Applications and Security Concerns of Satellite Based IoT Networks: A Conceptual View

Dr. Anjum Sheikh Qureshi

Rajiv Gandhi College of Engineering Research & Technology, Chandrapur

Abstract— **Internet of Things (IoT) connects objects or things from anywhere at any time. IoT therefore requires efficient communication networks to enable connectivity among the devices. Satellite technology is being recognized as one of the feasible solutions to connect the IoT devices scattered over the globe. Integration of IoT with satellite communication can be helpful in creating a global network by interconnecting a number of devices. Satellite based IoT is beneficial for the IoT users residing in the remote locations. The satellite based IoT networks are prone to security attacks. To develop trust among the users for IoT and increase its usage, protection from these security attacks should be a priority for the organizations using satellites for the IoT applications. Machine Learning and Blockchain have been considered to be some of the solutions for the security concerns of IoT. These techniques can be used for the satellite based IoT and therefore been discussed in this chapter.**

***Index Terms*-- Block-Chain, Internet of Things, Networks, Machine Learning, Satellite, Security**

1.INTRODUCTION

Internet of Things (IoT) is a versatile technology that has enabled connection of devices over a large area. It uses sensors, actuators and many other smart objects that are able to sense the changes in the environment around them and make decisions to establish a suitable communication between them. IoT mainly relies on wireless communication technologies depending on the applications and the preference of the consumers. Researchers working in different parts of the world have predicted that the number of IoT users is increasing rapidly and it is expected to increase further in the next few years [15]. According to a survey by Statista 2019, shown in fig .1 below, the IoT connected devices would reach 75.44 billion as compared to 15.41 billion in 2015.The wireless communication technologies currently used are broadly classified as short range networks and long range networks. The short range networks consist of technologies like local area network (LAN), personal area network (PAN), zigbee and near field communication (NFC) [16].The connectivity technologies of wide area networks use cellular networks like 2G, 3G, 4G and the low power wide area networks (LPWA) like LoRa and Sigfox. The selection of connectivity technologies for any IoT application is dependent on some primary factors that include range, bandwidth, latency, scalability and Quality of Services (QoS). One of the issues of concern for the IoT devices is regarding the coverage at remote locations. Many of the IoT applications that require disbursing of devices at remote locations are unable to work satisfactorily with the available technologies [1].

Satellite networks are one of the available methods that can solve the shortcomings of the long range and short range technologies [4]. Advancement of satellite technology has reduced the cost of deployment and development of satellite networks as compared to the large space base satellite networks that used bigger satellites. The existing technologies favor the production of small size satellites like the Nanosatellites that weigh less than 10 kilograms. The usage of nanosatellites is gaining momentum as they are able to perform nearly all the functions as the conventional satellites but at very less expenditure [11]. Satellite based IoT (SIoT) communication platforms are being developed to satisfy the requirements of universal coverage required by the IoT applications. This technology can enable communication in remote or under populated areas as well as for the places that lack terrestrial infrastructure where the cellular and internet based network is unable to reach. A group of satellites working together as a system is utilized to accomplish the objective of attaining uninterrupted communication while using SIoT. This group of satellites is able to gather more information and is insensitive to the failure of communication as experienced by the single satellite based system [5]. As satellite communication helps to solve the connectivity problem, security exploits tend to be another major concern that is attracting attention of the IoT users. If the service providers are unable to provide security updates for their devices the end users will be subjected to cyber attacks and breaching [8]. The security risks and the breaching of IoT devices can limit the growth of IoT in the increasingly connected world. This paper sheds light on the various IoT applications that will be benefited by using satellite networks, security risks involved and their possible solutions during connectivity through satellite. Some of the objectives of the study are as follows: (i) To study the IoT applications that can be implemented using Satellite networks (ii) To identify the security challenges of Satellite based IoT networks (iii) To identify some solutions for the security concerns of Satellite based IoT networks

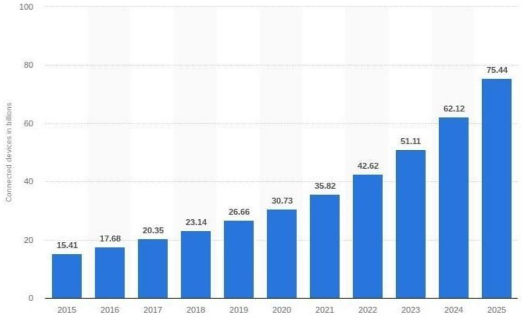

Fig.1. IoT connected devices installed worldwide from 2015 to 2025 (in billions) [19]

II.IOT APPLICATIONS BASED ON SATELLITE NETWORKS

Satellite communication when combined with the IoT provides great support for the interconnection of IoT devices and circuits that are scattered at different remote locations. A satellite based IoT network [17] is given in fig 2 in which an oval shaped boundary represents coverage area, red dots represent sensors and the triangular structures represent IoT trans-receivers. Satellite networks provide better coverage and require fewer resources as compared to the cellular networks due to which the researchers have shown interest in satellite networks for IoT applications. Larger coverage area facilitates multicasting of services through satellite networks while maintaining cost effectiveness and the energy constraints of the battery powered IoT devices. They also provide better availability and reliability than the wireless networks especially in the case of mission critical applications like military communications. The failure of networks cannot be tolerated for the mission critical applications as it would result in loss of lives of common people and property.

Some of the disadvantages associated with the SIoT are propagation delay and poor signal reception. Propagation delay is the time required for the transmission and reception of a signal. The value of propagation delay may seem to be negligible for a single communication but it can reduce the overall efficiency of communication for the satellites especially for long file transfer and large amounts of information exchange. Unnatural or slightly long pause during voice communication is an example of propagation delay. The quality of services provided by the satellite signals is affected by the extreme weather conditions like heavy rains, thunderstorms, snowfall and winds. Obstructions like tall buildings and trees and angle of the satellite receiver adversely affect the reception of satellite signals.

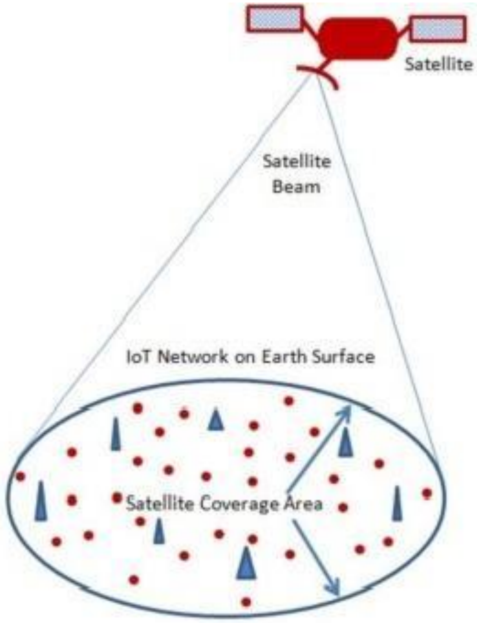

Fig 2. Satellite Based IoT Network [17]

In this section we would like to discuss some of the applications of satellite based IoT like smart healthcare, agriculture, smart gird, environmental monitoring and mission critical applications.

a. Health Care

Healthcare has been transformed into smart healthcare with the combination of medical facilities and IoT. The IoT devices have enabled people to find hospitals, doctors and get connected with them from any faraway places. Monitoring the health of elderly people or critical patients has become easier for the doctors with the help of wearables. But all these advantages of smart health care will not be able to work in the absence of cellular networks [16]. SIoT can be beneficial for health care applications as it provides ubiquitous coverage by which the health care facilities like remote monitoring, surgery, nursing and hospitalization can be provided to people at remote locations.

b. Smart Grid

A smart grid uses smart meters, automated monitoring systems and power management systems that help in energy efficient production, transmission and distribution of power. Due to all these factors smart grid has emerged to be a promising solution to the challenges faced by the conventional power grids like dispensation of electrical energy, reliability, security and lack of mechanism to store electrical energy. Smart grid meets the electrical energy requirements of the fast growing population by generating electrical energy which closely matches the demand. Performances as well as speed of the heterogeneous communication networks play a significant role in calculating capability of smart grids. Automated control and monitoring of substations at remote areas is presently done by SCADA systems. Real time monitoring of the grid is done by using large number of sensors deployed at different locations that will gather data about the grid, process it to detect future problems and act upon it. But the slow central network control of SCADA based systems is not able to act efficiently for accomplishing all these tasks and would raise issues of latency, reliability and data rates. Satellite based IoT systems can provide cost effective solutions for monitoring of substations at remote areas, offshore wind farms and solar energy systems in desert areas by providing back up links at instances where higher values of reliability are preferred. Some of the applications like distribution systems where time duration is of utmost important are unable to function properly with the present system because of the stringent delays that occur due to limited bandwidth [9]. SIoT network infrastructure can help to solve the problem of delay in distribution systems by using network management solutions to reduce signal congestions and logically group the IoT nodes based on their locations and services to optimize communication loads.

c. Agriculture

Agriculture is one of the main occupations of rural people living in developing countries. IoT devices and sensors can be utilized to collect information and analyze it to increase agricultural yield. The advantages of using SIoT are its cost effectiveness and its usage in rural areas which lack the facilities of cellular networks. As shown in fig 3., Sensors can be deployed at various locations to collect data for increasing crop yield by monitoring the levels of water, temperature, moisture, fertilizers, pests etc. Few more applications that can be implemented by using SIoT are equipment monitoring, fisheries management, weather forecast to decide the crops for the coming season, animal tracking to prevent pet animals and especially wild animals from entering the farm.

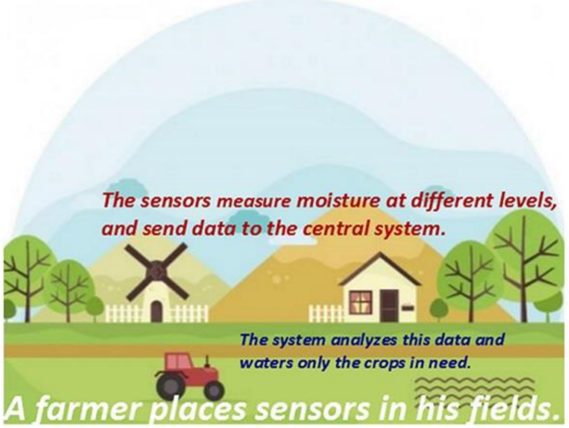
The sensors measure moisture at different levels, and send data to the central system.
The system analyzes this data and waters only the crops in need.
A farmer places sensors in his fields.

Fig3. Smart Agriculture [20]

d. Environmental Monitoring

Environmental monitoring through IoT systems can be used for dealing with crucial issues in big cities like waste management, vehicle tracking and for weather forecasting by monitoring air quality, temperature, humidity, wind speed , concentration of gases like carbon dioxide etc. Monitoring process would be more beneficial for the farmers, miners if they are able to use it at remote locations for which satellite networks can be utilized in absence of internet and cellular networks. Traditional satellite systems have not been used on a large scale for this purpose due to the enormous capital cost required for storage, power supply and sending data.

Nano satellites with IoT connectivity are solutions to these problems that provide higher data transfer efficiency at a lower cost. They provide uninterrupted coverage; have low bandwidth requirements, low power consumption and have high scalability as the data acquired by the satellites is sent to the ground station to be processed by the cloud software which can then be accessed by using traditional communication protocols [6] .

e. Mission Critical Applications

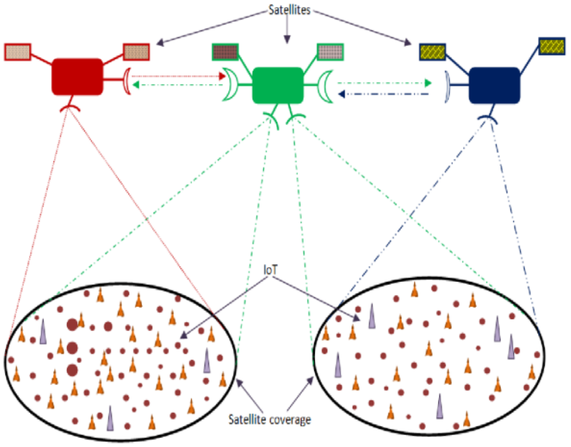

Fig. 4. Satellite IoT networks for mission critical applications [2]

Emergency and important services that require continuous network coverage for efficient functioning are called mission critical applications. Interruption in the network can cause communication failure which can damage the entire system or organization and in some cases can effect survival of people. Operations of aircraft, railways and marine transportation, online banking, electrical power systems are some of the mission critical applications that need high speed as well as uninterrupted network connection. Military data collection and transmission is another application that can be listed in this category while another is disaster management during natural calamities like floods, earthquakes, cyclones and hurricanes. All the mission critical applications require continuous network connection and a minor disruption can lead to sever losses like in the military application where a small delay can lead to loss of battles and can affect the security of the whole country. During natural calamities the available cellular networks stop functioning but satellite networks are not affected. The real time protocols of IoT have proved to be attractive solutions for functioning of these applications with higher reliability. Therefore proper deployment of IoT sensors along with satellites is always preferred for mission critical applications. Multi satellite based systems like the one depicted in fig 4 are considered preferable for the mission critical applications in which the coverage for IoT devices are provided by the satellite and inter-satellite connections are used to increase the scope of applications [2] . Unlike wireless connectivity technologies like Bluetooth, Zigbee or WiFi , satellite IoT is not limited in terms of area to be covered and also possess the ability to establish as well as handle multiple interconnections.

II.PROBLEM IDENTIFICATION: SECURITY CONCERNS OF SATELLITE BASED IOT NETWORKS

Satellite communications for Internet of Things has a lot of benefits like global coverage, enhanced reliability, speed, long life cycle and multicasting by which a single broadcast from the satellite can reach multiple units. Despite the numerous benefits of the technology there exist few barriers for the adoption of technology like scalability, higher communication as well as connectivity cost and security issues [18]. Satellites provide better security than cellular networks but SIoT faces significant security risks as the security solutions for SIoT have to be developed by considering the security issues faced by satellites and IoT [6]. Malicious software, denial of service (DOS), spoofing, and tampering and information disclosure are some of the cyber attacks which will affect all the systems and communication network of SIoT.

As SIoT uses satellites for establishing communication in IoT networks, the security algorithms for SIoT have to consider the issues faced by IoT devices and also the satellites. The service providers use different networks and some of the IoT devices do not have updated software and lack inbuilt security mechanisms. Large organizations have invested a sufficient amount on securing their networks but have paid less attention to secure the IoT devices. In the presence of all these issues of the IoT devices it is difficult to develop security algorithms for SIoT. More data exchange on the networks with the increasing number of devices is an additional challenge. Another challenge while framing security solutions for the SIoT is the energy constraints of IoT devices. These devices are battery powered and therefore possess limited energy. The security solutions require large storage space which s generally lacking in IoT devices. The solution to deal with the low storage space is being done by using cloud storage which further alleviates the security risks.

Many organizations are using satellites as an option for widening their networked ecosystem but they hardly possess direct control over security of their satellite networks. The chances of breaching are more in these networks as they are situated outside the earth's atmosphere. Cheap satellites and propagation of IoT satellites closer to the earth will enhance prospects of security breaching by the adversaries. Ground stations are easier to be hacked as they are operated by humans and also due to their internet connectivity [14]. These stations have terminals which act as access points to a satellite. Terminals are software programmed and regular upgrading of the software is needed to protect it. Moreover to avoid delay or any barriers in the operational actions these terminals are not protected by authentication which adds to possibilities of security attacks on these systems. The space has become cluttered and the satellites are facing a problem of lack of frequencies for communication and allocation of orbit is becoming difficult with the increasing number of satellites. Rise in the number of satellites actually increases the size of the attack surface and therefore increases the responsibility of security teams to decide defense mechanisms. Satellites are unable to tolerate transmission of short messages due to their data capacity and cost which results in higher transmission delays and low throughput. For short range transmissions using SIoT the process of data collection is implemented using LAN or PAN. Satellite networks provide main connectivity for a selected area which in turn depends on LAN or PAN to establish communication between the devices. These localized area networks are easier to be attacked as compared to the satellite networks. Another feature that increases the vulnerability of the satellites is the software defined functionality that helps to reprogram the satellite in the orbit. These software defined satellites require improved security controls to prevent hacking. Technological life cycle of satellites is entirely different from most of the technologies that are being used today. Therefore though many security solutions are available it is not possible to implement those solutions directly for the satellite networks.

The lack of security solutions can lead to problems like deletion and distortion of data that is being transmitted or received by using the satellite networks. An additional risk associated with the cyber threats on the satellites are the denials of service attacks that can diminish the amount of data being transferred in a given span of time. The wireless communication systems are easily affected by electromagnetic interference or jamming [13]. The satellite services are affected by two types of jamming called terrestrial jamming and orbital jamming. Terrestrial jamming includes jamming of the signals on the downlink i.e between satellites and receivers. This type of jamming will influence the operating efficiency of the receivers deployed at specific geographical locations. It is also called a wireless denial of service attack. On the other hand orbital jamming interferes with the signals in the uplink i.e the signals that are being transmitted from ground stations to the satellites. Orbital jamming tends to degrade the quality of the signals received by the satellite.

Spoofing is one more kind of threat faced by the satellites that alters the information being exchanged on the networks [12]. This group of attacks target receivers in which false signals are used to confuse the satellite receiver. The altered signals are introduced on the networks in such a manner that the receivers believe the signals to be coming from false locations. The cyber attacks on networks have been given a lot of importance but to ensure reliability of IoT networks that use satellites for connectivity there is a need to avoid attacks that aim to control satellites. In case the attackers succeed in gaining control over the satellite system they will be able to damage satellites by changing their orbits. A change in the orbit of a satellite tends to enter the orbit of another satellite which will cause collision of two satellites that can destroy either any one or both of them. These collisions will further lead to accumulation of debris in space and will also increase risks of collisions for other satellites. Many of the organizations are becoming aware of the security threats and are taking steps to avoid it. The organizations are unable to decide on the implementation of security methods due to its large costs. The cost of implementation of small satellite systems and in some cases devices or infrastructure required for cyber attacks are inexpensive as compared to the revenue that needs to be invested for securing our systems as well as our networks.

IV.SOLUTIONS FOR THE SECURITY CHALLENGES OF SATELLITE BASED IOT NETWORKS

Applying methods that will help to preserve and secure our satellites systems is always better than running our networks in the absence of security. Some of the possible solutions lie in using recent technologies like machine learning and block chain.

a. Blockchain

One of the promising technologies to ensure satellite security is blockchain technology which is a data structure that consists of time stamped and cryptographically linked blocks. Every block has a hash pointer that consists of a pointer to the location of the previous block and cryptographic hash of that block. The stored hash pointer is compared with the previous hash for verifying a block. When some data is updated on the block chain ledger it is not possible to change or discard any data from the Blockchain.

One of the types of attacks on satellites that can be prevented using Blockchain is Spoofing. According to research by [10] Blockchain can be used to secure communications by using Multifactor Authentication and creating virtual trusted space zones. Multi Factor Authentication can be used for verifying identity of satellites and ground stations by assigning codes to the block. Consider an example of two satellites A and B. Satellite A sends requests to B for enabling some communication. Satellite B asks for the code of the previous block and communication between the two satellites is enabled when A sends the code to B. Another feature for securing satellites is by creating virtual zones in which a zone master issues a virtual ID for all the satellites [7]. Requirements and registration rules for adding a new satellite are specified in a blockchain smart contract which is executed by the zone master. When a new satellite sends a request for joining the virtual zone, its request has to be verified by all the satellites. A verification algorithm that contains rules specified in the smart contract is executed to verify the identity of the new satellite. Zone master assigns a virtual Id to the new satellite and registers this new transaction in the blockchain after the verification of the satellite. If the transaction is found invalid the zone master declares it as an intruder and rejects the communication.

b. Machine Learning

Machine learning (ML) is a technology that helps to automate a process and makes the machine intelligent. These algorithms help the computers to become more authentic, learn from data, improve themselves and behave like intelligent data. While working with ML we don’t have to think about algorithms, we just need to supply huge amounts of data to the machine and then the machine will think about how to convert input data to output.

Machine learning can be used for preventing terrestrial jamming which is a kind of wireless Denial of Service (DoS) attacks. A research by [3] has suggested machine learning aided cognitive anti jamming for satellite to ground link communication. The cognitive engine uses reinforcement learning (a type of ML technique) to learn a suitable anti jamming communication policy. When a communication is initiated the cognitive engine may find that the link from satellite to ground or channel is jammed. The engine may spend a considerable amount of time to wait for the channel to become free. Once the channel is free, the cognitive engine stays in the channel for a long time without being jammed. But this technique increases the delay of communication over the link if the channel is jammed for a long time. Reinforcement learning can be used to implement good channel selection policies that will reduce waiting time in case of channel jamming. The cognitive engine uses this policy to randomly pick up a channel for sensing and waits there till the channel is jammed. Once jamming is observed in the channel the cognitive engine of the receiver helps the satellite transmitter to sense and randomly pick up a new channel that is predicted to remain free from jamming for the longest duration.

It is necessary for the organizations working with satellite based IoT networks to disseminate awareness and training among its staff to deal with the security threats.The service providers should be prepared to handle the changing nature of the security threats and therefore should keep themselves updated with the evolving security models. Blockchain and Machine learning can be considered to be possible solutions for securing the satellite based IoT systems against the escalating threats.

V.CONCLUSION

Satellite systems when used with the IoT applications help to meet the technical challenges especially establishing connectivity in the remote or suburban areas where internet facilities are unable to reach. Networks that use satellites thus provide connectivity at a global level thereby enabling intelligent communication among humans and devices irrespective of their locations. But the increasing number of IoT devices and satellites are giving rise to the risks of cyber attacks on these systems. If the cyber or security threats are not avoided it can affect the lives of people to a large extent. The organizations should divert more funds and efforts for devising solutions to ensure safe as well as secure IoT based satellite systems. As the technical requirements of satellite and currently used technologies are different it is not possible to apply the current security algorithms without any modifications. Block chain and Machine Learning are two promising technologies that can help to develop methods to secure IoT based satellite networks owing to their qualities of enhancing data transparency and meeting the device computational constraints respectively.

REFERENCES

[1] Greg Sadlier, Farooq Sabri, Nanosatellite Telecommunications: A Market Study for IoT/M2M Applications, *London Economics*, 2017

[2] Sudhir K. Routary, Abhishek Javali, Laxmi Sharma, Richa Tengshe, Sutapa Sarkar, Aritri Ghosh, Satellite Based IoT for Mission Critical Applications, *IEEE*, 2019

[3] Sudharman K. Jayweera Shuang Feng , Dale Mortense , Abriel Hollan , Marie Piasecki , Mike Evans3, Christos Christodoulou, Cognitive Anti-jamming Satellite-to-Ground Communications on NASA's SCaN Testbed, *NASA Technical Report Server*, 2019.

[4] Mauro De Sanctis, Ernestina Cianca, Giuseppe Araniti, Igor Bisio, Ramjee Prasad, Satellite Communications Supporting Internet of Remote Things, *IEEE Internet of Things Journal*, 2015

[5] Francesco Chiti , Romano Fantacci, Laura Pierucci , Energy Efficient Communications for Reliable IoT Multicast 5G/Satellite Services, *Future Internet 2019*, 11, 164; doi:10.3390/fi11080164

[6] A Narayanasamy, Y A Ahmad, M Othman, Nanosatellites Constellation As An Iot Communication Platform For Near Equatorial Countries, *6th International Conference on Mechatronics* -2017

[7] M. Shymala Devi, R. Sugana, P.M. Abhinaya, Integration of Blockchain and IoT in Satellite Monitoring Process, *IEEE*, 2019

[8] David Livingstone, Patricia Lewis, Space : The Final Frontier for Cyber Security, *International Security Department*, 2016

[9] A. Meloni and L. Atzori, The Role of Satellite Communications in the Smart Grid, *IEEE Wireless Communications*, vol. 24, no. 2, pp. 50-56, April 2017, doi: 10.1109/MWC.2017.1600251.

[10] Mohamed Torky, Tarek Gaber, Aboul Ella Hassanien, Blockchain in Space Industry : Challenges and Solutions, *arXiv.2002.12878 [eess. SP]*, 2020

[11] Natalia Vargas-Cuentas, Avid Roman-Gonzalez. Nanosatellites: Actual Mission That Can Perform., *67th International Astronautical Congress - IAC 2016*, Sep 2016, Guadalajara,Mexico. 2016. <hal-01403826>

[12] Gabriele Oligeri, Savio Sciancalepore, Roberto Di Pietro, GNSS Spoofing Detection via Opportunistic IRIDIUM Signals, *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20),* July 8–10, 2020, Linz (Virtual Event), Austria, https://doi.org/10.1145/3395351.3399350.

[13] Zixiang Jia, Anti-jamming Technology in Small Satellite Communication, *IOP Conf. Series: Journal of Physics: Conf. Series 960 (2018) 012013*, doi:10.1088/1742-6596/960/1/012013

[14] Adam Ali.Zare Hudaib, Satellite Network Hacking & Security Analysis, International *Journal of Computer Science and Security (IJCSS)*, Volume (10) : Issue (1) : 2016

[15] Shanzhi Chen, Hui Xu, Dake Liu, Bo Hu, Hucheng Wang, A Vision of IoT: Applications, Challenges and Opportunities With China Perspective, *IEEE Internet Of Things Journal*, Vol. 1, No. 4, August 2014

[16] Bikash Pradhan ,Saugat Bhattacharyya ,Kunal Pal, IoT-Based Applications in Healthcare

Devices,*Journal of Healthcare Engineering, V*olume 2021, Article ID 6632599,https://doi.org/10.1155/2021/6632599

[17] Sudhir K. Routary, Habib Mohammed Hussein, Satellite Based IoT Networks for Emerging Applications, *IEEE*, 2018

[18] M. De Sanctis, E. Cianca, G. Araniti, I. Bisio and R. Prasad, Satellite Communications Supporting Internet of Remote Things, *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 113-123, Feb. 2016, doi: 10.1109/JIOT.2015.2487046.

[19] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[20] https://www.tutorialspoint.com/internet_of_things/internet_of_things_environmental_monitoring.htm