iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** IV **Month of publication:** April 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.41202

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue IV Apr 2022- Available at www.ijraset.com*

# Internet-of-Things (IoTs) Architecture and its Diverse Layers Affect Safety, Transparency and Integrity

Utkarsh Sharma
*{B.Tech, CSE at MNNIT Allahabad (Prayagraj)}*

***Abstract:*** ***The Internet of Things (IoT), which includes anything as of conventional equipment to popular household gadgets like WSNs and RFID, has played an important role since its creation. With the enormous promise of IoT comes a slew of challenges. This research focuses on safety harms amongst other things. IoT security challenges will reveal themselves in IoT since it is based on the Internet. Furthermore, because the Internet of Things is made up of three layers: insight, transportation, and submission, this article will look at safety challenges at every layer unconnectedly and attempt to find out new harms and solutions. This research delves at cross-layer mixed addition obstacles and safety concerns, as well as IoT security issues in general and seeks to overcome them. Finally, this research compares and contrasts IoT and traditional network security concerns, as well as addressing new IoT security issues.***
***Keywords: The Internet of Things (IoT), Security, Authentication, Issues, Transparency, RFID, WSN.***

## I. INTRODUCTION

The Internet of Things (IoT) is a network of linked objects and people that provide services and share data to fulfill tasks in a variety of applications. The Internet of Things' main purpose is to change our daily lives and how we perform various tasks. From domestic to industrial, the Internet of Things offers a wide range of applications. For example, there are various smart automobiles and traffic control systems that employ IoT to establish a safe transportation system in the transportation industry. [1,2,3].

The Internet is a worldwide network that links people, software, and services. The Internet of Things (IoT), which allows common things to connect to the internet, is quickly developing. IoT network are circulated and dynamic deploying ICT that includes a huge number of devices (with sensors) that transmit and get vast amounts of data in real time. Things can think, see, and hear their environment using the Internet of Things to make decisions. [4-5].

As the IoT sector expands solutions for securing these networks and devices are being developed, ensuring a secure environment for from home appliances to mobility, logistics, healthcare, and smart cities, there are numerous applications. The Internet Research Task Force as well as the IEEE, for example, are rising the essential communication protocols to make IoT more secure. These technologies are necessary for the Internet of Things to become more dependable and energy efficient. The Internet of Things gives you a lot of flexibility and scalability. One of the key objectives is to guarantee that proper authentication solutions are available to avoid attacks that operations and accessibility of information and integrity are jeopardised. Data must always be available to permitted users, which is one of the most important criteria for IoT security. [5,6,7].

Ensured safety [8,9,10,] The most significant concerns concerning IoT expansion are security and privacy. This study looks at the safety In comparison to other applications and systems, aims and supplies for IoT systems. combining the Iot devices with other innovations, such as cloud computing. [11-13]

Other issues like as standards, scalability, and interoperability must be addressed. [14,15].

There are numerous problems and inconsistencies in research and development since IoT is a new paradigm. The goal of this essay is to address those issues and examine where the Internet of Things is now and where it is headed in the future. The following is how the rest of the paper is organised: We'll go into the history of IoT, including how did it happen? As well as some current patterns and predicted enlargement in the following section.

We'll go through the IoT structural design and procedure stack in part three. In Section 4, we'll look at some of the tools and approaches that may be used to conduct Internet of Things research. Section 5 delves into the technology that makes IoT possible, Section 6 deals with data security. that IoT presents. The industrialisation of IoT is discussed in Section 7. We get to a conclusion by identifying a number of research gaps.

## II. BACKGROUND AND STATISTICS

Since the 1980s, when Carnegie Mellon University installed the first Internet-connected soft drink machine, smart objects have been a popular notion. This machine could send information to its directory about how many drinks were left and if they were cold enough. In the 1990s, several firms experimented with the automation of our daily lives by trying From one node to another, data is sent in small packets. At the In 1999, the Global Market Forum was held. , Bill Joy suggested the notion of Hardware communication is a type of communication where two or more devices communicate with one other. Kevin Ashton coined the phrase. "Internet of Things" in the same year. After that, this field began to gain traction. Kevin Ashton wanted to characterise the Internet of Things (IoT) as a network of interconnected common things, with RFID and WSN as the major technologies that make it possible. [16,17].

In the year 2000, LG announced that it will produce refrigerators that could be connected to the Internet. Barcodes were still the most common retail technology at the time However, Walmart and the US Department of Defense were both employing RFID in industrial applications by 2003. Other articles about the Internet of Things appeared in publications such as the Guardian. during the same year. In 2005, the ITU-T published the first study on the Internet of Things. [18,19].

In 2011, another 2128 IPv6 addresses were made public, bringing the total number of IPv6 addresses to above 100. In 2013, Intel launched an IoT division, Google followed in 2015, when it began building IoT network services.. As a consequence of technology breakthroughs such as embedded systems and cyber physical systems, among others, people's opinions of IoT have altered considerably in recent years. Some current IoT statistics are as follows:[20]

*1)* According to Cisco, by 2020, each individual will have roughly 3.5 connected gadgets. [21].
*2)* IoT will be employed in roughly 80% of consumer services by 2020. [22].
*3)* In 2020, global IoT investment is predicted to increase by 15.6 percent annually to $1.29 trillion., according to IDC. [23].
*4)* North America, according to IoT Analytics, By 2021, it will have the greatest CAGR of 36 percent. Asia, with $616 million in revenue, will have surpassed Europe as the largest continental market. [24].
*5)* Smart Cities will have the fastest growth in IoT, according to IoT Analytics, with a 54 percent CAGR over the next six years. [25].

## III. THE INTERNET OF THINGS (IOT) ARCHITECTURE

Despite the lack of a common IoT design, several prototypes with three, four, or five layers have been developed. As previously said, the The most common IoT architecture has three structures: sensor, middleware, and implementation.

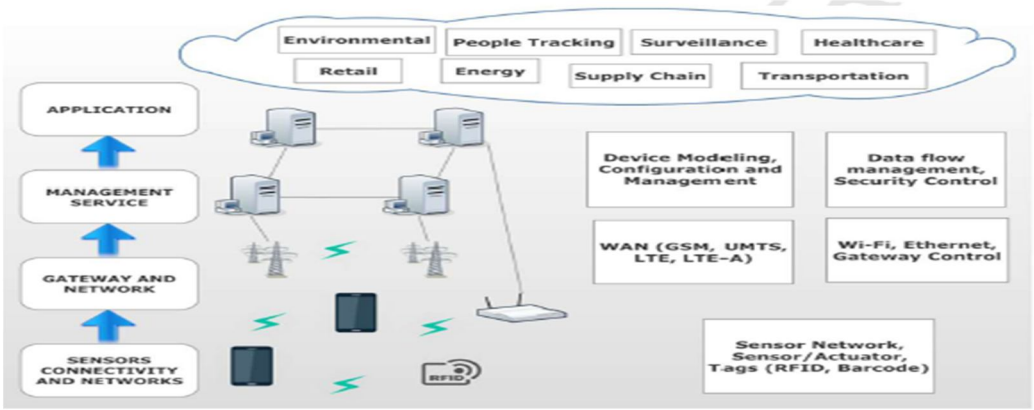



Figure 1: IoT Architecture

*1)* *Higher Layer of Perception/Sensors*: This layer's objective is to recognise entities in the Iot platform in a unique way, which may be accomplished by collecting data about them. Sensors or RFID tags make up this layer. They also interface with the environment and receive data, which they subsequently pass on to the higher levels for processing. [26].
*2)* *Middleware layer*: This layer's objective is to provide IoT network capabilities as well as a protocol stack. This layer can be separated into two components depending on the topology: The data obtained by the perception layer is processed by the controller node, which is followed by the storage layer. The datagram, which makes use of Bluetooth and Wi-Fi device is the other sub layer. It communicates with the perception layer by sending and receiving data. The system's objects are also assigned addresses using IPv6 addressing. [27, 30].

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue IV Apr 2022- Available at www.ijraset.com*

3) *Application Layer:* This layer is responsible for implementing application-specific features such Smart cities and health is examples of this. In certain designs, this layer might be divided into two portions. The core network, which monitors programs and deals with data security, is the first layer. The user interface layer, or the second layer, distinguishes between different applications. [27,28].

### A. *IoT Architecture: Privacy and Security*

In order to safeguard IoT applications, The security of each layer of IoT architecture is different. and privacy problems that must be addressed. In truth, all of these issues should be evaluated and handled right at the start of the system design process. For an IoT network as a whole, the current IoT design demands proper security assessments at the outset and at regular intervals. [29].
This section talks through the security concerns that arise at each level of the IoT design process.

#### 1) *Security Concerns at the Perception Layer*

WSN, RFID, and other forms of sensing are important technologies in the perception layers. and identifying systems.

This layer's most prevalent sorts of threats include [30]:

a) *Capture of Nodes*: The system gateway nodes are more prone to be hacked, which may effect in the escape of crucial information, jeopardising the whole network's safety.
b) *Malicious Data* and a Fake Node: The adversary inserts a rogue node into the existing system, letting them to send malicious programmes and data via the network, causing the entire machine to become infected
c) *Attack on Service Disruption*: The most common and fatal network attack are DoS and DDoS attacks. As a result of these assaults, network resources are drained, and service is disrupted.
d) *Attack Replay*: to sabotage network authentication and trust processes, the attacker delivers a previously transmitted the target node with a message

#### 2) *System Layer safety Concerns*

Risks to privacy, integrity, and scalability should be handled at the network topology.
At this layer, espionage, man-in-the-middle attacks, DoS/DDoS, and attract targeted are all important concerns. [31-33].

a) *Heterogeneity*: Because different technologies and protocols are used, security and system coordination are challenging to uphold. As a result, the system is susceptible.
b) *Issues with Scalability*: The Internet of Things is made up of a large number of gadgets and gadgets may join or go away the connection at dissimilar times, causing difficulties such authenticating challenges and network congestion, and so on. It also deplete a significant amount of possessions.
c) *Data Transparency*: The attacker may to be able to have access to crucial network information data by employing social engineering tactics. Because these devices together contain massive
d) *Using specific data recovery technique*: it is straightforward to recover in sequence from the nodes with large amounts of data.

#### 3) *Problems with Safety at the Application Layer*

This layer requires varied because security standards vary based on the program's requirements, safeguarding the application is challenging and time-consuming. The following are a few of the layer's security and privacy: [34,35]:

a) *Reciprocal identifying and verification of nodes*: Each application has its own number of consumers, each with different levels of access privileges. As a result, to prevent unauthorised access, strong authentication measures should be implemented.
b) *Information Security*: Each communication should respect the privacy of the user. Sometimes the processes employed to handle data are insecure, resulting in data loss and, in the long run, significant harm to the scheme.
c) *Information System*: As a result of large data collections, system complexity rises, necessitating a lot of capital and complicated algorithms to arrange data, as well as the data redundancy.
d) *Vulnerabilities in exact Applications*: Some susceptibility may be left behind while designing modules for an application that are unbeknownst to the end user The attacker can then take advantage of these weaknesses.

## IV. STACK OF IOT CHANNELS

The IETF (Internet Engineering Task Force) has developed many groups that are concentrating on designing protocols while keeping the limits of IoT networks in mind. Furthermore, These devices should be able to communicate with a variety of designs and programs.[36].

IoT devices employ a common channels stack that is divided into four categories:

*1)* IEEE 802.15.4 emphasises various channels stack that need less force for physical layer communication, offering a set of rules for interaction at the higher layers as well as a foundation for higher levels. [37].

*2)* IPv6 packet delivery is supported by the 6LoWPAN layer, allowing low-energy protocols to employ 102 bytes at higher levels. Packet fragmentation and reassembly mechanisms are also included in this layer. [38].

*3)* 6LoWPAN The Routing Algorithm Enables RPL routing for Low Power and Lossy Networks. It also allows for an adjustable framework to meet the routing and optimization requirements of Iot systems. [39,40].

*4)* Constrained Application Protocol (CoAP) is being developed by IETF work groups for interaction at the application layer Compatibility will also be ensured while connecting across many systems or networks. [41].

### *A. These Protocols' Security Prerequisites*

Rather of relying on external security models, The channels used at each layer should be used to address the integrated iot networks. The fundamental criteria for security design are secrecy, integrity, authentication, and anonymity. IEEE 802.15.4 modes, access control features, and time synchronisation are used to provide security. [42,43].

So yet, no security methods have been established for the 6LoWPAN layer. The associated RFCs, on the other hand, highlight security problems and the implementation of safety at the system layer RFC 6606, for instance, discuss the importance of synchronisation and localisation in security systems. [44,45].

Security modes are built into the RPL protocol. A 4-byte security field is included in the control message. The field code contains a higher cognitive bit value that determines whether or not the delivered message is secure. [46-48]].

In conjunction with DTLS, CoAP provides application-layer security (Datagram Transport Layer Security). At the application level, DTLS guarantees secrecy, integrity, and authentication. Figure 3 depicts the security designs at each layer at the protocol level. [49.50].

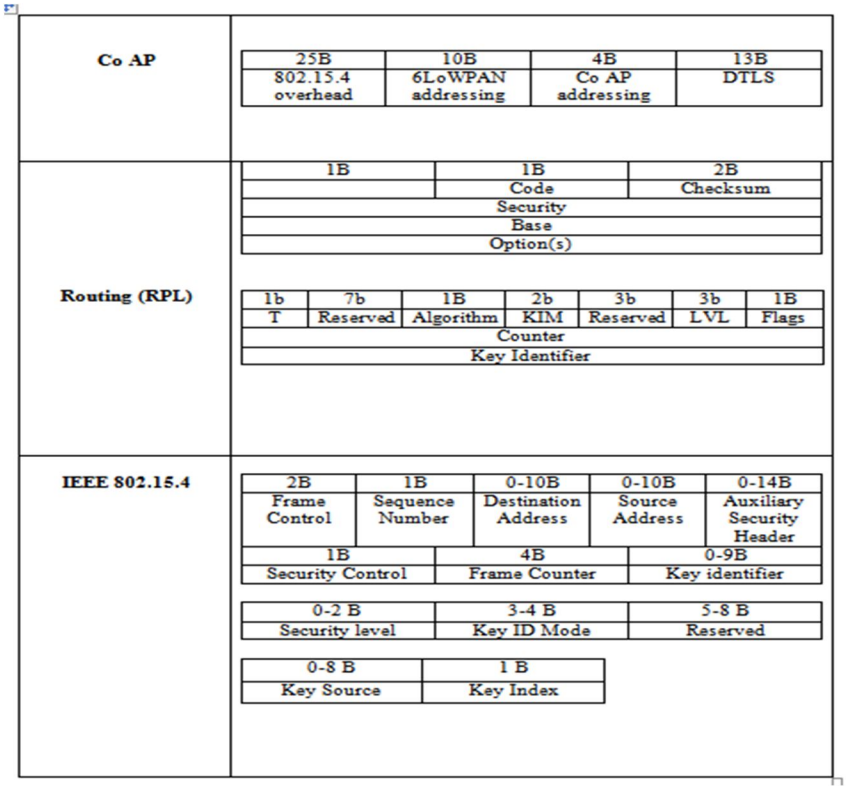



Figure 2. Different levels of security data type

## V. EXISTING IOT PLATFORMS

The availability The use of interface software in combination Using RFID chips or detectors has made it possible to install and operate IoT devices as well as link they're on the internet The systems for IoT devices have progressed significantly it possible to integrate them. of numerous software packages, enhancing network functionality and supporting more users in their day-to-day tasks. [51]. Though the safety issues that exist in IoT-based operating systems are not very alike to those found in traditional operating systems, the standards specified by the IETF enable mechanisms to safeguard such systems The following are some examples of IoT-based computer systems as follows:

1) *mbed*: ARM This computer system was designed to work with a Micro - controllers of 32-bit Cortex-M architecture. It is an open source operating system written in C and C++ and licenced under the 2.0 Apache Agreement. The mbed operating system comes with tools that allows you to create firmware for Connected systems. [52].
2) *RIOT:* It collaborated to create this mode of operation It is an open access operating system created in C and C++ licenced under the LGPL v2.1. It supports ARM Cortex-M3, M4, ARM7, and AVRAtmega processors. C and C++ programmes are supported by the SDK configuration. [53].
3) *Contiki*: Adam Dunkels originated this operating system, however it was later expanded upon by corporations like as Cisco, SAP, and Oxford University, among others. This operating system operates well on devices with little resources. For Contiki nodes, Cooja (a network emulator) is used. Contiki nodes are classified into three types: Nodes that are imitated, Java nodes and Cooja nodes. [54].
4) *Nano-RK:* This operating system is likewise developed in C and is free source. Carnegie Mellon University created it. It is intended for use with wireless sensor networks. This OS is supported by the Eclipse IDE for application development. [55].

## VI. IOT EXPERIMENTATION CHALLENGES

IoT has less resources and equipment with high design and installation costs in its early years of development. Although there has been tremendous expansion in this sector in recent years, resulting in lower resource costs, This has resulted in further scientific discoveries in this field. We can now immediately determine the limitations and benefits of IoT in respect to applications ranging thanks to new IoT technologies and real-time interfaces. To conduct a real-time investigation require large-scale data collection and analysis of an existing IoT network., multidisciplinary test beds that can assist us in overcoming the obstacles that these networks confront. We may use these test beds to see if new IoT solutions are possible; they also assess the extent to which these applications will be useful to customers. [56].

### *A. IoT Experimentation Requirements*

The majority of the test beds WSNs, which were predicated on doing tests on separated networks, are now utilised for IoT, and all development must be done within them. IoT networks, on the other hand, aim to connect these diverse networks in order to create a globally linked environment in which devices of different settings may communicate among each other. [57,58].

There are several prerequisites that these testbeds must meet in order to conduct IoT experiments.

The size of the network is increasing.: While WSN-based simulations have fewer nodes, but IoT networks sometimes Thousands of nodes function without human intervention; as a result, we need test beds that can analyses a higher number of sensor nodes in real time, as well as mistake prevention and diagnosis, on their have.

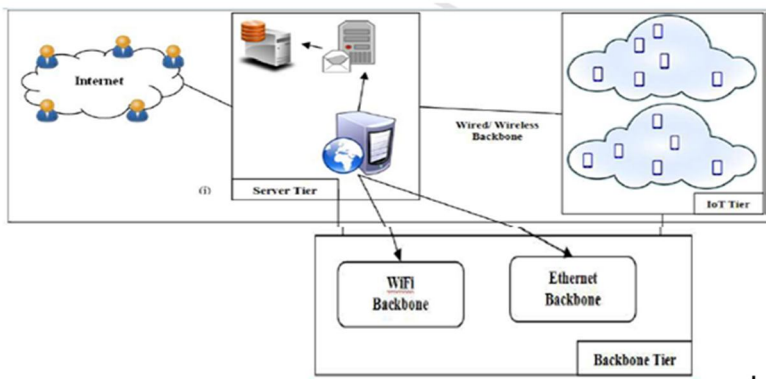



Figure 3. drawing Obstacles for IoT Test beds (i) 2nd stage (ii) 3rd stage

*B. The devices' Heterogeneity*

Devices of varied architectures should be able to be accommodated on the test beds. The networks existing at the gateway in WSNs only served as sink nodes; however, in IoT networks, these nodes must fulfill other roles. Multitasking: For IoT networks, multitasking is a must. Because the performance and resources of these systems are constrained. Distinct responsibilities may be allocated to different nodes. The IoT test bed should provide functionality to reduce the impact of several experiments running at the same time.

## VII. ELEMENTS OF IOT INTEGRATION WITH DIFFERENT DOMAINS IN TERMS OF SAFETY

*A. Internet of Things and Data Storeroom*

The fast rise of IoT has resulted in the creation of new types of devices in a variety of industries. The basic goal of any such network is to gather and analyse data in order to make judgments and learn more about the environment. The quantity of data transmitted via the Internet has expanded dramatically as the number of devices has increased. [60].

Data gets increasingly organised and intelligible as it's handled through the IoT's many levels (machine readable). For analysing and assessing IoT sensor data, big data and cloud apps provide a choice of capabilities. [61]. Due to the heterogeneity of device IoT networks have different design requirements than devices (in terms of connectivity, scalability, and security), as well as limited process technologies. presently utilised on the internet.[62].

As a result, in order to meet these standards. It introduced a novel semantic-oriented approach to data analytics in IoT. Semantics promotes successful data management, processing, and information extraction by promoting interoperability across various devices and data models. In this part, we will look at the latest advancements in semantic data analytics in IoT. [63].

*1)* Semantics alone aren't enough: Global data interchange is not possible using ontologies. Semantic identifiers must be processed and understood; semantic innovations aren't just catchphrases. [64].

*2)* Semantic Modeling and Taxonomy Development: By allowing several sources with disparate data to be compatible, semantic modelling and taxonomy development may be accomplished, semantics can assist to simplify data management. [65].

*3)* Sensor data that is linked: Sensor data that is linked allows distinct resources to be correlated with one another. IoT resources and computation may be brought together via semantic annotations, making scattered data more useful. IoT becomes more useful with the addition of a serial interface across several platforms. It also contributes to system compatibility by allowing different domains to interact with each other. The object's semantics data is connected to the object's domain-related information. characteristics, such as location, in IoT objects. Multiple resources may be connected together as a result of the use of various data models and ontologies. RDF is used to represent the existing related data. Annotating IoT data is the first step towards integrating it, which involves giving resource descriptions and service metadata, among other things. After that, the tagged data is processed and displayed as an RDB. It's also possible to use the related data. to annotate IoT data and serve as an information provider. [66].

*4)* IoT Network Issues: IoT devices capture a tremendous quantity of data. The data collected by local IoT networks should be collected by the local government. On a worldwide scale, though, we require a centralised authority to govern domains resource management understanding through good indexing in order to appropriately search for a certain resource or piece of data. Some resources and data can be shared freely, while others must be kept private. The vast bulk of Iot solutions is focused on services. The SOA (service oriented architecture) will assist systems in integrating and assuring compatibility of heterogeneous applications. [67-69].

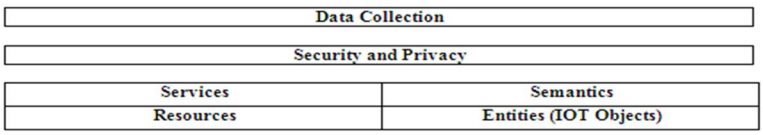



Figure 4. Requirements for IoT Data Integration

*5)* Tools for data reuse: Tools are necessary to make data and ontology reuse easier. Although there aren't many tools available right now, a handful have been built from the ground up or Customized for use in IoT systems from current tools These solutions are primarily targeted at making shared ontologies and data models easy to use so that common comments and compatibility may be facilitated. For accessing and displaying connected data, IoT devices can use a variety of semantic web engine technologies.. [70].

Sense2Web connected This application provides interfaces (GUI) for data augmentation, making it simple for users to connect data and publish RDF documents. [71]. Data is linked in two ways on this platform:

*a)* For data annotation, use globally connected resources as domain information.

*b)* Annotate data is made available as connected data resources.

*B. IoT and the Cloud*

Cloud compute enable for endless storage and low-cost processing by allowing ubiquitous networks to deliver on-demand services and a pool of common resources. The combination of cloud computing with IoT meets all of the IoT technology's criteria. Cloud computing provides a highly effective option. Management of IoT applications, services, and resources [72-75].

In this part, we will look at some of the challenges that have arisen as a result of Internet of Things (IoT) and Cloud Connectivity. [76-78].

1) *Consistency:* In the current environment, the majority of The cloud is connected to everything. which solves the storage problem while also delivering a variety of services. As a result, usual interfaces, protocols and APIs are urgently needed to assure interoperability among diverse platforms and to promote connectivity among elegant substance in order to deliver enhanced services.
2) *Integration:* The integration of cloud and elegant things that generate and analyse data in genuine time (from disparate devices) necessitates better cognitive capacities and clever conclusion making. As a result, a common integration technique with conventional procedures is necessary. The marriage of cloud and IoT necessitates the use of a standard platform to offer included services to many organisations while also controlling In the interconnected situation, computation and data are both important.
3) *Scalability:* Because elegant devices gather massive volumes of data, effective mechanisms for linking the acquired data with the applicable submission or event are required. Cloud computing provide expandable assistance and data management, which aids in the scalability of smart campaign and end users.
4) *Restrictions on Strength and Power:* In today's world, IoT applications integrate transmission of data and communication almost constantly, resulting in increased power consumption and energy needs. Data compression, efficient networking, and cache systems to conserve electricity and allow re-use of cached data are just a few of the features offered by cloud computing. In order to keep track of long-term data, the cloud also employs middleware technology.

Privacy and Security: In every application, the security and privacy of data in motion is always a high consideration. When IoT and Cloud are combined, data and occurrences from the actual world are mixed, heightening safety risks. The cloud ensures that policies are properly designed and that sensitive data is only accessible to authorised users.

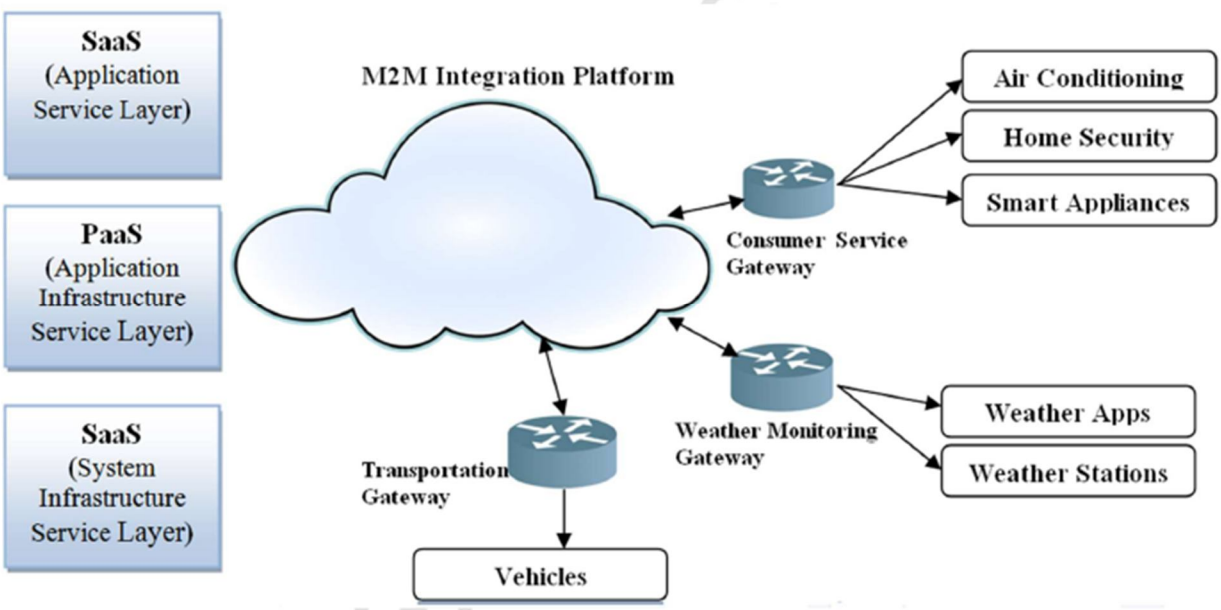



Figure 5. IoT and Cloud Integration

*C. Big Data and IoT*

Because of the heterogeneity and sound in the acquired data, IoT big data differs from customary big data. According to HP, by 2030, the sum number of sensors installed determination be in the trillions, making IoT a key contributor to big data. [81-82].

The major characteristics that plan Data from the Internet of Things (IoT) is being transformed into big data are as follows: [83]:

*1)* A massive number of sensors capturing massive volumes of data;
*2)* The majority of the information obtained is unorganised and duplicated.; and
*3)* Only after analysis can data be turned into valuable information.

IoT has the potential to be one of the key providers of big data, alongside smart cities, engineering, cultivation, shipping, healthcare, and trade. The primary characteristics of IoT-generated big data are as follows: [84-86]:

*a)* Big-scale data: data created in IoT network is termed big scale since it necessitates a large data collection instrument that collects massive volumes of heterogeneous data. It is occasionally necessary to keep previously processed data in arrange
*b)* Heterogeneity: data obtained by IoT devices can be manuscript, audio, or video in any arrangement or size, necessitating the use of a number of data collection strategy capable of gathering and analysing data with varying uniqueness.
*c)* Time and space association: Because time and space are critical for arithmetical analysis, all data collection devices include position monitor and all data packet carry time stamps.
*d)* Less effective data: technologies collect massive volumes of data, but only a small portion of it is truly valuable. For instance, while gathering a traffic observation video, only frame displaying rule breaches or accidents are added important than the remainder. [87].

*D. RFID and IoT*

One of the major enabling technologies for IoT is radio frequency identification (RFID). RFID is replacing bar codes in the majority of applications with RFID in conjunction with IoT, we may add verification techniques to improve the safety of the devices. Various RFID joint verification systems have been projected in recent years to protect IoT devices from security concerns. [88-90].
IoT relies heavily on RFID's capacity to recognise and be identified by other items, as well as interact with them. Most IoT applications today rely on distribution, receiving, and storing data [91]. The primary growth concerns confronting IoT are . [92-93]:

- Heterogeneity: IoT networks are made up of several sorts of devices that collect and store various types of data that must be processed into usable information.
- Because Iot systems have limited memory and a finite amount of electricity, we must use as little power as possible during discussions. Connection to a WSN node: While RFID integration with WSN is feasible for high-end applications, it comes with a number of drawbacks; for example, as compared to RFID, such nodes may have more than one sensor and extra connectivity. [94].

RFID system flaws: Among tags and the servers, the RFID reader acts as a channel; the system must constantly be scalable as the number of tags grows. As a result, the server must run a linear evaluation to find the tag for each tag request, and the time required for this search process rises in proportion to the amount of tags, decreasing authenticating performance of routing protocols and creating cognitive overload. [95].

*1)* *A summary of possible joint verification techniques for Lightweight systems:* Despite the fact that IoT devices have limited materials and effort, they must be updated and recognised on a regular basis by additional devices and the back end server. As a result, safety is a major concern, and authentication mechanism between communication partners is the most common method of achieving it. Given the limits of IoT devices, the authentication systems utilised for RFID Tags are often lightweight. Mutual authentication techniques are classified into four types based on their communication and computing capabilities. [96]:

*a)* Developed protocols: use traditional encryption, decryption and cryptographic with a substantial processing above your head.
*b)* Simple protocol rely on lightweight methods such as, PRNG, hash functions, ECC so on.
*c)* Lightweight protocols: Checksums in applications, confusion functions, and bitwise operation, among other things.
*d)* Protocols that employ solely bitwise operations, such as rotations and permutations, are considered ultra-lightweight. There are numerous RFID mutual authentication techniques [84-90] that may be used to safeguard IoT devices.

## VIII. IOT INTEGRATY/TRUST MANAGEMENT

The following objectives must be met in order to establish a trustworthy IoT network. [97-105]:

1) Trust management provides the measurement of the degree to which IoT network nodes are correlated and agree. It also makes it easier for them to come to an agreement and work together. The evaluation of Trust connection is necessary for autonomous intelligent trust management since it considers all entities in an IoT ecosystem at all levels. [106,107].
2) Fear of understanding: the trust managing solution should ensure that data is sent between network nodes in a secure manner. To do this, the system must make sure accuracy, persistence, and quick data collection. This is often done at the perceptual layer. [103].
3) Ensuring Privacy: The trust management software must follow policy in order to maintain the confidentiality and privacy of critical data in transit across the Network infrastructure. [108].
4) Reliable interaction: The trust control system must Guarantee the protection of data and communications travelling over the network. Any potentially dangerous network access is controlled using authorised certificates and key management. One of the most critical security requirements for IoT expansion is the objective of trust administration.. [109].
5) Quality of service: While this is primarily and although it is an application-specific (application-layer) aim, it does require help from other levels. The service quality ensures that The solutions are rendered to the appropriate end user at the appropriate time.. [110].

## IX. COLLISION OF IOT ON INDUSTRY

Implementations have increased as a result of the rapid growth of IoT, including healthcare and monitoring, environmental and animal monitoring, transportation, home help and safety, and so on. In this part, we'll look at IoT applications in the context of business. Developers must be able to strike a balance since many objectives are pursued by real-time sector Iot systems. [111].

On the other side The Internet of Things (IoT) is quickly developing and expanding. Internet of Things (IoT) Monitoring devices, health services, inventories and production planning, food supply chain (FSC), and transportation are among the sectors where solutions are being developed and/or implemented.

place of work and home assistance, safety, and observation present an overview of IoT applications in numerous fields. In contrast to their conversations, ours focuses solely on industrial IoT applications. Multiple goals must be considered while designing industrial IoT applications. Engineers may have to negotiate a tradeoff between such goals based on the intended industrial usage in order to accomplish a cost-benefit ratio. [112].

The following are some industrial IoT uses.

1) In the healthcare business, the Internet of Things (IoT) is used for the following purposes: The Internet of Things (IoT) brings up new possibilities in healthcare. Thanks to IoT's widespread All elements in health systems (people, technology, drugs, and so on) can be monitored and observed using identifying, sensing, and interconnection [113]. All healthcare-related information (logistics, diagnosis, treatment, recuperation, prescriptions, management, finance, and even everyday routines) may be conveniently retrieved, managed, and shared thanks to its worldwide connectedness. Sensors, for example, can record a patient's heart rate and send it to the doctor's office on a regular basis. Mobile web and personal desktop computers (laptop, cell telephone, tablet, etc.) connections can be used to make IoT-based health care mobile and customized (WiFi, 3G, LTE, etc.). [114]. The widespread availability of mobile internet has accelerated the development of IoT-powered in-home healthcare (IHH) services. Two key problems are security and privacy concerns. FSC to IoT applications [115]: The FSC of today is tremendously dispersed and complicated. It has a broad geographical and temporal scope, complicated operational processes, and a huge figure of players. A typical IoT solution for FSC (dubbed Food-IoT) consists of three components:
2) WSN nodes, RFID users, interface terminals, and other field machinery; b) the backhaul system, which consists of databases, servers, and other types of related or similar via dispersed computer networks, and so on; communication infrastructure projects such as WLAN, cellular, satellite, power line, Ethernet, and so on. Because the IoT system has ubiquitous networking capabilities, all of these components may be dispersed over the FSC. It also has enhanced sensing capabilities, allowing it to follow and monitor the food production process. The vast amount of unprocessed data may be exploited. and examined further to get better company processes and choice making. Big data analytics may be utilised to address the difficulty of evaluating the massive volume of FSC data.

3) IoT applications in the mining industry: Because of the working conditions in underground mines, mine security is a major difficulty for a lot of nations. To avoid and decrease mining accidents, IoT technology must be used to detect mine catastrophe signals, allowing for early caution, disaster forecasting, and underground production security enhancement. [116]. By utilising Mining businesses can follow the position of underground miners and assess crucial safety data acquired from sensors using RFID, WiFi, and other cordless wired networks and devices to enable effective information sharing between the surface and deep.

4) Internet of Things (IoT) applications in transport and logistics: The Internet of Things (IoT) will play an increasingly essential role in the transportation and logistics industries. In addition, the Internet of Things is predicted to provide possible choices for modernising transportation networks and automotive services. BMW has released the iDrive system, an intelligent informatics system that uses a number of sensors and tags to monitor the environment, including tracking the car's position and road conditions to offer driving instructions. [117]

Using RFID tags, sensors, and technological advancements in the field, developed a complete monitoring system for monitoring humidity and temperature in delivery trucks. Security and privacy protection are critical for IoT adoption in transportation and logistics since many truck drivers are concerned about data breaches and invasions of privacy. Reasonable technological, legislative, and regulatory steps are necessary to prevent unauthorised access to or disclosure of personal data In China, IoT apps are being utilised for crisis organization. Their IoT application architecture is made up of the sensor layer, communication layer, supporting layer, stage layer, and application server. Their Internet of Things architecture is designed to include both local and industry emergency generators. Developing guidelines for adopting Fire IoT is a crucial issue right now. [118-119]

## X. STUDY ISSUES AND CHALLENGES

The review of the bulk of IoT research presently focuses on technology, according to the literature. Given that the Internet of Things has yet to be deployed, this seems reasonable. IoT research will need to grow as technology advances into fields such as management, operations, law, economics, and psychology, among others. The examination of the literature generated several significant discoveries that might help scientists focus their research efforts.

IoT, as a sophisticated cyber-physical system, incorporates a variety of devices capable of The process includes processes such as sensing, recognition, processing, transmission, and networking. Sensors and devices, in particular, are becoming more powerful, less costly, and smaller, allowing for a larger range of applications. Uses in industry such as automated IoT devices are popular in monitoring, control, administration, and maintenance. The Internet of Things is predicted to become increasingly widely used in industries as a result of significant advances in technology and industrial infrastructure. The food sector, for example, is merging WSN with RFID to establish automation for tracking, monitoring, and tracing food quality across the supply chain in order to enhance food quality.

To research the trust features that drive trust relationships, divided them into five categories, and proposed that holistic consensus mechanism should handle some or all of them in various scenarios and for varied goals for complete IoT trust management. We discussed numerous goals for holistic IoT trust management and their supporting IoT layers, emphasising the need of vertical trust management in achieving trustworthy IoT on the foundation of a basic IoT system architecture. We use eight taxonomies to evaluate the applicability of previous work. For security management to highlight unresolved concerns, explain impediments, and suggest future study directions using the objectives as criteria.

In addition, research is needed to address the integration of IoT and communication technologies in a secure middleware that can handle the established security requirements. Another area of study is IoT security in mobile devices, which is becoming more prevalent nowadays. The international community has (and continues to) put forth a lot of work.

## XI. CONCLUSIONS AND DIRECTIONS FOR FUTURE RESEARCH

Examining the research, emphasising current trends, elucidating barriers to IoT adoption, and posing open research questions, this article summarises the current status of IoT research. Through automation and augmentation, the Internet of Things has the potential to improve people's lives. The IoT's capabilities may help people and businesses save time and money while also improving In a number of industries, decision-making and results are important. The Internet of Things incorporates current technologies such as RFID and Wireless Sensor Networks, as well as machine-to-machine communications guidelines such as those envisioned for the semantic web. One question is whether the Internet of Things will be a long-term innovation, or if it will only be a necessary step to a new approach. That is a question that only time will be able to answer. The Internet of Things, on the other hand, has the potential to transform our environment by linking current technologies together in creative ways.

The widespread use of IoT services necessitates the provision of tailored security and privacy settings. The survey's comprehensive overview raises a number of unresolved questions and sheds some insight on future research efforts in the realm of Internet of Things (IoT) security In a heterogeneous setting with a variety of technologies and modulation schemes, in particular, a cohesive vision for ensuring security and privacy needs is still lacking. Suitable solutions must be devised and implemented that are unaffected by the attacked platform and capable of providing user and thing gadget and user reliability, privacy, security systems, and private and adherence to specified security and privacy requirements.

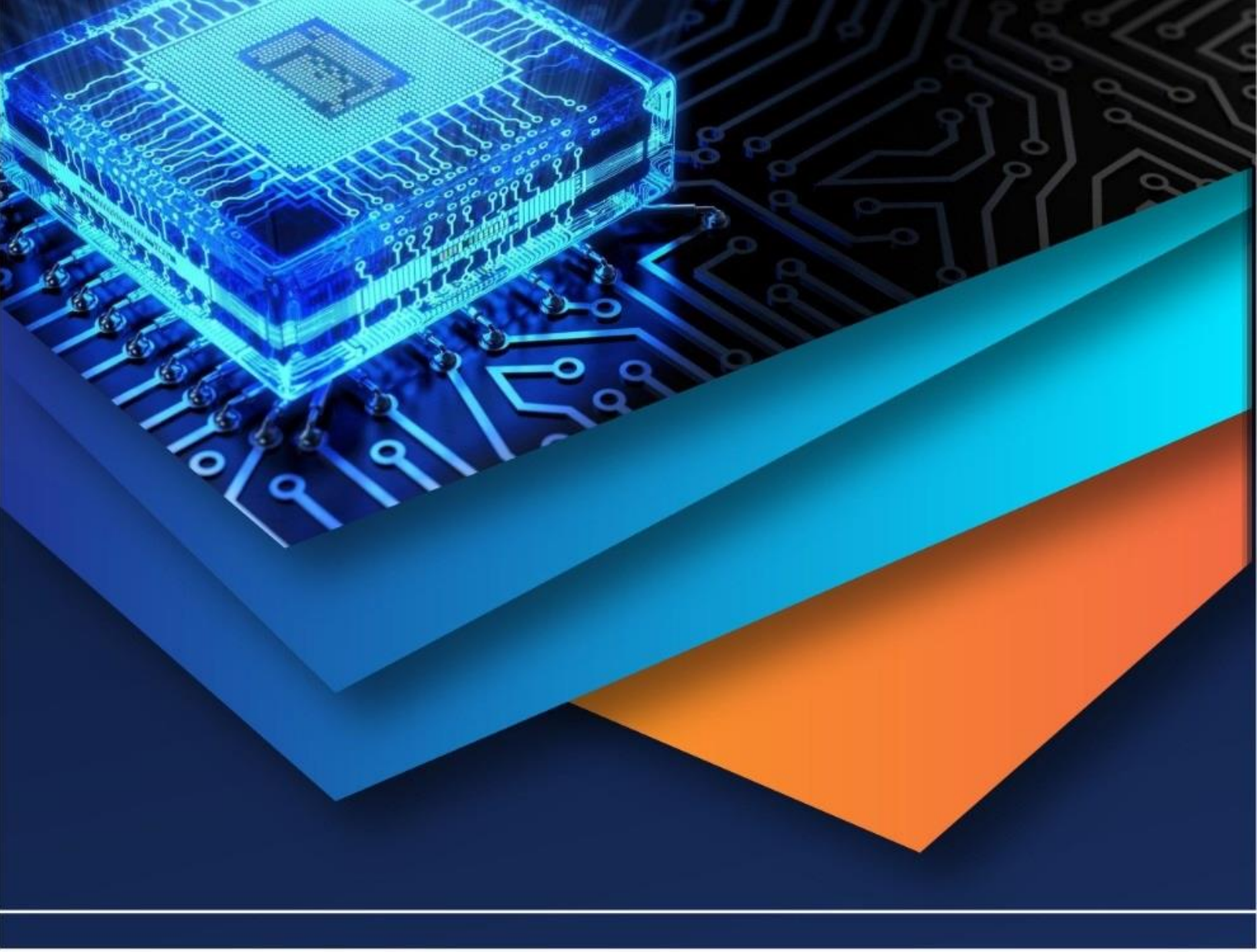
## REFERENCES

[1] K. Ashton, That ‘‘Internet of Things’’ thing, RFiD Journal (2009)
[2] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising theInternet of Things, Cluster of European Research Projects on the Internet of Things—CERP IoT, 2010.
[3] Memos, Vasileios A., et al. "An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework." Future Generation Computer Systems (2017).
[4] M. Zorzi, A. Gluhak, S. Lange, A. Bassi, From today’s Intranet of Things to a future Internet of Things: a wireless- and mobility-related view, IEEE Wireless Communications 17 (2010) 43–51.
[5] K. Ashton, That ‘‘Internet of Things’’ thing, RFiD Journal (2009)
[6] Memos, Vasileios A., et al. "An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework." Future Generation Computer Systems (2017).
[7] H.S. Ning, Z.O. Wang, Future Internet of Things architecture: like mankind neural system or social organization framework? IEEE Communications Letters 15 (2011) 461–463
[8] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, “Secrecy Cooperative NetworksWith Outdated Relay Selection Over Correlated Fading Channels,” IEEE Trans. VehicularTechnology, vol. 66, no. 8, pp. 7599-7603, Aug. 2017.
[9] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, “Secure Multiple Amplifyand-Forward Relaying With Cochannel Interference,” IEEE Journal of Selected Topics in Signal Processing, vol. 10, no. 8, pp. 1494-1505, Dec. 2016
[10] Md Zakirul Alam Bhuiyan, Jie Wu, Guojun Wang, and Jiannong Cao, "Sensing and Decisionmaking in Cyber-Physical Systems: The Case of Structural Health Monitoring," IEEE Transactions on Industrial Informatics, 12(6): 2103-2114, 2016.
[11] Yuan-Gen Wang, Dongqing Xie, and Brij B. Gupta, “A study on the collusion security of LUTbased client-side watermark embedding,” IEEE Access, 2018. DOI: 10.1109/ACCESS.2018.2802928
[12] Chong-zhi Gao, Qiong Cheng, Pei He, Willy Susilo, Jin Li. Privacy-Preserving Naive Bayes Classifiers Secure against the Substitution-then-Comparison Attack. Information Sciences. DOI:10.1016/j.ins.2018.02.058, 2018.
[13] Yuan-Gen Wang, Guopu Zhu, and Yun-Qing Shi, “Transportation spherical watermarking,”IEEE Transactions on Image Processing, vol. 27, no. 4, pp. 2063-2077, 2018
[14] M. Zorzi, A. Gluhak, S. Lange, A. Bassi, From today’s Intranet of Things to a future Internet ofThings: a wireless- and mobility-related view, IEEE Wireless Communications 17 (2010) 43–51.
[15] Sarah Vaila, “Internet of Things: New Challenges and Practices for Information Governance”, Available at: http://www.revasolutions.com/internet-of-things-new-challenges-and-practicesfor-information-governance/, Last accessed: April 2016.
[16] Jin Li, Xiaofeng Chen, Sherman S. M. Chow, Qiong Huang, Duncan S. Wong, Zheli Liu. Multiauthority fine-grained access control with accountability and its application in cloud. Journal of Network and Computer Applications. DOI: 10.1016/j.jnca.2018.03.006
[17] Bo Li, Yanyu Huang, Zheli Liu, Jin Li, Zhihong Tian, Siu-Ming Yiu. HybridORAM: Practical Oblivious Cloud Storage with constant bandwidth. Information Sciences. 2018 DOI:10.1016/j.ins.2018.02.019
[18] R. Roman, P. Najera, and J. Lopez, “Securing the Internet of Things,” Computer, vol. 44, no.9, pp.51-58, 2011.
[19] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision,architectural elements, and future directions,” Future Generation Computer Systems, vol.29,no.7, pp. 1645–1660, 2013.
[20] Near Field Comminications History “Timeline of RFID Technology”, Available at: http://www.nfcnearfieldcommunication.org/timeline.html, Last accessed: May 2016
[21] Postscapes, “History of Internet of Things”, Available at: http://postscapes.com/internet-ofthings- history, Last accessed: May 2016
[22] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision,architectural elements, and future directions,” Future Generation Computer Systems, vol.29,no.7, pp. 1645–1660, 2013.
[23] Postscapes, “History of Internet of Things”, Available at: http://postscapes.com/internet-ofthings- history, Last accessed: May 2016
[24] Giselle Abramovich, “15 facts about Intenet Of Things”, April 2015, Available at: http://www.cmo.com/articles/2015/4/13/mind-blowing-stats-Internet-of-things-iot.html
[25] Joe Hanson, “The 10 Challenges of Securing IoT Communications”, May 2015, Available at: https://www.pubnub.com/blog/2015-05-04-10-challenges-securing-iot-communications-iotsecurity/
[26] Cyber Security Ventures, “IoT Security Report, Q3 2015” Available at:http://cybersecurityventures.com/internet-of-things-security-report-q3-2015/, Last accessed: April 2016.
[27] HP, “HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack” Available at: http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.VyFG-tR97IU, Last accessed: April 2016.
[28] S. K. Datta, C. Bonnet, and N. Nikaein, “An IoT gateway centric architecture to provide novel M2M services,” in Proc. IEEE World Forum WF-IoT, 2014, pp. 514–519.
[29] M. A. Chaqfeh and N. Mohamed, “Challenges in middleware solutions for the Internet of Things,” in Proc. Int. Conf. CTS, 2012, pp. 21–26.

[30] S. K. Datta, C. Bonnet, and N. Nikaein, "An IoT gateway centric architecture to provide novel M2M services," in Proc. IEEE World Forum WF-IoT, 2014, pp. 514–519
[31] A. P. Castellani et al., "Architecture and protocols for the Internet of Things: A case study," in Proc. 8th IEEE Int. Conf. PERCOM Workshops, 2010, pp. 678–683
[32] Z. Yang et al., "Study and application on the architecture and key technologies for IOT," in Proc. ICMT, 2011, pp. 747–751.
[33] Z. Yang et al., "Study and application on the architecture and key technologies for IOT," in Proc. ICMT, 2011, pp. 747–751.
[34] Z. Yang et al., "Study and application on the architecture and key technologies for IOT," in Proc. ICMT, 2011, pp. 747–751.
[35] M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the Internet of Things," in Proc. Int. Conf. CTS, 2012, pp. 21–26.
[36] Z. Yang et al., "Study and application on the architecture and key technologies for IOT," in Proc. ICMT, 2011, pp. 747–751
[37] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, "Research on the architecture of Internet of Things," in Proc. 3rd ICACTE, 2010, pp. V5-484–V5-487.
[38] J. Granjal, E. Monteiro, and J. Sá Silva, ''Security for the Internet of Things: A survey of existing protocols and open research issues,'' IEEE Commun. Surveys Tuts., vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.
[39] IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendment 3: Alternative Physical Layer Extension to support the Japanese 950 MHz bands, IEEE Std 802.15.4d-2009 (Amendment to IEEE Std 802.15.4-2006), (2009) 1-27 doi: 10.1109/IEEESTD.2009.4840354.
[40] Raza S., Duquennoy S.,Voigt T., Securing communication in 6LoWPAN with compressed IPsec, International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), 1-8 2011 doi: 10.1109/DCOSS.2011.5982177.
[41] J. Vasseur et al., "RPL: The IP routing protocol designed for low power and lossy networks," Internet Protocol for Smart Objects (IPSO) Alliance, San Jose, CA, USA, 2011.
[42] T. Winter et al., "RPL: IPv6 routing protocol for low-power and lossy networks," Internet Eng. Task Force (IETF), Fremont, CA, USA, Request for Comments: 6550, 2012
[43] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained Application Protocol (CoAP).draft-ietf-core-coap-18," Internet Eng. Task Force (IETF), Fremont, CA, USA, 2013. [65] [66] R [67]
[44] J. Granjal, E. Monteiro, and J. Sá Silva, ''Security for the Internet of Things: A survey of existing protocols and open research issues,'' IEEE Commun. Surveys Tuts., vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.
[45] IEEE Standard for Information technology-Telecommunications and information exchang between systems-Local and metropolitan area networks-Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low- Rate Wireless Personal Area Networks (WPANs) Amendment 3: Alternative Physical Layer Extension to support the Japanese 950 MHz bands, IEEE Std 802.15.4d-2009 (Amendment to IEEE Std 802.15.4-2006), (2009) 1-27 doi: 10.1109/IEEESTD.2009.4840354.
[46] Zheng T., Ayadi A., Jiang X., TCP over 6LoWPAN for industrial applications: An experimental study, 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS),IEEE 2011.
[47] J. Vasseur et al., "RPL: The IP routing protocol designed for low power and lossy networks," Internet Protocol for Smart Objects (IPSO) Alliance, San Jose, CA, USA, 2011
[48] T. Clausen, U. Herberg, and M. Philipp, "A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL)," in Proc. IEEE 7th Int. Conf. WiMob, 2011, pp. 365–372.
[49] Z. Shelby, K. Hartke, C. Bormann, and B. Frank, "Constrained Application Protocol (CoAP).draft-ietf-core-coap-18," Internet Eng. Task Force (IETF), Fremont, CA, USA, 2013. [65] [66] R [67]
[50] W. Colitti, K. Steenhaut, N. De Caro, B. Buta, and V. Dobrota, "Evaluation of constrained application protocol for wireless sensor networks," in Proc. 18th IEEE Workshop LANMAN, 2011, pp. 1–6.
[51] Tuhin Borgohain, Uday Kumar, Sugata Sanyal, "Survey of Operating Systems for the IoT Environment", arXiv preprint arXiv:1504.02517, 2015/4/13
[52] Arm Limited MBed OS, Available at: https://mbed.org/technology/os/ Last Accessed: February 2018.
[53] E. Baccelli, O. Hahm, M. Günes, M. Wählisch, and T. C. Schmidt, "RIOT OS: Towards an OS for the Internet of Things," in Proc. IEEE Conf. INFOCOM WKSHPS, 2013, pp. 79–80.
[54] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki—A lightweight and flexible operating system for tiny networked sensors," in Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw., 2004, pp. 455–462
[55] Anand Eswaran, Anthony Rowe, and Raj Rajkumar. "Nano-rk: an energy-aware resource-centricrtos for sensor 5 networks." In Real-Time Systems Symposium, 2005. RTSS 2005. 26th IEEE International, pp. 10-pp. IEEE, 2005.
[56] A. Gluhak et al., "A survey on facilities for experimental Internet of Things research," IEEE Commun. Mag., vol. 49, no. 11, pp. 58–67, Nov. 2011
[57] A. Gluhak et al., "A survey on facilities for experimental Internet of Things research," IEEE Commun. Mag., vol. 49, no. 11, pp. 58–67, Nov. 2011
[58] E. Egea-L ´opez, J. Vales-Alonso, A. Mart´ınez-Sala, P. Pav ´on-Mario, and J. Garc´ıa-Haro, "Simulation tools for wireless sensor networks," in SPECTS, 2005.
[59] S. De, B. Christophe, and K. Moessner, "Semantic enablers for dynamic digital-physical object associations in a federated node architecture for the internet of things," Ad Hoc Netw., vol. 18, pp. 102–120, 2014.
[60] L. Xu, "Enterprise systems: State-of-the-art and future trends," IEEE Trans. Ind. Informat., vol. 7, no. 4, pp. 630–640, Nov. 2011.
[61] T. Kamiya and J. Schneider, "Efficient XML Interchange (EXI) Format 1.0," World Wide Web Consortium, Cambridge, MA, USA, Recommend. REC-Exi-20110310, 2011.
[62] T. Kamiya and J. Schneider, "Efficient XML Interchange (EXI) Format 1.0," World Wide Web Consortium, Cambridge, MA, USA, Recommend. REC-Exi-20110310, 2011.
[63] M. Kovatsch, Y. N. Hassan, and S. Mayer, "Practical semantics for the internet of things," in Proc. IEEE 5th Int. Conf. Internet of Things (IoT), 2015, pp. 54–61.
[64] L. Xu, "Enterprise systems: State-of-the-art and future trends," IEEE Trans. Ind. Informat., vol.7, no. 4, pp. 630–640, Nov. 2011.

[65] T. Kamiya and J. Schneider, "Efficient XML Interchange (EXI) Format 1.0," World Wide Web Consortium, Cambridge, MA, USA, Recommend. REC-Exi-20110310, 2011
[66] SPARQL Query Language for RDF. W3C Recommendation, from http://www.w3.org/TR/rdfsparql-query/
[67] Yu, L., and Liu, Y., Using the Linked Data Approach in a Heterogeneous Sensor Web: Challenges, Experiments and Lessons Learned, In Proc. Sensor Web Enablement (SWE) Workshop, Banff, Alberta, Canada, 2011.
[68] H. Chang, A. Hari, S. Mukherjee, and T. V. Lakshman, "Bringing the cloud to the edge," in Proc. IEEE Conf. INFOCOM WKSHPS, 2014, pp. 346–351
[69] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in Proc. 1st Edition MCC Workshop Mobile Cloud Comput., 2012, pp. 13–16.
[70] B. Rao, P. Saluia, N. Sharma, A. Mittal, and S. Sharma, "Cloud computing for Internet of Things and sensing based applications," in Proc. 6th ICST, 2012, pp. 374–380.
[71] S. Ziegler, C. Crettaz, and I. Thomas, "IPv6 as a global addressing scheme and integrator for the Internet of Things and the cloud," in Proc. 28th Int. Conf. WAINA, 2014, pp. 797–802
[72] F. Li, M. Voegler, M. Claessens, and S. Dustdar, "Efficient and scalable IoT service delivery on cloud," in Proc. IEEE 6th Int. Conf. CLOUD, 2013, pp. 740–747
[73] C. Wang, Z. Bi, and L. D. Xu, "IoT and cloud computing in automation of assembly modeling systems," IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1426–1434, May 2014
[74] B. Rochwerger et al., "The reservoir model and architecture for open federated cloud computing," IBM J. Res. Develop., vol. 53, no. 4, pp. 535– 545, Jul. 2009.
[75] G. C. Fox, S. Kamburugamuve, and R. D. Hartman, "Architecture and measured characteristics of a cloud based Internet of Things," in Proc. Int. Conf. CTS, 2012, pp. 6–12.
[76] J. Gantz and D. Reinsel, "The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east," IDC iView: IDC Anal. Future, vol. 2007, pp. 1–16, Dec. 2012. [10] S. Taylor, "The next generation of the Internet revolutionizing the way we work, live, play, and learn," CISCO, San Francisco, CA, USA, CISCO Point of View, 2013
[77] Gartner, "The Importance of 'Big Data': A Definition", June 21, 2012, https://www.gartner.com/doc/2057415/ importance-big-data-definition, accessed June 12, 2014.
[78] Rubinstein, I.S., "Big Data: The End of Privacy or a New Beginning?", International Data Privacy Law, 3(2), 2013, pp. 74-87.
[79] M. Chen, S. Mao, Y. Liu, "Big Data: A Survey", ACM/Springer Mobile Networks and Applications, Vol. 19, No. 2, pp. 171-209, April 2014.
[80] Y. Sun, H. Song, A. J. Jara, and R. Bie, ''Internet of Things and big data analytics for smart and connected communities,'' IEEE Access, vol. 4, pp. 766–773, Mar. 2016, doi: 10.1109/ACCESS.2016.2529723.
[81] Z. Lv, H. Song, P. Basanta-Val, A. Steed, and M. Jo, "Next-Generation Big Data Analytics: State of the Art, Challenges, and Future Research Topics," IEEE Transactions on Industrial Informatics, DOI: 10.1109/TII.2017.2650204, 2017.
[82] S. Fosso Wamba, S. Akter, A. Edwards, G. Chopin, and D. Gnanzou, "How 'big data' can make big impact: Findings from a systematic review and a longitudinal case study," International Journal of Production Economics, vol. 165, pp. 234-246, 2015.
[83] M. Bolic, D. Simplot-Ryl, I. Stojmenovic, "RFID Systems: Research Trends and Challenges", Wiley, 2010.
[84] H.-Y. Chien, "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 4, pp. 337-340, 2007.
[85] G. Tsudik, YATRAP yet another trivial RFID authentication protocol, International Conference on Pervasive Computing and Communications, 2006, pp. 640-643.
[86] G. Tsudik Family of dunces: trivial RFID identification and authentication protocols, Symposium on Privacy-Enhancing Technologies, 2007, pp. 45-61.
[87] M. Ohkubo, K. Suzuki, and S. Kinoshita, cryptographic approach to privacy-friendly tag, Proc. of RFID Privacy Workshop (2003)
[88] S.Weis, S. Sarma, Ronald Rivest, and D. Engels, Security and privacy aspects of low-cost radio requency indentification systems, Proc. of the 1st Security in Pervasive Computing, LNCS (2004), 201{212.
[89] S.Weis, S. Sarma, Ronald Rivest, and D. Engels, Security and privacy aspects of low-cost radio Frequency indentification systems, Proc. of the 1st Security in Pervasive Computing, LNCS (2004), 201{212
[90] A. Juels and S.Weis. Authenticating pervasive devices with human protocols. In Victor Shoup, editor, Advances in Cryptology – CRYPTO'05, volume 3126 of Lecture Notes in Computer Science, pages 293–308. Springer-Verlag, 2005.
[91] G. Tsudik, YATRAP yet another trivial RFID authentication protocol, International Conference on Pervasive Computing and Communications, 2006, pp. 640-643.
[92] A. Juels and S.Weis. Authenticating pervasive devices with human protocols. In Victor Shoup, editor, Advances in Cryptology – CRYPTO'05, volume 3126 of Lecture Notes in Computer Science, pages 293–308. Springer-Verlag, 2005.
[93] A. Juels and S.Weis. Authenticating pervasive devices with human protocols. In Victor Shoup, editor, Advances in Cryptology – CRYPTO'05, volume 3126 of Lecture Notes in Computer Science, pages 293–308. Springer-Verlag, 2005
[94] M. Feldhofer, S. Dominikus, J. Wolkerstorfer, Strong authentication for RFID systems using AES algorithm, in: Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Cambridge, MA, USA, August 2004
[95] P. Tuyls and L. Batina, "RFID-tags for anti-counterfeiting," in Proc. Topics Cryptol.(CT-RSA), 2006, pp. 115–131
[96] C. Schnorr, "Efficient identification and signatures for smart cards," in Proc. Adv. Cryptol.(CRYPTO'89), 1989, pp. 239–252.
[97] L. Batina et al., "Public-key cryptography for RFID-Tags," in Proc. IEEE Int. Workshop Pervasive Comput. Commun. Secur., 2007, pp. 217–222.
[98] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," in Proc. Adv. Cryptol.(CRYPTO'92), 1992, pp. 31–53.
[99] Y. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol," in Proc. IEEE Int. Conf. RFID, 2008, pp. 97–104.
[100] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Network Comput. Appl. 42 (0) (2014) 120–134.

[101]Bao F., Chen I. Trust management for the Internet of Things and its application to service composition. In: Proceedings of the IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM); 2012. p. 1–6
[102]Bao F., Chen I., Guo J. Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems. In: Proceedings of the IEEE eleventh International Symposium on Autonomous Decentralized Systems (ISADS); 2013. p. 1–7.
[103]Chen D, Chang G, Sun D, Li J, Jia J, Wang X. TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things. Comput Sci Inf Syst 2011;8 (4):1207–28.
[104]Erkin Z, Veugen T, Lagendijk RL. Generating private recommendations in a social trust network. In: Proceedings of the international conference on Computational Aspects of Social Networks (CASoN); 2011. p. 82–7.
[105]Gessner D, Olivereau A, Segura AS, Serbanati A. Trustworthy infrastructure services for a secure and privacy- respecting Internet of Things. In: Proceedings of the IEEE 11th international conference on trust, security and privacy in computing and communications (TrustCom); 2012.p. 998–1003.98. Grandison T, Sloman M. A survey of trust in Internet applications. IEEE Commun Surv 2000;3(4):2–16.
[106]Liu Y, Wang K. Trust control in heterogeneous networks for Internet of Thing. In: Proceedings of the International Conference on Computer Application and System Modeling (ICCASM); 2010. p. 632–6.
[107]Nitti M, Girau R, Atzori L, Iera A, Morabito G. A subjective model for trustworthiness evaluation in the social Internet of Things. In: Proceedings of the IEEE 23rd international symposium on Personal Indoor and Mobile Radio Communications (PIMRC); 2012. p. 18–23.
[108]Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Network Comput. Appl. 42 (0) (2014) 120–134.
[109]Bao F., Chen I. Trust management for the Internet of Things and its application to service composition. In: Proceedings of the IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM); 2012. p. 1–6.
[110]Erkin Z, Veugen T, Lagendijk RL. Generating private recommendations in a social trust network.In: Proceedings of the international conference on Computational Aspects of Social Networks (CASoN); 2011. p. 82–7.
[111]Gessner D, Olivereau A, Segura AS, Serbanati A. Trustworthy infrastructure services for a secure and privacy- respecting Internet of Things. In: Proceedings of the IEEE 11th international conference on trust, security and privacy in computing and communications (TrustCom); 2012. p. 998–1003
[112]Liu Y, Wang K. Trust control in heterogeneous networks for Internet of Thing. In: Proceedings of the International Conference on Computer Application and System Modeling (ICCASM); 2010 p. 632–6.
[113]Nitti M, Girau R, Atzori L, Iera A, Morabito G. A subjective model for trustworthiness evaluation in the social Internet of Things. In: Proceedings of the IEEE 23rd international symposium on Personal Indoor and Mobile Radio Communications (PIMRC); 2012. p. 18–23.
[114]Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on Industrial Informatics, 10(4), 2233–2243.
[115]H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," Comput. Netw., vol. 54, no. 15, pp. 2688–2710, 2010.
[116]I. Plaza, L. Martín, S. Martin, and C. Medrano, "Mobile applications in an aging society: Status and trends," J. Syst. Softw., vol. 84, no. 11, pp. 1977–1988, 2011.
[117]Z. Pang, Q. Chen, W. Han, and L. Zheng, "Value-centric design of the internet-of-things solutionfor food supply chain: Value creation, sensor portfolio and information fusion," Inf. Syst. Front., to be published.
[118]Z. Ji and A. Qi, "The application of internet of things (IOT) in emergency management system in China," in Proc. 2010 IEEE Int. Conf. Technol. Homeland Security (HST), pp. 139–142.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY