# Studies of Challenges to Mitigating Cyber Risks in IoT-Based Commercial Aviation

**Chiragkumar D. Aboti**
M. Tech. Student
Faculty of Technology, Marwadi University, Gauridad, Rajkot, Gujarat, India

*Abstract*— Recent years have seen exponential development in IoT as well as commercial aviation. IoT-based commercial aviation is in demanding in this era. The technologies of IoT security are expanding day by day and developing to meet the ongoing demands of the IoT and Cybersecurity landscape as a whole. Cyber security is major concern in successful implementation of IoT in commercial aviation. Need more attention to secure IoT-based commercial aviation. Mitigation of Cyber risk is primary concerns and proper authentication mechanism can fulfill this requirement. In this paper we studied challenges to mitigating Cyber risk in commercial aviation and proposed three phase authentication mechanism to mitigate Cyber risks.

***Keywords:*** Cyber Challenges; Risk Mitigation; Vulnerability Assessment; IoT Authentication; Aviation Security

## I. INTRODUCTION

The objective of this studies is to propose Cyber risk mitigation in IoT based commercial aviation. Computing and communications have undergone remarkable changes in recent decades. Computation is preferred on the go with a huge demand of mobility support in communicating [9, 10]. Commercial aviation covers many segments, business aviation, personal aviation, transportation, etc. There are many segments involved in the operation and maintenance of these sectors, and as such it is a highly regulated market, with authority control of airspace and airspace operations. Opportunities exist now days for the deployment of IoT in to the commercial aviation. These opportunities span both operational efficiencies in commercial aircraft as well as opportunities to exploit real-time device data to provide integrated predictive maintenance and intelligence linked into advanced management. Cyber risks are major concern in commercial aviation to the deployment of IoT. In the near future, maybe around the year 2021 with high bandwidth network, billions of heterogeneous things will be part of the IoT. Privacy and Cyber security will be the major concern during this phase. Due to large number of users in wireless environment communication paradigm also have shifted to the concept of Cognitive Radio Networks [7, 8] for better utilization of wireless spectrum. Commercial aviation needs more attention while implementing IoT-based services.

In IoT, Wearable technology creating painless and effective experience to passengers, crew member, airport's management. There are many innovative wearable devices, which makes smoother operation in commercial aviation. Like smart watches, smart uniform, smart head phones, smart googles, etc. A wearable device which can be establish painless journey to passenger and effective operation management to commercial airport's staffs are smart watches (for boarding pass, navigation, notification, etc., from

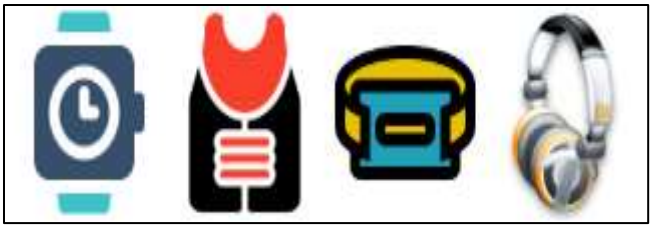

Fig. 1: Wearable devices

passenger's perspective), smart uniforms (for communicate in-between airport's staff, authorities as well as crew member, in built sensor useful to monitor environment conditions, etc.), similarly smart head phones and smart goggles innovate overall operations and services in commercial aviation premises.

## II. CYBER RISKS AND CHALLENGES

There are various types of spoofing attacks. Spoofing means to gain access to a victim's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. Spoofing is often the way a bad unauthorized person gains access in order to execute a larger Cyber-attack. Among the various spoofing attacks, we seen the following spoofing attacks, as they are launched on behalf of clients and destroy the data center's resources.

### *A. Hiding Attack:*

Fig. 2: depicts hiding attack. Attackers simultaneously send a large number of spoofed packets with random IP address. This creates chaos at the data center regarding which specific packets should be processed as legitimate packets. Data center cannot identify specific packet.

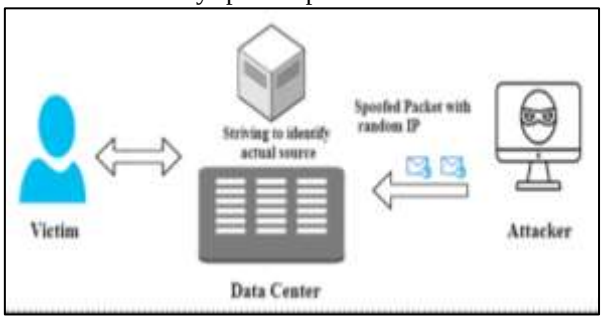


Fig. 2: Hiding Attack

### *B. Reflection Attack:*

Fig.3 depicts reflection attack. Attackers send spoof packets with the source IP address of the victim to any unknown user. This causes unwanted responses to reach the victim from unknown users and increases the flood rate.

 

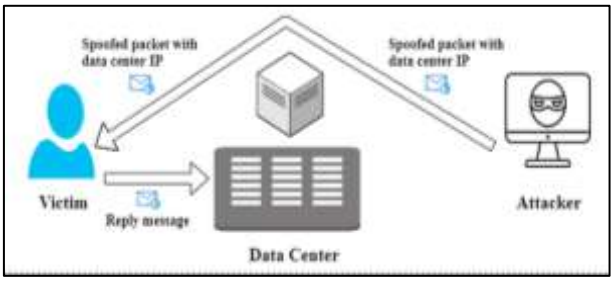


Fig. 3: Reflection Attack

*C. Impersonation Attack:*

Fig. 4 depicts impersonation attack. Attackers send spoof packets with the source IP address of any unknown legitimate user and acting as a legitimate user. This is equivalent to a man-in-the-middle attack. The spoof attacker receives requests from clients, spoofs IP, and forwards the requests to the Data Center, acting as a legitimate user. The responses of the Data center are again processed intermediately and sent to the clients. This leads to confidentiality. If a proper spoof detection mechanism is not in place, the Data canter could respond badly, leading to a partial shutdown of services.

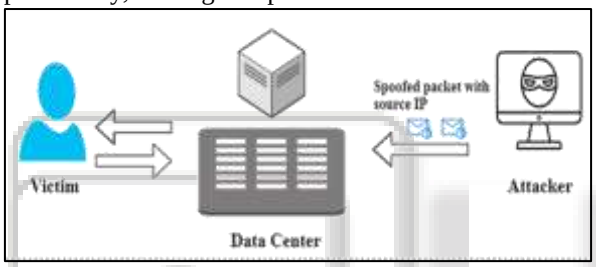


Fig. 4: Impersonation Attack

In network-level DDoS, the attackers will try to send invalid requests with the aim of flooding the cloud service provider; for example, requests for a half-open connection. In service-level DDoS, the attacker will be sending requests that seem to be legitimate. Their content will be similar to a request made by a legitimate user. Only their intention is malicious.

*D. Components Level Attacks:*

The IoT connects "everything" through the Internet. These things are heterogeneous in nature, communicating sensitive data over a distance. Apart from attenuation, theft, loss, breach, and disaster, data can also be fabricated and modified by compromised sensors. Fig. 5 shows the possible types of attacks at the component level. Verification of the end user at the entry level is mandatory; distinguishing between humans and machines is extremely important.

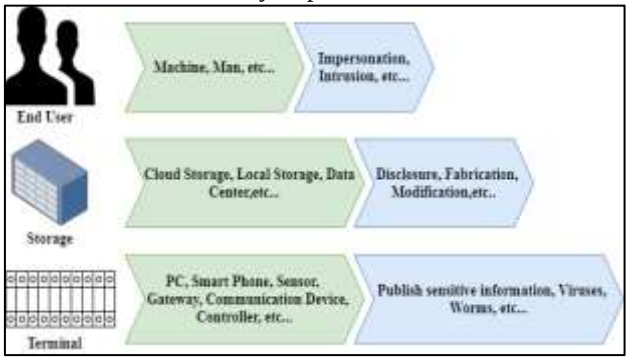


Fig. 5: Components level attack

*E. Physical Security:*

Due to distributed and fragmented nature of IoT, a larger attack surface and physical access to the devices take place and combination of these two factors make physical security a vulnerabilities and potent threat. Hardware involved in serving clients must be continuously monitoring and audited with a safe checkpoint for the identification of threats. There are multiple types of physical security attacks (Like, Side-channel, Power glitching, Frequency tampering, etc.).

*F. Software Security:*

Many IoT devices have not any firmware updates and cannot be patched for specific security flaws, limited or non-existent user interfaces is another contributing factor to IoT's lack of security. Corruption or modification of application software by threats could affect several clients who depend on that particular application programming interface (API) and related software interfaces. Software security is play important role to protect IoT devices.

*G. Network Security:*

Securing the network connecting IoT devices on the internet is a bit more challenging than traditional network security because there is a wider range of device capabilities, standards, and communication protocols, all of which pose significant issues and increased complexity. Bandwidth attacks such as DDoS can cause severe congestion the network and also affect normal operations, resulting in communication failure. Network security must be as strong as it meant to be.

*H. Reasons behind Cyber risks and challenges:*

IoT devices are very complex in nature, it is possible that most of the IoT devices that we encounter will have security issues. Some of the reasons that stand out as a cause of security issues when building these IoT devices are mentioned below.

*I. Mobile Application Vulnerabilities in IoT:*

The mobile applications are an integral part of most of the IoT devices in commercial aviation. Very much any device that we find, will have a mobile application that helps us to control the IoT device or analyze the data collected by the IoT device. However, unless required attention is paid to the Cyber security of these applications, their chances are high that the applications can be vulnerable, leading to the Cyber risks of the entire IoT-based commercial aviation solution.

*J. Web Application Vulnerabilities in IoT:*

IoT devices, will in some cases also have a web interface for users to interact with other peripheral. It is essential for us to understand how to analyze web interfaces for IoT devices for security issues and how to mitigate vulnerabilities. Web application Vulnerabilities gives easiest access to unauthorized entries and exploitation can impact on entire IoT-based network.

## III. METHODOLOGY

This research is basis on desk research method. We are using external desk research method. External desk research method gives various required information about commercial

 

aviation and IoT. In external desk research method, we gathered information via online desk research. Which gives sufficient amount of information. Literature review gives broad idea about ongoing trends in IoT and commercial aviation. We analyze challenges and Cyber risk using empirical and qualitative studies.

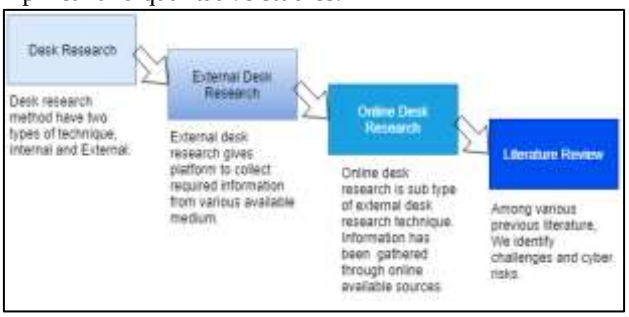


Fig. 6: Research Methodology

## IV. RELATED WORK

In this paper, we are studying and proposing a novel Cyber risks mitigation mechanism for IoT-based commercial aviation. The analysis conducted considers the impact of cyber-attacks and deployment of the three phases of authentication in commercial aviation's network comprising of IoT devices. Considering the previous work and comparative analysis of different security mechanism, we are proposing three-phase authentication mechanism for IoT-based commercial aviation to established strongest security.

### *A. Paper 1: Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices.*

The first approach is Cyber-Attack Mitigation and Impact Analysis for Low-power IoT Devices. We have seen huge development IoT, Users nowadays want to control all these "smart" wireless home devices through their smartphones using an internet connection. Attacks such as distributed attacks on these devices will render the whole system vulnerable as these attacks can record and extract confidential information as well as increase resource (energy) consumption of the entire network. In this paper, author proposed a Cyber-attack detection algorithm and present an impact analysis of easy-to-launch Cyber-attacks on a low-power mote (Z1 Zolertia) as a model IoT device. We also present detailed results of power consumption analysis with and without attack along with when the mitigation algorithm for intrusion detection is implemented [1].

### *B. Paper 2: Cyber security — IoT.*

The second approach is an Arduino device firmware which coded in c for authentication. As per author, there are already 6 billion devices on the internet and within a few years these number is anticipated to scale to 20 billion devices. PCs and mobiles 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. IoT solutions is not just software but an entire ecosystem of hardware, software, cloud, web and mobile interfaces. This ecosystem is not very mature and there are still major concerns lurking around IoT adoption primarily due to security threats. IoT top Security Concerns: Device Cloning, Sensitive Data Exposure, Denial of Service, Unauthorized Device Access and Control, Tampering Data. This research work accomplishes the need to mitigate IoT security challenges Device Cloning and Sensitive Data Exposure [13].

### *C. Paper 3: IoT Object Authentication for Cyber Security: Securing Internet with Artificial intelligence.*

The third approach is securing Internet with Artificial intelligence. The Identification of the objects and human can bring lot of facilities but it can provide security also. Many researchers say that the data that is used for giving IoT features can be misused for purpose of hacking into the crucial data and privacy. This issue can also be solved using IoT. Identification of Objects is the foremost requirement of any kind of IoT technology and it plays an important role. Because recognizing you as you or you as someone else is really easy without IoT, and creating a fake identity on internet is easy in today's world and leads to issues like hacking of data an intrusion in privacy. Realizing the person's real identity and to provide security on which we can depend upon completely becomes vital. And all these ideas discussed above can be implemented using IoT. Our goal is to achieve real time working principle of above idea [5].

### *D. Paper 4: Vulnerability Assessment for Security in Aviation Cyber-Physical Systems.*

The fourth approach is Vulnerability Assessment for Security in Aviation Cyber-Physical Systems. In this paper, author present a vulnerability assessment framework that could be used to assess and prevent cyber threats related to wired and wireless networks and computer systems. We have performed vulnerability assessment tests for aviation systems including data loaders and in order to meet aviation industry requirements for wireless network security. Our contributions include detecting Cyber vulnerabilities in these aviation systems by using vulnerability assessment and penetration testing tools such as Metasploit Pro and Back Track and improving security and safety of aircraft. Based on our test results of Cyber vulnerabilities, the corresponding solutions will be developed to fix these vulnerabilities. New vulnerability assessment tests will be conducted again until our solutions are secure and safe to use. Some results of our vulnerability assessment tests against our software-hardware products are presented [12].

### *E. Paper 5: Situation Assessment to Secure IoT Applications.*

The fifth approach is Situation Assessment to Secure IoT Application. In this paper, author proposed situation assessment. IoT has provided a promising opportunity to build powerful industrial and enterprise systems that in turns offers conveniences and efficiency to achieve better quality of life. With the lucrative IoT benefits, also come new security and privacy challenges in terms of the confidentiality, authenticity, and integrity of the data sensed, collected, and exchanged by the IoT objects. These challenges make IoT deployments extremely vulnerable to different types of security attacks, resulting in insecure IoT environments. Therefore, it is necessary to carry out situation assessment to identify possible security risks to develop a complete picture of secure IoT deployments. In this paper, we present basic elements of IoT models and provide situation

 

assessment for IoT applications. Author highlighted the security enhancement measures for the IoT applications based on the three domains (local, transfer and data storage) of the IoT model. Trends within situation assessment for security area will be highlighted in addition to identification of niche areas where future efforts will be directed.

*F. Paper 6: AMELIA: An application of the Internet of Things for aviation safety.*

This paper presents AMELIA: Aircraft Monitoring and Electronically Linked Instantaneous Analytics as an application of the Internet of Things (IoT) for aviation safety—a safety critical use-case—from an edge computing perspective. AMELIA is a multi-layered edge computing system that automatically detects aircraft emergencies, and only transmits relevant data and information to enable quicker and more efficient response to emergencies. We describe a prototype of AMELIA to illustrate, explore, and motivate the potentials of the IoT for aviation safety, and lay a foundation for the design of diverse high-impact edge computing systems on the IoT. AMELIA acts as a delay-tolerant one-way node. Unlike passive devices, such as the aircraft's data and cockpit voice recorders, that only store voice and aircraft data, AMELIA implements an active aircraft's data recorder that can intelligently transmit data when necessary [4].

*G. Paper 7: On-demand security configuration for IoT devices.*

IoT, as one of the main focuses, links various kinds of devices to the Internet and even exchanges its data. The advent of IoT which has vast number of connected devices enables us to monitor and control of real world and changes our daily lifestyle never available before. With such a massive number of devices, if we don't set and organize security features on them properly, we will face inexperienced challenges on security issues. In this paper we propose the on-demand security configuration technique that we can configure required security functions and reorganize them without recreating device image. With the help of this approach, if there is a change on this security service, we can substitute the old modules for new ones without regenerating device image [2].

*H. Paper 8: Remote security management server for IoT devices.*

Internet of Things (IoT) devices are exposed to many security vulnerabilities and various security threats because they are resource-constrained and heterogeneous devices are interconnected to provide various application services. In this paper, author proposed the functional architecture of remote security management server to improve security and safety of IoT devices in the IoT environment [8]. The remote security management server provides and manages various security functions integrally and systematically. Accordingly, various infringement incidents that may occur in the IoT environment can be prevented in advance, and damage can be minimized by enabling quick and effective countermeasures even if a severe attack occurs. The Mirai Distributed Denial of Service (DDoS) attack in the United States in 2016 is a typical example of an attack on an IoT device that has been infected by malicious code. The Mirai DDoS attack uses the default ID password (ID/PW) set at the time of shipment, so it can be easily infected with Mirai malicious code and cause large DDoS attack traffic [14].

*I. Paper 9: Securing IoT Devices and Securely Connecting the Dots Using REST API and Middle-ware.*

Internet of Things (IoT) is a fairly disruptive technology with inconceivable growth, impact, and capability. Author present the role of REST API in the IoT Systems and some initial concepts of IoT, whose technology is able to record and count everything. They as well highlight the concept of middle-ware that connects these devices and cloud. The appearance of new IoT applications in the cloud has brought new threats to security and privacy of data. Therefore, it is required to introduce a secure IoT system which doesn't allow attackers infiltration in the network through IoT devices and also to secure data in transit from IoT devices to cloud. They provide the details on how Representational State Transfer (REST) API allows to securely expose connected devices to applications on cloud and users. In the proposed model, middle-ware 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 [3].

*J. Paper 10: Low Power Data Integrity in IoT Systems.*

Devices in the IoT produce large amounts of sensitive data. However, the use of the public Internet for data transfer by IoT devices makes them susceptible to Cyber-attacks. Among these attacks, data tampering or modification attacks to disrupt or bias the states of applications using these data may result in widespread damage and outages. To detect such attacks, this paper proposes an efficient and simple technique to detect data tampering in IoT systems. The proposed mechanism uses a random time hopping sequence and random permutations to hide validation information. They also present a formal security analysis of the proposed protocol. Performance analysis of the proposed protocol shows that it has low computational complexity and is suitable for IoT systems [6].

## V. PROPOSED MECHANISM

We proposed three phase authentication mechanism for commercial aviation. Three phase authentication mechanism provide strong security to commercial aviation. Fig. 6 depicts three phase authentications; it shows three phase of authentication mechanism. Phase-1 covers whole premises of commercial aviation. Phase-2 covers Airport's inside premises including runway. Phase-3 covers aircraft's premises. Each phase of authentication mechanism is unique and each and every entity pass through this phase while entering in commercial aviation premises. If any device meets 1st phase of authentication, then only it can eligible for further phase of authentication.

First Phase of authentication consist Web-Application-Firewall (WAF), Which covered whole area of commercial aviation including outside as well as inside the airports. Second Phase of authentication covered by Management unit (command and control centre), C&C monitor and grant access to smart devices and provide specific access inside the airport premises. Third phase of

 

authentication take place at the time of entering in particular commercial aircraft. Below we explained phase-wise authentication mechanism.

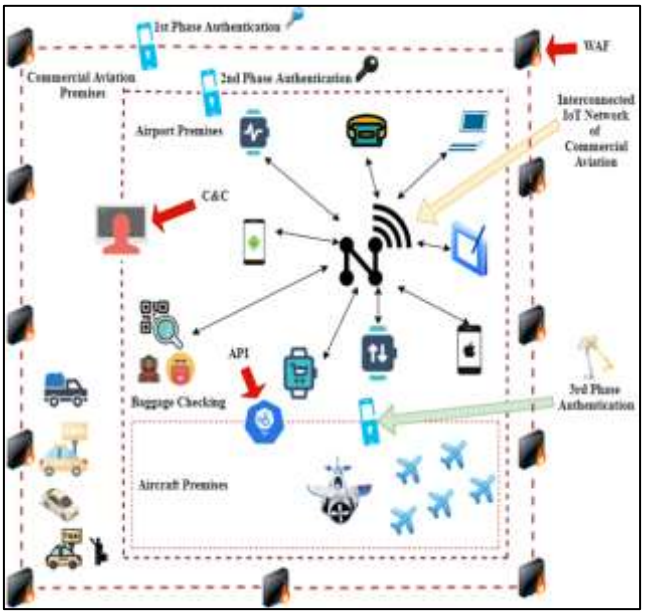


Fig. 7: Three-Phase Authentication

### A. *First Phase Authentication:*

First phase of authentication to secure commercial aviation through WAF. WAF configured with list of rules and policies. If any unauthentic device trying to entering in commercial aviation network then it can't able to gain access. WAF secure entire network of commercial aviation's premises. This authentication phase protect network and connected smart devices from attacker (Who trying to gain access from outside the commercial aviation). WAF is one type of reverse-proxy, its protect server from exposure by having clients pass through the WAF before reaching the server.

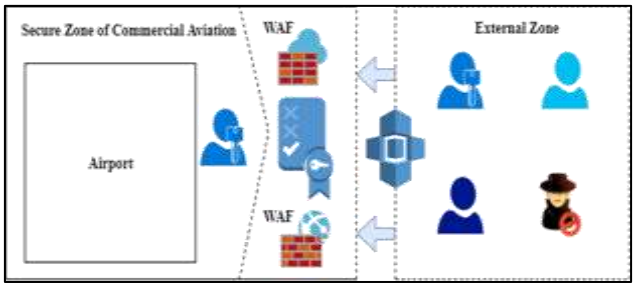


Fig. 8: Web-Application-Firewall

### B. *Second Phase Authentication:*

Second phase of authentication covered inside premises of airport's including runway. This phase of authentication governed by command and control centre. C&C grants appropriate access to passenger's devices as well as other devices which entered inside the airport premises. All passenger get access as per his/her business class, economy class, services assigned by specific aircraft's service provider, etc. Simultaneously airport's staff as well as airport's stalls, etc... are under monitoring of C&C.

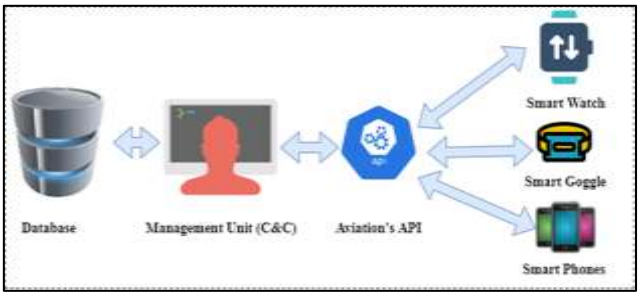


Fig. 9: Management Unit (C&C)

### C. *Third Phase of Authentication:*

Third phase of authentication covered inside the aircraft. This phase of authentication takes passenger's device subscription and shared credential as per class (Business class, Economy class, etc.). Key manager distribute credentials and scope of credential depends on class and services. This authentication phase recognizes the passenger and on basis of reorganization, passenger's device get access to resources. Unauthorized user can not able to gain access of resources. This authentication phase restricts multiple devices from single passenger as well as crew member and other staff. Authenticate crew member and staff can easily provide granted services to specific passenger on demand and authentic passenger can avail granted service using his/her device.

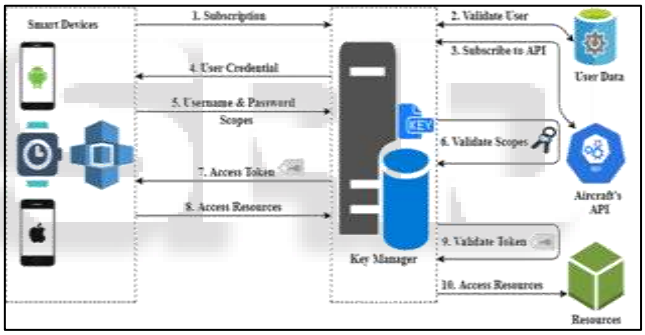


Fig. 10: Key management and User credential

## VI. ANALYSIS SUMMARY

Three-phase authentication mechanism secure commercial aviation phase-wise.

1) 1st Phase cover whole premises of commercial aviation through web application firewall (WAF). WAF is the first phase of defense between the device and the internet traffic inside the commercial aviation. Configured with list of rules and policies. It restricts unauthorized device to gain access. WAF monitors and filters internet traffic and stop malicious requests. WAFs are deployed as hardware devices, software application, both and operate with a specific set of rules and policies. WAF protects from various Cyber risks like, Cross site forgery, cross site scripting (XSS), SQL Injection
2) 2nd Phase cover inside premises of commercial aviation through command and control center. C&C monitor all device and grant required access to specific devices. If any malicious activity take place inside the commercial aviation then C&C can able to take action over activity. C&C provides up to the mark security inside the commercial aviation, as continuous monitoring ongoing.

 

3) 3rd Phase cover inside the aircraft's services. Specific passenger gain access as per their class (Business class, Economy class, etc.). Legal device only authenticates inside the aircraft's, passengers as well as aircraft's staff can only able to use register devices. This phase of authentication secures all activities, which take place inside the aircraft.

## VII. SUMMARY OF TECHNOLOGY

| Sr. No. | Phase | Premises | Technology |
|---|---|---|---|
| 1 | WAF | Entire Commercial Aviation | Network based WAF |
| 2 | Aviation API | Inside Airport | Hybrid API (Angular) |
| 3 | Aircraft's API | Inside Aircraft | |

Table 1: Technology Detail

### *A. Network-based WAF:*

There are basically three types of WAF, Host-based, Network-based and Cloud based. Among these, Network-based WAF is slightly expensive than other. But network-based WAF is more secure comparatively other options. A network-based WAF is hardware-based firewall. It is installed locally and it can minimize latency, but network-based WAF require the storage and maintenance of physical equipment.

### *B. Hybrid API:*

Command and control centre (C&C) manges inside airport's IoT devices. C&C gives permission to access resources and monitoring activities inside the airport premises. Using angular and Node JS, API configuration will be done. Similarly, aircraft's API also configured using angular and Node JS.

## VIII. CONCLUSION

In this paper, we studied challenges to mitigating Cyber risks in IoT-based commercial aviation. Authentication is most important aspect of security and privacy. We proposed Three-Phase authentication mechanism for IoT-based commercial aviation. Proposed authentication mechanism establishes effective security and privacy from various types of Cyber risks (Like, Trapdoors, Trojans, DDoS, Backdoors, etc.). Proposed authentication mechanism secures all over premises of commercial aviation including aircraft. IoT-based commercial aviation become smarter but security is major concern in it's, so more attention needs to implement this technology. Proposed authentication mechanism can be costly but Cyber security must be primary goal while any commercial aviation adopts IoT.

## ACKNOWLEDGEMENT

This research work would not have been possible without the support of Marwadi University, Rajkot and Einfochips—An Arrow company, Ahmedabad. I am especially indebted to Dr. Nitul Dutta, HoD of the Department of computer engineering-PG, Mr. Alok Bhatt, Techanical Lead (Aerospace BU—Einfochips, Ahmedabad) and Mr. Manish B. Patel, Delivery Manager (Aerospace BU—Einfochips, Ahmedabad) who have been supportive of my career goals and who worked actively to provide me with the protected academic time to pursue goals

## REFERENCES

[1] A. 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] 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.
[3] 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
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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
[12] 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.
[13] 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.
[14] 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. 1162-1164.



 