Internet of Things for Military Applications

Lalita Mishra
Department of Information Technology
Indian Institute of Information Technology, Allahabad
Prayagraj, INDIA
rsi2018502@iiita.ac.in

Vikash
Department of Information Technology
Indian Institute of Information Technology, Allahabad
Prayagraj, INDIA
rsi2016503@iiita.ac.in

Shirshu Varma
Department of Information Technology
Indian Institute of Information Technology, Allahabad
Prayagraj, INDIA
shirshu@iiita.ac.in

***Abstract*— The main purpose of IoT technology is to connect the real world to the virtual world with anytime-anywhere connectivity. IoT is trying to generate a world of living beings along with physical objects together with virtual data and the environment. So that everything can interact with each other. An immense number of devices are used and thus an ample amount of data is generated on an everyday basis. Further, IoT is sending this generated data to the designated place without hampering the security constraints. In this paper, the applications of IoT technology in defense are the key concern. Further, we will discuss the use of IoT in Object tracking, health care monitoring, underwater & underground monitoring, drone-based monitoring, digital forensic environment, etc, as a defense perspective. Further, we will discuss how can we use edge devices and edge technology for the collection of data in the military domain and how can we use those collected data to make our defense system more secure and robust.**

Keywords—Internet of Things, defense system, health-care monitoring, drone-based monitoring, intrusion detection, wireless sensor networks, pervasive computing.

I. INTRODUCTION

The Internet of Things (IoT) is used in each and every field at present because of its pervasive nature (computation, communication, and sensing). Nowadays, if we talk about the smart environment (like smart city, smart industry, smart health care, smart home, smart classes, and so on), everything is dealing with IoT. Everything is equipped with sensors (to sense the environmental data of its designated type), processors (to process that sensed data accordingly) and communicators (to communicate among themselves). We can classify these sensors as 1. Traditional sensors (temperature, soil, humidity, & pressure sensors), 2. Non-Traditional sensors (Television, refrigerator, door, & other appliances) and 3. Biosensors (pills, plants, & chemical sensors). All these types of sensors are useful in the military environment also, because the operating space, i.e. the battle-space, is dynamic in nature. Sometimes we need to sense the environmental conditions (traditional sensors) for the establishment of acclimatization centers, to make the soldiers adapt the environmental conditions. Plant and chemical sensors (biosensors) need to be used to distinguish between useful and harmful plantations, and last but not the least nontraditional sensors can be used to sense any abnormal activity in or near the camp, to detect the presence of any intruder.

Further, in the case of the defense system, we cannot rely on one centralized cloud, because privacy and security are the most important aspects of the military. Instead, the use of tactical clouds is preferable in defense systems; we are not mentioning that tactical clouds are secure but tactical clouds are more secure than centralized clouds. Tactical clouds can be defined as providing the capability of cloud computing at the tactical edge level. Tactical cloud computing provides the potential to war-fighters to access and analyze the gathered data locally, instead of establishing a connection to the base camp or headquarter. It is useful for keeping the data secure without disclosing to any third party, as many manufactures want complete access to data which is not the case in tactical clouds.

The power requirement for governing the sensors to work properly is a challenge in the defense system. As sensors have limited battery and processing capabilities. Further, the defense is operating from easy-going areas to the areas with a hostile environment. In areas where energy is not a constraint, the sensors can be provided with a change of battery or deployment of similar type of sensors, but in areas where even living conditions are not easy, the power consumption is a crucial constraint.

The next important aspect is device utilization. The device utilization should also be at an optimum level. The term device utilization can be defined as the percentage of the time for which one device is used in 24 hours. For example, if there is a sensor node S, which is being used 6 times in 24 hour time, then the device utilization is given as [4]:

$$\text{Device Utilization} = (\text{NumberofTimesDeviceUsed} \div 24) \times 100 \quad (1)$$

So, device utilization for S using (1) can be given as,

$$\text{Device Utilization} = (6 \div 24) \times 100 = 25\%$$

Hence, from the above calculation we can conclude that, if a sensor node is used 6 times a day, its utilization is 25%, which is a good observation in terms of sensors, as the sensing devices are used only when there is a change in environmental condition.

Use of Internet of Things in military or more specifically Military of Things is the need of the hour. The reason behind this is, we are moving from Human-in-the-loop technology to

978-93-80544-38-0 /20/$31.00 ©2020 IEEE

Human-on-the-loop technology. Human-in-the-loop technology basically deals with an artificially intelligent branch that combines both, the machine and human intelligence for creating machine learning models. In this technique first, the data is labeled, then the model is tuned with the edge cases and lastly, testing is done to make sure that the desired output is coming or not. All three steps of training, tuning, and testing constitute continuous feedback to make the model smarter and more accurate. On the other hand, Human-on-the-loop technology, which can also be termed as human-supervised weapons, is dealing with the applications of artificial intelligence in the military domain. This also deals with connecting the human minds to the Internet by implanting a chip to that person's brain, so that to get confidential information, which can be beneficial in the nation's security. The ongoing research in Human-on-the-loop technology is connecting the human brains to each other. By this, with the help of artificial intelligence, the natural intuitions of the human mind can be manipulated or some unreal intuitions are fed to the human brain, which is called as artificial intuitions.

The Human-on-the-loop technology together with Human-in-the-loop can help in communication among different decision making authorities as and when required, for example at the time of war. As shown in Fig. 1 the planning agent and field responders can connect to headquarter directly, to decide which action should be taken at any point in time. Here, the planning agent is an individual or a team, who analyze the exact situation according to the gathered data, and the filed responder is a person or team coordinating and giving directions to the actual troop deployed at the war zone.

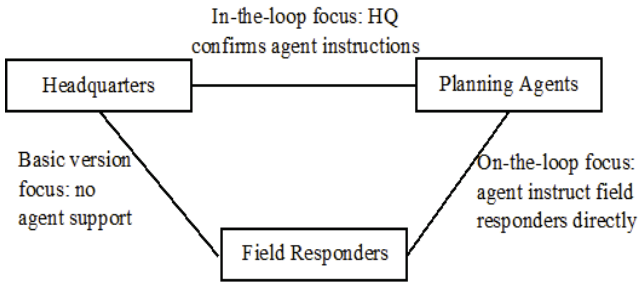

Fig. 1. Human-in-the-loop with Human-on-the-loop.

II. OUR CONTRIBUTION

We have provided a detailed review of the usage of IoT in the defense perspective. Out of the entire discussed aspects, drone-based monitoring is most important since it will detect the presence of intruders or harmful weapons without the spot involvement of human being which provides security to our soldiers. Further, we introduced a novel concept of smart camps, which is still not in practice will be advantageous for the defense system, if we adopt this in practice.

III. CHALLENGES WHILE USING INTERNET OF THINGS IN MILITARY DOMAIN

There are several challenges we have to face while using IoT technology in the military domain. Jung et al. [20] very clearly explained the challenges in IoT technology in the defense environment. They study many challenges and then categorize them according to their nature and priority. The first challenge is problems with the communication network, and this is the most prioritized challenge. The challenges with communications networks can be the security-related challenge as Denial of Service and Distributed Denial of Service attack, vulnerabilities caused by protocols used for communication, inappropriate usage of firewalls, etc. The second challenge is related to application services. The challenges related to application services are unsafe password attacks, deliberate and mistakenly created errors, viruses/worms/trojans, etc. The next type of challenge in continuation is challenges related to devices used. These challenges can be a fake signal attack, battery discharge attack, and unsafe firmware attack. The challenge prioritized as fourth is related to the platform (operating system) used by the system. These attacks can be operating system vulnerability attack, deliberate and mistakenly created errors and unauthorized access attack.

IV. USE OF THE INTERNET OF THINGS IN DECISION-MAKING PROCESS OF DEFENSE SYSTEM

We can depict the decision making the process of defense system using IoT as shown in Fig. 2. The first step of the process is situational understanding. The situation is analyzed first that is it the situation for war or some ceasefire breaking is there or some other situation. After that, the authorities will hypotheses the plan for tackling the situation against the questions raised by the team, according to the situation.

Fig. 2. Use of Internet of Things in Decision Making Process of Defense System.

After the plan was finalized on paper, it is fed to the system for analysis of the plan according to gathered data. The allotted sources will process the data in four steps. Data aggregation (process of gathering the data for analytical purpose), data linking (process of collecting data from different sources for analysis), data correlation (process of finding to which extent the data is linked to each other according to the context), and data fusion (process of physical tracking of environmental data). This processed data will send for the collection unit.

The collection process is the combination of data discovery (the process of data observation, to get a vision according to hidden data patterns and trends), data filtration (process of removing errors and noisy data), data contextualization (process of identifying specific data related to the context) and data extraction (process of retrieving meaningful data from various sources). Data processing and collection phases are occurring in a cyclic manner. After these phases, only relevant data and information is sent as a report of the whole process, and then this report is translated from machine to human understandable format (Human-in-the-loop process) and sent for decision making to the designated authorities.

Thus, by helping in data processing and analysis, IoT plays an important role in the decision-making process followed by the defense system.

V. Data Collection From Different Environment Through Edge Devices

For the better analysis of data, it is required to collect the data from authenticated sources as well as in a defined format. Since, if the data is in a defined format, we need not clean the data, before the actual processing of the data is done [5].

We can collect the data in an underwater scenario, with the help of mobile edge elements (autonomous underwater vehicles (AUV)) as presented in [17]. In this, they consider the mobility characteristics (direction and velocity) of mobile edge elements that are closed to AUVs in the 3D environment. They designed a target selection algorithm by taking into account the storage and computation capability and mobility ability of AUVs, to calculate the path for data collection. Their target selection algorithm reduces the power consumption of nodes, provides efficient data collection, along with an extended lifetime.

Data collection in smart transportation scenarios is very time-sensitive, as Zubair et al. discussed in [18]. The sensitivity is of the milliseconds when we talking about the safety intimations given by smart vehicles, such as a warning for tire likely to burst. It can bear a delay of minutes in live tracking of vehicles and even a day when we monitoring the road surface or crater fixing task is there in a normal scenario. But, if we talk about the defense area, the monitoring of road surface is even as important as other safety measures. Thus, while collecting the data in defense zone we need to program our system accordingly.

Smart health care deals with all the healthcare-related activities, such as time to time monitoring of the patient, on-time drug delivery, a system to timely read and notifies the reclamation/deterioration of the patient, all health care solutions based on the smartphone, etc. MOVEeCloud project uses specialized wearables to track the activities of the patient and thus, provide the facility to primary care and store the data to notify when the patient needs to go for the checkup [19].

In healthcare-related data collection, there should be as minimum error as possible, because even an unsubstantial error in the collection of data may lead to severe condition or death of the patient.

VI. Applications Of Internet Of Things In Defense System

The various IoT applications in the perspective of defense system are described as under:

A. Object Tracking

IoT enables the objects (sensors of any type) to sense the environmental data according to their designated type, enable communication among them as and when required, and make them cooperate with each other to perform some assigned task. These objects can either be in mobile condition or of static nature. Some objects need to move from one place to another to accomplish the objective of their deployment. Moving object tracking can be done using IoT by attaching RFID (Radio Frequency Identifier) tag with the mobile object. The RFID tag will sense and transfer the traveling information of the mobile object to the cloud server by using the Internet until the object reaches its destination point [1]. Some partners are attached to each mobile object throughout the travel. These partners are entities, traveling with RFID readers attached to them. These RFID readers, attached with partners are used to read the information, which is collected by RFID tags. The RFID readers use radio frequency wave signals to read the necessary travel information automatically within the area under the coverage range of that particular mobile node [2]. However, the limitation associated with the use of these RFID tags and readers is they need to share the information over the untrusted wireless channels, which makes the node vulnerable to security risks [3]. The tracking of deployed mobile or static objects is a necessity when it comes to the defense system because a piece of information that seems to be of least importance for the normal scenario can be of a crucial type in the defense system.

Through object tracking [5], the defense personnel team can get crucial information about any unusual activity or presence of any unwanted thing around them. The object tracking system should not be traceable by the enemy, the reason behind this is, the enemy team will try to make all the necessary cautions in installing their objects by somehow avoiding the tracking system, or they can perform cryptanalysis to bypass the tracking system.

B. Intrusion Detection [6]

According to its functionality, the IDS can be of many types. The Network Intrusion Detection System (NIDS), can track the inbound and outbound network traffic, to find an unusual activity, if any. The Host Intrusion Detection System (HIDS) is running on all the devices connected to the network and has direct access to the enterprise internal network and the Internet. It can detect any divergent network packet originating

from the organization. HIDS are able to detect malicious network traffic also, which is not possible by using NIDS, because NIDS is not configured to do so. The third type is the Signature-based Intrusion Detection System. This IDS monitors the data packets passing over the network and matches them with a database of malicious signatures, like anti-virus software. The fourth type is the Anomaly-based Intrusion Detection System. This system is also responsible to monitor the network traffic, and match that network traffic with an already established baseline to find if the traffic traveling on the network is suitable for the network or not, according to protocols, bandwidth, ports, etc.

Intrusion Detection Systems can also be classified as passive IDS and active IDS. Passive IDS will detect the unusual activity, and then generate notifications or log entries, but it will not take any preventive action against that unusual activity. Whereas, when the active IDS will detect some malevolent activity, it will also generate the notifications or log entries as well as taking preventive actions, like IP blocking or controlled resource access to malicious devices, etc.

C. *Energy-Efficient Routing [7]*

The sensors should be deployed in an energy-efficient manner because the defense operations operations are conducted in very harsh conditions. Energy-efficient routing is needed for helping the defense system because the sensors have very limited battery power. So, if the sensor has stopped been working or is sending malicious data, it is of no use.

We can use the concept of device utilization, discussed in the introduction section along with needed calculations, to find out the efficiency of routing and the importance of that type of sensors in the particular region. If that type of sensor is not useful for the region, then we can use some other type of sensor which is required for the monitoring of the particular area or objects.

D. *Smart Transportation*

Smart transportation is used in a defense scenario, since it will provide better sensing of unusual things, like land mines.

Smart transportation system can be defined by using sensors with vehicles, or mobile devices connected to the Internet, that are installed in smart cities [11]. By using a smart transportation system, it is possible to have optimized routes, advanced parking reservations, accident detection, accident prevention, automatic driving, etc. A smart transportation system is performed by integrating IoT with transportations. Route optimization is the most momentous aspect of smart transportation system because, in the present era, people have everything but no time. By optimizing the route, energy consumption by the vehicle can also be reduced and so as the air pollution. The optimized routes will help at the time when our deployed team need some help from the headquarters or need some backup at the time of war, the help or backup will be present at the required place in the shortest possible time.

Smart transportation system works by collecting the data from the user's mobile device [12] that is connected to the Internet and trying to estimate the congestion on a particular road, and then recommend optimal route options to curtail the traveling time.

The next advancement in the same area is the smart street light system. In this system, the street lights are smart enough to detect the traffic on the road. If there is traffic or someone is passing by the road, the light is turned on, and when the road is idle, the light will get turned off automatically. This system is also working well for reducing energy consumption, as well as very much helpful in defense areas. By using this system two main benefits to the army can be, first, when the road is idle there is complete blackout situation, an intruder who is not familiar with the road cannot find where to go, and second is, if any intruder trying to enter in the military zone by taking the advantage of murk, the intruder will surely get caught because the lights will automatically be turned on.

The next benefit of a smart transportation system is, it is intelligent enough to detect the bad road conditions for the detection and prevention of accidents. This feature is useful for defense in finding and destroying land mines deployed by the enemies. Since the condition of the road will surely be affected or more specifically damaged at the time of deployment of land mines. IoT is also providing a vehicle to vehicle connectivity that will help to inform all the vehicles in the troop that some unusual thing is found and be alert for the preventions [13].

E. *Smart Health Care [10]*

Smart health care is much needed for common people as well as for the soldiers. The IoT devices can facilitate remote monitoring of health conditions as well as the generation of emergency notifications. These devices can be blood pressure or heart rate monitor, a Fitbit electronic wristband, some advanced implantation devices for health care, such as a pacemaker, etc.

The soldiers can be injured severely in the war zone. Sometimes, they cannot even walk, or move their bodies in any direction because of multiple fractures in their bodies. In these cases, smart beds can help them in performing such tasks. These smart beds can sense the pulse of the patient laid on it and decide whether he/she is trying to move his/her body, trying to change the posture, feeling some uneasiness or something else. In the case of changing posture, the bed is smart enough to make itself in a position in which the patient will feel comfortable. In the case when the patient is feeling uneasy or he/she wants to call the doctor, the bed can generate an alarm to intimate the doctor that the patient is in need of them. The bed will also produce an alarm to intimate the nurse that it is the time for medication; by this feature, the hospitals need not appoint a dedicated nurse for each and every patient.

Further, IoT is coming up with more health monitoring devices and the devices which can help one to oversee their physical disabilities, like, DEKA Research and Development Corporation invented LUKE (Life Under Kinetic Evolution) arm for armless people. This arm is smart enough to sense the pulse of the person wearing it and decide which work the person wants to do, and accomplish it. Such type of inventions is very helpful for defense personnel, because they may lose some of their body parts during the war. Another invention in

the same direction is a smart wheelchair, which can even be used on an uneven surface, a variety of seating options are there, is able to climb the staircase, etc. These innovations will help humans in need.

F. Smart Camps

IoT can be used to incorporate a large number of heterogeneous end devices in one place while providing access to some subsets of data for the advancement of opulent digital services. Smart camps are just a hypothesis. If defense camps can be smart just like smart homes, it will be very much helpful for the soldiers to detect the unusual activities around the camps. After this hypothesis come into action we can be able to sense the presence of intruders and explosives around the camps to prevent the would-be attack and possible destruction. We can hope that after the establishment of smart camps, the whole camps will not be destroyable and we can prevent more casualties like after Uri Base camp attack in September 2016 and many other attacks, where the whole camp, when it is full of our soldiers were destroyed and our loss after that cannot be overcome by any means.

G. Use of IoT in Digital Forensic Investigation

Digital forensic techniques are required to deal with many security challenges like logical (Denial of Service) or physical menace (theft or tempering), authentication & authorization of access, the privacy of users, etc. [16].

A seven-phase forensic investigation model was designed by Oriwoh et al. in [15]. This model is capable of performing the forensic investigation in a smart home environment. Phase 1 ensures the availability of forensic experts with the desired skill set so that any type of unusual activity can be detected without failure. The second phase deals with the secure storage of extracted information, following the chain of custody. A proper fulfillment of chain of custody is required because if there is any loophole at any point in the investigation process, then the whole process is of no use and the pieces of evidence are not eligible to prove or disprove the crime on any further point of time. In the third phase, all the collected shreds of evidence are preserved and the phase is termed as cordoning off the crime scene. The fourth phase creates a global picture of the scenario (topology). This is done by using the proper photography of the crime scene. All types of evidence are marked at their exact places so that any damage or dislocation of the evidence at any time can be traceable by the forensic experts. This phase can be termed as the marking of evidence. In the fifth phase, all the required security checks are performed. The next phase deals with locating and acquiring evidential data. In the last phase, the forensic experts draw some meaningful results from all the gathered and analyzed pieces of evidence. All the phases are fully dependent on the successful execution of their previous phase, because if the previous phase is a failure, then there is no meaning of further investigation, as the investigation and pieces of evidence are of no use because of damaging of the evidence due to any supine act.

Further, for analyzing the DJI Phantom-III drones forensically, Clark et al. in [14] proposed an open-source tool called DRone Open source Parser (DROP). This tool can parse the encrypted and encoded.DAT and.TXT files, extracted from the internal storage of drone. The analysis of.TXT files will provide us much useful information such as the battery and flight time of drone, it's location on the GPS system, etc.

The forensic investigation of IoT devices will help in the defense system also in getting the actual cause and material used in the attack. It will be helpful in defining the severity of the attack accurately.

H. Drone Based Monitoring

Drone-based monitoring is very important for defense use in many ways. We summarize some different types of research using drone-based monitoring in several aspects. In [8], Kalra et al. presented a drone-based facial recognition system, by maintaining the dataset DroneSURF. In this, they surveyed the crowded places like a stadium, markets at the time of some festival, shopping malls at peak hours, or other highly crowded places. They also included places with some calamity, like flooded areas, areas itinerant with earthquake, etc. They basically include those areas under observation, where the inspection of places is difficult for the human being. After that, they perform face recognition irrespective of having different variations in poses, the intensity of light, illumination, the effect of motion of people, resolution of the camera, the distance of the people from the camera, etc. They have two different types of monitoring, active monitoring, and passive monitoring. In active mode of monitoring, the drone is capturing the images and videos while actively monitoring the person from a few meters, focusing on the subject (person) themselves. In a passive mode of monitoring, the drone is directed to capture the image or video of an event or any area without focusing on the particular subject. This passive type of monitoring can be helpful for monitoring the borders of the country. Many times, the defense system needs to inspect the areas which are insurmountable for any individual; this type of drone-based surveillance is useful at those places.

Another type of drone-based monitoring is proposed by Marathe et al in [9]. In this report, the author proposed the monitoring system of pipelines using drones. They consider the pipelines covering cross-country regions. These regions are hundreds and thousands of kilometer wide, where monitoring is a challenging but important & necessary task. They detected thermal leakage, methane/ethane gas leakage by deploying high resolution, infrared and thermal imaging, and methane/ethane analyzer respectively. Such type of high-resolution imaging can help when some unwanted activity like infiltration is happening. In such scenarios, this drone-based monitoring can help the defense system.

VII. Performance Comparison Of Exiting Work Based On IoT Attributes

Table 1 will illustrate the comparison of existing work on the basis of IoT applications, which we have accommodated in our paper along with standard IoT performance metrics.

TABLE I. COMPARISON OF IOT ATTRIBUTES WITH IOT PERFORMANCE METRICS

Performance Metric / IoT Applications	Throughput	Scalable	Energy Consumption	Latency	Network Overhead	Interoperability
Object Tracking	High	Yes	Low	Low	Low	High
Intrusion Detection	Moderate	Yes	Moderate	Low	Low	High
Energy Efficient Routing	Moderate	Yes	Low	Low	Low	High
Smart Transportation	High	Yes	Moderate	Low	Moderate	High
Smart HealthCare	High	Yes	Moderate	Low	Moderate	High
Use of IoT in DF Investigation	Moderate	No	Low	Low	Moderate	Moderate
Drone Based Monitoring	High	Yes	Moderate	Low	High	High

VIII. CONCLUSION & FUTURE SCOPE

IoT is an important and brilliant concept for using technology in all aspects of living. Further, the concepts of IoT are used to create new innovative applications in the defense perspective. IoT is the extended feature of the Internet according to the design point of view, so the issues regarding security and privacy with the Internet also go hand in hand with IoT.

The current industrial approach for use of IoT is, they are trying to standardize the IoT applications in the best possible way to get the most valuable outcomes out of it. All the developed and developing countries are moving towards IoT applications in every field. Thus, we, as a research contributor tried to get the attention of industries and researchers towards the defense field to make a more powerful, smarter, robust and secure defense system. Many developed countries are started using IoT technology in the security of the nation, but India is lagging behind in the direction of IoT in defense. Thus, the research community needs to do some outstanding and application-oriented research in this field for the improvement of the current architecture of our defense system.

As future work, we can suggest the implementation of these IoT applications in a real-time scenario. We will look forward to the practical use of the hypothetical concept of smart camps.

REFERENCES

[1] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," In 2nd international conference on consumer electronics, communications and networks (CECNet), pp. 1282–1285, April 2012.

[2] S. S. Park, "An IoT application service using mobile RFID technology," International Conference on Electronics, Information, and Communication (ICEIC), pp. 1–4, January 2018.

[3] B. Baruah, and S. Dhal, "An IoT Based Secure Object Tracking System," Wireless Personal Communications, vol. 106, no. 3, pp. 1209–1242, January 2019.

[4] D. Jadhav, V. Muddebhalkar, and L. Khandare, "Utilization of Resource's in IoT," International Journal of Computer Applications, vol. 167, no. 3, 2017.

[5] K. H. N. Bui and J. J. Jung, "Computational negotiation-based edge analytics for smart objects," Information Sciences, vol.480, pp. 222–236, April 2019.

[6] S. Venkatraman, and B. Surendiran, "Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems," Multimedia Tools and Applications, pp. 1–18, 2019.

[7] A. V. Dhumane, and R. S. Prasad, "Multi-objective fractional gravitational search algorithm for energy efficient routing in IoT," Wireless networks, vol. 25, no. 1, pp. 399–413, 2019.

[8] I. Kalra, M. Singh, S. Nagpal, R. Singh, M. Vatsa, and P. B. Sujit, "Dronesurf: Benchmark dataset for drone-based face recognition," In 2019 14th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2019), pp. 1—7, 2019.

[9] S. Marathe, "Leveraging Drone Based Imaging Technology for Pipeline and RoU Monitoring Survey," In SPE Symposium: Asia Pacific Health, Safety, Security, Environment and Social Responsibility. Society of Petroleum Engineers, April 2019.

[10] C. G. Jordaan, N. Malekian, and R. Malekian, "Internet of Things and 5G Solutions for development of Smart Cities and Connected Systems," Communications of the CCISA, vol. 25, no. 2, pp. 1-16, 2019.

[11] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A Review of Machine Learning and IoT in Smart Transportation," Future Internet, vol. 11, no. 4, p. 94, April 2019.

[12] J. Yang, Y. Han, Y. Wang, B. Jiang, Z. Lv, and H. Song, "Optimization of real-time traffic network assignment based on IoT data using DBN and clustering model in smart city," Future Generation Computer Systems, December 2017.

[13] B. Jain, G. Brar, J. Malhotra, S. Rani, and S. H. Ahmed, "A cross layer protocol for traffic management in Social Internet of Vehicles," Future Generation Computer Systems, vol. 82, pp. 707–714, May 2018.

[14] D. R. Clark, C. Meffert, I. Baggili, and F. Breitinger, "DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III," Digital Investigation, vol. 22, pp. S3–S14, August 2017.

[15] E. Oriwoh, and G. Williams, "Internet of things: The argument for smart forensics," In Handbook of research on digital crime, cyberspace security, and information assurance, pp. 407–423, 2015.

[16] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," pp. 544–546, 2018.

[17] S. Cai, Y. Zhu, T. Wang, G. Xu, A Liu, and X. Liu, "Data Collection in Underwater Sensor Networks based on Mobile Edge Computing," IEEE Access, vol. 7, pp. 65357-65367, May 2019.

[18] N. Zubair, K. Hebbar, and Y. Simmhan, "Characterizing IoT Data and its Quality for Use," arXiv preprint arXiv:1906.10497, June 2019.

[19] H. Hiden, S. Woodman, P. Watson, and J. Cala, "Developing cloud applications using the e-science central platform," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, vol. 371, no. 1983, January 2013.

[20] S. H. Jung, J. C. An, J. Y. Park, Y. T. Shin, and J. B. Kim, "An Empirical Study of the Military IoT Security Priorities," International Journal of Security and Its Applications, vol. 10, no. 8, pp. 13—22, August 2016.