Challenges and Opportunities of Integrating, and Securing IoT technology in public places

Zina Abohaia, 20194621@ug.buid.ac.ae

Security

Security, and in particular, cybersecurity, is the current focus of the century. As mentioned by Lykou, Anagnostopoulou and Gritzalis (2018), “Cybersecurity is becoming a key enabler for safety”, and so how do we protect information exchanged by IoT devices from leakage? How do we protect data on IoT clouds or devices from being hacked, or stolen? Just like that we see how necessary it is that, as stated by Koroniotis et al. (2020), “the development and configuration of effective security tools to detect attacks and mitigate them is crucial to protect IoT networks”.

IoT has the ability to connect devices seamlessly, and so we need to revise existing cybersecurity solutions to be able to address new threats, as well as detect and solve existing threats (Koroniotis et al., 2020). How do we ensure the safety of passengers using IoT? How do we secure busy areas such as in airports, rail stations, or ports using IoT? These are only a couple of the questions we have sought to answer in this section.

Lykou, Anagnostopoulou and Gritzalis (2018) lists the five main threats caused by IoT:

* Network and communication attacks: These include jamming signals, Denial of Service attacks, which disrupt the airport’s system, that may result in delaying and cancelling flights, loss of trust of customers, damage to the airports’ reputation, and financial damages.
* Malicious software: Malware may compromise an airport’s devices as well as passengers’, and have a huge impact on an airport’s infrastructure.
* Tampering with Airport Smart Devices: This includes unauthorized modification of data, tampering with it, deleting it, or corrupting it. This type of security attack may lead to attackers gaining control over an airport’s system, and may result to physical safety breaches and great damage to an airport’s system.
* Misuse of Authorization: This includes attackers taking part in credentials theft of employees, and using it to misuse their privileges, damaging the airport’s assets.
* Social and Phishing attacks: Includes social engineering to manipulate people to perform actions given by the attacker, and they can infiltrate the system using employee’s accounts.

Some of the countermeasures or resilience measured proposed by Lykou, Anagnostopoulou and Gritzalis (2018) are:

* Attack detection
* Classification and response tools
* Block illegitimate traffic
* Reporting malicious attacks to IT, and any affected stakeholders
* Effective contingency to be planned
* Update software and hardware on time
* Monitoring systems and log files
* Train IT staff to isolate infected systems, remove them, and recover from the experience
* Provide backup systems
* Train all employees in basic security awareness
* Provide redundancies by keeping legacy systems at standby
* “Incident response capabilities for security staff should be developed and regularly tested”

As noted by Koroniotis et al. (2020), security frameworks have the following in common: Understand the environment and its context, identify, analyse, evaluate, mitigate and monitor risk. However, to eliminate human error, they have studied the effectiveness of an AI cybersecurity tool, with applications in IDS, Firewalls and anti-malware, threat intelligence, risk assessment, and ai-enabled cognitive security.

Furthermore, the terrorist attacks occurring in public places have pushed “the development of new automated solutions to spot and notify possible menaces as fast as possible” (Santamaria et al., 2019). They have explored the use of a decentralized architecture for IoT, including mist computing, and adding computational modules to objects that compose a system to reduce the load on the cloud. They have observed a maximum of 30% increase in efficiency, and a minimum increase of 5%. This proves that there is potential for automated solutions, and that it may offer a lot of new opportunities to enhance security.

Gaba et al. (2020) proposes a cybersecurity measure in distributed smart environments, robust and lightweight authentication (RLMA) to achieve mutual authentication and session key establishment, message integrity and freshness, lightweightness, and safeguard to popular attacks between authorized devices. This method makes sure that only authorized devices are connected, reducing computation and communication complexities. The research includes mathematical and informal proofs which support this application. It would be very interesting to see it actually applied and used one day.

The following table summarizes the points researched by Koroniotis et al. (2020):

|  |  |  |
| --- | --- | --- |
| IoT technology | Risks | Existing solutions |
| RFID | * Cloning * Eavesdropping * Attacks use false data to interact with device * Deactivation attack | No completely existing solutions; proposed ones are either too expensive, the resources are not available, or partially vulnerable. |
| Bluetooth | * Information stealing * Device takeover * Eavesdropping * Man-in-the-Middle (MITM) attacks * Denial of Service attacks | Only security tips such as keeping devices in proximity, turning off bluetooth when not needed and not sharing sensitive information over bluetooth (Cybersecurity, 2022). |
| LoRaWAN | * Denial of Service attacks * Replay attack * Wormhole attack * Power-draining attacks * Attackers can hack the system and use the keys by using the physical nodes | As long as its keys are kept secure, and there are sufficient resilience measures in place, it should be quite secure. |
| ZigBee | * Denial of Service attacks * Ghost-in-the-zigbee attack * Wormhole attacks | key establishment, key transportation and frame protection via symmetric cryptography (Zigbee Security 101 (Non-5G IoT Connectivity Options), 2022). |

Santamaria et al. (2019) discussed how object detection could be used as a security measure in public areas. They proposed a decentralized system to use surveillance systems such as surveillance cameras, and unmanned vehicles to sense and detect objects, and a system to analyse the images (a processing layer), reporting back to the human to confirm the action to be taken.

Another measure that could be taken and enhanced in the future is discussed by p-risk, which is passenger risk assessment to reduce security checking times, enhancing the passengers experience, and correctly deal with any threats. Their classification had three levels: “known, ordinary, and dangerous targets”. The system was built on getting information in real-time using IoT, machine learning, group decision theory, improved analytic hierarchy, the user’s credit, and much more.

These are just some of the examples of how IoT could be used to secure public places, and there certainly is a lot of room for future work such as improving current solutions and security measures, and enhancing their performance (Koroniotis et al., 2020).

Integration and innovative IoT applications

Both Adetayo O. and Feyisola O. (2021) and Pacios Álvarez, Ordieres-Meré, Loreiro and de Marcos (2021) emphasized that the greatest challenges to fully integrating IoT are user awareness and the lack of skills of stakeholders. Adetayo O. and Feyisola O. (2021) has observed that there is an association between employee’s, specifically marshals’, awareness of IT and both their acceptance of an integrated IoT system and their opinion that this system is a threat to their job (will result in their unemployment).

Pacios Álvarez, Ordieres-Meré, Loreiro and de Marcos (2021) made it clear that the “main limitation is the lack of skills of all stakeholders”. Also, Adetayo O. and Feyisola O. (2021) used behavioural science to state the importance of a “positive attitude needed for an ICT system to be successful” and that employee’s perceived usefulness and ease of use of a system greatly affects how they interact with the system. Therefore, we see the necessity to make sure employees are properly educated in ICT, and that they receive a thorough training in whatever the system they’re using. Developers should also aim to make systems as straightforward as possible, especially if they are meant to be used by people who aren’t developers.

Lei, Niu and Zhang (2017) saw an opportunity for integrating IoT in high rail stations (HRS) to reduce waiting times, and improve waiting room management. They aimed to integrate “train management, station capacity management, waiting room management and passenger flow management” using “information exchange and heuristic algorithms”. Their case study was successful and it reduced waiting times significantly.

It is important to find the best way to manage these limited spaces that only get more crowded every day, and digitalization and IoT have a big role to play in that. However, it also highlighted another major challenge in research related to integrating IoT and that is that they don’t test their methods, programs, and algorithms using data gathered in real-time.

There is also a rise in papers that research integrating IoT into the production process, and into the maintenance of ports and roads. Göçmen (2021) discussed the use of an automated robot in the baggage handling system. The robot is tasked to take the baggage from the conveyor to the gate, safely, avoiding any obstacles or objects in its way, using an artificial intelligence algorithm. This contributes to an airport’s logistics zone, a busy area, and one where error is not an option. A smart logistics zone still requires a lot of research to be fully planned.

As an example, for how IoT can be used in maintenance, Pacios Álvarez, Ordieres-Meré, Loreiro and de Marcos (2021) discussed opportunities in airport pavement management, integrating between building information modelling (BIM), IoT, and distributed ledger technology (DLT). The research focuses on how digitalization can help control and supervise road pavement and other refurbishments at airports. The model has to go from measuring all factors, to planning and coordinating the work done. Such a system would also be able to accommodate external factors using forecasts, or predictive models, to plan the maintenance as accurately as possible.

Talking about forecasts, Tascón and Díaz Olariaga (2021) proposed a system dynamics approach to forecast air traffic, and how it can be used with IoT. Forecasting would be much more accurate if historical data was recorded using IoT, instead of by employees, since that eliminates human error. Forecasting air traffic helped the airport expand runway by runway, when it was necessary. As I mentioned in the previous paragraph, forecasting that would play into the maintenance and improvement of the airport.

Faisal, Fatihah, Aprilia and Wiliyanda (2020) took the application of IoT, and its integration in a different direction. They researched the potential of smart airports as tourist attractions, and what factors in a smart airport would attract tourists most. The airport they chose for their study didn’t have all the smart airport applications, however, they showed that it is possible, and that it is an experience passengers enjoyed. Raising customer satisfaction, raises the airport’s reputation, and the chance that more planes and people would pass by there, working towards the increase in tourism and economy of that country. It is an application that has the potential to attract people to use smart airports, and help them accept the integration of IoT.

The next application presents an opportunity to measure the environmental impacts of ports, all in one index. The research done by Široka et al. (2021) aims to make smart ports more sustainable, and integrates IoT by using the data taken from its sensors in real-time and analysing it to update the ports’ environmental index. The index suggested takes into consideration air, “noise, light, and odor emissions, waste accumulation, and water pollution”. It also includes indices to other indexes. There has been a great recent interest in sustainability, and using eco-friendly items, and IoT has the chance to be a great player in that.

The final application I would like to discuss is an IoT framework developed by Kusuma and Tseng (2020); It seeks to support the whole maritime industry by including and accommodating all stakeholders: “port authorities, shipping companies, commodity products companies, and government officials (with their different policies in each island region) including customs officials”. They framed their solution as a mobile phone’s application, and found improved service process performance with IoT. For countries with many ports, this type of integration of IoT could simplify their services, increase customer satisfaction, and reduce processing times.

Conclusion

After analysing, and reviewing the available research and applications, we have found that we do not have the necessary skills and resources to research the security of IoT, or AI-based security. However, we are very interested to do research in this field, and once we have the skills and resources available, we will pursue it.

As we have seen, integration is a very strong theme, and so is catering to stakeholders. Therefore, the project we want to pursue further is developing an application that links all airport stakeholders, from passengers, employees, to the government, and use IoT to develop a smart airport model that communicates with the aforementioned application.

In our smart airport model, IoT will be used to manage and check resources, schedule maintenance of runways, janitor optimisation, locate employees and passengers, manage waiting rooms, boarding gates, baggage movement from check in to gates, as well as risk assessment of passengers and objects. These are just a number of the things we want to include, and using the application and biometric IDs, each stakeholder will have a different access level.

We will also use the research we reviewed here to choose the suitable IoT technology for each application, and the best topologies to optimise transmission times, as well as efficiently use networks. We will also seek to improve current applications of smart airports, and take the financial side of things into consideration in our research.

Table of paper reviews

Defining statement is our conclusion summed up in one sentence, from reading the paper. The rest are all from the papers and our analysis of them.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Research | Defining statement | Premise (Main Points) | Methodology (If relevant) | Future Work (If mentioned) | Limitations |
| (Široka et al., 2021) | “Get information in real time using integrated IoT technology and use it effectively” | Research proposed a Port Environmental Index (PEI) to integrate pollution factors in one assessment using IoT to assess environmental impacts of port operations in real-time. | Used a statistical toolbox, namely normalization, and the PIXEL platform to show how information reads to PEI.  Assumption used: “Management of port is conducted in a centralized fashion”. | Since there is no one standardized practice, the researchers see that this can be still used, and improved on for each practice. | There isn’t a standardized practice and here are data sharing concerns (security, privacy, and business). |
| (Faisal, Fatihah, Aprilia and Wiliyanda, 2020) | “Smart Airports as a Tourist Attraction” | Research studied how smart airports model as a tourist attraction, and use interviews and observations to show the effectiveness of this model, and suggestions on how to improve it. | Used a data analysis tool called triangulation on data from interview with airport managers, passengers, and public through observation. | They gave suggestions such as adding a sign to where self-service machines are, and to study the model then. As well as suggesting doing a more systematic study. | This study lacks the data used to reach conclusions, and its analysis of it. It also conducted the study in an airport that does not include all the self-service options now available, only one or two in each category.. |
| (Koroniotis et al., 2020) | “Solutions and suggestions for IoT networks and their security” | Research discusses how augmentation and automation creates risk and security threats, and suggests adopting and developing AI cyber defence techniques. | Analysed research published on the topic, highlighting the limitation of each, and why this research was necessary. Discussed different IoT technology (RIFD, Bluetooth, LoRAWAN,..) and their security issues, as well as providing a {comprehensive risk profile}. | - Zero-day vulnerability detection  - Designing of secure network architecture- Passenger owned smart devices as attack vectors  -Effectiveness of rule-based cyber-defence tools | For its defined premise, I have not found any limitations. All the information is analysed soundly, and written in a detailed, clear manner. |
| (Lei, Niu and Zhang, 2017) | “Information Integration is capable of maximizing High Speed Rail (HSR) stations” | Research proposes a systematic approach to facilitate passenger flow in HSR stations by utilizing waiting room capacity, and minimizing passenger walking distance, in the form of an integrated app. | Uses Information exchange, and heuristic algorithms, and outlines steps of the integrated approach. | Benefitting more from IoT by efficiently using real-time data, and “IoT intelligent railway management system” | Data used in research was not real-time data, but observations and historical data. |
| (Adetayo O. and Feyisola O., 2021) | “Raising Awareness of ICT leads to greater success and acceptance of technology” | Research investigates Marshals’ acceptance of a Visual Docking Guidance System (VDGS), discussing the visual docking system’s technology, behavioural science, and the steps to be taken. | Used Null hypothesis using Chi square test to find associations between the factors explored, which data was collected by interviewing the Marshals’. | -Association between Marshal’s awareness about ICT and: their opinion that technology is a threat to their job, and the acceptance of the system.  The above associations, as well as additional ones support the findings and recommendation that a “positive attitude is needed for an ICT system to be successful”, thus they recommend studying the effectiveness of educating people about ICT, and awareness of VDGS | The sample size was not big, only 20 people surveyed. |
| (Tascón and Díaz Olariaga, 2021) | “Air traffic forecast is essential to determine an airport’s needs” | Research explored how system dynamics can be used to forecast air traffic. | Uses correlations indexes and system dynamics causality diagrams to analyse and study different inputs. | To have more applications in forecast using system dynamics. | Only have data for a couple of years of one airport so should be made on a bigger scale to be more accurate. |
| (Göçmen, 2021) | “Smart baggage transportation system using an autonomous robot” | Research studies how “a well-functioning transportation system improves operations efficiency and passenger experience”. | Uses analytical hierarchy process (AHP) and fuzzy interference system (FIS). Implements {international standards}  + smart logistics | Examine the effect of covid on airport processes, and to explore different scenarios to reduce human-to-human contact. As well as the “social and cultural aspects of smart airport applications” | Simulation tests have not been done, and so this is a main limitation until the system is tested |
| (Hiekata et al., 2020) | “Impact of different combinations IoT technology in maritime industry on profit, number of incidents, and delay time” | Research compared IoT technology for carrying out certain tasks in the maritime industry, and concluded that the weight of a ship is the greatest factor affecting profit, while controlling the damage of a ship’s haul by operative is the most important factor for safety. | Used a simulation to evaluate the different IoT technology tested, and checked different combination of IoT technology and their effectiveness. They also carried out quite a useful sensitivity analysis, encompassing all the different factors. | There was no consideration of cost of introducing the technology, but the main limitation is the research’s focus on just one ship. Furthermore, the researchers set the parameters of IoT technology. | How market uncertainty (for example fuel price) would affect shipping systems, as well as developing models that take environmental impact (like from reducing GHG emissions) into consideration. |
| (Kamolov and Park, 2019) | “A dedicated IoT-based system for automating linkage procedures by searching for available locations via port-mounted sensors and planned ship notification”. | | Used smartphone as an alternative to the client-side vessel of the system. Included scenarios, outlined IoT layers, compared using WiMAX and LTE for network layers, implementation and experimental requirements, as well as examples. | They proved that the sensors can work, and communicate, however they have not proven how it is better than other working systems. | They plan to expand the system especially with “an automated ship reporting system”. Also, study “big data, and cloud solutions for smart ships and smart ports”. |
| (Kusuma and Tseng, 2020) | “An integrated IoT framework in the form of an app to support maritime highway and stakeholders” | Research discusses why a good, integrated, system is needed in a ports hub such as Indonesia, as well as the history and other examples available of similar systems.  App on play store to include shipping companies, port authorities, government, consumer external, and freight operators. | Compares maritime transportation between different countries, implements Enterprise Resource Planning (ERP), and IoT architecture used. | The major implication they faced was that not all data can be freely shared and accessed, and so this is a huge obstacle to the project. | The development of IoT will encourage better data protection practices that can then be used in the integration of the app. |
| (Pacios Álvarez, Ordieres-Meré, Loreiro and de Marcos, 2021) | “Integration of stakeholders is a step forward but the lack of skills of stakeholders is the main limitation” | Research explores how digitalization can help control and supervise road pavement and refurbishments at airports, and how Building Information Management (BIM) and Distributed Ledger Technology (DLT) provides the right opportunities for digitalization in construction. | Conducts analysis using use case, and explains the integration of BIM and IoT well, and highlights the requirements clearly. Proposes BIM deployment with general APMS included. | Has not been tested, so there is no proof for its success or effectiveness. However, it is a proposal worth considering. | Establishing a strong and standardised procedure to fully take advantage of information collected from stakeholders and integrate and use it effectively. |
| (Chen et al., 2021) | “Passenger security assessment using IoT and ML to reduce security check times” | Research develops a passenger integrity system based on the basic information of passengers and their related credit system using 5G-IoT devices to monitor passengers in real time. | Machine Learning (ML) analyses passengers’ risk level and integrates improved analytic hierarchy process (AHP) with group decision theory GD-AHP. Classify passengers into known, ordinary, and dangerous, and accordingly decide security check times, and improve passenger experience. | Results of the simulation used was not clear, despite the mathematical proof used was very clear and went into great depth to explain the factors, and methodology. Also, the sample used was relatively small. | There is not a sufficient number of materials that can be used to evaluate passenger risk grade factors, and there are even less implemented. Therefore, the system can be further studied and improved. |
| (Gaba et al., 2020) | “RLMA is an efficient security measure that can be used to increase the security of IoT devices” | Research focused on how Robust and lightweight mutual authentication (RLMA) can be used to ensure that only authorized devices are being connected, reducing computation and communication complexities. | Analysis of security breaches, and related works, as well as outlining security goals. Their proposed scheme is introduced, and theoretical proofs are used to show how they are more secure to other frameworks. | Using a simulation would’ve given more proof onto how RLMA is effective against security breaches. | To expand it from device-to-device to also be used between users and devices in IoT. |
| (Lykou, Anagnostopoulou and Gritzalis, 2018) | “Malicious threats and their motives” | Research reviews the implementation rate of cybersecurity measures, malicious threats due to IoT, threat mitigation actions, as well as malicious attacks motives, concluding that lack of security awareness is the greatest risk, then internet connectivity. | Preform risk scenario analysis for IoT malicious attacks with threat mitigation actions, as well as a detailed malicious threats analysis. Also perform an online survey in different airports, to analyse the greatest risks to security. | There were no notable limitations; the survey had a sufficient sample size, and the analysis and subsequent explanation were extensive. | Research proved the need to educate IT experts, passengers, and airport personnel on cybersecurity areas, and risks posed by IoT. |
| (Santamaria et al., 2019) | “Using a decentralized architecture with IoT to detect unusual objects in certain areas, increasing security” | Research studies the use of a decentralized architecture to manage patrolling drones and cameras exploiting lightweight protocols used in IoT, using mist computing, to detect unusual objects. | Use computer vision algorithm to recognize unusual objects, and analyse its correctness by the different shapes and colours of objects, and use mist computing to reduce the latency between end devices and computational modules. Furthermore, they analysed average detection time and how it changes with the number of consecutive frames, as well as the latency between cloud and edge detection. | There were no notable limitations, however there were some obstacles that resulted in the worst case for increase in efficiency to be 5% while the maximum increase in efficiency is 30%. | Focus on the development of embedded hardware to improve the efficiency of the detection system. |
| (Building a Connected, Smart Port of the Future, 2018) | “Smart ports are safer and more efficient in profit and in time”. | Research focused on how IBM and Amsterdam use IBM cognitive IoT technology in the production process, which uses a robotic welding arm to apply high-quality metal layer to create ship components. This saves money, and is more efficient since it ensures the maximum amount of cargo is used at one time, and reduces times. It also mentions digital dolphins and buoys that provide insight on berthing terminals, and water conditions to find the optimal docking time and place.  Statistics are included. | | References are not included which makes this article not reliable. | To include and integrate more smart technology in different parts of ports, and phases of the production processes in ports around the world. |

References

Široka, M., Piličić, S., Milošević, T., Lacalle, I. and Traven, L., 2021. A novel approach for assessing the ports’ environmental impacts in real time – The IoT based port environmental index. *Ecological Indicators*, 120, p.106949.

Faisal, F., Fatihah, A., Aprilia, S. and Wiliyanda, W., 2020. Smart Airport Model Implementation as A Tourist Attraction in West Java International Airport Kertajati. *Digital Press Social Sciences and Humanities*, 4, p.00008.

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P. and Janicke, H., 2020. A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. *IEEE Access*, 8, pp.209802-209834.

Adetayo O., A. and Feyisola O., A., 2021. Acceptance Of Visual Docking Guidance System By Ground Marshallers In Nigerias’ Airport. *International Journal of Advanced Networking and Applications*, 13(01), pp.4845-4854.

Tascón, D. and Díaz Olariaga, O., 2021. Air traffic forecast and its impact on runway capacity. A System Dynamics approach. *Journal of Air Transport Management*, 90, p.101946.

Lei, D., Niu, F. and Zhang, Y., 2017. An information integration approach for waiting room management in high speed railway stations. *Information Discovery and Delivery*, 45(1), pp.45-54.

Kamolov and Park, 2019. An IoT-Based Ship Berthing Method Using a Set of Ultrasonic Sensors. *Sensors*, 19(23), p.5181.

Pacios Álvarez, A., Ordieres-Meré, J., Loreiro, Á. and de Marcos, L., 2021. Opportunities in airport pavement management: Integration of BIM, the IoT and DLT. *Journal of Air Transport Management*, 90, p.101941.

Chen, W., Huang, Y., Yang, H., Li, J. and Lu, X., 2021. A passenger risk assessment method based on 5G-IoT. *EURASIP Journal on Wireless Communications and Networking*, 2021(1).

Gaba, G., Kumar, G., Monga, H., Kim, T. and Kumar, P., 2020. Robust and Lightweight Mutual Authentication Scheme in Distributed Smart Environments. *IEEE Access*, 8, pp.69722-69733.

Lykou, G., Anagnostopoulou, A. and Gritzalis, D., 2018. Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors*, 19(1), p.19.

Santamaria, A., Raimondo, P., Tropea, M., De Rango, F. and Aiello, C., 2019. An IoT Surveillance System Based on a Decentralised Architecture. *Sensors*, 19(6), p.1469.

*Material Handling & Logistics*, 2018. Building a Connected, Smart Port of the Future. [online] Available at: <https://www.proquest.com/docview/1993311072?accountid=178112&parentSessionId=NPyzCluz6aRg8rXL0MVXzAGKCFLLpZzCF4AYe7hKu0I%3D> [Accessed 2 February 2022].

Göçmen, E., 2021. Smart Airport: Evaluation of Performance Standards and Technologies for a Smart Logistics Zone. *Transportation Research Record: Journal of the Transportation Research Board*, 2675(7), pp.480-490.

Hiekata, K., Wanaka, S., Mitsuyuki, T., Ueno, R., Wada, R. and Moser, B., 2020. Systems analysis for deployment of internet of things (IoT) in the maritime industry. *Journal of Marine Science and Technology*, 26(2), pp.459-469.

Kusuma, L. and Tseng, F., 2020. IOT Framework to Support Maritime Highway Program. *Journal of Cases on Information Technology*, 22(3), pp.35-50.

Cybersecurity, A., 2022. Bluetooth security risks explained. [online] Available at: <https://cybersecurity.att.com/blogs/security-essentials/bluetooth-security-risks-explained> [Accessed 2 February 2022].

5G Security by Marin Ivezic. 2022. Zigbee Security 101 (Non-5G IoT Connectivity Options). [online] Available at: <https://5g.security/5g-security-privacy/zigbee-security-overview/#:~:text=Zigbee%20is%20considered%20to%20be,frame%20protection%20via%20symmetric%20cryptography> [Accessed 2 February 2022].