International Journal of Scientific Research Engineering & Technology (IJSRET) ISSN: 2278–0882
EATHD-2015 Conference Proceeding, 14-15 March, 2015

Internet of Things Advancement in Defence

Gopal Singh
B.tech (3rd year): Department of EEE
Lovely Professional University, Phagwara, India

Abstract
A world which was once imaginable where billions of objects can sense, communicate and share information, all interconnected through public or private internet protocol networks is coming reality since people are striving towards technology and developing rapidly over the past few years. These interconnected objects have data regularly collected, analyzed and used to initiate action, providing a wealth of intelligence for planning, management and decision making. This is the upcoming world which will constitute of the Internet of Things (IOT). This is a revolutionary change in today's time, most of the industries and companies are trying to adopt the concepts. Thus, saying it is the future of the world and research in this field would help us gain advancement in technology. A brief discussion about the paper has been given hereby. Discussing the trending term 'Internet of Things' its challenges and opportunities, architecture of IoT, describing most used technologies like M2M communication, cloud computing, IPv6, 4G-LTE , RFID technology. Thus explaining the use of IoT in different fields. Here, we are aiming at representing a model with its demonstration by diving the whole system into five stages and explaining each one of them. Also, showing the upcoming challenges for the successful implementation of IoT in defence. Lastly, we give a brief overview of all possible applications of IoT.

Keywords— API, CEP, Cloud computing, Internet of things, LTE-4G, M2M , Machine Learning, etc.

I. INTRODUCTION

IoT concepts striving to enable things to get connected anytime, anyplace with anything and anyone ideally using the internet or any network connecting any service. IoT is a new revolution of the internet. Objects make them recognizable and they obtain intelligence, they can communicate information about themselves and they can access information that has been aggregated by other things [1].

With more physical objects and smart devices connected in the IOT landscape, the impact and value that IOT brings to our daily lives become more prevalent. People make better decisions such as taking the best routes to work or choosing their favorite restaurant. New services can emerge to address society challenges such as remote health monitoring for elderly patients and pay-as-you-use services [3]. For government, the convergence of data sources on shared networks improves nationwide planning, promotes better coordination between agencies and facilitates quicker responsiveness to emergencies and disasters. For enterprises, IOT brings about tangible business benefits from improved management and tracking of assets and products, new business models and cost savings achieved through the optimization of equipment and resource usage.

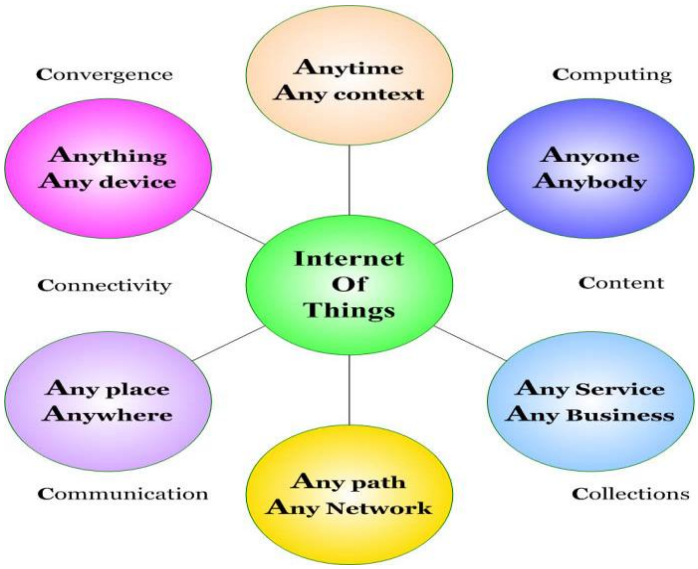

Fig. 1 The internet of things [2]

IoT's developing technology will provide person from personal goods to commercial one with unimaginable work. Through the medium of internet, people can have benefits by its proper utilization, working by sitting at their own place. Significant benefits over the applications can be detailed us, helping user save energy, enhance comfort get better healthcare and increased independence, in short meaning happier and healthier lives.

II. ARCHITECTURE OF IOT

It serves to illustrate how various technologies relate to each other and to communicate the scalability, modularity and configuration of IoT deployments in different scenarios. The different layers of IoT can be discussed as follows [3]–

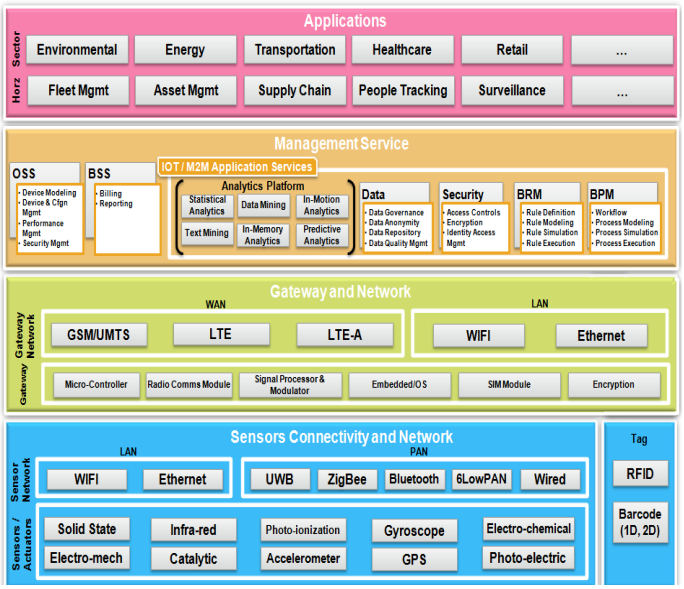

Fig. 2. The complete architecture of IoT [3].

A. Sensor Layer:

The interconnection of the physical and digital worlds are enabled with the help of sensors. Sensors can be grouped according to their unique purposes such as environmental sensors, body sensors, home appliance sensors and vehicle telematics sensors etc.

B. Gateway and Networks:

Massive volume of data will be produced by these tiny sensors and this requires a robust and high performance wired or wireless network infrastructure as a transport medium. Most sensors require connectivity to the sensor aggregators (gateways). This can be in the form of a Local Area Network (LAN) such as Ethernet and Wi-Fi connections or Personal Area Network (PAN) such as ZigBee, Bluetooth and Ultra- Wideband (UWB). For sensors that do not require connectivity to sensor aggregators, their connectivity to backend servers/applications can be provided using Wide Area Network (WAN) such as GSM, GPRS and LTE. Sensors that use low power and low data rate connectivity, they typically form networks commonly known as wireless sensor networks (WSNs). WSNs are gaining popularity as they can accommodate far more sensor nodes while retaining adequate battery life and covering large areas [3].

C. Management service layer:

The management service renders the processing of information possible through analytics, security controls, process modelling and management of devices.

D. Application layer:

The IoT promises to bring smart devices everywhere, from fridge in your home to sensor in your car, even in your body. Those application offer significant benefits: helping user save energy, enhance comfort get better healthcare and increased independence, in short meaning happier and healthier lives. And further more details will be shown upon more application.

III. SOME ENABLING TECHNOLOGY

A. RFID:

The IoT evolution can be said from the technology named radio frequency identification, and it is the first industrial realization of IoT and after that the related application of IoT comes in other fields. The RFID technology is used to track and monitor goods wherever we required and mainly in logistics and supply chain sector. And its frequency ranges from 125 kHz (low frequency/LF) up to 5.8 GHz /super high frequency (SHF) and RFID tags have at least three basic components [4].

- The I.C. holds information about goods or products to which it need to be track and transfer the data to reader wirelessly by using an air interface.
- The antenna allows transmission of the information to/from a reader.
- The packaging encases chip and antenna, and allows the attaching of the tag to an object for identification.

There are several other technology to track and detect objects such as one dimensional bar (ID), it has a significant contribution to the supply chain and other businesses such as asset management and also in various fields such as defence and industries. . Two dimension (2D) bar codes have provided a richer source of data but, once printed, are not up-datable. But in contrast with other technology RFID has its special ability to ADC (automated data collection) techniques collect process data in its environment, is proving as the present as well as probably future technology for the identification of goods. There are various industry but mainly logistics have looking RFID as tagging solutions to improve their tracking and monitoring processes [5].

There are various application possible with possible with RFID such as automatic meter reading, remote home automation and real time vehicle tracking. And also in future time it have potential to provide automated data collected scheme that have information system with real time, item specific data and the important thing is that they are flexible to place in extremely small space and location, i.e., coil on chip technology.

B. M2M (machine to machine) technology:

It is a type of communication. M2M session will outnumber H2H mobile session by a factor of more than 30 to one in 2020.souce: forester. M2M uses a device (sensor, meter, etc.) to capture an 'event' (temperature, inventory level, etc.), which is relayed through a network (wireless, wired or hybrid) to an application (software program), that translates the captured event into meaningful information (e.g., items need to be restocked) [6].

Basically M2M is small model of IoT and it has working environment as follows: It uses different kind of sensors

and detectors to internment an event such as temperature, inventory level, humidity, etc. which is communicated through a network (wireless, wired or hybrid) to an application (software program), that translates the apprehended event into meaningful information (e.g., items need to be restocked). And that's why there is a well-defined hierarchy with a broad layer M2M architecture. Basically under this technology the user get connected to various customer devices/applications like Cameras, Sensors, and Readers with embedded wireless communication modules. And then this architecture is used in various fields such as defence, industry, rescue management, security, Fleet management and health care device and inter-operate in wireless technology domain. At last we required some API (application program interface), software application that are used to collect and enable intelligent decision around IoT based system [7].

C. Cloud Computing :

It refers to the delivery of computing resources over the internet instead of keeping data on your own hard drive or updating application as our own needs, you use a service over the internet, at another location, to store information or use its application. Doing so many give rise to certain privacy implications [8].

D. IPv6 (internet protocol version 6):

6LoWPAN is an acronym for "IPv6 over Low power Wireless Personal Area Networks". It is a communication standard that allows the low-power devices to communicate and exchange data via IPv6. There are many benefits of using IP-based connectivity to form the sensor access network:

- IP connects easily to other IP networks without the need for translation gateways or proxies.
- IP networks allow the use of existing network infrastructure.
- IP is proven to work and scale. Socket API is well-known and widely used
- IP is open and free, with standards, process and documents available to anyone. It encourages innovation and is well understood.

IPv6 is 128-bit Internet address scheme that is used to replace IPv4 addresses which were officially exhausted in February 2011 (in the Asia Pacific Network Information Centre or APNIC). With IPv6, there are approximately 3.4×10^{38} unique IPv6 addresses [9].

E. LTE and LTE-A :

LTE is a 4G wireless broadband technology developed by the Third Generation Partnership Project (3GPP), an industry trade group. 3GPP engineers named the technology "Long Term Evolution" because it represents the next step in a progression from GSM, a 2G standard, to UMTS, the 3G technologies based upon GSM. LTE provides significantly increased peak data rates, with the potential for 100 Mbps downstream and 50 Mbps upstream, reduced latency and scalable bandwidth capacity. Future developments could yield peak throughput to the order of 300 Mbps.

LTE-A is a major enhancement of the LTE standard developed by 3GPP and has been approved by the International Telecommunication Union (ITU) as the 4th generation (4G) radio technologies system. LTE-A is backward compatible with LTE and uses the same frequency bands while LTE is not backward-compatible with 3G systems. LTE-A has the potential for even faster peak data rates, with the potential for 1 Gbps downstream and 500 Mbps upstream [10].

F. Adaptive learning analytics (Machine learning):

Adaptive learning analytics is a range of analytics algorithms that is performed by sensors and mobile devices to make intelligent analyses of real-time data.

Extracting useful information from a complex sensing environment at different spatial and temporal resolutions is a challenging research problem in artificial intelligence. Current state-of-the-art methods use shallow learning methods where pre-defined events and data anomalies are extracted using supervised and unsupervised learning [11].

Under machine learning we have to make such algorithms that are able to take decision based upon situation and don't required any human intervention, and there are several algorithms which work with a lot of data to predict a future value based upon past experiences and also it includes classification of data into different categories and such type of classification of data used to determine that which information is useful for which user or it may be useful in case of pattern recognition etc. so we can see that it is very useful and widely used but here it is very important to implement the concept of IoT.

IV. IOT'S ADVANCEMENT IN DEFENCE

Since we have already discussed the architecture of IoT and enabling technology for compliance of IoT concepts. There is a wide variety of IoT applications in different fields, but moving into defence and applying the ideas we can change the whole system. Here, in brief discussing the architecture and changes that can be performed we can covert the existing system in connected battlefield. India's DRDO (Defence Research & Development Organization) and DOD (Department of Defence) has been using IoT concepts and are improving their warfare systems. DOD's vision of net-centric warfare has four key elements-networked forces with improved information, information sharing and collaboration that enhances quality and situational awareness, shared situational awareness that enables self-synchronization, and the combination of the other three elements to increase mission effectiveness [12].

The military has been adapting new ideas to have asymmetrical warfare and an evolving real-time threat matrix which requires new approaches to military operations. In the midst of technological shift from the fixed-location work models to the PC era to the mobile, social, virtual and collaborative models of today, Advancement in information based technology has become more acknowledged than the overwhelming force. To address those needs, defence has been adopting new technologies and placing them into existing environments keeping in view the ability to manage complex systems all without sacrificing security and information. Defence technologies allow unification of computing, storage and network with sensors, devices and collaborative applications. An integrated architecture for Internet of everything(IoE) creates interconnected physical and virtual environments that combine IoT devices with secure virtualization, mobility, unified communication and other advanced technologies like M2M, cloud computing, IPv6, RFID, LTE-4G, machine learning, etc.

Our IoT concept will have the base of machines and personnel i.e., warfighters that are interconnected with network that enables mission planning, execution and analysis of continuous flow of information the base constituting the IoT system.

So, for constituting the IoT model in defence we divide the whole scenario in the following stages.

A. Stage 1:

It involves the embedment of Intelligence to platforms through system that provides the capacity to monitor and control the platforms performance. As known this is the base level of all machines which includes embedded system i.e., controllers or processors and a large category of sensors. Sensors can be of different types including IR sensors, photoelectric, laser, vibration etc. These sensors can be grouped according to their unique purpose such as environment sensor, home appliance sensor, body sensor and vehicle telematics sensors etc. Processor or controllers that are required here are of high quality and high performance and are programmable as per the requirement. There are a wide variety of options available which can be used like AVR, PIC, ARM, and Arduino.

There is an increasing need for sensing applications e.g., are motion detectors and ambient intelligence systems. These are used to exchange data with other devices such as tags, sensors, network nodes and routers. Working of these sensors and tags depends on the chips which communicate heterogeneously across various communication protocols, Chip design allows additional RF components (e.g., for Bluetooth, ZigBee, Wireless LAN and FM functionality) to be a part of the monolithic/single chip device. Monolithic chip can be defined as a type of integrated circuit that contains both active and passive devices such as transistors, microcontrollers and capacitors that are made on the single piece of silicon wafer. The 'Planar Technology' used in a single block allows to interconnect with the insulating layer over the same body of the semiconductor to produce a solid integral monolithic chip. If the devices are interconnected with dangling wires over the chip then it is not a monolithic chip but a hybrid chip.

Monolithic chips not only helps in communicating with the reader but allows to exchange data over the devices. The designs produces a cost-effective solution for industries looking to integrate sensors with communication devices such as mobile phones, notebooks, navigation systems etc. [13].

Capabilities in defence -The capabilities of the devices that are used in defence can be effective in the detection of mines in coastal regions, it can be used to localize modern diesel electric submarines operating littoral waters, identification and localization of mortars, artillery and small fire arms, the effective measurement of trace concentrations of explosives, toxic chemicals, and biological agents, the tracking of soldiers, the detection of snipers, and the management of parametric surveillance in sensitive areas. The IoT concepts have also been theoretically implemented. These can capture information from people, equipment, and materials in military environments by means of sensing devices (i.e., the sensing layer) and shares collected data among military objects, monitoring systems and control centers, through a communication infrastructure. The data from the sensing layer can be exploited for use in controlling and implementing intelligent military applications.

IoT aided robotics applications in military environments – IoT is system that can change any system when applied in a useful manner. It expands the robotic field applications in defence. To acquire information as possible in a broad and unknown environment, for detecting the presence of harmful chemicals and nuclear/biological weapons-smart objects can be deployed, also presence of humans can be done in any case, publicly as well as on the battlefields, the layout of the environment and geographical structure could be learnt. And similarly in industries it can be used for acquire data about chemical and physical phenomena [14].

Some relevant activities with the IoT aided robotics applications [15]-

- Autonomous and smart detection of harmful chemicals and biological weapons;
- Deactivation of nuclear weapons in unsecured environments;
- Control of land vehicles and aircrafts, without neither the presence, nor the coordination of humans;
- support civil operations and war actions;
- Access control and identification of illegitimate intrusions of people in restricted areas.

Devices made till date- Existing devices which are made by the use of IoT concepts but lag and are needed to be developed.

Daksh ROV -Daksh is an electrically powered Remotely Operated Vehicle (ROV) designed and developed by India's DRDO. It was primarily designed to recover improvised explosive devices that could locate, handle and destroy all type of hazardous objects. The ROV is based on a motorized pan-tilt platform. It can be remotely controlled from a range of 500m. The vehicles manipulator arm can handle hazardous objects of up to 20kg from 2.5m and 9kg from a 4m distance. Daksh can climb steps and negotiate steep slopes.

Fig. 3. Daksh ROV [16].

The solid rubber wheels of Daksh can withstand blast impacts. The vehicle can tow suspected platforms and operate continuously for three hours once fully charged [16].

Main drawbacks of Daksh – The main drawback that can be discussed is not autonomous and we the distance of controlling is very less (500metres). Thus there is a requirement of some devices that are automated as well as useful for surveillance.

Humming Bird Drone – A drone of the humming bird being invented in the field of defence, nothing like any other drones available. It was a small, low flying drone beating its wings like a bird [17].

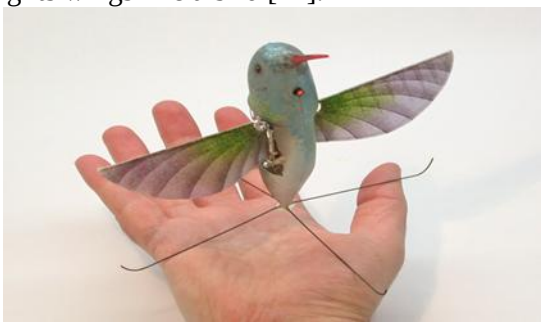

Fig. 4. HummingBird drone [17].

A tiny new unmanned air vehicle with flapping wings can hover, fly at high speed and negotiate indoor and outdoor environments while sending back video imagery, even though it weighs just nineteen grams. The Nano Humming bird can fly at 11 miles per hour (18km/h) and move in three axes of notion. The artificial bird can flap its wings for propulsion and altitude control. According to DARPA, the Nano Air Vehicle's configuration will provide the warfighter with unprecedented capability for urban mission operations. DARPA's development plans for the NAV include indoor navigation without GPS, automated collision avoidance and improved power and communication systems.
There are some drawbacks relating to the technical specifications. Pitch is done actively. Kinematic parameters variation more complex for increasing flight speed. Twisting phenomena along the axis is present.

Telemax explosive ordnance robot – One of the most advanced and versatile robot available in the market, when packed up small enough to fit in the back of a SUV but when opened can reach over 2.4m height. A four-track running gear has been used in Telemax, making it the first time in a vehicle of this size, which offers a good mobility compared to other forms of running gear. It can handle gradients of 45 degrees without any difficulty. It can also overcome obstacles of up to half a metre in height without problems and also trenched of 60cm in width [18].
India has been lacking behind in this field a lot, it has only applied counter IED technology and some basic operations. Autonomous operations of such devices in the tactical battle area are still a distant thought for the country.
In order to test the use of robots in tactical battle area, French and German troops conducted an experiment last year. It demonstrated advanced war fighting concepts introduced by modern command and control systems and evaluate the effectiveness of digitization in combat area. The forces operating in the experiment included a command centre, some armoured vehicles, robots, drones and a group of soldiers. The experiment was organized by the French procurement agency DGA and industry group that comprised French majors such as Thales, Nexter and Sagem. Mini robots such as Cobham's Telemax and MiniRoc (developed by French companies) performed important roles such as observation, localization, surveillance, load carrying, and sentry operations. The robots were also tested for autonomous operations in a battle situation [18].

B. Stage 2-

This stage mainly includes communication importance and mostly used protocol. And talking about defence we require connectivity all the time with intelligent and automated machines, personnel altogether. Therefore, we give a good detailing idea about adaptive communication technologies and IEEE standards for communication which will benefit us in the architecture of defence.

Here, embedment of enhanced connectivity to platforms through advanced communication systems that enables the existing systems to talk with each other seamlessly. The communication model aims at defining the main communication paradigms for connection entities, as defined in the domain model. Providing a reference communication stack, together with insight about the main interactions among the actors in the domain model.

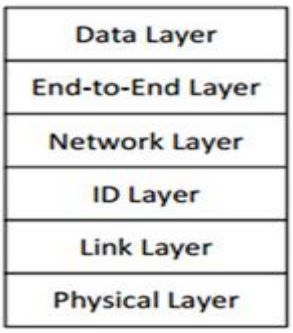

Figure 3: The communication stack.

We developed a communication stack similar to the ISO OSI 7-layer model for networks, mapping the needed features of the domain model unto communication paradigms. We also describe how communication schemes can be applied to different types of networks in IoT [19].

There are several standards which are made by IEEE that we should follow in different cases [20].

IEEE 1451: The IEEE 1451, a family of Smart Transducer Interface Standards, describes a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.

IEEE 1888.3-2013 - "IEEE Standard for Ubiquitous Green Community Control Network: Security"

IEEE 1905.1-2013 - "IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies"

IEEE 802.16p-2012 - "IEEE Standard for Air Interface for Broadband Wireless Access Systems"

IEEE 1377-2012 - "IEEE Standard for Utility Industry Metering Communication Protocol Application Layer"

IEEE P1828 - "Standard for Systems with Virtual Components"

IEEE P1856 - "Standard Framework for Prognostics and Health Management of Electronic Systems"

Various communication Protocols are [20] –

Wireless Hart-"Wireless HART technology provides a robust wireless protocol for the full range of process measurement, control, and asset management applications."

Digi Mesh-"Digi Mesh is a proprietary peer-to-peer networking topology for use in wireless end-point connectivity solutions."

ISA100.11a - "ISA100.11a is a wireless networking technology standard developed by the International Society of Automation (ISA). The official description is "Wireless Systems for Industrial Automation: Process Control and Related Application"

IEEE 802.15.4- IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs). It is maintained by the IEEE 802.15 working group. It is the basis for the ZigBee, ISA100.11a, Wireless Hart, and MI-WI specifications, each of which further extends the standard by developing the upper layers which are not defined in IEEE 802.15.4. Alternatively, it can be used with 6LoWPAN and standard Internet protocols to build a wireless embedded Internet.

NFC - Based on the standard ISO/IEC 18092:2004, using inductive coupled devices at a center frequency of13.56 MHz The data rate is up to 424 kbps and the ranges with a few meters short compared to the wireless sensor networks.

ANT - ANT is a proprietary wireless sensor network technology featuring a wireless communications protocol stack that enables semiconductor radios operating in the 2.4 GHz Industrial, Scientific and Medical allocation of the RF spectrum ("ISM band") to communicate by establishing standard rules for co-existence, data representation, signaling, authentication and error detection.

Also there are other protocols like Bluetooth that are the most commonly used commercially and domestically. ZigBee is another protocol. Both Bluetooth and ZigBee operate on 2.4GHz frequency but ZigBee can use a 128 bit AES encryption. Also there are protocols as EnOcean, Dash7, Thread, WiMAX based on wireless technologies And GPRS, 2G/3G/4G based on cellular technologies.

The vision for the Internet of Things (IoT) demands that material objects acquire communications and computation capabilities and become able to automatically identify themselves through standard protocols and open systems, using the Internet as their foundation. Yet, several challenges still must be addressed for this vision to become reality. A core ingredient in such development is the ability of heterogeneous devices to communicate adaptively so as to make the best of limited spectrum availability and cope with competition which is inevitable as more and more objects connect to the system. Here is an overview of current developments in this area, placing emphasis on wireless sensor networks that can provide IoT capabilities for material objects and techniques that can be used in the context of systems employing low-power versions of the Internet Protocol (IP) stack.

The evolutionary paradigm of the IoT exhibits several distinct characteristics. First, it relies upon wireless as its main mode of communication. Indeed, the vast majority of things in the IoT interconnect with each other and

access the Internet infrastructure and services through the use of low-power wireless which is critical for their operation. Second, communication devices participating in the IoT systems are clustered in geographically proximal groups. Specifically, things typically concentrate at specific locations, for example where end-users reside or work, such as intelligent house or smart office environments. Third, the IoT systems are highly heterogeneous. IoT incorporates a wide variety of intelligent devices such as WSNs, embedded devices, and smartphones.

With constantly evolving technologies, the range of object types is likely to keep widening. Finally, instead of demanding explicit or manual intervention to make responses, IoT objects are able to react autonomously to stimuli, including environment events or user instructions. In this paper, we surveyed a multitude of techniques that can be incorporated to achieve adaptive communications in order to meet the challenges of the Internet of Things (IoT) that can be applied perfectly in the field of defence. 6LoWPAN enables the seamless integration of various intelligent artifacts and the existing Internet at a connectivity level, the service abstraction and context awareness provided by IoT middleware facilitate the interoperation from a user-oriented angle. The delay- and disruption-tolerant overlay at the application layer is also reviewed. Such technology is particularly important in case of highly unstable connectivity and distant transmissions [21].

A cross-layer ideology is either implicitly or explicitly employed, as the stringent distinction between layers has already lagged behind the advanced requirement of IoT. Such a trend is inevitable for designing adaptive communications for IoT and more forthcoming studies in this area are anticipated. The challenge of interoperability in IoT is addressed at both the network and application layers. Whilst 6LoWPAN enables the seamless integration of various intelligent artifacts and the existing Internet at a connectivity level, the service abstraction and context awareness provided by IoT middleware facilitate the interoperation from a user-oriented angle. The delay- and disruption-tolerant overlay at the application layer is also reviewed. Such technology is particularly important in case of highly unstable connectivity and distant transmissions. Thus, describing communication system which can be very useful in the defence system. Here communication can be done over long distances without any instability.

C. Stage-3-

Application programming interfaces (APIs) are in effect in the key enablers of the multi-screen internet age we now find ourselves in. As more devices get web-connected, everything from street lights to cars and a variety of ambient sensors in our homes, on our bodies and on the street will come with APIs [22].

At the application level, the key aspect will be the ability of the software tools to provide the right formatted information, with right time to the right person. This indicates the need for allowing end-user needs to drive the technology side of IoT. Storage and processing should be happening at different levels and their dissemination should be prioritized. The centralized storage and processing of data will provide accessible historical record for non-mission functions while decentralized real-time processing and relay will provide the data for situational awareness for mission functions at the tactical level.

Since the sensing and transmission segments of data flow are pretty much covered, the emphasis, in my view, has to be on processing and serving of data. The data-processing side of IoT will take place as it is those software-based systems that will be analyzing the data and providing them in useful formats. This comes down to high performance computing services which will handle large volumes of data to provide the necessary 'Big-Picture' trends that military managements can base their decisions on [23].

IoT has the potential for new openings across vertical markets such as insurance, consumer electronics, medical, transportation to develop use cases which can control this technology to reduce costs, increase customer approval, and create new business models based on the analysis of the data collected. Microsoft Stream Insight is a powerful platform for developing and deploying highly scalable and low potential CEP applications. It is designed to provide event-driven processing solution to continuously arriving data without writing the data to disk for analysis and querying. With Stream Insight, IoT applications can provide better and faster CEP solutions to incoming data in near-real time, as the data gets acquired from the sources as compared to the analytics solutions based on the traditional database reports and dashboards.

A typical IoT application will be allied to a huge number of devices that will endlessly provide it with the input data in the form of events. Traditional relational database centric application progress models may not be sufficient for building such uses and they can use “Complex Event Processing (CEP)” technology instead. The application will need to capture the events, study the data to come up with insights and patterns. IoT applications by nature will be not only complex but also critical, because the insight provided by its out output will be often triggering some other event of decision making. Due to these reasons an enterprise will need to come up with a robust, scalable and proven CEP and analytics platform, which can leverage this online data for providing advanced CEP solution for various benefits such as business insight, better decision making and cost reduction etc.

Dashboard - Dashboard application will be answerable for showing the data and alerts generated by the CEP.

The dashboard has the capabilities to plot the data in the chart format and displaying alerts in near real time.

D. Stage 4-

There are various security needs which are to be made in concern for the defence industry. The seizure of data links and unauthorized access will be covered by the IoT system. This technologies have to be carefully optimized and ruggedized for their compatibility with defence functions.

Defence in depth and breath- The IoT threatens the pattern which was long pursued by traditional IT security arena for 'Defence in depth'. It determines a tactic to defend a system from any particular attack using several independent methods. There are many new addition that can be made to the IoT system of defence in order to manage connections and protocols, all being potential intrusion points. Here, we can consider the unique challenges of IoT and synchronizing of different tools which are to needed to strategically address them [25].

In areas of network protocol security, Internet Protocol Version 6 (IPv6) is the next generation protocol for the Internet; it contains addressing and security control information, i.e., IPSec to route packets through the Internet. In IPv4, IPSec is optional and connecting computers (peers) do not necessarily support IPsec. With IPv6, IPSec support is integrated into the protocol design and connections can be secured when communicating with other IPv6 devices. IPSec provides data confidentiality, data integrity and data authentication at the network layer, and offers various security services at the IP layer and above. These security services are, for example, access control, connectionless integrity, data origin authentication, guard against replays (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality [26].

With the IOT-distributed nature of rooted devices in public areas, threats coming from networks trying to spoof data access, collection and privacy controls to allow the distribution of real-time information, IOT security has to be implemented on a strong foundation built on a holistic view of security for all IOT elements at various interacting layers. With the gradual popularization of the Internet of things in people's lives, security of IoT is facing more and more challenges. Traditional cryptographic algorithms cannot reach the inconsequential, lack of mutual authentication between user and nodes, not suit to the open environment of IoT. An efficient ECC-based authentication and the attribute-based access control policy were proposed in order to attain mutual authentication between user and nodes and fine-grained access control. Mutual authentication ensures the security of the communication between user and nodes, whose process is simple to solve the resource-constrained problem of the IoT perception layer. Accessing the data on the basis of user attribute certificate in access control authority can achieve flexible fine-grained access control [27].

E. Stage 5-

The end part of a system can be discussed us management of all the devices and responsibility for privacy and security issues. In case of defence, the government controls all the management issues. As, it is responsible for asset management and privacy of data which is most concerned, lastly it effects the reputation and integration of the company or country working on the process.

Data management is the ability to manage data information flow. With data management in the management service layer, information can be accessed, integrated and controlled. Higher layer applications can be shielded from the need to process unnecessary data and reduce the risk of privacy disclosure of the data source. Data filtering techniques such as data anonymisation, data integration and data synchronization, are used to hide the details of the information while providing only essential information that is usable for the relevant applications. With the use of data abstraction, information can be extracted to provide a common business view of data to gain greater agility and reuse across domains [29].

V. APPLICATIONS OF IOT

The major objectives for IoT are the formation of smart environment and things which are self awared (like, smart transport, smart cities, buildings, rural areas, energy, health, living, etc.) for climate, food, energy, mobility, digital society and health application", as in following figure:

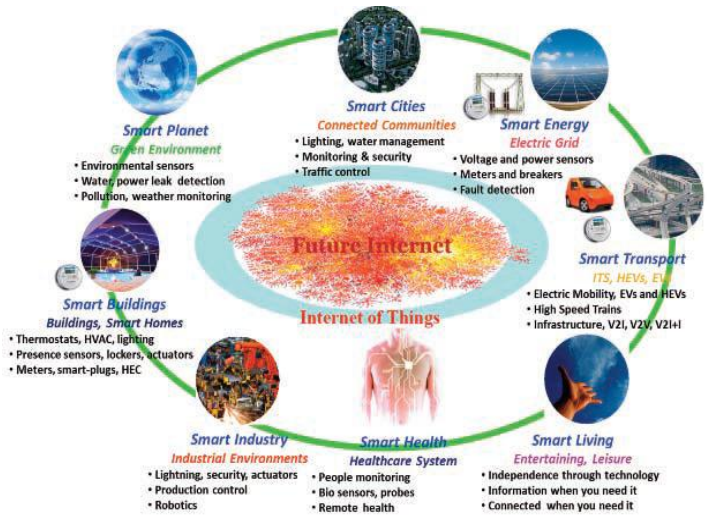

Fig. 6. Application overview for IoT [1].

There was a survey done on IoT-I project ran during 2010 and conclude 65 application scenarios were identified, grouped in 14 domains and some important domains are: Transportation, Smart Home, Smart City, Lifestyle, Retail, Agriculture, Smart Factory, Supply chain, Emergency, Health care, User interaction, Culture and tourism, Environment and Energy. That analysis was completed on 270 responses from 31 countries and

scenarios inviting the most interest were: smart home, smart city, transportation and health care [29].

Smart cities: Smart parking, structural health, noise urban maps, traffic congestion, smart lightening, waste management, intelligent transportation system, etc. comes under smart city application layer.

Smart Environment: Forest fire detection, air pollution, landslide and avalanche prevention, earthquake early detection etc. are part of smart environment.

Smart health (e-health): Fall detection, medical fridges, sportsman care, patients surveillance, ultraviolet radiation control.

Industrial control: M2M application, indoor air quality, temperature monitoring, ozone presence, indoor location, vehicle auto diagnosis

Smart water: water quality, water leakages, river flood control etc.

Smart metering: Smart grid, tank level, photovoltaic installations, water flow, silos stock calculation etc.

Security and emergencies: perimeter access control, liquid presence, radiation levels, explosive and hazardous gases etc.

Retails: supply chain control, NFC payment, intelligent sopping application, smart product management etc.

Logistics: quality of shipment conditions, item location, storage incompatibility detection, fleet tracking etc.

Smart agriculture: wine quality enhancing, green houses, golf courses, meteorological station network, compost etc.

Smart animal farming: offspring care, animal tracking, toxic gas levels etc.

Domestic and home automation: energy and water use, remote control appliances, intrusion detection system, art and goods preservation etc. [30]

VI. RESEARCH CHALLENGES FOR IOT

Application design: Design of open APIs on all levels of the IoT ecosystem.

Standardization -Design of standardized formats for description of data generated by IoT devices to allow mashups of data coming from different domains and/or providers [1].

Silo IoT solution: There is problem in today's IoT domain is that we are available with variety of solution targeted at specific application domain. These application developments have limited interoperability between systems and technologies, and they do not adopt a common standardization and understanding of the IOT domain [13].

Cost versus Usability: IOT uses technology to connect physical objects to the Internet. For IOT adoption to grow, the cost of components that are needed to support capabilities such as sensing, tracking and control mechanisms need to be relatively inexpensive in the coming years.

Privacy and Security: As the adoption of IOT becomes pervasive, data that is captured and stored becomes huge. One of the main concerns that the IOT has to address is privacy. The most important challenge in convincing users to adopt emerging technologies is the protection of data and privacy. Concerns over privacy and data protection are widespread, particularly as sensors and smart tags can track user movements, habits and ongoing preferences. Invisible and constant data exchange between things and people, and between things and other things, will take place, unknown to the owners and originators of such data. IOT implementations would need to decide who controls the data and for how long. The fact that in the IOT, a lot of data flows autonomously and without human knowledge makes it very important to have authorisation protocols in place to avoid the misuse of data [31].

Interoperability: Different industries today use different standards to support their applications. With numerous sources of data and heterogeneous devices, the use of standard interfaces between these diverse entities becomes important. This is especially so for applications that supports cross organizational and various system boundaries. For example in the Logistics sector, the supply chains involve multiple stakeholders like retailers, manufacturers, logistics, the IOT systems need to handle high degree of interoperability in order for information to be processed down the value chain [31].

Network Capacity Constraints: With convergences brought about by connected machines and smart mobile devices, there is an increasing demand for network infrastructure to support these data "hungry" 39 devices with a certain level of expected QoS. New mobile applications that perform contextual-aware services may require frequent bursts of small blocks of data for updating and synchronizing. These sessions will typically occur in "rapid-fire" bursts for a few seconds or minutes with size of the payload in few kilobytes. The rapidity of these sessions will have an impact on the latency and bandwidth of the network. [3].

Ethical question against IoT: The digital society raises questions not just technological or political – but philosophical, social, legal, ethical and psychological. The ethical implications of tomorrow's internet are complex, and require broad public debate, with an active role of all stakeholders including public policy makers, business and civil society. While ICT offers opportunities like a platform for freedom of speech, social contact and enhanced democratic accountability, there are also ethical problems online: for example important questions like privacy and data protection. As ICT becomes ever more important, pervasive and useful, we need to raise and discuss these ethical questions [1].

VII. CONCLUSION

Thus we conclude that IoT is the most concerned topic in today's world. The most developed and developing countries are moving rapidly in this field. So why do we not use this concept in the defence industry and make a powerful and secure defence industry. Many countries defence organization have taken their steps towards the development but Indian defence is still lagging behind the technology. So we require to do some research showing some interesting innovations in the field and improve the architecture of defence. We with the help of experts in the government and industries have to find the answer to the following questions: What are Air Force, Navy, Army, and DHS plans and strategies for creating the IoT-driven enterprise? What are the architectural challenges and emerging solutions? What are the security and privacy concerns? What role will IPv6 addressing, mobility, and ad hoc services play? [31] Large-scale data and predictive analytics? How do we create the intelligent, programmable network to exploit emerging IoT capabilities? We have to determine the direction of IoT, M2M and battlefield connectivity for future military and national security operations. We need to analyse and decide about DoD and DHS plans for embedding IoT throughout the defence and national security enterprises.

Acknowledgment

We have completed our paper on **Internet of Things** under the guidance of Mr. Sonit Sukhraj and a supporter Mr. Chirag Sehgal, So We are very thankful to them for helping me to complete the paper.

References

[1] Ian G Smith, Ovidiu Vermesan, Peter Friess and Anthony Furness, "The Internet of Things 2012 *New Horizons*", IERC - Internet of Things European Research Cluster 3rd edition of the Cluster Book, pp:5-8.
[2] Internet of Things – Strategic Research Roadmap by Cluster of European Research Projects on the Internet of Things (CERP-IoT) developed in 2009 its Strategic Research Agenda (SRA)
[3] https://www.ida.gov.sg/~/media/Files/Infocomm%20 Land scape/Technology/TechnologyRoadmap/InternetOfThings.pdf.
[4] Ian Smith, Professor. Dr. Ken Sakamura, Ricky Ma, Yong-Woon Kim, "CASAGRAS, an EU framework 7 project", pp:29-45.
[5] Sridhar Iyer, IIT Bombay RFID: Technology and Applications, 2005.
[6] Dr. Bheemarjuna Reddy Tamma, IIT Hyderabad, "CPS: Communications".
[7] Krishnan V, Bhaswar Sanyal, "M2M Technology: Challenges and Opportunities" by techMahindra.
[8] Fiche d' information, Factsheet, " Introduction to Cloud Computing".
[9] Dimitris Tsaimos (CSE), Norbert Vicari (Siemens), Werner Liekens (ALU BE), Alexis Olivereau (CEA), Andreas Nettsträter (FHG IML), Michele Rossi (CFR), Pierpaolo Giacomin (HEU)," Project Deliverable D3.1 - Initial M2M API Analysis".
[10] http://postscapes.com/internet-of-things-protocols
[11] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions".
[12] http://defense.ge-ip.com/news/the-military-internet-of-things/n3099
[13] https://www.google.co.in/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=communication% 20protocol%20and%20methods%20for%20internet%20of%20 things
[14] M. A. Hussain, P. Khan, K. K. Sup, Wsn research activities for military application, in: 11th IEEE International Conference on Advanced Communication
Technology, 2009, pp. 271-274.
[15] L.A.Grieco, A.Rizzo, S.Colucci, S.Sicari, G.Piro, D.Di Paola, G.Boggia, "IoT-aided robotics applications: technological implications, target domains and open issues".
[16] http://www.army-technology.com/projects/remotely-operated-vehicle-rov-daksh/
[17] http://www.pbs.org/wgbh/nova/tech/hummingbird-drone.html
[18] http://www.forceindia.net/EraofMachines.aspx
[19] http://in.linkedin.com/title/defence/in-in-6891-Chennai-Area,-India/
[20] http://www.hindawi.com/journals/ijdsn/2014/158252/
[21] Peng Du, and George Roussos, "Adaptive Communication Techniques for the Internet of Things".
[22] Dimitris Tsaimos (CSE), Norbert Vicari (Siemens), Werner Liekens (ALU BE), Alexis Olivereau (CEA), Andreas Nettsträter (FHG IML), Michele Rossi (CFR), Pierpaolo Giacomin (HEU)," Project Deliverable D3.1 - Initial M2M API Analysis" p: 23-25.
[23] http://www.cio.com/article/2843814/developer/how-to-develop-applications-for-the-internet-of-things.html
[24] Building Intelligent Internet of Things Applications using Microsoft Streamlnsight, April 2014 by IGATE Global Soloution, p: 6-7.
[25] http://www.infosecurity-magazine.com/news/cisco-issues-300000-internet-of/
[26] Ning YE, Yan Zhu, Ru-chuan WANG, Reza Malekian, and Lin Qiao-min, "An Efficient Authentication and Access Control Schemefor Perception Layer of Internet of Things".
[27] https://www.ida.gov.sg/~/media/Files/Infocomm%20 Landscape/Technology/TechnologyRoadmap/InternetOfThing s.pdf., pp:15-16.
[28] http://www.libelium.com/top_50_iot_sensor_applica tions_ranking/
[29] Building Intelligent Internet of Things Applications using Microsoft Streamlnsight, April 2014 by IGATE Global Soloution, pp:4-5.
[30] https://www.ida.gov.sg/~/media/Files/Infocomm%20 Landscape/Technology/TechnologyRoadmap/InternetOfThing s.pdf., pp:38-40.
[31] http://www.defenseinternetofthings.com/