

A Systematic Review of The Internet of Things; Use for New Era of Defense Strategies in Military

Muhammad Kashif¹, Muhammad Sheraz Arshad Malik², Muhammad Umair³ Prince Waqas Khan⁴
Sheikh Muhammad Amir⁵

¹Department of Information technology, GC University, Faisalabad, Pakistan

²Department of Information technology, GC University, Faisalabad, Pakistan

³Department of Computer Science, Chongqing University of Posts and Telecommunications, Chongqing, China

⁴Department of Information technology, GC University, Faisalabad, Pakistan

Abstract

In modern days, the role of Internet of Things (IoT) is very important in many fields of life. Every developed and developing country has an army for their defense. In this era every country is trying to transform their military's weapons into advanced technology for quick defense response of every imaginable situation. IoT has an advanced technology in this era many countries are using this technology in different sectors of military which is very useful for quick and reliable response against any threat of defense. In this paper we will explain the architecture and technologies of IoTs. IoT's improvement in military, internet of things military's applications, how to transform the conventional system of defense into advanced technologies (IoT) through different techniques, and challenges for implementing the IoT and battlefield connectivity for future military operations.

Keywords

IoT; Internet of things; Military applications; defense.

1. INTRODUCTION

The term Internet of Things (IoT) has been authored moderately as of late however has profound roots in numerous different regions of research including digital physical system, inescapable and pervasive figuring, inserted frameworks, portable specially appointed systems, remote sensor systems, cell systems, wearable registering, distributed computing, enormous information investigation, and in addition astute operators. Moreover, late advances in scaling down, Radio Frequency Identification (RFID), low power processing, and vehicle to vehicle communication have additionally filled the development of IoT and the business and modern divisions have officially committed impressive regard for the field. As a to a great extent business innovation, advancements in IoT originate from and advantage the military's areas under the more extensive topical zones of digital physical system and implanted registering [1]. In any case, the effect of advances in business IoT will progressively have impact on the military due to the military's association with business and mechanical accomplices and procedures.

We expect that the far reaching selection of IoT will fundamentally affect the military in less than four key zones:

- 1) new detecting and calculation stages with combination in military procedures;
- 2) progresses in fundamental IoT empowering influences;
- 3) convention changes identified with IoT accessibility and capacities. To start with, given the market drivers of rivalry and economies of scale, current business IoT offers economical and strong stages that could be utilized to supplement and broaden the detecting and calculation abilities given by military level hardware. In this way, we hope to see co deployment and conjunction of business IoT advances adjoining conventional military advances [2].

Second, we expect the hidden empowering agents for IoT (e.g., scaling down, sensors, vitality productivity, and so forth.) to be utilized for conventional military gear. A huge number of stages, going from boats to air ship to ground vehicles to robots to weapon frameworks, will be affected by IoT advances. Further, as IoT advancements turn out to be more omnipresent, the quantity of associated "things" could develop to incorporate therapeutic supplies, sustenance, water, ammo, and different consumables and segments. The effect will be noteworthy, from all the more in the nick of time upkeep to diminished downtime to enhancements in the coordination and production network forms.

At the end, we expect that the ideas that underlie IoT will in a general sense change the teaching and the Techniques, Tactics, and Procedures (TTPs) without bounds military war zone, which will be a highly connected operating environment, with ad-hoc and large-scale deployments of capillary and high compactness personal and environmental sensors systems. The possibility of everything in the combat zone being an arranged substance, paying little mind to how little or vast, essentially builds the potential for enhanced circumstance mindfulness at numerous levels.

Similarly, as the approach of correspondences systems introduced the time of Network-Centric Warfare, we anticipate that IoT will introduce another time of IoT-

Enabled Operations, with the development of inventive and advanced digital physical applications. Particular applications will definitely incorporate biometric officer observing, signal upgraded interchanges, shared and swarm detecting, savvy data provisioning through enlarged reality, and coordination and inventory network mechanization.

2. IoT ARCHITECTURE

A. Sensors

Sensors are all over the place, sensors sense information from climate or any specific area. e.g. light sensor (LDR) detects the light and send them output to circuit. The circuit give the output against any specific task. The (LDR) Light dependent resistor is mostly use for automated light functionality in different sectors of life. If this kinds of devices attached through IoT technologies, then our system is more reliable and user friendly for all stakeholders. And also they will give the information of data from any positions, Conditions, appliances, and other things.”.

B. Internet of things (IoT) framework gateway

It is a gateway to internet for every one of the gadgets that we need to communicate with. Gateways go about as per transporter among the inner system of device hubs with the outside Internets. They do this by gathering the information from device hubs and communicating it to the web foundation. Please do not revise any of the current designations.

C. Cloud

The IoT servers have distinctive purposes, similar to organization, observing, information social affair and examination. They are totally particular, in light of open-source undertaking stages that give the capacities that are required for the server-side of the IoT design, to associate with gadgets. The information that is transmitted through the server door is prepared and put away safely utilizing huge information examination. This information is then utilized when performing savvy activities on our gadgets, generally, making them 'shrewd.' Reliability is another part of IoT servers, being incomprehensibly more solid than conventional servers because of the sheer accessibility of servers. In the event that and when there are issues with one server, the assets will naturally be moved to another server which will replace the failing one. Servers like the WSO2 IoT server work as a total arrangement, empowering gadget producers and ventures to oversee gadgets, manufacture applications, secure their information and gadgets, oversee occasions and envision sensor information scalable. These servers additionally offer venture portability administration arrangements which address the difficulties looked by undertakings today in the versatile figuring situation.

D. Mobile/User Applications:

Mobile applications or user applications are used for monitoring and controlling the IoT system by sending and receiving commands. User sends the command to specific device the command is stored/transmitted via cloud and gateway to any sensors. The sensors send the output to users according to the conditions. In these applications we can set the automatic functionality for any motion, temperature, and pressure sensors. For example, a metal detector robot working with ZigBee (device which is mostly use for IoT system in projects) the robot is controlled through mobile application. The admin sends the instructions to robot via mobile application forward, back, left, and right, the receiver follows the instructions and performed the task. The connected sensors with robot give the output through this system on admin's mobile application.

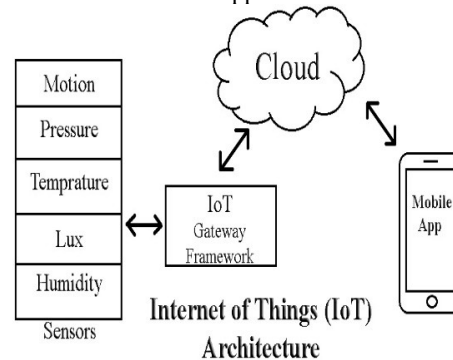


Figure 1: IoT Architecture

3. TECHNOLOGIES

E. RFID Technology and Internet of Things

Another advancement in IoT system with help of RFID (radio frequency identification). It is primary mechanical acknowledgment of Internet of things. It is used for different sectors of life. The RFID innovation is utilized to track and screen products wherever we required and fundamentally in coordination and store network segment [3]. Furthermore, its ranges from 125 kHz up to 5.8 GHz and RFID tags have no less than three fundamental parts.

The integrated circuit (IC) collects and monitors the all information about any input and output of products to which is important for output the data transfer without any guided media to person who reads through air. The transmitter device responsible for transmit the information in form of signals to sender and receiver. The bundling covers chip and transmitter, and enables the appending of the tag to a question for ID. There are a few other innovation technologies to track and recognize questions, for example, one dimensional bar (ID), it has a critical commitment to the production network and different organizations, for example, resource

administration and furthermore in different fields, for example, defense and ventures. Two dimensional (2D) standardized tags have given a more extravagant wellspring of information in any case, once printed, are not up-datable. In any case, interestingly with other innovation RFID has its exceptional capacity to ADC (automated data collection) procedures gather process information in its condition, is demonstrating as the present and additionally likely future innovation for the distinguishing proof of products. There is a different industry yet fundamentally coordination has looking RFID as labeling answers for enhance their following and checking forms. The bundling covers chip and radio wire, and enables the connecting of the tag to a question for distinguishing proof [4]. There are a few other innovations to track and identify questions, for example, one dimensional bar (ID), it has a critical commitment to the store network and different organizations, for example, resource administration and furthermore in different fields, protection and businesses. 2D standardized tags have given a more extravagant wellspring of information in any case, once printed, are not up-datable. In any case, interestingly with other innovation RFID has its extraordinary capacity to ADC procedures gather process information in its condition, is demonstrating as the present and in addition likely future innovation for the recognizable proof of merchandise. There is different industry however essentially coordination has looking RFID as labeling answers for enhance their following and observing procedures. There is different application conceivable with conceivable with RFID, for example, remote home computerization and constant vehicle following. And furthermore in future time it can possibly give computerized information gathered plan that have data framework with ongoing, thing particular information and the vital thing is that they are adaptable to put in greatly little space and area, i.e., relation between coil and circuit in chip innovation. There is different application conceivable with RFID, for example, remote home computerization and constant vehicle following. And furthermore in future time it can possibly give computerized information gathered plan that have data framework with ongoing, thing particular information and the vital thing is that they are adaptable to put in greatly little space and area, i.e., relation between coil and circuit in chip innovation

F. IPV6 (Internet Protocol version 6):

The IPv6 is new addressing system for internet services and devices. It needs for assigning the more internet addresses to consumers which rate is gradually increase day by day on graph of internet users in the world. The second name of this new addressing system is Internet protocol next generation. The Internet Engineering Task Force has studied this latest version to replace the IPv4 in IETF standard committees for giving the more addresses to billions of connected devices on internet in future. IoT devices have also the combination of equipment's which are connected to the internet for output against any input by user. That's why the IPv6 is very useful and important for IoT devices for better results in any field of life [5]. The benefits of IPv6 is auto

configurable when any device connected to services it will be configure automatically no more manual sub netting, multi cast routing will be improved, flexibility in extension, predefined authentication and privacy support, and provide the proper quality of services.

G. Cloud Computing

The relationship between cloud computing and IoT is very important for research in emerging new technologies in the field of Internet of Things. Both have a balancing relationship for any task or invention of new trends in Information Communication technologies ICT. The amount of data generates by IoT is very large whereas cloud computing provides the facility with different communications techniques to store the data, protect the data, efficient data, and send it to accurate destination without any physical infrastructure, applications, and software's. it is increase the speed and efficiency of work. Its cost is much less as compared to physical devices for services (SaaS, PaaS, and IaaS). You can access the all information of your data via internet any time and any place. The IoT devices are directly connected to this facility when any output will generate against any input then it will be processed and stored in cloud computing storage and services [6].

H. Fog Computing

Next innovation in cloud computing is fog computing it is an advance technology which is introduced after the consumption of cloud computing in different sectors of life via internet. Different IoT have not power of computing. Fog computing provides the facility to received and processed the data from powerless computing devices. It is also called an edge computing the research agencies works on the combination of different kinds of sensors and connected machines which are sends the information to nearby edge computing devices such as switch and checks the output and results for future work. In future everything will connected to internet and advancement in current technologies is very important for upcoming days.

4. IoTs IMPROVEMENT IN DEFENSE STRATEGIES

There are many IoT applications in different fields of life, IoT concept is also use in defense in this era if this idea will apply in whole system of military we can change and improve defense system of armed forces. The 21st century is called connected battlefields through advanced technologies. Many countries in the world gives the tasks to their Research and development agencies transformed military's defense system into advanced technologies for preparing the next level connected battlefields. US military research and development agency DARPA (Defense Advanced Research Projects Agency) has a vision for how the military will utilize Internet of Things sensors in future. DARPA needs to abuse the intensity of the IoTs to encourage the U.S. leads the connected battlefields. DARPA will fund the improvement

of radars, sensor's equipment and Artificial Intelligence (AI) frameworks possibly will support break into, extricate, and examine data from any opponent's attack which is generated through communication devices. The mechanisms will support the U.S. with more statistics information to investigate opponent tactics. Information is basic part in combat activities, and DARPA requirements to transform the technology that can breakdown the opponent's systems. The agency requirements to develop the structure of modern sensors, radar and automated system that could break into point-to-point guided and unguided media communications, even ones that are not connected to the internet. DARPA is additionally investigating ways the IoT can be utilized in network security on account of an assault on US soil. Research program went for stopping assaults including radio logical and other atomic threats has effectively created and exhibited a system of cell phone measured cell phones that can recognize the littlest hints of radioactive materials.

The abilities of the gadgets that are utilized in military can be helpful for detecting the different kinds of things which is harmful for security concerns, and also used for identification of artillery's guns and other fire arms, the successful estimation of follow centralization of explosives, the tracing of armed forces, the finding of sharpshooters, and the managing of investigation in complex zones [7]. The concept of IoT has been executed in theoretical form. These can collect data from individuals, equipment, and materials in military environment by methods for detecting gadgets (devices) and offers gathered information among military articles, observing frameworks and control focuses, through a correspondence foundation.

5. DRONE TECHNOLOGY TRNSFORMING INTO IoT TECHNOLOGY IN FUTURE

The Internet of things IoT technology is broadly extending the basic gadgets (devices) and very quickly into power in drone industry. Principle favorable position of utilizing M2M (Machine to Machine) and IoT technology in drones is the ability to perform ramble activities from any PC associated with the internet. Along these lines, UAV administrators can control drone flying worldwide at the time it is conceivable to screen drone swarm flights from the principle control focus [8]. M2M multi point organize structures grants to have the same number of hubs in the system as required, including automatons and control station. It licenses to interconnect the same number of gadgets (devices) as required, controlling and observing different UAVs from numerous control stations all the while. Another advantage of M2M combination in drones is the ability to work interconnected drones as swarms. These systems flying all the while can share data for empowering propelled flight modes. Arrangement flights and shared sense and stay away from joining turns into a reality with this interconnection. UAV flight information observing is additionally a key

component given by the coordination of IoT in Drones. Utilizing this innovation makes conceivable to keep a refreshed flight log record accessible on the web. This is an intense instrument for checking flights by administrators as well as for putting away a flight record database that can be utilized for separating framework unwavering quality information or for controlling organization profitability.

6. MILITARY APPLICATIONS OF IoTS:

The military activities during war and professional exercises are much critical in these days. Many countries have adopted high-tech Scientific abilities for defense as well as our enemies that's why advancement in defense via new technologies is very important. The research and development agencies think tanks to take action in progressively under pressure atmospheres and controlled situations. The Internet of Things (IoT) is a possible solution for this issue [9]. By incorporating frameworks of sensors, actuators, and control frameworks into current military foundations, the military can turn out to be more productive and powerful. Underneath we have laid out three separate areas for IoT military applications.

I. Data Warfare

By gathering information from an extensive variety of military platform including fighter jets, weapons, and formation of soldiers themselves. the military can expand the adequacy of their insight and observation frameworks. This abundance of data will enable the military to distinguish key dangers quicker and with more exactness.

J. Smart Bases

Consolidating IoT gadgets into military headquarters can have a few constructive outcomes. Robotized security screening, for instance, builds wellbeing while at the same time diminishing manpower, and security enhance by high-tech digital cameras which are connected via controlled and secure sub networks. The smart observational gadgets are also attached for observing the all types of movement for better performance. These sub systems are connected with central administrative system which is associated with internet. This kind of system overcome the security threats in any physical conditions. Brilliant administration of assets and its system with different formats will expand the performance of military headquarters while guaranteeing the whole security of all assets and people of headquarter.

K. Applications in Logistics

The IoT has effective impact on logistic and inventory system in these days for example, agribusiness and human services have as of late profited. The military has also a logistic department which is responsible for moving the assets and equipment's one place to another place. The developed countries have used the applications which are associated with observational gadgets and advanced system

of IoT. RFID technology can enhance the management of supplies [10]. The system provides the facility to look after the assets source to destination.

7. CHALLENGES:

Internet of things (IoT) is a latest invention in the field of research. There are some challenges when we will implement this technology in any field of our life. The challenges are:

A. Standardization

The research organizations are yet to design an identical standard format for explanation of data information created by IoT devices to permit collecting of data coming for different domains and providers [11]. Further, while research organizations have lots of solutions at a specific domain, they have limited interoperability with other systems and technologies.

B. Ethical Significance

The ethical significance will be complex in future for Internet devices. For example, how ethical it is to scientifically manufacture a robot that associates with IoT and takes an interest in battle. What will the legitimate repercussions be if there should arise an occurrence of a disappointment in a basic task? These issues require open discussion among all partners including open approach producers, business and common society.

C. Costs

The cost of Internet of things equipment's is much expensive as compared to other devices. The implementation structure, design, sensors, tracking devices, and supporting material cost is also expensive. In future when consumption usability will be grow in different areas then the cost of these things reasonable for everyone.

D. Privacy and Security

IoT has a vast field in the form data collection through different devices. The Internet of things (IoT) smart tags and sensors can track every movement of all things which are connected through different communications platforms. The collection of data will be stored in form of big data through different datacenters and places. That's way privacy and security of data is very important against any threats/misuse of data.

E. Interoperability

In the Logistics department for example, the supply chains include different partners like retailers, makers and different coordination's providers. Here, the IOT frameworks need to deal with high level of interoperability with the end goal for data to be prepared productively.

8. CONCLUSION:

The Internet of things (IoT) is latest innovation in this era. Some areas of military technology, most types of sensors, vehicles, nuclear and chemical weapons seem unlikely to change dramatically. But perhaps a true military revolution will occur even without such developments with the help of IoT. Any Country can implement the concept of this technology in defense sector for improving defense strategies against any harmful activity and make a strong secure defense system. Proper research work for improvement in the conventional structure of defense system into latest structure of defense system is needed. If the stockholders of government and experts will start the research on transforming the all dimensions of armed forces defense system into IoT technology and other latest technologies, then this is very important for country's future defense. We can also find the solutions of security and privacy of all data of system, implementation of IPV6 over IPV4, develop the intelligent AI based network for IoT devices and sensors, and decide the way of IoT, vehicle to vehicle communication and connectivity of military assets in warzone for future military and country's security activities in a synergistically way.

REFERENCES

- [1] Zheng, D. E., & Carter, W. A. (2015). Leveraging the internet of things for a more efficient and effective military. Rowman & Littlefield.
- [2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7), 1645-1660.
- [3] Tortonesi, M., Michaelis, J., Suri, N., & Baker, M. (2016, April). Software-defined and value-based information processing and dissemination in IoT applications. In *Network Operations and Management Symposium (NOMS)*, 2016 IEEE/IFIP (pp. 789-793). IEEE.
- [4] Lee, C. H., & Chung, C. W. (2011). RFID data processing in supply chain management using a path encoding scheme. *IEEE transactions on knowledge and data engineering*, 23(5), 742-758.
- [5] Ziegler, S., Crettaz, C., Ladid, L., Krco, S., Pokric, B., Skarmeta, A. F., ... & Jung, M. (2013, May). Iot6-moving to an ipv6-based future iot. In *The Future Internet Assembly* (pp. 161-172). Springer, Berlin, Heidelberg.
- [6] Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: challenges. *IEEE Communications Magazine*, 55(1), 26-33.
- [7] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347-2376.
- [8] Chae, H., Park, J., Song, H., Kim, Y., & Jeong, H. (2015, July). The iot based automate landing system of a drone for the round-the-clock surveillance solution. In *Advanced Intelligent Mechatronics (AIM)*, 2015 IEEE International Conference on (pp. 1575-1580). IEEE.
- [9] YOU, C. Y., ZHU, G. B., & WANG, Y. (2011). The Internet of Things and Its Military Applications [J]. *Journal of Military Communications Technology*, 1, 016.
- [10] Yang, Y. (2018). Research on Military Applications of Internet of Things.
- [11] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In *Frontiers of Information Technology (FIT)*, 2012 10th International Conference on (pp. 257-260). IEEE.