# THE INTERNET OF THINGS IN DEFENCE APPLICATIONS

**Lakshmi, Defence Electronics Research Laboratory**
**DRDO, Hyderabad – 500005 , laksh_sambhavi@yahoo.com**
**(IETE Life Time M**
**embership No.: F-143017)**

**Abstract**

**Military commanders have always lived and died by information both in quality and quantity. *IOT* brings with its organizational and security challenges that present both opportunity and obstacle .**

## I. INTRODUCTION

The Internet of Things became possible because of four factors, first the rise of RF and communication technologies, secondly the miniaturizations of Chips because of developments in microelectronics and nano technologies, thirdly the data handing, storage and capacity of computational devices and fourth the advances in software and firmware. The Internet of Things (*IOT*) in Defence is a model based on "network-centric warfare". Networked forces generate improved information, information sharing and collaboration , better situational awareness , shared situational awareness, situation adaptive responses, self synchronization put together to increase mission effectiveness. It provides networking to connect peoples, things, applications and data through internet. It is Remotely controlled, managed and interactive integrated service with unique RFIDs devices . It is estimated that 70 billion connected devices will be connected by the year 2025 using *IOT* technologies. Overall, *IOT* would allow the automation of everything in society around us. Research on *IOT* has important economic and social value for the development of the next generation of information, network, and communication technologies. Military is hunger for technology and tools that provide processing information and improve communication. *IOT* connects disparate objects into lager networks.

## II. IOT IN DEFENCE

The *IOT* related technologies in the defence has primarily focused on human performance, medical facilities, Logistics supplies and maintenance , Tracking of unmanned systems, different platform sensors and actuators , applications for Command, Control,

Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and fire-control systems . *IOT* is an ecosystem of many technologies that generates, shares, analyzes, and creates value from enormous big data which is gathered from trillions of sensors connected through an vast and extensive network infrastructure of communication and connectivity. In the prospective of Defence , Security vulnerabilities can allow adversaries to take control of or disable automated systems, preventing Units and platoons from carrying out their mission or even using our own assets against us. The valuable data can be potentially manipulated or altered to deliver a misleading picture of the tactical landscape to concerned authorities.

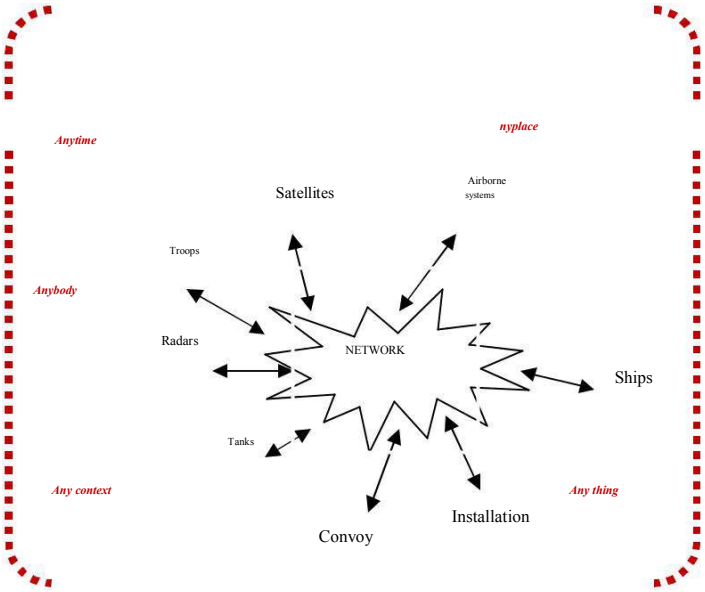


Figure 1

The security of data is of paramount importance which can limit the ability to communicate across systems . This can also limit the generation of scale or synchronization from different types of collected data. This increase in data forces upgrade of system network integration and increase the bandwidth , performance of intelligent data filtering and throttling by edge devices.

As shown in Figure 1. *IOT* is a big Dynamically configured network of networks, network on demand which can integrate various Troops, Tanks, Installations, Convoy on move, Radars Ships, Satellites etc and it can be used at anyplace, anywhere, by anybody at anytime with anycontext .Military network takes sufficient time to build up because of limited storage and wireless connectivity.

*A*pplication of *IOT* technologies to Net-centric warfare described even before the concept of *IOT* was introduced in the military missions. Embedded devices like FPGAs in combination of Internet connectivity, RF technology and software driven data analysis forms the modern concept of *IOT*.

*IOT* represents the convergence of interdisciplinary fields of:

- Wireless Sensing Technologies
- RFID technologies
- Networking
- Embedded Hardware
- Radio Spectrum
- Nano technologies
- Mobile Computing
- Communication Technologies
- Software Architectures
- Energy Efficiency
- Information Management
- Data Analysis
- Data integrity and securities

*IOT* is the integration of three domains:

1. The physical domain, where events takes place and operations are conducted, generating data from sensors and human observers
2. The information domain, in which data is transmitted and stored
3. The cognitive domain, in which the data is processed and analyzed for opaqueness of decision making.

In the physical domain all the devices are connected and they promise revolutionize modern warfare by leveraging data and automation to deliver greater lethality and survivability to the war fighters while reducing ost and increasing efficiency. For Securities , Surveillance , alarms, Real time objects and people tracking, *IOT* plays an important part. In Transportation , Fleet management, Road safety, real time Convoy monitoring. For Supplies to fleet and units, its distribution and monitoring *IOT* is very handy. Automation in building and campus can also help reduce personnel costs. This translates into a greater ability to deny and defeat enemies, and to protect troops.

In information domain, *IOT* is also revolutionizing the defence airborne systems. The modern aircraft engines are capable of producing several terabytes of data per flight with variety of sensors on board. In Combination with other in-flight data, the

information can improve engine performance. It manages the maintenance and reduce fuel costs, shorten travel times and increase efficiency. Military aircraft and logistics systems are highly connected support systems which enhances mission reliability and security both for life and resources. Integration of software and hardware security features to create a platform that endures over the lifetime of the development with a wide range of software builds.

In cognitive domain the data collected by *IOT* devices, facilitate more complex data analysis and real time faster reactions by reducing human error, delivering more precise and efficient capabilities. The raw data is collected with sensors and actuators devices, these data is unstructured . These are also collected from human intelligent (HUMINT) and user experts. This is stored in huge data repository, the relevant data with human intention is translated into data which is understood by computers. The situation is understood then the decision will be taken by the authorities for engaging the resources to act with the known information. This data is also displayed and disseminated in the form which is understood by the humans.

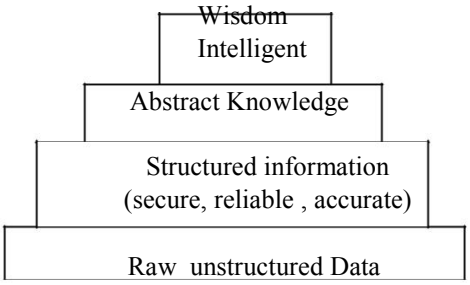


Figure 2

As shown in figure 2 , the data is stored is represented by inverted triangle . Advance situational awareness allows military commanders to make decisions based on real time analysis generated by integrating information from manned and unmanned sensors, cameras mounted on ground and on soldiers themselves.

## III. CONCLUSION

I. At present the defence does not have sufficient network connectivity, particularly on the battlefield, to support broader *IOT* deployment. 85 % of devices are not yet connected.

II. Data analytics, process capacity, and lack of interoperability are additional limiting factors, 4 out of 5 data is unstructured.

III. Most *IOT* technology devices transmits and receives on radio frequencies which makes them susceptible for getting detected by adversaries radars. Direction finding and location fixing devices from transmitters can compromise the location of soldiers or vehicles hence *IOT* implementation makes systems vulnerable to electronic warfare. RF jammers can be deployed by adversaries to block signals communication with parent units.

IV. Despite the challenges of adopting *IOT* for the defence, Technology can help the defence adapt to a modern world in which adversaries are more sophisticated .

V. Real-time information management and accurate tracking can be achieved by better network of networks.

VI. The complexity and high cost of defence system remain in service for many year. Which pose challenge in upgrade and enhancing their capability for new *IOT* technologies.

VII. With *IOT* systems defence can reap the benefits of transforming its system in next generation high value network enable solution by affordable *IOT* for defence.

VIII. Needs to have combat cloud to integrate military *IOT* systems.

About Author

Lakshmi was born in Kanpur (UP ) did her BSc. from Kanpur University , B Tech (ECE ) from North Eastern Hill University ( NEHU ) and pursuing MS (ECE) from JNTU, Hyderabad . She joined ( DLRL, DRDO, Hyderabad ) in Data Communication Group in 1998. She has designed and developed communication systems for Voice and Data Communication and tested various module. At present she is working as Scientist – F. Her field of Interest are Communication , Networking and Satellite Communication . Her research experienced is 20 years in Design & Developement of state of art communication systems for Electronics Warefare (EW ) , At present she is Head of 'SIGNALS' division of DLRL and provids 24X7 Communication networks of telephones in Campus. She authored papers for International and National Conferences . She has given several Invited Talks in Various Institute.