AI implementation in Airport System: A study of Vulnerabilities and Countermeasures

Seif Elsallamy
School of Technology
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
seifbook0@gmail.com

Nor Azlina Abd Rahman
Forensic and Cyber Security Research Centre
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
nor_azlina@apu.edu.my

***Abstract*— Many organizations are using the AI and IOT to make their operations run smoothly. The AIOT is even better since it combines technology and removes the burden of sending the data to be processed outside the IOT device. In this paper the focus will be on the Facial Recognition Cameras that are being used in airports and their ability to detect criminals and passengers who approach doing illegal activities. This technology saves time and effort to the airport employees and passengers and offers security. It might bring some concerns too, since the facial recognition data are biometric data, the passengers might be concerned about their facial data to be abused or sold or accessed by other organizations. In this paper the NIST Risk Management Framework will be applied to an airport organization which is using the facial recognition technology to verify passengers. Also, the Disaster Recovery Plan and Business Continuity Plan will be developed to such organization. The Top Ten IOT vulnerabilities from OWASP, that might affect the facial recognition application will be listed and detailed. Finally, a framework will be proposed to show the organization security and awareness, and eight security policies which have been selected from SANS policies templates will be listed and detailed**.

Keywords—component, formatting, style, styling, insert

I. Introduction

Many devices are now using Internet of Things (IOT) in variety of application (Abdulla et al., 2022; Kalilani et al., 2021; Murugiah et al., 2021; Rasheed et al., 2021; San et al., 2022; Singh et al., 2021). Those devices do collect data and send them to be processed and receive a response to take the next step. This great technology and the power it offers still have limitations. It is difficult to send huge amount of data for processing and get a response in a limited amount of time. Artificial Intelligence (AI) on the other hand has shown noticeable success in variety of areas as in language processing, speech, and image recognition. Combining those powerful technologies AI with IOT will create a technology that has more speed in decision taking which is called Artificial Internet of Thing (AIOT) (Zhang & Tao, 2021). In this paper the focus will be the implementation of face recognition technology in airports.

The Facial Recognition has been used in the last 10 years, there are 109 countries that has already implemented or approved to implement the technology in future for surveillance purposes. Bringing many privacy concerns with it (Surfshark, 2020).

Fig 1. show the statistic of facial recognition usage around the word while table I shows the status of facial recognition around the world. The statistic shows that the facial recognition is widely being used and very few being banned.

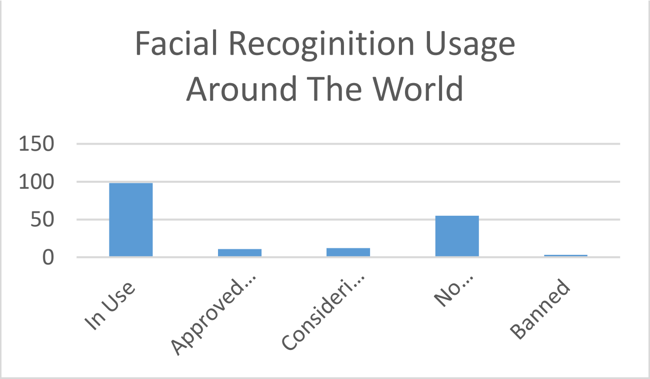


Fig. 1. Facial recognition around the world

TABLE I. Facial Recognition Status

Facial Recognition Status	*Number of Countries*
In Use	98
Approved To Be Used	11
Considering the Technology	12
No Evidence of Use	55
Banned	3

A. *Facial recognition implementation in airport*

In April of year 2019 MacKenzie Fegan did't understand what happened to her in the airport when she was able to board to the airplane without anyone checking her passport. She tweeted about the question that never left her head to JetBlue and indeed they replied that facial recognition was used instead of checking the travel document (Francesca Street, 2019), This technology can be used to capture criminals in airports. Even if they have a valid travel document, face recognition can be added as a secondary security mechanism.

B. *Technology*

The face recognition has been used in British Airways for more than 8 years and in the US for more than 20 years. It is used to monitor international travelers to not board on domestic flights. In the first security check the camera captures the face and creates a digital version of the face which is called a biometric template, it allows the programs to process the biometric data. When the domestic travelers enter their flight, another picture is taken by the camera. If the first and second pictures match by a certain level of accuracy, then the traveler is okay to board to the domestic flight. If both pictures don't match, then more measurements will be taken to verify the travelers. This technology allowed 240 travelers to board in only 10 minutes which has saved too much time and effort and allowed travelers to avoid crowdedness.

The process takes 2 seconds with an accuracy rate of 98%. The process is not compulsory if travelers are not feeling comfortable using such technology, they may be verified manually (Francesca Street, 2019). The benefits of AIOT are visible here, the time and efforts it saved with high level of accuracy, easier process for both the passengers and the workers and the safety and security it offers.

C. Concerns

San Francisco banned Face Recognition after the police identified the suspect in a crime using the technology (Conger et al., 2019). There were concerns about this technology since it can be abused by the police and other organizations. They might sell facial information to other marketing companies. Then instead of receiving notifications about products that interests you, you might find a salesman approaching you with a product that you were searching for in Walmart. Abusing such powerful technology by wrong organizations can be very costly for civilians. As an example, a company can use such technology to find for their clients a specific person by an image. This is currently possible in limited areas as airports, but in the future, it might be possible in larger areas as cities or countries. Such technology can be used to find children lost from their parents, and it can have many benefits, but it is too powerful to be fallen in the wrong hands. Using this technology should have strict and clear policies.

If a passenger in an airport refuse to be scanned by facial recognition, then there must be other options to verify the passengers' identity and the process should be easy for the passenger not complicated or requiring too much time than the face recognition option.

II. POSSIBLE VULNERABILITIES AND ATTACKS (OWASP TOP 10)

A. Weak Passwords

IOT devices usually come with default hardcoded passwords or weak passwords. The camera used to secure places can be a great security hole if it is left with the default credentials. Any attacker who joins the network which the cameras are connected to, might be able to connect to the web interface of the cameras using the IP address which can be easily found by network tools as Nmap. Then, by banner grabbing the camera's software version and searching for the default password on the internet, or by brute forcing the password. There are variety of things that an attacker can do after having access to security cameras. The attacker can abuse the service and spy on people, or he might be able to shut it down before further crimes.

B. Vulnerable Network Services

The network protocols that are used in the IOT devices can be insecure. It might be vulnerable to attacks such as buffer overflow or denial of service. A criminal might be able to exploit such vulnerabilities in a way that allows him to pass through the facial recognition procedure without being detected in the airport. The buffer overflow vulnerability allowing attackers to inject arbitrary code to be executed in the computer's memory. Which can give them unauthorized access to a system. The denial of service or (DOS) can be used to stop the service from running. Which also give a potential for a criminal to bypass the facial recognition scan.

C. Weak Ecosystem

IOT devices are usually controlled by cloud, backend API, web, or mobile interface. If an attacker can compromise those then he can control the device or a part of it. There are many vulnerabilities that might exist in each of them. The authentication, authorization and weak or no encryption and lacking user's input sanitization are the common issue facing such interfaces (OWASP, 2018). The use of such vulnerabilities can have different impacts, for example a SQL injection vulnerability in a web interface of the facial recognition camera can give the attacker all the data recorded by the camera which in this case are high confidential data.

D. Lack of Updates and Upgrades

The lack of updates or the failure to make an update securely through a secure connection as https, or the lack of validation of the firmware. For example, through hashing, or the lack of notifying the user of a new update (OWASP, 2018). This might leave the IOT device exposed to zero days. Suppose that the Facial Recognition cameras had a security update to secure it against a potential denial of service vulnerability that was just discovered few hours ago. The camera's manufacturer didn't properly design the cameras to be notified for new updates or it might even have been not designed to be updated at all. This might cause a security gap that will be getting wider by time.

E. Use of outdated components

The use of outdated programming libraries, hardware, software, or any vulnerable third-party component in an IOT device can cause it to be compromised. The components that have been used to build the IOT device should be up to date. For example, the IOT device might be using an older version of Linux which is vulnerable to attacks that has been discovered and fixed in the newer updates. The impact can be low to critical it is fully depending on what component has which vulnerability. Hikvision is a security camera which had a security issue, it was vulnerable to remote code execution through command injection CVE-2021-36260. This can allow an attacker to take over the device and maybe more devices from the network (Jessica Haworth, 2021). The outdated component here is the firmware, if the airport was using this type of cameras with the outdated firmware, then an attacker can compromise the cameras and do further attacks.

F. Lack Protection of Privacy

Stored users' data are used insecurely or without permission. The facial recognition information can be used in an insecure way. For example, transferring the facial scan results to the ecosystem with an unencrypted protocol. The data can be used in a way that it shouldn't. For example, it can be used to find the location of a specific person. The privacy issue is a concern to such technology, the passengers might feel uncomfortable using it and prefer manual process instead. The airport should be clear in the usage policy for such data. If the data fell in the wrong hands through unauthorized access or even through buying the data in a legal way, it might be abused.

G. Non-secure Data Storage and Data Transfer

Many IOT devices are found to be vulnerable to variety of attacks, and in many scenarios, there were few to no security mechanisms applied to such devices (Abdalla & Varol, 2020). Since IOT devices are using network protocols.

Then if a vulnerable protocol is used for communication this will give the opportunity to the attackers to use those weaknesses. If the non-encrypted protocol http is used to transfer data in the airport network to other devices, then MITM attacks can be used in such network. If an attacker succeeded in joining the camera's network, then the attacker can intercept the data. In current days there are many security mechanisms which are applied to minimize the MITM attacks. The data at rest should be protected through hard disk encryption.

H. *Lack of Management*

The lack of network monitoring and analysis of the network traffic and system changes and the lack of response to the found issues. These processes and procedures are necessary to find potential threats and respond to them. The Mirai Malware primary targets were IP cameras and home routers. It used them to make a botnet and launch DDOS attack using the botnet later. So, with monitoring any potential malware or threat can be noticed through the coming or the leaving traffic and through system changes. After the security if an analyst team finds a potential issue, the response team should start acting to remove the malware and to check how the malware accessed the device then to patch the weaknesses and make any extra necessary actions.

I. *Non-secure Default Settings*

Vendors might lock the settings while they are insecure so operators will not be able to change the settings even if they wanted to. Operators might keep the default settings as it, without doing any changes which gives a potential opportunity for the attackers to have unauthorized access. For example, the cameras' manufacturer name is XYZ, product name is ABC and the version is 2.9. By using search engine to search for this information the attacker can successfully find the default credentials for this specific camera. Any attacker in the network can easily connect to the cameras and control them in case the default password had worked. The attacker then can abuse it to spy on the passengers or to try to shut it down so, then he might bypass the facial recognition verification.

J. *Weak Physical Security*

The airport Wi-Fi is provided for the passenger as a service that might be connected to the security cameras' system as well. This can make a huge security hole because any passenger who connects to the Wi-Fi can then connect to the security cameras and the local network. First the attacker goes physically to the target and tries to find information about the technologies used then he leaves and continues the investigation with the information he gathered, then he might be able to compromise the network. For example, an attacker might go to the airport gateway and check the camera's type. Then leave the airport and search for security holes in this type of cameras. The attacker then finds that, this type of cameras is using Wi-Fi. Wireless devices mostly are vulnerable to jamming attacks because of their availability (Hossein Pirayesh and Huacheng Zeng, 2021). Then it will be vulnerable to DOS (Denial of Service) attack. The cameras should be wired to the network to decrease the probability of this attack from being happened.

K. *Application Specific Vulnerability*

Samsung are warning their users from facial recognition in their devices, and they are saying that it is less secure than pattern, pin, password, and fingerprint recognition. A high-resolution image can be used to unlock the Samsung device (Samsung, 2021). If such flaw exists in the airport cameras, a high-resolution 3D printed masks can be used to impersonate other passengers. This might allow an un-authorized access or to bypass security mechanisms designed by the airport. So, there should be more security measures in places since the facial recognition might not be enough to identify a person. The airport might check the travel document or the passport and visas and verify the information on them. However, that might take more time for processing the passengers' documents and all benefits gotten from the AIOT will be lost, so there should be a solution that is not very strict as checking and verifying all the documents after applying the face recognition and not very easy as only verification by the face recognition without checking any documents. The strict rate depends on the current stability of the country, if a country has a high crime rate, they might do more restrictions than a country with low crime rate. Old crime data can be analyzed to design the right parameters.

III. RISK MANAGEMENT

In this paper, the Risk Management Framework (RMF) by NIST has been selected. It provides risk management to security, privacy, and supply chain as an extension to the business operation. The efficiency and effectiveness have been considered in addition to the constraints due to laws, policies, business direction, business standards, orders of executives and organization approach. The RMF can be applied to all systems E.g., IOT or control systems, regarding of its size (NIST, 2021).

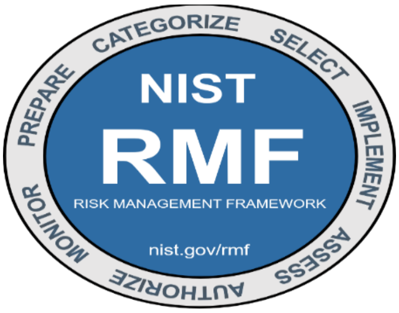


Fig. 2. NIST RFM (NIST, 2021)

A. *NIST Risk Management Framework*

Fig. 2 shows the NIST Risk Management Framework that consist of several stages as stated below:

a) Prepare: It is the first steps by organization to be able to manage the security risks, in this step the AIOT cameras should be installed. The devices that will be used to receive data from the camera should be prepared. The management systems should be installed.

b) Categorise: The data should be processed, saved, and sent according to its priority. If the cameras for example, identified a wanted criminal then this should have more priority than an international passenger who tries to get in a domestic flight.

c) Select: Select and document the necessary controls to protect the business and the system to handle the risk (The controls can be selected from NIST SP 800-53). Suitable controls for the technology should be selected. For example, face recognition can make the verification process in airports easier and safer, but does it invade privacy? Will people really feel safe using this technology? Wouldn't the passenger think that their facial data might be sold? So, there should be some controls in place to prevent that.

*d) Implement:*Implement the selected controls and make a documentation for the deployment.

e) Access: Verify if the controls are working as expected and generating correct outputs. Everything might look perfect, but the results might be different from the excepted or contain errors. For example, after selecting a suitable control to make the facial recognition an optional verification process for passengers. How then international criminals can be identified without scanning their faces?

f) Authorize: A senior official should verify that all the applied controls regarding security and privacy are acceptable. The system might still contain some flaws that only an expert can notice. So, after the system is ready to be used it should be authorized by a senior official.

g) Monitor: Keep monitoring and controlling the implementations that has been done to the system. The system might need hardware or software updates. For example, the cameras might be outdated and needs to be replaced by newer faster cameras. A security vulnerability affects a software which is being deployed so it must be updated.

IV. Recovery plan

A. *Disaster Recovery Plan*

There are two pieces of information that should be backed up in case of disaster. The first is the facial recognition data and the second is the results history of the verification process. Suppose that a criminal has been detected in the airport, but he was able to escape and then a disaster had happened. Then all the evidence will be vanished.

Businesses do need Disaster Recovery Plan (DRP) to survive disasters and continue their business with minimum losses. If an organization is not prepared for a disaster, it might destroy the whole business (Alhazmi & Malaiya, 2013). The disaster can be a natural one like an earthquake, tsunami, volcano or an intended one as ransomware which is a malicious software that can encrypt organization data or DOS (Denial of Service) attacks that can bring down the services. Each organization should select a suitable plan for their needs and the amount of money they are willing to pay in the selected plan.

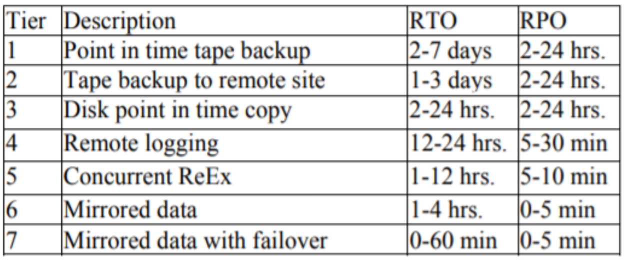
Backups are a copy of the data that the organization want to survive a disaster saved in a safe place. There are some parameters that the organization should select from and choose the most suitable values for their needs and for the money they are willing to pay.

B. *RPO & RTO*

RPO (Recovery Point Objective) answers the question, how much data can a business lose? E.g., If the backup is done every four hours, then there is a four-hour gap. If a disaster happened to the business, it would lose the data in the four hours before the disaster. So those 4 hours are the RPO.

RTO (Recovery Time Objective) answers the question, how much time does the business need to recover? The organization might take time to put everything into place. E.g., After a disaster had happened, the business needs some time to recover. So, this recovery time is the RTO. Table II shows detail of recovery plan levels.

TABLE II. Recovery Plan Levels (Alhazmi & Malaiya, 2013)



Tier	Description	RTO	RPO
1	Point in time tape backup	2-7 days	2-24 hrs.
2	Tape backup to remote site	1-3 days	2-24 hrs.
3	Disk point in time copy	2-24 hrs.	2-24 hrs.
4	Remote logging	12-24 hrs.	5-30 min
5	Concurrent ReEx	1-12 hrs.	5-10 min
6	Mirrored data	1-4 hrs.	0-5 min
7	Mirrored data with failover	0-60 min	0-5 min

C. *Cost*

Initial Cost, Storage Cost, and transfer Cost, those are the costs that the organization should consider while making their recovery plan. The Human-based Disaster vs Natural Disaster probabilities must be identified and linked with the cost for the best possible cost-efficient plan (Alhazmi & Malaiya, 2013).

D. *Bussiness community plan*

There are several reasons that can make the facial recognition out of service. the reasons don't necessarily mean a cyber-attack or a disaster, it might be some maintenance or an update or upgrade to the hardware or the software of the cameras. So, the obvious solution would be to do the verification manually by checking the travel document or the passport of the passenger. If the facial recognition is a must, then a high-quality image can be taken by a normal camera for the passengers then it can be added directly to the facial recognition algorithm when the system is up. According to (Samsung, 2021) a high-quality picture can be used to bypass facial recognition algorithm in mobiles, so they do recommend using the patterns, finger recognition and passwords instead, this was more detailed in the 'Application Specific Vulnerability' section.

V. Organizational Security, Awareness, and Information Sharing

A. *Operation security framework*

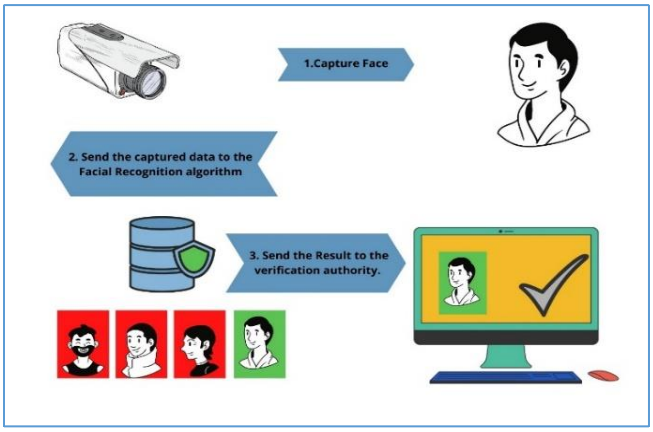

1.Capture Face
2. Send the captured data to the Facial Recognition algorithm
3. Send the Result to the verification authority.

Fig. 3. Operational Security Framework

There are mainly three steps in the proposed framework as shown in Fig. 3. However, there might be an extra step if the algorithm is running outside the camera device. Each of those steps and their security will be discussed in the following lines.

The first step is capturing the face, this step might be vulnerable to impersonation as was discussed in the "Application Specific Vulnerability" section. A passenger might wear a mask to impersonate someone else or a passenger can be able to do changes to their faces through makeup. So, they are no longer identified as the same person. There should be a replacement for the facial recognition as a part of the continuity plan and not because all users feel comfortable using this technology. The concerns are their biometric data to be abused or sold. The verification through face recognition only is not enough, but it can be used as a second security layer. However, the airport will not have its benefits which is saving up time and effort while verifying passengers if the technology has been used as a second verification method. So, there should be something in between. The airport should come up with not very strict processes to verify the users depending on the airport's country current security state. The verification process might be fully strict (by applying both face recognition and manual verification through checking the travel document) in case if a passenger is suspicious. This can be determined through his behavior which might need a specialized security person to notice or through checking the baggage, which might include something suspicious.

The second step is running the algorithm on the captured picture data. So, the camera changes the picture to biometric data and then it runs the facial recognition algorithm on it, there might be a third step if the camera is sending the data to another device to be processed. However, the camera is getting other biometric data from the database server which should be well secured against database attacks and its credentials should be encrypted. If an attacker can compromise the cameras, the information that can be extracted from them should be minimal. There should be a backup for the database as a part of the disaster recovery plan. Since disasters are rare, the managers do ignore it so a policy should be made for the managers to require them to give the appropriate time and effort developing the disaster recovery plan and to support it financially. The camera device should be well configured and all the default settings that are related to the security as passwords should be changed to secure ones. Since the cameras are holding the algorithm and the database credentials it is highly confidential. If an attacker was able to steal the algorithm source code, he might then try to reverse engineer it and to find how to bypass the verification system.

The third step is sending the result to the verification authority, which is a security person or a security group who should be well trained against social engineering. The process of transferring the result to another device should be well secured against communication attacks as using unencrypted protocols like ftp and http which should be totally avoided. If an attacker can connect to the local network. He might be able to intercept and modify the unencrypted traffic. Then, inject a fake result to bypass the verification process if one of the unencrypted protocols is in use. In case of social engineering, the employees should be well trained. For example, if a pregnant lady arrived at the airport late, and there are only a few minutes left for her flight, she might be able to bypass the verification process. Such manipulating methods are used by social engineers to use the time scarcity, sympathy, and other methods. The employees should be well trained to detect, react and to report any situation related to a social engineering attempt. Reporting social engineering attempts should be an easy process to allow the employees to report such issues as soon as possible. All those steps should be made in one of the organization policies.

B. Policies

The policies address the relationships of employees between each other and between them and the business assets and their behavior and what to do in some situations. It also puts constraints to restrict access to some places or to limit access. Eight business policies which are relevant to the Airport Security and Facial Recognition Cameras have been selected from (SANS, n.d.). SANS have many policy templates which are free to use for organizations.

1) *Pandemic Response Planning Policy:* This policy addresses the business continuity in case of pandemic, since the business continuity plan doesn't necessarily address the case of pandemic, so another types of trainings and procedures should be followed to assure the continuity of the business. In an airport how will the face recognition cameras deal with the face masks? What are the procedures that should be taken to verify someone's face? Who are the employees who can work from home and who cannot?

2) Information Logging Standard: It identifies the requirements for generating logs for auditing that can be integrated with the log management procedure. The logs from facial recognition cameras must be convenient with the log management system. So, then it can be added to other systems like SIEM for example. This will increase the usability of the logs to be adopted by other systems, policies, or templates.

3) Data Breach Response Policy: This policy defines the business objectives and gives an image to the breach response procedure. It defines the roles and responsibilities to prioritize the incidents. Also, it addresses the reporting recovery process. What process is to be taken if the facial recognition data has been compromised. How to recover, and what are the priorities. The data breach might include data other than the facial recognition data; it might include credit cards data for example. So, which one has priority over the other?

4) Disaster Recovery Plan Policy: Since disasters don't happen daily thankfully, the managers might not consider the disaster recovery plan. The policy requires from the management to support the recovery plan financially and to take the appropriate time and effort to design it. The airport should make backups for its important data as the facial recognition data. If any disaster happens to hit the airport's data center, then the airport can recover its data from the backup.

5) Social Engineering Awareness Policy: This policy defines guidelines to be followed against social engineering attacks. It provides awareness and gives the employees knowledge on how to detect such attacks and how to deal with them and who to contact from the organization. For example, if a pregnant lady has arrived late to the airport. She might bypass the verification processes. So, what should the employees do in such cases and whom should they contact.

6) Database Credentials Policy: This policy addresses the storage and access of database credentials. For software access to one or more of the databases in the company's network. If the software accessing the database does not store the credential properly, the database might be compromised. For example, the facial recognition cameras store the data into a database. This database needs a username and a password to give access to the cameras. So how would the cameras store the database username and password in non-clear text format?

7) Router and Switch Security Policy: This policy addresses the minimum-security configurations that can be applied to routers and switches in the company's network. Since the cameras would be connected to the local network, it must be well secured. If an attacker was able to reach a router's port, he might connect a device into it and get a local access to the airport's network. Then, he might try to enumerate the devices that are connected to the local network which includes the facial recognition cameras.

8) Wireless Communication Policy: Due to the spread of smart phones, tablets, and electronic devices in the last years, a policy should be made to address the wireless connectivity for only those who meets the standards to protect company assets from unauthorized access. Only the devices that meets the standards can connect to the wireless network. The facial recognition cameras might be connected to the network as well beside other network assets. An attacker might be able to compromise one of the employees' devices and then access the network. So, this policy only allows devices meeting the standards to connect.

VI. CONCLUSION

In this paper a framework has been proposed to show how the security operation might look inside an airport which is by using the facial recognition technology. Eight policies have been selected, listed, and discussed in detail from SANS policy templates. Top 10 IOT vulnerabilities from OWASP that might be faced by the organization have been listed and discussed in detail that is related to the facial recognition and the facial recognition system or application specifically. This paper also showed how a risk management framework can be applied to an organization and the development of the disaster recovery plan and the business continuity plan that needed by the organization.

REFERENCES

Abdalla, P. A., & Varol, C. (2020). Testing IoT Security: The Case Study of an IP Camera. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 1–5. https://doi.org/10.1109/ISDFS49300.2020.9116392

Abdulla, R., Haziq, M., & Noor, I. (2022). Smart IoT-based security system for residence. *Journal of Applied Technology and Innovation* , *6*(1), 18–23.

Alhazmi, O. H., & Malaiya, Y. K. (2013). Evaluating disaster recovery plans using the cloud. *2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS)*, 1–6. https://doi.org/10.1109/RAMS.2013.6517700

Conger, K., Fausset, R., & Kovaleski, S. F. (2019). *San Francisco bans facial recognition technology*. The New York Times, 14. https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

Francesca Street. (2019, October). *How facial recognition is taking over airports.* . https://edition.cnn.com/travel/article/airports-facial-recognition/index.html

Hossein Pirayesh and Huacheng Zeng. (2021). Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey. *ArXiv Preprint ArXiv:2101.00292.*

Jessica Haworth. (2021). *Zero-click RCE vulnerability in Hikvision security cameras could lead to network compromise*. https://portswigger.net/daily-swig/zero-click-rce-vulnerability-in-hikvision-security-cameras-could-lead-to-network-compromise

Kalilani, M., Shyan Lai, N., & Abdulla, R. (2021). IOT based neonatal incubator for the developing world and conflict zones. In *Journal of Applied Technology and Innovation* (Vol. 5, Issue 4).

Murugiah, K. van, Subhashini, G., & Abdulla, R. (2021). Wearable IOT based Malaysian sign language recognition and text translation system. In *Journal of Applied Technology and Innovation* (Vol. 5, Issue 4).

NIST. (2021, November). *NIST Risk Management Framework*. https://csrc.nist.gov/Projects/risk-management

OWASP. (2018). *OWASP TOP 10 INTERNET OF THINGS 2018*. https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

Rasheed, W., Abdulla, R., & San, L. (2021). Manhole cover monitoring system over IOT. *Journal of Applied Technology and Innovation*, *5*(3), 1–6.

Samsung. (2021, September). *Can you unlock face recognition with a picture on Galaxy device*. https://www.samsung.com/ph/support/mobile-devices/can-you-unlock-face-recognition-with-a-picture/

San, L., Abdulla, R., & Zainudin, Z. (2022). Smart hand sanitizer dispenser. *Journal of Applied Technology and Innovation*, *6*(1), 9–13.

SANS. (n.d.). *Security Policy Templates*. Retrieved November 24, 2021, from https://www.sans.org/information-security-policy/?per-page=100

Singh, H., Abdulla, R., & Kumar Selvaperumal, Assoc. Prof. Dr. S. (2021). Carbon monoxide detection using IoT. *Journal of Applied Technology and Innovation* , *5*(3), 7–12.

Surfshark. (2020, March). *The facial recognition world map*. https://surfshark.com/facial-recognition-map

Zhang, J., & Tao, D. (2021). Empowering Things with Intelligence: A Survey of the Progress, Challenges, and Opportunities in Artificial Intelligence of Things. *IEEE Internet of Things Journal*, *8*(10), 7789–7817. https://doi.org/10.1109/JIOT.2020.3039359