International Journal of Digital Crime and Forensics
Volume 11 • Issue 3 • July-September 2019

CloudIoT:
Towards Seamless and Secure Integration of Cloud Computing With Internet of Things

Junaid Latief Shah, Sri Pratap College Cluster University Srinagar, Srinagar, India
Heena Farooq Bhat, Department of Computer Science University of Kashmir, Srinagar, India
Asif Iqbal Khan, Department of Computer Science University of Kashmir, Srinagar, India

ABSTRACT

The Internet of Things (IoT) is seen as a novel paradigm enabling ubiquitous and pervasive communication of objects with each other and with the physical/virtual world via internet. With the exponential rise of sensor and RFID-based communication, much data is getting generated; which becomes arduous to manage given the constrained power and computation of low-powered devices. To resolve this issue, the integration of Cloud and IoT, also known as CloudIoT, is seen as panacea to create more heterogeneous smart services and handle increasing data demands. In this article, the authors examine and survey literature with a focus on the integration components of CloudIoT and present diverse applications including driving factors for CloudIoT integration. The article also identifies security vulnerabilities implied by the integration of Cloud and IoT and outlines some suggested measures to mitigate the challenge. Finally, the article presents some open issues and challenges providing potential directions for future research in this area.

KEYWORDS

CloudIoT, IoT, RFID, Sensor

INTRODUCTION

Technological innovation in wireless communication allows real time scanning, management and transmission of sensitive data (Zorzi et al., 2010). Since 2011, the population of internet enabled devices has already surpassed the number of human beings on earth. Cisco Systems predict that by the year 2020, the global internet will be an amalgam of over 50 billion connected devices which include sensor nodes, output actuators, mobile and GPS connected smart devices and technologies (Nordrum, 2016). The Internet of Things (IoT) is seen as a technological evolution having distinct applications in human life rendering future connectivity and accessibility. The IoT involves interconnection of small devices embedded with sensing software and hardware that permits these objects to acquire

DOI: 10.4018/IJDCF.2019070101

and transmit data to the cloud or internet using a wireless medium (Chen et al., 2014). These sensors use diverse enabling technologies and protocols for data transmission such as Bluetooth, Near Field Communication (NFC), Zigbee and Radio Frequency Identification (RFID). For long distance data transmission; they can also use mobile data communication services such as GSM, GPRS-Edge, 3G and 4G over LTE (Devipriya, 2017). IoT working is based on autonomous Machine-to-Machine (M2M) communication without any human interaction. The application areas of IoT such as smart home systems, remote environment monitoring, automated industrial systems, and remote healthcare generate and deliver data which needs to be processed in real time (Soliman et al., 2013). This in turn necessitates support for high network volume traffic being generated by heterogeneous systems. As these heterogeneous devices keep on increasing, IoT performance tends to decrease given the constrained power and bandwidth limitation (Botta et al., 2014). In such a scenario, there is a demand of data mapping from physical IoT world to virtual world of Cloud computing. The Cloud computing platform offers a suitable, on-demand, extensible and seamless access to pool of networked computing resources (Cook et al., 2018). These remote resources dispense enormous processing power for computations and scalable storage that augment the low power and storage drawbacks of IoT devices, hence offering complimentary and coherent platform for ubiquitous computations by end users (Aazam et al., 2016).

The integration of Cloud and IoT known as CloudIoT or Cloud of Things (CoTs) was recently conceived by MIT's Auto-ID labs to signify interconnection between heterogeneous physical objects and virtual cloud (Distefano et al., 2012). The IoT's are represented by small physical objects that are highly distributed in nature and suffer limited processing power and storage. These constraints generate issues affecting performance, reliability, security, trust and privacy in IoT devices (Parwekar, 2011). Cloud computing technology on the other hand provides robust, scalable and immense capacity solution to IoT issues. With Cloud of Things, the two independent technologies are expected to work together for energy efficiency, planned resource management, and creating new and extended range of services (Aazam et al., 2016). Delay sensitive applications as well as mission critical services can benefit from this new technological prototype. The integration of Cloud and IoT is highly pervasive given the fact that large volumes of data are being generated which entails requirement for virtual storage resources. This data after pre-processing should create not only information, but also knowledge and wisdom that will help in developing smarter application for the users (Khodkari et al., 2016). The CoT framework is highly scalable and distributed in nature owing to the fact that computational resources are offered as service. CoT allows easier deployment of applications harnessing benefits of cloud service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). There is also a provision for ensuring that Quality of Service (QoS) is maintained dynamically (Velte et al., 2010). For example; when application requests increase from a user, the cloud must scale up to suffice the growing load. On the contrary, when the load decreases, the cloud must automatically scale down to accommodate the change. The CoT finds diverse application areas because of its economical, flexible, extensible, management-less and subscription-based model. The cloud service providers offer services through internet on a subscription or pay-per-use basis. Some precise advantages of CoT implementation include massive data storage and processing power, distributed nature of service for supporting location independence of users, platform independence and cross application support, multi-versioning application support, power and resource efficient and support for Quality of Service (QoS). Given the advantages of CoT framework, the process of integration of Cloud and IoT is not that simple (Aazam et al., 2016). In addition to data and resources, issues with respect to business point of view need to be taken care of. The framework offers bigger business platform and opportunities, which in turn invites attack from malicious users. In case of hybrid clouds, major concern and emphasis should be laid on security and privacy which also includes identity preservation (Velte et al., 2010). Other concerns in CoT framework include secure transmission of sensitive data and secure data storage (Cook et al., 2018). This necessitates use of cryptographic techniques and encryption during data processing and storage. Additionally, deployed

IoT devices should be made tamper proof so as to prevent any physical damage. The integration of IoT and cloud computing involves disparate networks underpinning varied data and services. These heterogeneous networks should be agile and open-ended to accommodate changes with QoS support.

In this paper, we carry an in-depth discussion on Cloud of Things framework with focus on driving factors for integration. The paper also presents diverse applications of CloudIoT and issues that need to be addressed. Later, the paper identifies security vulnerabilities with respect to integration and suggested measures that need to be kept in mind. Finally, the paper concludes with some open issues and challenges which provide directions for further research in this area.

RELATED WORK

The Cloud and IoT have witnessed exponential and autonomous mushroomed growth over the years with researchers working tenaciously for their seamless integration. On the contrary, CloudIoT is still in its infancy with no standard architecture available for data transmission, storage of media and computation (Aazam et al., 2016). As IoT harbors heterogeneous technologies and protocols, the properties such as reliability, integrity, scalability and performance become difficult to achieve. Also, since IoT has limited power and storage, its integration with cloud will aid in subduing these challenges. The cloud dispenses services for IoT by providing an interface for its applications and service management. In return, Cloud benefits from IoT by elevating its scope to interact with real word things (Lee et al., 2010; Botta et al., 2014). A lot of surplus literature is available on Cloud and IoT integration; however most of them provide very condensed and abstract overview of the concept.

In (Botta et al., 2014), authors present a detailed overview of Cloud and IoT integration. Their work attempts to identify extensive features of Cloud and IoT and the main drivers of CloudIoT integration. The authors have carried a detailed research review to identify research challenges in this field. The paper also discusses various CloudIoT platforms and projects including open issues and future research directions in this domain. A similar work has been done in (Parwekar, 2011) where the authors aim to assess the feasibility of services offered by Cloud and IoT integration. In (Distefano et al., 2012), authors discuss the concept of CloudIoT and figure out the steps to realize CloudIoT vision. The authors also present a high level modular architecture of CloudIoT; however notable problems have been reserved and not touched. In (Yuriyama & Kushida, 2010), researchers propose Sensor-Cloud infrastructure that can handle physical sensors on cloud platform. Although the paper presents Sensor-Cloud infrastructure, architecture and its implementation, their work only emphasizes on virtualizing a physical sensor as a virtual sensor on the cloud platform. A similar work has been carried in (Hassan et al., 2009) whereby author's present pub-sub based model for seamless integration of sensor networks with cloud-based applications. Although authors assert to have addressed challenges in this regard, the work does not address key issues inherent in sensor-cloud integration. Since growth of IoT and deployment of applications in the cloud has been exponential, there has been no breakthrough in integration of heterogeneous and geographically scattered sensors in an acceptable and practical manner. In (Fox et al., 2012), authors propose "IoTCloud" which is a cloud based open source messaging system that enables designers to write extensible and highly efficient IoT and sensor compatible applications. The application is written in Java programming language and software is designed on top of a popular open source package such as Apache Active MQ and JBoss Netty. The authors have used Future-Grid cloud test bed to check performance of experiments. On the similar lines, authors in (Soldatos et al., 2015) present an overview of OpenIoT project which is an open source IoT platform permitting seamless interoperability of IoT in the cloud. The OpenIoT project also offers a middleware for collection of data from almost any deployed sensor and also simultaneously ensuring their absolute observation. It also includes diverse domain of visual tools that allow effortless deployment of IoT applications. In (Grozev & Buyya, 2014), authors discuss current fundamental nomenclature for Inter-cloud architecture and argue on how present Inter-Cloud frameworks assist organization of distributed applications across clouds, keeping in mind their non-

functional requirements. The authors also survey existing literature and identify open issues in this area. However, the paper does not discuss anywhere its relationship with IoT. Similar works have been carried by authors in (Buyya et al., 2010; Villegas et al., 2012) without discussing any relation with IoT.

IoT devices such as smart-phones, tablets, media sensors, etc., demand coherent multimedia processing systems. From the available literature, media cloud seems to be only feasible solution that will satisfy the escalating drift towards multimedia data and consumption. However, for multimedia transmission, maintaining QoS will be a demanding task. To support this, it is recommended that IPv6 be used, that provides Flow Label field which offers end-to-end QoS provisioning mechanism. To enhance performance and reduce network delay in media streaming, efficient QoS techniques need to be designed. In (Zhu et al., 2011), authors present a media-edge cloud (MEC) architecture which is composed of storage space, central processing unit (CPU), and graphics processing unit (GPU) clusters. The multimedia aware cloud performs distributed parallel computation and dispenses QoS provisioning for various multimedia services in the network. However, the performance cost of this proposed work is not discussed. In (Khodkari et al., 2016), authors aim to evaluate integrity requirements of CloudIoT so that QoS is guaranteed. The authors also define CloudIoT QoS metric equation and observe that end-to-end QoS provision is a multidimensional and convoluted problem that needs substantial solutions.

Most of the Literature cited above provides an abstract overview of CloudIoT without discussing in-depth detail of its integration or working scenarios. Some papers present an overview of cloud structure only without expressing any relationship with IoT. However, this paper takes a deeper overview of CloudIoT integration with focus on potential issues and their solutions. The paper also attempts to address security issues segregated at different layers of IoT along with issues inherent in the Cloud.

INTERNET OF THINGS

The term Internet of Things (IoT) also known as Internet of Objects was first coined in Future of Internet and Ubiquitous computing by a British innovator Kevin Ashton who was one of the founding members of Auto-ID center at Massachusetts Institute of Technology (MIT) (Wu et al.,2010). Kevin used the term to outline a system where physical world is connected to internet via sensors. This pervasive innovation represents the future of interconnection networks which is totally different from traditional networks. The IoT integrates disparate devices from divergent manufacturers having heterogeneous functions (Kovatsch et al., 2012). The “things” in IoT refers to any device or object in the physical world irrespective of whether it can communicate or not. Unlike traditional networks, these objects use Radio Frequency Identification (RFID) tags and communicate over internet. IoT provides an efficient platform for interaction of humans with the environment around using technological innovation.

Regardless of universal acceptance of IoT, there is no single standard definition available for the term. In fundamental terms, IoT defines a communication network of interconnected objects or things. These objects/things sense their environment using various sensors, gather the data and exchange this data with similar objects. On the basis of gathered data, some objects can even make decisions on their own regarding triggering of events or sending data to server machines over internet for further processing (Liu et al., 2005). The IoT sensors can be deployed in many applications such as house hold refrigerators, ovens or even industrial process control systems. Similarly, RFID chips can be used as tags in everyday products that we use (Meingast et al., 2007). All of these objects use communication protocols such as Bluetooth and Zigbee having shorter data transmission range and low power consumption. IoT devices are mainly classified as either wearable devices or microcontroller/ microprocessor based embedded IoT devices. Some common examples of IoT devices are Android wear, Misfit, Google Glass, Arduino, Raspberry-pi and Intel Galileo.

Layered Architecture

Owing to popularity and future implications of IoT, Intel introduced and termed it as an embedded internet. The reason being that, in future, embedded devices will have the capability to communicate with each other over internet. This idea is analogous with conventional IoT and will largely bring new innovative opportunities for revenue generation. As shown in Figure 1, the fundamental IoT architecture although not yet standardized is divided into four layers: perception/physical layer, network layer, middleware layer and application layer. Each layer has a predefined functionality.

Perception Layer

Also known as Physical layer, this is the bottom layer in the IoT architecture and is composed of hardware sensors, RFID's, barcode labels, GPS etc. The purpose of this layer is to perceive or gather data from the environment and report this data to the server or to the sink nodes. Like OSI model, the data collected by this layer is submitted to the layer above it for further processing.

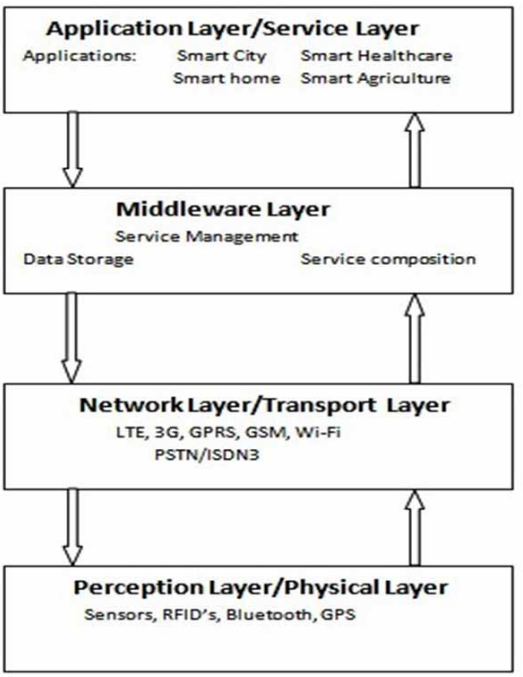
Network Layer

This is the second layer in the IoT architecture and is analogous to the network layer in OSI model. This layer is an amalgam of internetworking protocols and standards which support transfer of data packets from source to destination host across network boundaries. The host and destination are identified by unique IP address.

Middleware Layer

This layer receives data from the network layer and is responsible for filtering, collecting, storing and service management of data. This layer dispenses an abstraction of services and information processing capabilities of the IoT devices. The output of this layer is passed on to application layer.

Figure 1. IoT layered architecture



Application Layer

This is the topmost layer in the IoT architecture and is responsible for final presentation of the data. This layer provides varied application services distributed over middleware layer to various users and applications. Examples of application services foster many industries like healthcare, transportation, supply chain, etc.

CLOUD COMPUTING

Cloud Computing is a technological on-demand computing model that provides access to shared pool of distributed and ubiquitous resources like storage and processing. The concept minimizes management effort on account of users and facilitates rapid elasticity (Mell & Grance, 2011). The cloud platform facilitates robust, scalable and pervasive virtual servers, storage, networking that can be customized according to user's requirements. Some of the essential features of cloud computing platform are: on-demand service, broader network access, resource pooling, rapid elasticity and measured service (Mell & Grance, 2011).

On Demand Service

A user is at liberty and free will in choosing server time for storage and computational processing capabilities. This is allowed using automatic service delivery model with no or minimal human interaction. Such a service model is useful for devices that function and execute their operations remotely.

Broader Network Access

The potential of cloud computing is exploited over the network by using heterogeneous devices like mobiles, laptops, tablets and also workstation models.

Resource Pooling

Various computing resources of cloud such as storage, processing power, physical memory, etc., are combined together to form a large repository model that serves users as per demand. These resources are assigned dynamically with user having no perception or control of the exact location where resource resides. The resource or data center location details are highly abstract in nature.

Rapid Elasticity

The resources are assigned and released dynamically at any point in time. This allows the server machine to scale up and scale down as per demand and load.

Measured Service

Cloud systems monitor resource utilization e.g. storage, computational processing, network bandwidth, etc., which enables them to optimize resources and leverage pay-per-usage model. The monitoring mechanism ensures transparency in the service level agreement between the user and the service provider.

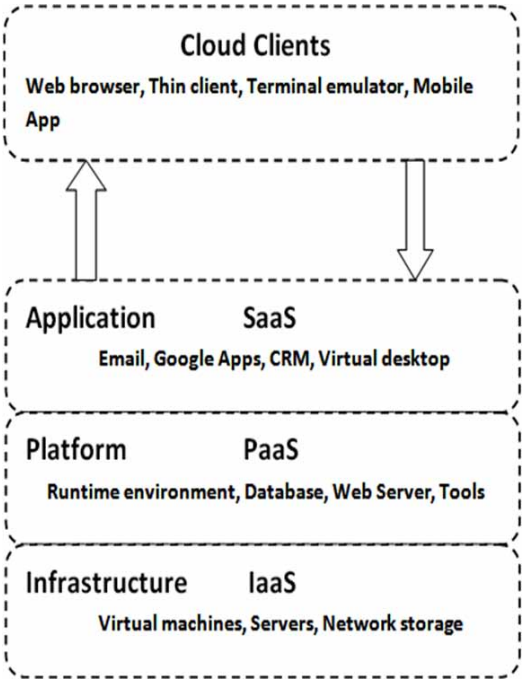
Cloud Service Models

From the service delivery point of view, cloud architecture is viewed as a resource allocator across the internet to a number of distributed clients (Villegas et al., 2012). As shown in Figure 2; Cloud Computing offers services at three different infrastructure levels.

Infrastructure as a Service (IaaS)

IaaS allows modeling of virtual environment wherein hardware resources such as servers, load balancers, routers, firewalls and network bandwidth etc. is offered as a service. This model offers

Figure 2. Cloud Service Models



a billing system where resource usage and value-added service charges are computed on per hour basis. Common examples of IaaS include storage services offered by Amazon EBS, Amazon S3, Google compute engine etc.

Software as a Service (SaaS)

SaaS is an on-demand service model in which clients are provided access to business application software and database directly over the internet. The cloud users are not bothered about the infrastructure and management of the platform and users are free from installing any separate application on their system which simplifies maintenance and support. Examples include services such as Gmail, Google docs, Google Apps, Microsoft Office 365, etc.

Platform as a Service (PaaS)

PaaS model presents an application development and runtime environment, a platform for programming language execution, software and database development tools to permit direct deployment of applications over the web. PaaS cloud model is tailored mostly for application developers and software testers and as such offers a platform where entire software development life cycle is realized. Common examples of PaaS include Amazon EC2, Google app engine, Microsoft Azure, IBM smart cloud etc.

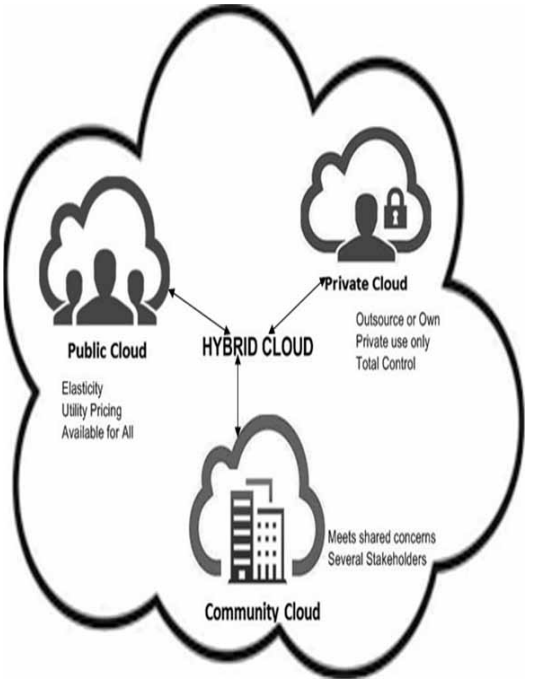
Cloud Deployment Models

The cloud deployment models are segregated into four categories as shown in Figure 3.

Public/External Cloud

This deployment model allows public or open access to the cloud infrastructure. It is generally owned by the cloud service provider and users pay for its resources. The users can scale up or down their

Figure 3. Cloud Deployment Models



resource consumption according to their demands. Examples of cloud service providers include Google, Amazon, Microsoft, Salesforce etc.

Private/Internal Cloud

This deployment model is owned or rented by the organization strictly for its personal use. This model provides cloud services dedicated to an organization e.g. business critical applications.

Community Cloud

This cloud deployment model is managed by homogeneous organizations with similar activities and goals.

Hybrid/Virtual Private Cloud

This model is a combination of private/public/community clouds wherein the resources and infrastructure can be moved from within to outside of organization (for example; shifting computational jobs from private to public cloud).

CLOUDIOT: INTEGRATION OF CLOUD WITH IOT

With an exponential rise in ubiquitous computing, a myriad number of sensor devices are getting connected to the internet. Proportional to this, there has been considerable increase in the amount of data that is getting generated. The local and interim storage of this data is not feasible given the constrained storage space available on IoT devices. Initially, these devices used to transfer data to mainframes which had the required computing resources. But this method had a limitation. First, the mainframe computing was very costly and second, it represented a central point of failure. The other approach was distributive in nature wherein these devices were equipped with little storage and

processing power for communication. However, this also resulted in additional cost which included cost of replacing failed IoT devices and cost of powering up each device. In recent years the demand for cheaper IoT devices with more computing resources has only increased. To meet this demand, integration of Cloud Computing with IoT also known as CloudIoT presents a flexible, less complex and cost effective potential solution (Aazam & Huh, 2014; Bonomi et al., 2012). The IoT will generate data and communicate with outside world through pervasive devices and networks while as cloud computing will provide agile and scalable computing resources to meet the growing demands (Zhou et al., 2013). Figure 4 provides the operational and communication scenario of CloudIoT. As shown, the data passes through different IoT layers until it reaches the cloud. The cloud stores, secures and processes this data corresponding to the design objective of service. Once the service is designed, it is made accessible to the end user. The Cloud and IoT are two different technologies, however available literature reports, their complementary characteristics that drive the motivation for integration of CloudIoT paradigm. These characteristics as extracted from literature are reported in Table 1. Typically, in CloudIoT, the cloud operates as an intermediate layer between IoT devices and end user applications. This layer abstracts the arduous operations and services from the end user.

Some of the driving factors for integration and adopting CloudIoT model are discussed below.

Storage

The IoT interconnects billions of devices which generate humongous amount of data from different information sources. This data also known as big data can either be semi-structured or non-structured

Figure 4. CloudIoT operational scenario

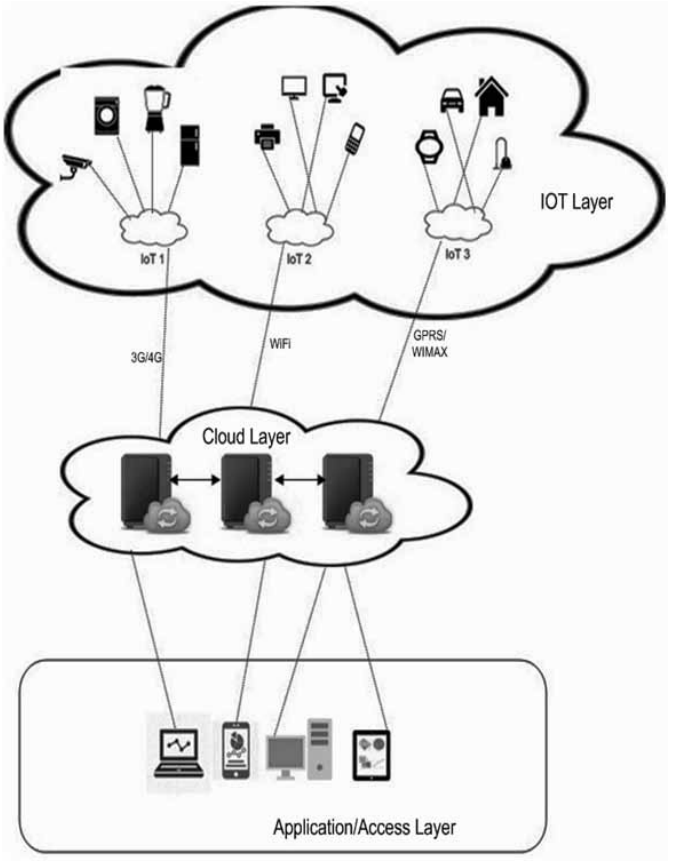


Table 1. Complimentary characteristics of IoT and Cloud

Characteristic	IoT	Cloud
Displacement	Pervasive (things are everywhere)	Clustered and Centralized
Availability	Restricted	Ubiquitous (resources accessible from anywhere)
Device Nature	Things are real world devices	Virtual resources available online
Computational Power	Limited computational capacity	Virtually unlimited computational power
Memory Space	Sparse in nature	Scalable as per demand
Role of Internet	Uses internet as convergence place	Uses internet for service delivery
Big Data	Contributes as source of big data	Processes and manages big data

(Aguzzi et al., 2013) and will have three major properties (Zikopoulos & Eaton, 2011): volume (i.e. magnitude of data), variety (i.e. heterogeneous data types) and velocity (i.e. data generation rate). Hence it becomes imperative to collect, process, analyze and store such large volumes of data. As such, the cloud offers an effective and flexible option to tackle the data generated by IoT devices (Rao et al., 2012). Once the data has been stored in cloud, it receives homogeneous treatment through standard application API's. Also, secure algorithms can be applied over the data to protect it and this data can further be accessed from anywhere.

Computing Capabilities

IoT devices have limited energy source and constrained processing power which limits their ability for onsite and complex data computation. Instead the gathered data is transferred to more powerful nodes where data is grouped together, and complex processing is possible. However, scalability is still challenging to achieve given underlying infrastructure. On the contrary, cloud offers limitless virtual computational capacity and an on-demand service model (Susiu et al., 2013). Using cloud; IoT's computational demand can be properly satisfied for performing real time data analytics and for implementing agile and real time data driven decisions for sensor specific applications.

Communication

One of the design objectives of IoT is to enable data and application sharing and to dispense IP based communication among connecting devices using reliable hardware. To assist and underpin such communication is cost sensitive and not feasible. In such a case, Cloud provides an effectual and economical solution for connection, managing and customizing anything from anywhere using tailored web portals or apps (Rao et al., 2012). These portals are complimented by high speed broadband networks that aid in remote monitoring and administration of data (Susiu et al., 2013). Although Cloud can substantially refine and ameliorate IoT data transfer, it can still limit down capability or act as a gridlock in some situations. The last 20-year data analysis reveal that storage density and computational power have increased by a magnitude of 10^{18} and 10^{15} respectively while as increase in broadband capacity rate is only 10^{4} (Jeffery, 2014). Therefore, pragmatic constraints and limitations can arise while transferring prodigious amounts of data from internet gateway onto the cloud.

New Capabilities and Paradigms

The large heterogeneity of IoT devices and protocols make scalability, reliability, availability and security very difficult to achieve. The CloudIoT works out solution to this problem by dispensing easy access of resources, usability and less deployment costs (Zaslavsky et al., 2013; Chen et al., 2014). The integration of Cloud and IoT permits new smart services and applications that handle new and real life scenarios. Extracted from literature (Botta et al., 2016), Table 2 shows list of new models

Table 2. New models and paradigms enabled by CloudIoT (Source (Botta et al., 2016))

Acronym	Expanded Form	Description of Service
SaaS	Sensing as a Service	Providing global access to sensor data
SAaaS	Sensing and actuation as a service	Enabling automatic control logistics implemented in the cloud
SEaaS	Sensor Event as a service	Transmitting messaging services triggered by sensor events
SenaaS	Sensor as a service	Enabling distributed management of remote sensors
DBaaS	Database as a service	Enabling distributed database management.
DaaS	Data as a service	Enabling ubiquitous access to any sort of data
EaaS	Ethernet as a service	Providing distributed layer-2 access for remote devices
IPMaaS	Identity and Policy management as a service	Providing distributed access to identity and policy management
VSaaS	Video Surveillance	Providing access to recorded video and performing complex analysis

and paradigms that emerged from this integration. As no standard exists, these terms and acronyms vary in different cases and have no clear distinction.

CLOUDIOT APPLICATIONS

The Integration of Cloud and IoT has increased potential of creating opportunities and exploiting the power of web and pervasive computing. There are three basic ways by which these internet-enabled devices communicate (Cook et al., 2018). First, between Machine-to-Machine (M2M) communication e.g. sensor providing data to actuator which raises an alarm when some motion gets detected. Second, between Human-to-Machine (H2M) communication, e.g. human voice recognition. Third, between Machine-to-Human communication (M2H), e.g. biometric systems. The heterogeneous integration of Cloud and IoT lays foundation for number of real world applications.

Healthcare

A large amount of healthcare data of patients is stored by hospitals using sensor networks. The use of smart devices and cloud services is being encouraged to provide cost effective and pervasive facilities which continuously contribute for innovation in healthcare systems. This area generates enormous amount of data which needs to be stored and can be studied later and techniques such as data mining can be applied on them for decision making. The use of smart phones is being employed for communication purposes which necessitate need for security and good quality of service.

Smart City

This is one of the important applications envisioned by integration of Cloud and IoT. The aim is to improve city and urban life by dispensing better applications. Examples can be Intelligent Transport system to reduce city traffic. Similarly detecting amount of waste using smart containers to schedule a pick up.

Smart Home

The IoT provides a larger platform for automating appliances in home setup using embedded systems (Soliman et al., 2013). Integration with cloud service allows user to remotely assist and control installed devices in home. The cloud provides the flexibility of metered facility for recognition of appliances and smart control of heating, lighting, energy consumption, and air purifiers.

Remote Video Surveillance

This is a novel feature with respect to security that helps in remote monitoring and supervision. The sensor devices record the data with a high definition camera and transmit this data over internet to cloud servers. The cloud fulfills adequate requirement for storage and processing which otherwise was not possible.

Environment Monitoring

CloudIoT can also help in monitoring the behavior of the environment around us. Sensors can be deployed in water bodies as well as in industries to help detect the amount of pollution levels on daily basis. This data can thereafter be transferred to labs where experts decide the future policies.

SECURITY ISSUES AND VULNERABILITIES

The CloudIoT creates a network of interconnected objects overlaying varied real-world applications such as smart homes, smart city, smart traffic networks, industry automation systems as well as communications between them (Gubbi et al., 2013). The cloud services are configured in a way to enable seamless access to shared resources such as computation, storage, applications and necessary data mining, analytics and aggregation (Armbrust et al., 2009). Although CloudIoT delivers benefits and ease in our daily life; however, its design component bears no consideration to security (Jing et al., 2014; Khorshed et al., 2012). In case of a successful attack, the CloudIoT network could be rendered non-functional which could result in leakage of critical information or tampering of physical infrastructure. With integration of Cloud and IoT, the situation will become more complicated and will expose further vulnerabilities and drawbacks. These vulnerabilities can be exploited by malicious users to abuse CloudIoT ecosystem supporting billion of connected devices. Subsequently, drawbacks of CloudIoT network will outweigh its advantages. Also, it is neither recommended nor feasible that sensor nodes be changed and replaced periodically. The underlying security infrastructure must be durable and robust enough to last for considerable amount of time given the large deployment of sensor nodes and cloud infrastructure.

Security Features and Goals

CloudIoT permits communication including data transfer among nodes and users to attain certain goals. In such a distributed environment, authenticity, access privilege and control are significant to fortify safe communication. However; given the constrained resources (computational power, storage) of devices; the environment requires adjustments in existing techniques to meet well defined security goals (Sicari et al., 2015).

Confidentiality

The confidentiality factor prevents unauthorized access to the data and protects it from being snooped covertly. CloudIoT employs sensors and RFID's to record data from the environment and this data must be protected from neighboring devices as well as from malicious users. To secure information and safeguard confidentiality, improvised encryption methods and protocols should be designed and used (Capkun et al., 2003).

Integrity

Integrity ensures prevention from data fiddling or tampering during the data transmission process from legitimate source to intended destination. The integrity principle verifies that valid and accurate data is received by authorized users. Integrity can be imposed by leveraging end-to-end security in data transmission and reception.

Availability

The availability principle ratifies that data and applications services are available for authenticated users as per their request. CloudIoT nodes demand services and data in real time without enduring any processing delays. Any delay on account of requested resource would contribute to failure of the interconnected nodes.

Identity and Authentication

Identification and Authentication ensures that legitimate data is transmitted in the CloudIoT network by authenticated devices. However, this process is very cumbersome given the nature of Sensor/IoT nodes and the heterogeneity of the overall system (Roman et al., 2013). The required solution should enforce strict authentication mechanism between entities and objects of the network.

Privacy

The privacy factor ensures limited access to the data only by the legitimate user. Unlike confidentiality, which may encrypt data to prevent it from tampering, the privacy ensures that user has limited access without concealing any other valuable information from it.

Security Vulnerabilities

The security challenges of CloudIoT include vulnerabilities in IoT nodes as well as those in cloud services. In this section, we first discuss vulnerabilities in each layer of IoT architecture and then focus on security loopholes in cloud services.

Issues in IoT Layers

The layered structure of IoT is vulnerable to attacks from malicious users. The attacks can be segregated as active and passive depending on their nature of action. An active attack is more malignant in nature as it directly impacts the service from running smoothly. The passive attack behaves like a Trojan and monitors behavior of network communication covertly (Abomhara & Koien, 2014). The detailed security analysis of each layer is described as follows.

Perception Layer Issues

As the main objective of perception layer is to sense and collect data from environment, the security vulnerabilities mainly focus on tampering nodes or counterfeiting collected data. These sensor nodes operate in an outdoor environment; as such invite attackers to execute *Node Capturing* attacks to carry out physical damage and tampering of hardware devices (Zhao & Ge, 2013). If a sensor node gets compromised to attacker, the vital information such as encryption keys could be exposed. The attacker can also replicate legitimate node by using copied information to connect to the IoT network. Additionally, the attackers can leverage a code injection attack in which they control the behavior of a sensor node by inserting malicious code and data into the memory of a node. The code gives malicious user access to the IoT system which further degrades its functionality.

Replay attack is another type of attack in which attacker exploits a compromised node to transmit legitimate information to the destination node in order to obtain its trust (Mo & Sinopoli, 2009). Once trusted, the attack compromises authentication routines used in IoT system. The sensor nodes in perception layer are also vulnerable to Sleep Deprivation attack in which the attacker drains the battery or power resources of the system. The sensor nodes in the IoT system are battery powered. In order to increase their working life span, they follow special programmed sleep routines to save power consumption. The Sleep deprivation attack can tamper with the sleep routines and make devices continuously work even when not required. Ultimately, the devices loose power and shutdown (Andrea et al., 2015). In order to avoid this, alternate sources of energy such as solar or wind energy need to be explored.

Network Layer Issues

The IoT network layer is highly vulnerable given the amount of collected data that it transmits. The main security emphasis lies on the effect of availability of resources (Lin et al., 2017). The security issues also focus on the integrity and authentication of information that is being transmitted over the network. Some of the common network layer issues are discussed below:

- **Eavesdropping and Interference:** As most IoT devices use wireless medium for transmission of information, vulnerability lies in the fact that communication line can be interfered by non-authenticated users. The efficiency of wireless signals transmitted between IoT nodes could be compromised by imposing jamming waves (Gubbi et al., 2013). To safeguard transmission medium and to maintain accuracy, secure cryptographic algorithms need to be designed and implemented;
- **Denial of Service (DoS) Attack:** This is one of the common network attacks aimed to make machine or network resources unavailable to its intended users. The attack is executed by directing massive network traffic towards the victim which it cannot handle, thus rendering the node unavailable. Common attack schemes include Ping of death, UDP flooding, Teardrop etc which consume resources such as bandwidth, disk space, memory and processor time. To defend against this attack, strong firewall, network policies and rule base need to be implemented;
- **Spoofing Attacks:** These attacks include IP spoofing, RFID spoofing, etc., whose main task is to gain access to the IoT and send malevolent data into the system. With IP spoofing, attacker can spoof legitimate IP address of a node and send malicious data across the system that appears to be valid. In the case of RFID spoofing, the attacker can record and spoof legitimate RFID tag and send data into the system with this tag (Lin et al., 2017);
- **Routing Attacks:** Routing is required at the network layer; as such Routing attacks tamper routing protocols and exploit routing paths to create route loops that contribute in packet loss. This in turn increases congestion and network delay in IoT (Andrea et al., 2015). Sometimes the compromised node asserts extraordinary computational capabilities in order to obtain neighbors trust and act as forwarding node in routing process. This in turn makes compromised node obtain large amount of data which can serve as launch pad for additional attacks. This type of attack is called as Sink Hole attack. In addition to above, the other attacks that network layer is vulnerable to includes Worm Hole attack, Sybil Attack and unauthorized node access attack.

Application Layer Issues

The principle objective of application layer is to provide interface for user requests, therefore issues in this layer are hinged mainly on the software side. As IoT lacks standardization, issues related to application security are paramount and need substantial solutions. Different applications demand diverse authentication and authorization policies and to integrate these solutions is a difficult task. The security policies should focus on application privacy and identity authentication. Some of the common application level vulnerabilities include malicious code injections such as SQL injections, inefficient coding which serves as launch pad to cross site scripting attacks, social engineering such as Fishing attacks and many more (Andrea et al., 2015).

Issues in Cloud Services

Although the security issues in conventional cloud systems are also inherently present in CloudIoT; however, its integration with sensor nodes establishes new attack definitions that are easier to launch (Grobauer et al., 2011).

As end user employs cloud services for data storage and computation, the most sensitive issue prevalent is about data confidentiality and privacy. The cloud users seek knowledge about where

actually, their data gets stored and information about service providers, who control their data. The end user also wants to ensure that unauthorized access to the data is blocked.

The on-demand self-service model of cloud entails for an organized management platform that cloud users can access. Unlicensed and unwarranted access to this management platform could result in a serious threat given the distributed nature of the cloud. Abuse and manipulation of this platform could serve as a launch pad for further attacks (Suo et al., 2012).

The cloud is also vulnerable to network protocol threats. Given the pervasive and distributed nature of cloud, the end users access cloud services using internetworking protocols. Most of these network protocols are stateless in nature and therefore vulnerabilities such as DoS and Eavesdropping are always admissible to the cloud (Grobauer et al., 2011).

Vulnerabilities also exist in state-of-the-art cloud offerings. These include poor authentication processes and injection threats such as SQL injection and command injection which targets cloud database. Code injection threats such as cross site scripting targets victims' browser through which user receives cloud services. Table 3 provides a summary of CloudIoT vulnerabilities.

Some Suggested Measures

It is apparent that integration between Cloud and IoT will elevate the security vulnerabilities considerably; therefore, robust security and defense mechanisms need to be put in place so that threats could be mitigated (Lin et al.,2017). The security framework should address both layered architecture of IoT as well as the cloud infrastructure. For example, at IoT perception layer, authentication of legitimate nodes should be imperative to avoid unauthorized node access. Second data encryption procedures should be operated to safeguard confidentiality of information. This however necessitates using Lightweight cryptographic protocols and algorithms such as elliptic curve cryptography (ECC) complemented with efficient key management schemes to avoid resource draining (Sicari et al., 2015). Since the sensor devices are battery powered, efficient energy harvesting operations should be employed to increase their life cycle. This includes harnessing and exploiting alternate sources of energy such as wind, solar etc. Another issue prevalent is the physical tampering of sensor nodes. This could be avoided by periodic monitoring checks and analysis of the data to sense for any irregularity. At the network layer, robust firewall and packet filtering mechanisms need to be implemented to mitigate attacks like DoS, DDoS, Man-in-the-Middle and packet Sniffing. Also, to ensure protection against replay attacks, secure timestamp schemes should be designed and implemented. The use of secure communication protocols such as TLS/SSL and IPsec that provide end-to-end encryption should be encouraged. This ensures that confidentiality, integrity and authenticity of communication are achieved (Suo et al., 2012). At the application layer, attacks such as malicious worm, cross site scripting and injection attacks are mainly directed towards software management interface. To defend this, efficient coding, script detection techniques including vulnerable code rewrite techniques need to be implemented. In case of Cloud, access control protocols need to be strictly enforced. The access to storage and files should be encrypted and authorized, leaving no room for data leakage. Since cloud is distributed and multiple users access the cloud interface simultaneously, a certain degree of balanced isolation is required together with data sharing to enable secure data aggregation and analytics. Different countries across the globe have different pre-requisites for obtaining evidence on illegal behaviors. Tracing network crimes on CloudIoT platform becomes extremely hard for forensic investigators when data source comes from varied multi-level third-party vendors. To understand and recover from any security breach, all CloudIoT operations should be logged and kept in a separate file, so that at a later point in time, it can be checked by digital forensic experts and appropriate contingency measures could be applied. The integration of Cloud and IoT poses a great challenge to forensic investigators given the fact that both are heterogeneous platforms and both require different level and type of security protocols. To trace a cybercrime would require a great detail and unprecedented access to the distributed cloud servers. Also, device identity parameters and network that compromised

Table 3. Summary of CloudIoT vulnerabilities

Layer	Vulnerability	Issue	Mitigation
Perception Layer	Node capture attack	Control the sensor node by physically replacing entire node or tampering the node	Effective monitoring and detection of malicious code
	Malicious code/data injection	Injecting malicious code/data into the memory of sensor node to grant access or behave abnormally	Code authentication and data filtering schemes need to be developed and implemented
	Replay attack	Obtain trust of sensor node/device by destroying validity of certification	Use of secure timestamp techniques should be encouraged
	Side channel attacks/ Cryptanalysis	Obtain encryption key from cipher-text or plaintext	Secure encryption and key management techniques should be used
	Signal Interference	Send noise data or jamming signal to interfere in wireless transmissions	Secure noise filtering techniques to filter noise data and restore original signal are required
	Sleep deprivation attack	Break programmed sleep routines to keep the device awake all the time until they shutdown	Explore alternate sources of energy. Secured duty cycle mechanism need to be studied
Network Layer	Denial of service	Consumes all available resources by flooding network with massive traffic	Strong firewall and packet filtering mechanisms need to be studied
	Spoofing attack	Attacker gains access to the network and sends malicious data across the system. e.g. IP spoofing, RFID spoofing	Secure trust management, identification and authentication need to be implemented
	Sinkhole attack	Compromised node claims exceptional power capacity and computation so that it gets selected as forwarding node in data routing process	Techniques such as secure multiple routing protocols need to be applied
	Man-in-the-middle	The malicious node acts as a middle device to store and forward all data between two compromised nodes outside their knowledge. It violates confidentiality, integrity and privacy	Secure encryption and key management techniques should be used. Data leakage should be avoided.
	Routing attacks	Routing information is manipulated to create route loops and packet drops	Techniques such as secure multiple routing protocols need to be applied
Application Layer	Phishing attack	Attacker obtains confidential data of users such as identification and passwords by spoofing authentication credentials using infected mails and websites	Awareness among web users and spam filtering
	Malicious worm attack	Infects the network with self-propagating worms, Trojans, viruses etc to obtain and temper with confidential data	Reliable firewall and virus protection in the network is required
	Cross site scripting	Injects scripts to steal confidential and authentication information	Secure coding practices during designing of web interface

device might have used needs scanning and access. If proxy Cloud servers are used, it might further add to the challenge of restructuring and analyzing digital information for forensic investigation.

INTEGRATION CHALLENGES AND OPEN ISSUES

It is apparent that cloud adds novel attributes and seamless benefits to the IoT; however, their integration also presents some inherent issues which require substantial and durable solutions (Diaz et al., 2016).

Security and Privacy

As discussed in earlier sections, Security and Privacy are well known vulnerabilities given the ubiquitous and pervasive environment offered by CloudIoT. The sensitive data stored in the cloud must be protected so that Confidentiality, Integrity and Availability of data is maintained (Cook et

al., 2018). Any security contravention in confidentiality or integrity could result in theft or tampering of personal data. The problem becomes severe incase the data is exposed and used for further malicious activities. Therefore, data security must be ensured both on IoT devices as well as on Cloud machines. Also, security framework must ensure network and protocol security for heterogeneous device communication including identity management and also protect privacy for big data produced by IoT devices.

Protocol Support and Need for Standards

As IoT is yet to be standardized, divergent protocols need to co-exist. Even if the devices were homogeneous, there is a possibility that sensors would use heterogeneous protocols such as IEEE 1451, Zigbee, CoAP and 6LOWPAN. Some of these protocols would be supported by data aggregation gateway while as others would be incompatible. The problem would elevate more once devices are integrated with cloud environment. Therefore, standard protocols and architectures are demanded from the scientific community to achieve seamless integration of interconnected services and heterogeneous objects.

Efficient Energy Utilization

With pervasive use of IoT and its interoperability with the Cloud, a lot of data gets exchanged which consumes power from energy constrained devices. In case of surveillance video, more power gets consumed because multimedia data (e.g. video) is transmitted. The use of interim power supply such as silicon batteries is not recommended, because they require replacement after periodic intervals. With enormous number of sensor devices deployed, it is beyond comprehension to have such a backup. Hence alternate sources of energy need to be harnessed such as solar power or wind energy which are re-usable and more efficient (Evans, 2011). Similarly, other option to save power would be that devices go on a sleep mode when there is no sensing activity in a given period.

Latency and Bandwidth

The Cloud environment offers vast amount of computing resources; however, it cannot guarantee lower delay or limitless bandwidth since this factor is outside the domain of cloud service provider. The ideal approach is to place an intermediate layer between Cloud and IoT also known as Fog Computing. Placing resources locally would ensure low latency in bandwidth for Jitter sensitive applications (Bonomi et al., 2012; Cook et al., 2018).

Quality of Service (QoS)

Given the amount of data that is being generated and exchanged between IoT devices, Quality of Service (QoS) becomes an important factor in determining overall efficiency of the network. A large number of requests need to be handled by the Cloud some which may be critical and delay sensitive. This would require using QoS improvisation techniques such as queuing algorithms and request prioritization to avoid packet data loss. The use of IPv6 is therefore recommended which provides QoS features such as Traffic class and Flow label. The cloud service provider must also ensure scalability. i.e. when application load increases from a user, the cloud must scale up to satisfy growing requests. On the contrary, when load decreases, the cloud must automatically scale down to adjust the change.

DISCUSSION AND CONCLUSION

The IoT concept has increasingly become popular as the key enabler of novel applications impacting our daily lives. The integration of Cloud with IoT is primarily influenced by demand for IoT infrastructures and application improvement in terms of computational resources, storage, performance and scalability. Additionally, Cloud also acts as an antidote to vanquish several issues inherent to IoT paradigm

distinguished by heterogeneous objects with technological constraints. Most of the literature available reviews Cloud and IoT independently, highlighting main features, supporting technologies and issues, however this lacks a wide and detailed analysis of CloudIoT paradigm including open issues in this context. To bridge this gap, this paper surveyed literature and presented broad panoramic view of the state-of-the-art research on the integration components of CloudIoT. The paper also discussed varied CloudIoT applications including motivating factors for CloudIoT integration. This paper also identifies layered security vulnerabilities affecting CloudIoT with some suggested mitigation measures. In the last section, the paper recognizes some open issues and challenges impeding CloudIoT integration. From the survey carried out in this paper, it is evident that substantial amount of further research is required to achieve seamless and secure integration of Cloud with IoT. The potential directions for future research includes developing more secure and robust algorithms so that only authorized and authenticated devices/nodes access the CloudIoT system resources and sensitive data. There is also a need to devise privacy policy so that data leaks could be prevented which could affect the cyber physical environment. Data should be properly encrypted so that unauthorized access could be blocked. The security algorithms should be light weight (e.g. ECC) and energy efficient keeping in mind the limited power backup of IoT nodes. To supplement energy efficiency, alternate renewable sources of energy need to be harnessed which are re-usable and more efficient. There is also a clear necessity to develop standard architectures, interfaces, protocols and API's in order to enable seamless integration of heterogeneous smart devices and facilitate creation of enhanced services for CloudIoT paradigm. Also Cloud decentralization known as Fog computing will ensure low latency in bandwidth for delay sensitive applications. This should be complemented with enforcing Quality of Service and performance measures (e.g. Traffic class and Flow label) dispensed by IPv6.

REFERENCES

Aazam, M., & Huh, E. N. (2014, August). Fog computing and smart gateway based communication for cloud of things. In *2014 International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 464-470). IEEE.

Aazam, M., Huh, E. N., St-Hilaire, M., Lung, C. H., & Lambadaris, I. (2016). Cloud of things: integration of IoT with cloud computing. In *Robots and Sensor Clouds* (pp. 77–94). Cham: Springer. doi:10.1007/978-3-319-22168-7_4

Aazam, M., Hung, P. P., & Huh, E. N. (2014, April). Smart gateway based communication for cloud of things. In *2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)* (pp. 1-6). IEEE.

Abomhara, M., & Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)* (pp. 1-8). IEEE.

Aguzzi, S., Bradshaw, D., Canning, M., Cansfield, M., Carter, P., Cattaneo, G., & Stevens, R. (2013). Definition of a research and innovation policy leveraging cloud computing and IoT Combination (Final Report). *European Commission, SMART*, *37*, 2013.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015, July). Internet of Things: Security vulnerabilities and challenges. In *2015 IEEE Symposium on Computers and Communication (ISCC)* (pp. 180-187). IEEE.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., & Zaharia, M. (2009). Above the clouds: A Berkeley view of cloud computing (Vol. 4, pp. 506-522). University of California, Berkeley.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16). ACM. doi:10.1145/2342509.2342513

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2014, August). On the integration of cloud computing and internet of things. In 2014 international conference on Future internet of things and cloud (FiCloud) (pp. 23-30). IEEE. doi:10.1109/FiCloud.2014.14

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems*, *56*, 684–700. doi:10.1016/j.future.2015.09.021

Buyya, R., Ranjan, R., & Calheiros, R. N. (2010, May). Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services. In *International Conference on Algorithms and Architectures for Parallel Processing* (pp. 13-31). Springer. doi:10.1007/978-3-642-13119-6_2

Capkun, S., Buttyán, L., & Hubaux, J. P. (2003). Self-organized public-key management for mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, *2*(1), 52–64. doi:10.1109/TMC.2003.1195151

Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with china perspective. *IEEE Internet of Things journal*, *1*(4), 349-359.

Cook, A., Robinson, M., Ferrag, M. A., Maglaras, L. A., He, Y., Jones, K., & Janicke, H. (2018). Internet of Cloud: Security and Privacy Issues. In *Cloud Computing for Optimization: Foundations, Applications, and Challenges* (pp. 271–301). Cham: Springer. doi:10.1007/978-3-319-73676-1_11

Devipriya, S. (2017). Contribution of internet of things: a survey. *Journal of Web Development and Web Designing*, *1*(1, 2, 3).

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer Applications*, *67*, 99–117. doi:10.1016/j.jnca.2016.01.010

Distefano, S., Merlino, G., & Puliafito, A. (2012, July). Enabling the cloud of things. In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)* (pp. 858-863). IEEE. doi:10.1109/IMIS.2012.61

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything [white paper]. CISCO.

Fox, G. C., Kamburugamuve, S., & Hartman, R. D. (2012, May). Architecture and measured characteristics of a cloud based internet of things. In *2012 International Conference on Collaboration Technologies and Systems (CTS)* (pp. 6-12). IEEE. doi:10.1109/CTS.2012.6261020

Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. *IEEE Security and Privacy*, *9*(2), 50–57. doi:10.1109/MSP.2010.115

Grozev, N., & Buyya, R. (2014). Inter-Cloud architectures and application brokering: Taxonomy and survey. *Software, Practice & Experience*, *44*(3), 369–390. doi:10.1002/spe.2168

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. doi:10.1016/j.future.2013.01.010

Hassan, M. M., Song, B., & Huh, E. N. (2009, February). A framework of sensor-cloud integration opportunities and challenges. In *Proceedings of the 3rd international conference on Ubiquitous information management and communication* (pp. 618-626). ACM. doi:10.1145/1516241.1516350

Jeffery, K. (2014). Keynote: CLOUDs: A large virtualisation of small things. In *The 2nd International Conference on Future Internet of Things and Cloud (FiCloud-2014).*

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks*, *20*(8), 2481–2501. doi:10.1007/s11276-014-0761-7

Khodkari, H., Maghrebi, S. G., & Branch, R. (2016). Necessity of the integration Internet of Things and cloud services with quality of service assurance approach. *Bulletin de la Société Royale des Sciences de Liège*, *85*(1), 434–445.

Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, *28*(6), 833–851. doi:10.1016/j.future.2012.01.006

Kovatsch, M., Mayer, S., & Ostermaier, B. (2012, July). Moving application logic from the firmware to the cloud: Towards the thin server architecture for the internet of things. In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)* (pp. 751-756). IEEE.

Lee, J. Y., Lin, W. C., & Huang, Y. H. (2014, May). A lightweight authentication protocol for internet of things. In *2014 International Symposium on Next-Generation Electronics (ISNE)* (pp. 1-2). IEEE. doi:10.1109/ISNE.2014.6839375

Lee, K., Murray, D., Hughes, D., & Joosen, W. (2010, November). Extending sensor networks into the cloud using amazon web services. In *2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications (NESEA)* (pp. 1-7). IEEE. doi:10.1109/NESEA.2010.5678063

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125–1142. doi:10.1109/JIOT.2017.2683200

Liu, W., Zhao, X., Xiao, J., & Wu, Y. (2005, July). Automatic vehicle classification instrument based on multiple sensor information fusion. In *Third International Conference on Information Technology and Applications ICITA 2005* (Vol. 1, pp. 379-382). IEEE.

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity authentication and capability based access control (IACAC) for the internet of things. *Journal of Cyber Security and Mobility*, *1*(4), 309–348.

Meingast, M., King, J., & Mulligan, D. K. (2007, March). Embedded RFID and everyday things: A case study of the security and privacy risks of the US e-passport. In *IEEE International Conference on RFID* (pp. 7-14). IEEE. doi:10.1109/RFID.2007.346143

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Mo, Y., & Sinopoli, B. (2009, September). Secure control against replay attacks. In *47th Annual Allerton Conference on Communication, Control, and Computing Allerton 2009* (pp. 911-918). IEEE. doi:10.1109/ALLERTON.2009.5394956

Nordrum, A. (2016). Popular internet of things forecast of 50 billion devices by 2020 is outdated. *IEEE Spectrum*, 18.

Parwekar, P. (2011, September). From internet of things towards cloud of things. In *2011 2nd International Conference on Computer and Communication Technology (ICCCT)* (pp. 329-333). IEEE. doi:10.1109/ICCCT.2011.6075156

Rao, B. P., Saluia, P., Sharma, N., Mittal, A., & Sharma, S. V. (2012, December). Cloud computing for Internet of Things & sensing based applications. In *2012 Sixth International Conference on Sensing Technology (ICST)* (pp. 374-380). IEEE. doi:10.1109/ICSensT.2012.6461705

Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer*, *44*(9), 51–58. doi:10.1109/MC.2011.291

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. doi:10.1016/j.comnet.2012.12.018

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. doi:10.1016/j.comnet.2014.11.008

Soldatos, J., Kefalakis, N., Hauswirth, M., Serrano, M., Calbimonte, J. P., Riahi, M., & Skorin-Kapov, L. (2015). Openiot: Open source internet-of-things in the cloud. In *Interoperability and open-source solutions for the internet of things* (pp. 13–25). Cham: Springer. doi:10.1007/978-3-319-16546-2_3

Soliman, M., Abiodun, T., Hamouda, T., Zhou, J., & Lung, C. H. (2013, December). Smart home: Integrating internet of things with web services and cloud computing. In *2013 IEEE 5th International Conference on Cloud Computing Technology and Science (CloudCom)* (Vol. 2, pp. 317-320). IEEE.

Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G., & Suciu, V. (2013, May). Smart cities built on resilient cloud computing and secure internet of things. In *2013 19th International Conference on Control Systems and Computer Science (CSCS)* (pp. 513-518). IEEE. doi:10.1109/CSCS.2013.58

Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In 2012 international conference on Computer Science and Electronics Engineering (ICCSEE) (Vol. 3, pp. 648-651). IEEE. doi:10.1109/ICCSEE.2012.373

Thepparat, T., Harnprasarnkit, A., Thippayawong, D., Boonjing, V., & Chanvarasuth, P. (2011, April). A virtualization approach to auto-scaling problem. In *2011 Eighth International Conference on Information Technology: New Generations (ITNG)* (pp. 169-173). IEEE. doi:10.1109/ITNG.2011.173

Velte, A. T., Velte, T. J., Elsenpeter, R. C., & Elsenpeter, R. C. (2010). *Cloud computing: a practical approach*. New York: McGraw-Hill.

Villegas, D., Bobroff, N., Rodero, I., Delgado, J., Liu, Y., Devarakonda, A., & Parashar, M. et al. (2012). Cloud federation in a layered service model. *Journal of Computer and System Sciences*, *78*(5), 1330–1344. doi:10.1016/j.jcss.2011.12.017

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30. doi:10.1016/j.clsr.2009.11.008

Wen, Q., Dong, X., & Zhang, R. (2012, October). Application of dynamic variable cipher security certificate in internet of things. In *2012 IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS)* (Vol. 3, pp. 1062-1066). IEEE. doi:10.1109/CCIS.2012.6664544

Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010, August). Research on the architecture of Internet of things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)* (Vol. 5, p. 484). IEEE.

Yuriyama, M., & Kushida, T. (2010, September). Sensor-cloud infrastructure-physical sensor management with virtualized sensors on cloud computing. In *2010 13th International Conference on Network-Based Information Systems (NBiS)* (pp. 1-8). IEEE. doi:10.1109/NBiS.2010.32

Zaslavsky, A., Perera, C., & Georgakopoulos, D. (2013). Sensing as a service and big data. arXiv:1301.0159

Zhao, G., Si, X., Wang, J., Long, X., & Hu, T. (2011, June). A novel mutual authentication scheme for Internet of Things. In *Proceedings of 2011 International Conference on Modelling, Identification and Control (ICMIC)* (pp. 563-566). IEEE.

Zhao, K., & Ge, L. (2013, December). A survey on the internet of things security. In *2013 9th International Conference on Computational Intelligence and Security (CIS)* (pp. 663-667). IEEE. doi:10.1109/CIS.2013.145

Zhou, J., Leppanen, T., Harjula, E., Ylianttila, M., Ojala, T., Yu, C., & Yang, L. T. (2013, June). Cloudthings: A common architecture for integrating the internet of things with cloud computing. In *2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD)* (pp. 651-657). IEEE. doi:10.1109/CSCWD.2013.6581037

Zhu, W., Luo, C., Wang, J., & Li, S. (2011). Multimedia cloud computing. *IEEE Signal Processing Magazine*, *28*(3), 59–69. doi:10.1109/MSP.2011.940269

Zikopoulos, P., & Eaton, C. (2011). *Understanding big data: Analytics for enterprise class Hadoop and streaming data*. McGraw-Hill Osborne Media.

Zorzi, M., Gluhak, A., Lange, S., & Bassi, A. (2010). From today's intranet of things to a future internet of things: A wireless-and mobility-related view. *IEEE Wireless Communications*, *17*(6), 44–51. doi:10.1109/MWC.2010.5675777

Junaid Latief Shah is an Assistant Professor in the Department of Information Technology, Sri Pratap College, Cluster University Srinagar, India. He completed his Bachelor's in Computer Science and Master's in Computer Science from University of Kashmir. He also obtained his PhD in the field of Next Generation Networks and IPv6 from University of Kashmir. Besides this, he has qualified UGC National Eligibility Test (NET) and State Eligibility Test (SET) in Computer Science and Applications. His Research areas include Computer Networks and Security, Web Security and Testing.

Heena Farooq Bhat is a Research Scholar in the Department of Computer Science University of Kashmir, India. She completed her Bachelor's in Computer Science and Master's in Computer Science from University of Kashmir. She also obtained her M.Phil in the field of Data Mining from University of Kashmir. Her Research areas include Artificial Intelligence and Data Mining.

Asif Iqbal Khan is a Research Scholar in the Department of Computer Science University of Kashmir, India. He completed his Bachelor's in Computer Science and Master's in Computer Science from University of Kashmir. He also obtained his M.Phil in the field of Artificial Intelligence from University of Kashmir. His Research areas include Artificial Intelligence and Data Mining.