iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** III **Month of publication:** March 2020

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue III Mar 2020- Available at www.ijraset.com

Cyber Security for Connected Commercial Aviation: Case Study

Chiragkumar Aboti
Student of M.Tech Cyber Security, Computer Engineering, Faculty of Technology, Marwadi University, Gujarat, India

Abstract: ***Any devices connected to IoT-based network in commercial aviation are also connected with each and every other device, and these devices are potentially vulnerable for black hat or grey hat hackers. Protecting information and data from cyber-attacks need more attention. This paper cover precautionary measures that we can take to protect information and data in connected commercial aviation. We are discussing various cases, where cyber security play important role. Before adopting any technologies in commercial aviation, we must focus on concerns of security and privacy of information and data breaches.***
Keywords: Cyber Security, Internet of Things, Cloud, Hackers, Commercial Aviation, Risks Mitigation, Vulnerability

I. INTRODUCTION

Forthcoming commercial aviation consists various technologies to established fast and passenger centric services. As numbers of airlines increasing in significant manner and commercial aviation booming. Adopting emerging technologies in this era are common but cyber security is major concern to successful implementation of these technologies. Commercial aviation is an important part of the economy of nation as well as regional growth and development. It will bring many different organizations and interest groups in one group; from commercial aircrafts, ground staffs, and air-side traffic management to passengers. Among each of this group are many entrepreneurs with different potentiality, goals and functions. Commercial aviation must not get to only large but they also must get to smart. Emerging technologies such as cloud, IoT, AI, etc… can make it possible to established smart commercial aviation.

Increasing complexity of forthcoming commercial aviation networks also magnifies the cyber security challenges faced by such networks. The complexity of forthcoming commercial aviation networks is attributed to the large number of devices connected to the Internet along with large data generated by devices. Attacks are possible as the devices in the forthcoming commercial aviation network are an easy target for intrusion. Once compromised, black hat or grey hat hackers can get control over the system and carry out malicious activities and attack other devices close to the compromised node. Opportunities exist in this era for the deployment of Artificial intelligence (AI), Internet of Things (IoT) and Cloud computing in to the commercial aviation. These chances expand both functional efficiencies in commercial aviation as well as chances to exploit vulnerable device data to provide integrated forecasting maintenance and high-level management. Cyber security is major concern in commercial aviation to the deployment of these technologies.

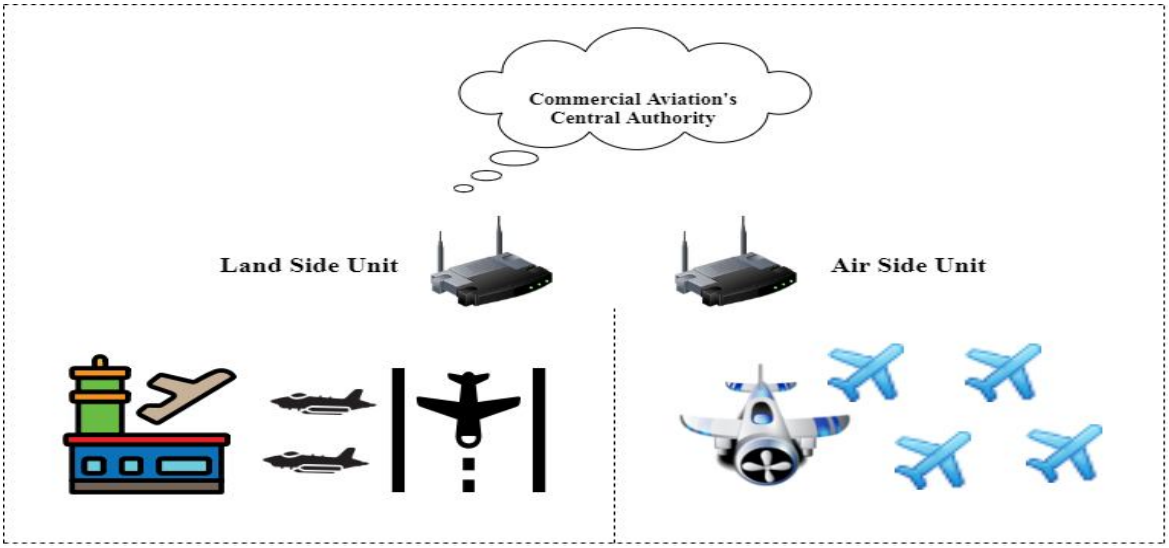


Fig. 1 Connected Commercial Aviation

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue III Mar 2020- Available at www.ijraset.com

II. LITERATURE REVIEW

A.Bandekar and A. Y. Javaid proposed Attack mitigation algorithm and present impact analysis of cyber-attack with IDS and without IDS [1]. As per S. Naik and V. Maral, there are already six billionIoT-based devices on the internet and within a few years these number is anticipated to scale to 20 billion devices. Computer system and smartphoes have dozens of software security solutions to protect them from most of the attacks but similar security solutions are missing to protect the rest of the internet of things [2]. K. Verma and N. Jain proposed AI System, which can make internet an artificially intelligent system and it is actually an effortless way of living life [3]. In this paper, S. A. P. Kumar and B. Xu proposed a "Vulnerability Assessment Framework", which used for assessment and secure from cyber-attacks concerned to wireless and wired networks and systems [4]. In this paper, P. K. Chouhan, S. McClean and M. Shackleton present basic elements of IoT models and provide situation assessment for IoT applications [5]. In this paper J. Pate and T. Adegbija introduce commercial aircraft's monitoring framework as an application of the IoT for commercial aviation security and safety [6]. In this paper B. Chung, J. Kim and Y. Jeon propose the "On-Demand-Security" configuration mechanism that we can configure required security functions and reorganize them without recreating device image [7]. In this paper S. Yoon and J. Kim proposed remote security management server to enhance to the security of IoT devices by integrally and systematically providing and managing various security functions [8]. In this paper H. Garg and M. Dave proposed model, middleware is primarily used to expose device data through REST and to hide details and act as an interface to the user to interact with sensor data [9]. In this paper M. N. Aman and B. Sikdar proposed unique protocol, which useful in random permutations and random time hopping sequence to skulk validation data/information. Author also covers formal security analysis mechanism of proposed protocol [10]. Chiragkumar Aboti proposed three phase authentication mechanism to secure commercial aviation phase wise [11].

TABLE I
ISSUES MATRIX

Issues / Papers	Malware	Device cloning	Data tampered	Unauthorised access
[1]	Yes	No	No	Yes
[2]	Yes	Yes	Yes	Yes
[3]	Yes	No	Yes	Yes
[4]	Yes	No	Yes	Yes
[5]	Yes	Yes	Yes	Yes
[6]	Yes	No	Yes	Yes
[7]	Yes	No	Yes	Yes
[8]	Yes	Yes	Yes	Yes
[9]	Yes	Yes	Yes	Yes
[10]	Yes	No	Yes	Yes
[11]	Yes	Yes	Yes	Yes

Issue matrix (Table-I) provide various types of cyber risks, which author considered in past research. We study same in commercial aviation perspective. Similarly, observed parameter matrix (Table-II) provide various types of mitigation approaches, which proposed by author in past research. Using this literature review, we analysis all cases of cyber security in commercial aviation perspective. Forthcoming commercial aviation must have prior risk mitigation framework with accordance to technology, whatsoever take place in commercial aviation services.

TABLE III
OBSERVED PARAMETER MATRIX

Parameter / Papers	Cyber risks Mitigation	Risk Assessment	Malware Detection/Prevention	Authentication
[1]	Yes	No	Yes	No
[2]	No	Yes	Yes	Yes
[3]	Yes	No	No	Yes
[4]	Yes	Yes	Yes	Yes
[5]	Yes	Yes	Yes	Yes
[6]	Yes	No	Yes	Yes
[7]	Yes	No	Yes	Yes
[8]	Yes	Yes	Yes	Yes
[9]	Yes	Yes	Yes	Yes
[10]	Yes	No	Yes	Yes
[11]	Yes	Yes	Yes	Yes

III.VARIOUS CYBER SECURITY CASES IN COMMERCIAL AVIATION

We study various cases of cyber security in commercial aviation. As we know, different technologies have different challenges and vulnerabilities. Computing as well as communications have undergone remarkable changes in recent decades. Computation is preferred on the go with a huge demand of mobility support in communicating [12, 13].

A. Cloud Based Connected Commercial Aviation and Cyber Security

If commercial aviation devices are connected to the Internet, more chances of probably cloud-connected devices. IoT is anthology of cloud-based connected devices, which linked to any source. It has changed passenger's living way that they use the Internet. For any instance, which ever so using cloud-based connected devices we are now able to connect to our phones, to our account, to our airlines, to airports, etc. We can use these could-based connected devices that work to gather to access data/information anywhere we are and, on any connected devices. These networks of cloud-based connected devices must not to be taken leisurely. Hackers are always in such attempt for new ways to gain access to our private data/information. Devices, which connected to the network and to every possibly connected are believable gateways that hacker can use to gain access and exploit our data and private information. There are safety measures that we may take when it comes to keep our private and professional data/information safe and secure while using private IoT. Due to large number of users in wireless environment communication paradigm also have shifted to the concept of Cognitive Radio Networks [14, 15] for better utilization of wireless spectrum.

IoT devices are smart device and these devices are actually intelligent because of the huge amount of data/information that they gathered and kept. Each and Every day all IoT-based connected devices monitor and gathered data and information. IoT internal sensors in forthcoming commercial aviation's devices and appliances such as smart aircraft's departure and arrival system, Smart airport's services for purchasing goods or services and wearable devices collect huge amount of data. They collect information such as how many times we arrived at particular airports, how many times we used particular airlines, how many times we visited particular services desk at airport, what applications we most likely use at certain times, and how many stalls we've visited in a day. This is the way to gain insight about our activity that what we actually do so commercial aviation can enhance the passenger's experience at airports. However, actually we have not any idea about data/information that what kind of private information these devices are storing. Even, we have no idea about what commercial aviation do with this type of data/information. Is it really useful to collecting this type of data/information? issues occur when our could-based devices, IoT-based devices, Internet connection, or data/information, actually not secure by any mechanism or not safeguard properly. It's always important for us to firstly we ensure any device, verify cyber security policies. Check that the commercial aviation policies and our cloud service provider policies of privacy and security majors. It's very important to confirm about not use our private information for sell to any other business or any social marketing purpose. It's always recommended to all to ensure the commercial aviation's data theft, misuse and prevention

against any attacks policies as well, so that we have idea about, what will happen with our data/information that store in commercial aviation database, in case of any data theft or attacks. Software updates always important to our digital security and safety. We always get notification about software updates but unfortunately, many of us neither seriously take care about it nor remembering it to upgrade software update which necessarily required for security reasons. This seems as harmless offense, but in reality, this can move our data/information in vulnerable state.

B. Embedded System in Connected Commercial Aviation and Cyber Security

We can't avoid that if we have to safe and secure cloud-based connected devices, we must have to safe and secure the important embedded parts of any devices. There is significant spout that required to be addressed in order to safe and secure any hardware. An embedded system built with set of various features that can be imperil at various levels by malicious discrepancy. In most of the cases, embedded design and prototyping, followed by developing take place before the any software application has been developed by developer. This is what we actually take care about the system development. Embedded system mostly considered the last defence whenever it comes from outside cyber-attacks. If hackers compromise the embedded system, then software security protection may become outmoded. Embedded system has long life then software and embedded system can't be upgraded, where software can be upgraded because software doesn't wear out but hardware does.

1) *Processing Power*: Processing power is very much important, when we consider performance of any hardware devices. If we check current architecture of embedded system, then we found that most of them are not compatible with present cyber security mechanism. This is happening because of increasing rates of data over internet and the complexity of cyber security protocols.
2) *Battery Consumption*: This is another thing, which take place in embedded system, because of consuming high-level power by any embedded system. Capacity of battery is very low and, in this decade, also security measurement not considered by manufacture so battery consumption is also major loopholes. This is happening because of battery manufacture or designer focus on performance of battery over cyber security concerns.
3) *Network*: Any embedded system, which connected with many different networks over lease line, broadband or any wireless connectivity among other connections. This is one more area where hacker try to target but cyber security protocols are also taking place to safeguard. Here, its required to established cyber security architecture with more flexibility to adapt security changes.
4) *Malicious Software:* Cyber-attacks mainly take place because of malicious software such as backdoors, worms, viruses or Trojan horse, these are the most basics threats, which faced by any embedded system. Exploitation take place, when these types of vulnerability are present and these types of vulnerability can disrupt system's functionality. Using these hackers can steal confidential data, break integrity and manipulate sensitive data.

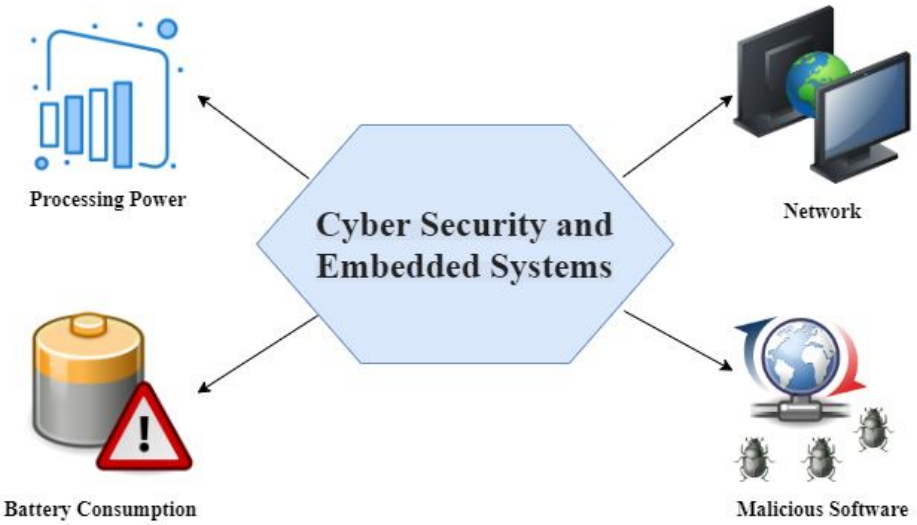


Fig. 2 Cyber Security and Embedded System

C. Case 3: Logistic and Transportation in Connected Commercial Aviation and Cyber Security

The logistics and transportation of passenger's baggage and/or other luggage are one of the most vulnerable to hackers. As well as many commercial aviation connected solutions rising to increase efficiency, securing cyber-physical complex systems will require multiple layer cyber security mechanism. While we have to addressed important commercial aviation challenges, there also have operational challenges that must need to be addressed, because it will be enhancing the commercial aviation security and improving connected commercial aviation logistics and transportation services. We also required to look out for firmware updates, authentication and device provisioning across node population, it also acquiring robust device management system, which can be handle remotely. Different sensors on commercial IoT devices use multiple communication protocols like Wi-fi, ZigBee, Bluetooth Low Energy etc. to transform data feeds, which gateways required to process.

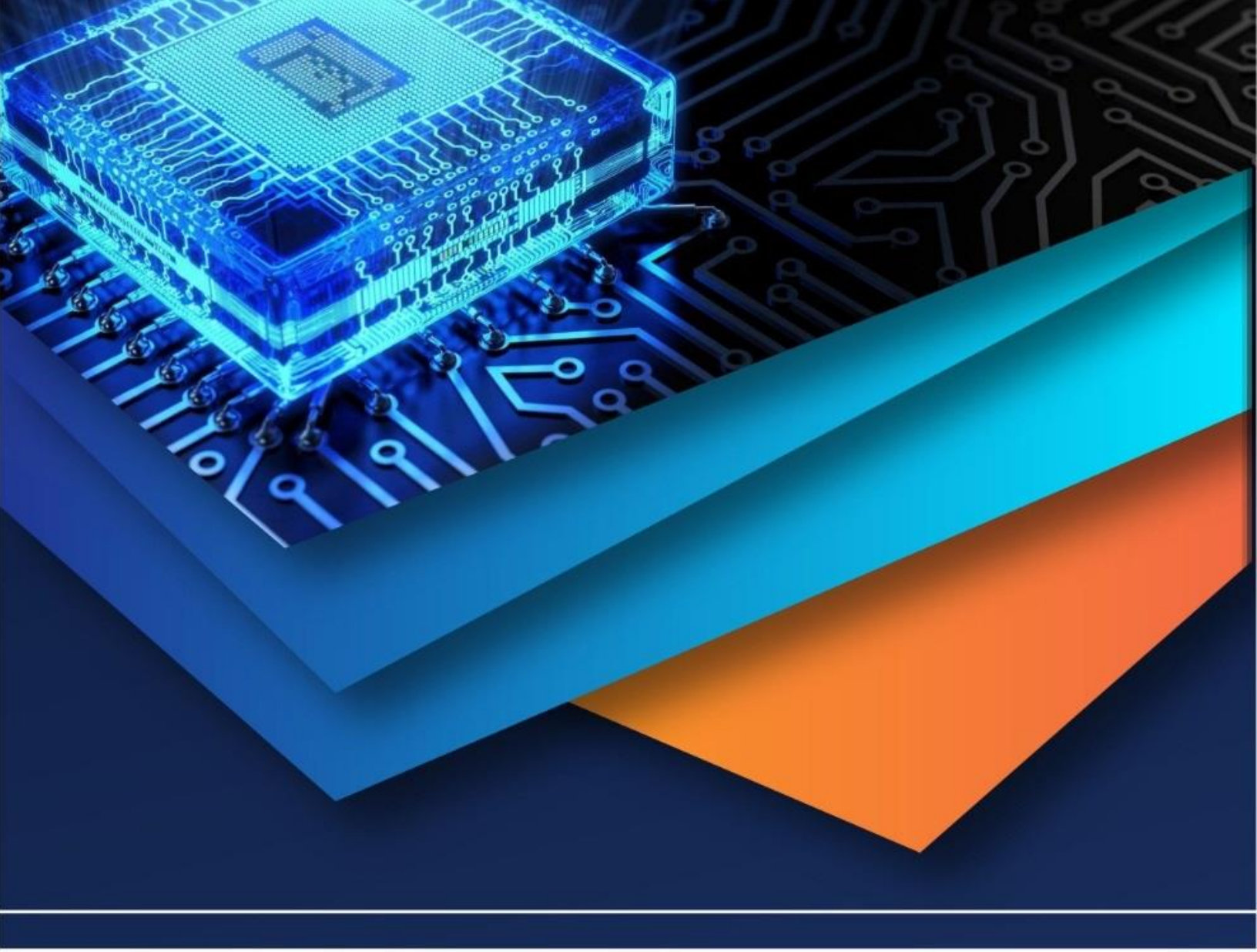
Forthcoming commercial aviation might be running IoT workloads depends on cloud services to run their IoT-based data management workloads and passenger's applications. Economy of corporate allow leading cloud service organization to invest in cyber security infrastructure as well as remarkable cyber security policy models, therefore required security measure of cloud side of IoT stack take places. Cloud security is more complex, can't managed locally where edge can and therefore increase huge cyber security risks.

IV. CONCLUSIONS

The goal of this case study is to put cyber security in limelight in commercial aviation perspective. Before adopting any emerging technologies in commercial aviation, we must design cyber security mechanism to mitigate cyber risks. Forthcoming commercial aviation reduces processing time of services, enhance passenger's experience, increase nation's economy and many more, but hackers are always there to exploit such vulnerable system, which have not proper cyber security mechanism. So, need more attention to implement emerging technologies in commercial aviation.

REFERENCES

[1] Bandekar and A. Y. Javaid, "Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices," 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Honolulu, HI, 2017, pp. 1631-1636
[2] S. Naik and V. Maral, "Cyber security — IoT," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, 2017, pp. 764-767.
[3] K. Verma and N. Jain, "IoT Object Authentication for Cyber Security: Securing Internet with Artificial intelligence," 2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, 2018, pp. 1-3.
[4] S. A. P. Kumar and B. Xu, "Vulnerability Assessment for Security in Aviation Cyber-Physical Systems," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, 2017, pp. 145-150.
[5] P. K. Chouhan, S. McClean and M. Shackleton, "Situation Assessment to Secure IoT Applications," 2018 FIFTH INTERNATIONAL CONFERENCE ON INTERNET OF THINGS: SYSTEMS, MANAGEMENT AND SECURITY, Valencia, 2018, pp. 70-77
[6] J. Pate and T. Adegbija, "AMELIA: An application of the Internet of Things for aviation safety,"2018 15TH IEEE ANNUAL CONSUMER COMMUNICATIONS & NETWORKING CONFERENCE (CCNC), Las Vegas, NV, 2018, pp. 1-6.
[7] B. Chung, J. Kim and Y. Jeon, "On-demand security configuration for IoT devices,"2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2016, pp. 1082-1084.
[8] S. Yoon and J. Kim, "Remote security management server for IoT devices,"2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2017, pp. 11621164.
[9] H. Garg and M. Dave, "Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IOT-SIU), Ghaziabad, India, 2019, pp. 1-6
[10] M. N. Aman, B. Sikdar, K. C. Chua and A. Ali, "Low Power Data Integrity in IoT Systems," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3102-3113, Aug. 2018.
[11] Chiragkumar Aboti. "Studies of Challenges to Mitigating Cyber Risks in IoT-Based Commercial Aviation." International Journal for Scientific Research and Development 7.11 (2020): 133-139.
[12] N. Dutta and IS Misra," Multilayer hierarchical model for mobility management in IPv6: a mathematical exploration", Wire. Pers. Comm. (Springer), vol.78 (2), pp.1413-1439, 2014.
[13] N. Dutta and IS Misra, "Mathematical modelling of HMIPv6 based network architecture in search of an optimal Performance", IEEE 15 th ADCOM, Guwahati, India, pp. 599-605, 2007.
[14] N. Dutta, HKD Sarma and Z. Polkowski, "Cluster based routing in cognitive radio Adhoc networks: reconnoitering SINR and ETT impact on clustering", Com. Com., (Elsevier), pp. 10-20, vol. 115, 2018.
[15] N. Dutta and HKD Sarma, "A probability based stable routing for cognitive radio Adhoc networks", Wire. Net., (Springer), vol. 23(1), pp. 65-78, 2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY