open challenges are discussed based on the IoT elements presented earlier. The challenges include IoT specific challenges such as privacy, participatory sensing, data analytics, GIS based visualization and Cloud computing apart from the standard WSN challenges including architecture, energy efficiency, security, protocols, and Quality of Service. The end goal is to have Plug n' Play smart objects which can be deployed in any environment with an interoperable backbone allowing them to blend with other smart objects around them. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding the momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. Despite the trumpeted business and technical advantages of cloud computing, many potential cloud users have yet to join the cloud, and those major corporations that are cloud users are for the most part putting only their less sensitive data in the cloud.

8. References

1. Alliance for Telecommunications Industry Solutions. Homepage URL: http://www.atis.org. Amazon S3 Availability Event: (2008). URL: http://status.aws.amazon.com/s3-20080720.html (Accessed on November 29, 2012).
2. AOL Apologizes for Release of User Search Data (2006). URL: news.cnet.com/2010-1030_3- 6102793.html. August 7, 2006.
3. Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinsky A, Lee G *et al*. Above the Clouds: A Berkley View of Cloud Computing, 2009.
4. Technical Report No. UCB/EECS-2009-28, Department of Electrical Engineering and Computer Sciences, University of California at Berkley. February 10, 2009. Available on line at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf (Accessed on: November 20, 2012)
5. Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. In Proceedings of the ACM Workshop on Cloud Computing Security (CCSW'09), Chicago, Illinois, USA, November, 2009, pp 85-90, ACM Press, New York, USA.
6. Cloud Security Alliance. Home page URL: https://cloudsecurityalliance.org. Cloud Security Alliance (CSA)'s Security Guidance for Critical Areas of Focus in Cloud Computing (2009). CSA, April 2009. Available Online at: https://cloudsecurityalliance.org/csaguide.pdf (Accessed on: November 29, 2012).
7. Flexiscale Suffers 18-Hour Outage, 2008. URL: http://www.thewhir.com/web-hosting-news/flexiscalesuffers-18-hour-outage. October, 2008. (Accessed on: November 20, 2012).
8. FTC Questions Cloud Computing Security. 2009. URL: http://news.cnet.com/8301-13578_3-10198577-38.html?part=rss&subj=news&tag=2547-1_3-0-20. (Accessed on: November 29, 2012).
9. Gajek S, Jensen M, Liao L, Schwenk J. Analysis of Signature Wrapping Attacks and Countermeasures. In Proceedings of the IEEE International Conference on Web Services, Los Angeles, California, USA, 2009, 575-582.
10. Garfinkel S, Shelat A. Remembrance of Data Passed: A Study of Disk Sanitization Practices. IEEE Security and Privacy. 2003; 1(1):17-27,
11. Google Trends, Google. http://www.google.com/trends (n.d.).
12. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: Vision, hype, and reality for 27 delivering computing as the 5th utility, Future Generation Computer Systems 2009; 25:599-616.
13. Tilak S, Abu-Ghazaleh N, Heinzelman W. A taxonomy of wireless micro-sensor network models, Acm Mobile Computing and Communications Review. 2002; 6:28-36.
14. Tory M, Moller T. Rethinking Visualization: A High-Level Taxonomy, Information Visualization, 2004. INFOVIS 2004. IEEE Symposium on. 2004, 151-158.
15. Welbourne E, Battle L, Cole G, Gould K, Rector K, Raymer S *et al*., Building the Internet of Things Using RFID The RFID Ecosystem Experience, IEEE Internet Computing. 2009; 13:48-55.
16. Juels A. RFID security and privacy: A research survey, IEEE Journal of Selected Areas in Communication. 2006; 24:381-394.