**The design and development of a sports stadium monitoring and management system to provide early detection and prevention of cyber threats to Internet of Things (IoT) devices**

**Richard Meadows**

**12688825**

**Capstone Project**

**MSc Cyber Security**

**University of Essex (Online)**

**August 2023**

**Contents**

[Introduction 1](#_Toc141541661)

[Research Question 1](#_Toc141541662)

[Aim 1](#_Toc141541663)

[Objectives 2](#_Toc141541664)

[Hypothesis 2](#_Toc141541665)

[Literature Review 2](#_Toc141541666)

[Internet of Things 2](#_Toc141541667)

[IoT Architecture 3](#_Toc141541668)

[IoT’s Use in The Modern World 6](#_Toc141541669)

[Smart Stadiums 7](#_Toc141541670)

[Cyber Security Challenges in Sports Stadiums 9](#_Toc141541671)

[IoT Technology and Cyber Security in Sports 11](#_Toc141541672)

[Methodology 15](#_Toc141541673)

[Ethical Considerations 17](#_Toc141541674)

[Timeline 18](#_Toc141541675)

[Design 19](#_Toc141541676)

[Network Architecture 19](#_Toc141541677)

[Communication Architecture 20](#_Toc141541678)

[Messaging Protocols 23](#_Toc141541679)

[Prevention and Detection Model 26](#_Toc141541680)

[Results 39](#_Toc141541681)

[Mitigations 39](#_Toc141541682)

[Detection Algorithm Implementation 48](#_Toc141541683)

[Discussion and Evaluation 53](#_Toc141541684)

[Research Limitations 54](#_Toc141541685)

[Conclusion and Future Work 55](#_Toc141541686)

[Lessons Learned 56](#_Toc141541687)

[References 60](#_Toc141541688)

[Appendices 84](#_Toc141541689)

# Introduction

The sports industry has become a honeypot for hacktivists, cyber-terrorism and financially motivated attacks. Sports stadiums are firmly in the spotlight, as demonstrated by the National Cyber Security Centre (NCSC) producing their first ever report on cyber-crime in sport (NCSC, 2020). With the advancement of technology enabling physically-operated and cyber-connected devices, machines are interacting with the real world and the lines between cyber-crime and human safety have been blurred (Benslimane, 2022).

The proliferation and excitement of introducing technology into sports stadiums has led to them containing an exponential numbers of devices aimed at providing better functionality and guest experience, however too often they are failing to sufficiently consider security. Therefore, the device safeguarding, and ensuring the need for their accurate and consistent operation is ultimately a life and death matter.

This project aims to draw attention to the lack of the Internet of things (IoT) security in sport stadiums, by investigating current issues and mitigation techniques, before designing a monitoring algorithm using a Proof of Concept (PoC) management system model for preventing and detecting threats to the IoT in sports stadiums.

## Research Question

How can the safety and security of IoT systems in sports stadiums be improved through the integration of a management system?

## Aim

To design a sports stadium management system PoC model which monitors IoT devices in sports stadiums and provides pre-emptive detection and protection against cyber-threats.

## Objectives

* To investigate the current cyber security of sports stadium IoT devices, the problems, and state of the art.
* To identify likely cyber threats to sports stadium IoT devices using threat modelling.
* To design a management system, including the creation of a detection algorithm simulator using known indicators of compromise (IoC) to identify relevant threats.
* To measure the model’s effectiveness using empirical evidence.
* To create a detailed report on the research findings.

## Hypothesis

That affordable tools are successfully able to monitor the status of IoT devices deployed in sports stadiums using secure transmissions, providing an early warning of possible threats or malfunction, and mitigations to the defined vulnerabilities.

# Literature Review

## Internet of Things

The IoT allows real world items to communicate with computing and other IoT devices on public and private networks, with each ‘thing’ being a real world device possessing a network address, and unique ID enabling it to become ‘smart’. The proliferation of the IoT is exponential, and by 2021 there were 12.2 billion globally active IoT endpoints (Hasan, 2022), surpassing traditional Internet-connected devices such as personal computers and smart phones along the way (Lueth, 2020). IoT continues to grow, and together with artificial intelligence (AI) and other technologies, is forming the fourth industrial revolution, better known as Industry 4.0 (Iberdrola, 2016).

Devices classed as IoT divides opinion, however they are generally classified into one of two categories (Alahmadi et al., 2023):

1. *Consumer IoT (CIoT)* – A connected system of physical and digital objects designed to benefit consumer lifestyle. These typically include smart personal and home devices, implemented to improve data gathering, sharing and processing with minimal need for human involvement. Consumer devices can leverage edge or fog computing, and be orchestrated from devices such as laptops, tablets and smart phones.
2. *Industrial IoT (IIoT)* – Have a more organisational, system-centric focus and include devices designed to improve workflows and minimise human error. Temperature, humidity and toxicity can all be monitored automatically. IIoT is often responsible for controlling heavy moving parts known as cyber-physical systems (CPS) which interact with the real world directly, and so high availability is of optimum importance in IIoT, as is greater scalability and transparency. Multiple sectors are now reaping the benefit of IIoT, including energy, agriculture, manufacturing, transportation, healthcare. Safety considerations are also paramount in IIoT, and so predictive maintenance is also important.

CIoT and IIoT also overlap depending on use case. For example, wearable technology is considered CIoT, however when worn by industrial engineers to monitor their location and radiation levels, it is suitably declared IIoT.

## IoT Architecture

There are three fundamental layers of IoT architecture (Alaba et al., 2017; Burhan et al., 2018; Abughazaleh et al., 2020; Mei et al., 2020):

* **Perception/Sensing**: comprising of sensors attached to physical devices that collect data, and actuators that act on it.
* **Network/Transportation**: responsible for connecting devices together, and the data transmissions between themselves, gateways, and data centres. This is most commonly achieved through communications technologies such as Ethernet, Wi-Fi, Bluetooth low energy (BLE), near field communications (NFC).
* **Application**: allows humans to interact with the IoT. For example, through a control panel displayed on a mobile phone, an API, or a dashboard on a workstation.

There are also four (Zubaydi et al., 2023; Navarro et al., 2020), and commonly recognised five layer (MongoDB, N.D.) variations, see Figure 1, and even seven layer models for higher IoT design granularity.

In the four-layer model, the Network layer, often called Transport layer, continues to deal with messaging and connectivity. However, a new Processing, often called Middleware, layer is introduced and is responsible for processing data from its raw form, and performing data analytics to provide meaningful insights and aid decision making. The five-layer model introduces a Business layer for IoT in organisations where business intelligence is carried out on data, enabling them to build better products and improve processes.

Additional levels are added as many believe the three-layer architecture is not sufficient for some applications, (Burhan et al., 2018). Furthermore, Sethi et al. (2017) add that additional layers allow for IoT specific research to be conducted at a more granular level. Burhan et al. (2018) provide a review of architecture layers, the threats that apply to each of them, and propose a six-layer architecture addressing security. Various other domain-specific models are discussed by Jabraeil Jamali et al. (2020: 9–31).

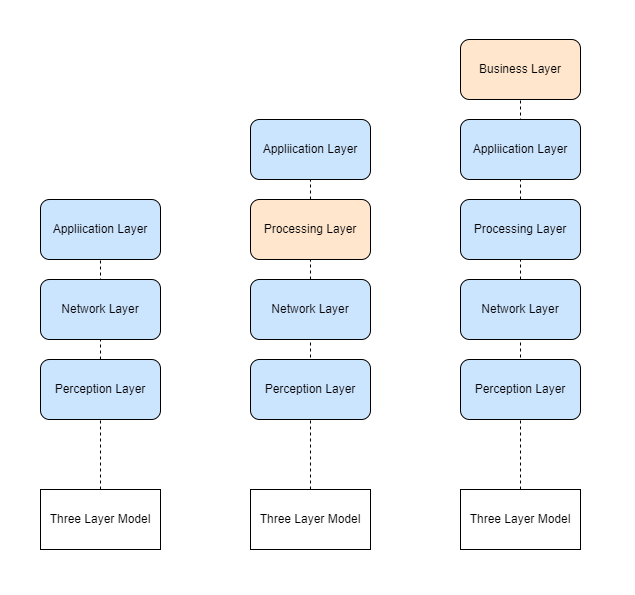


Figure 1: IoT Architectures

IoT architecture is also described as having four stages: Sensors and Actuators, Internet gateways (Data Acquisition), Edge computing, and Data centre / Cloud (MongoDB, N.D.).

This better describes how edge computing is incorporated into IoT. Sensors generate data, and actuators act on it, which is analogous to the Perception layer. Internet gateways proxy data between the IoT network and the Internet, allowing local IoT devices to communicate across the Internet while keeping sensitive data segregated in a local environment. Data acquisition and aggregation happens at this stage, converting analogue data collected from multiple heterogenic sensors into digital form. Edge computing is incorporated to pre-process critical data, allowing decisions to be made in real time before being offloaded in bulk to the cloud, or local data centre for deeper analysis. By processing data at the network’s edge, local network devices receive feedback much quicker than if data were being sent to, and from data centres. Furthermore, security is enhanced by limiting network exposure to untrusted parties. Finally, the Data Centre / Cloud stage performs heavier work on the resultant big data, involving analytics to find patterns and obtain meaningful insights, in addition to providing archiving capabilities.

## IoT’s Use in The Modern World

Planet Earth is moving toward becoming a fully connected world with almost 30 billion IoT Internet-connected devices expected by 2030 (Statista, 2023). This is despite the global COVID-19 pandemic, and curtailed forecasts following a recent global chip shortage (Onag, 2021), as reflected in IoT Analytics’s trends from Leuth (2020) and Hasan (2022).

IoT is already widespread in multiple sectors. For example, healthcare IoT (H-IoT) is already prevalent, and is another area where human life is clearly paramount. Wearables monitoring heartbeats, blood pressure, and body temperature provide telemetry-based health metrics which are used to predict or detect otherwise undiscovered diseases, and therefore enables potential for them to become treatable or preventable (Qadri, Y.A. et al., 2020). IoT assists those recovering, the elderly, or those with disabilities, with everyday life, relieving caregiver workload, and supports life inside and outside of a hospital setting (Yin et al., 2016). In agriculture, sensors report on humidity levels, soil quality, temperatures, and crop and livestock health. Deployed remote cameras monitor disease, and actuators activate sprinklers on schedules, or when specific criteria are met, increasing revenues for the farmer (Farooq et al., 2019).

Smart homes are omnipresent with the CIoT. Families are more connected to the outside world than ever, with more than one in three Americans now owning a smart speaker (Woodall, 2021), and with a multitude of devices including smart televisions, lamps, fridges, and washing machines available, even smart plugs enable any mains powered device to have its power controlled by an app, turning mains-powered devices into somewhat intelligent ones. Common communication technology for smart homes include WiFi, Bluetooth, Zigbee and Z-Wave (Danbatta & Varol, 2019).

The energy sector further benefits from smart meters in the home, making it easier for customers to monitor usage, while providers simultaneously monitor collective information to efficiently manage energy delivery across smart grids, one of many components in a fully connected smart city (Abate et al., 2018). Predicted energy savings for smart cities are to reach $96 billion in 2026 (Juniper Research, 2022), and by moderating power supply usage across the city using intelligent devices for services such as automated street lighting and traffic management, smart grids are integrated to help it become truly connected.

Manufacturing floors are the forerunners to Industry 4.0 and IoT plays a huge part by monitoring production flow to maximise efficiency and minimise waste, introducing predictive maintenance, and maintaining quality assurance and a safe work environment (Kalsoom et al., 2021).

Furthermore, sport is also highly affected by IoT. Athletes use wearables such as smart vests and wristwatches to monitor their performance, location, heartrate and pressure (Aroganam et al, 2019). Cameras are enabling on-field decisions with systems such as Hawkeye, goal line technology and Video Assistant Referee (VAR) (Harrod Sport, 2018), ball inserted sensors track spin, speed and trajectory (Gowda, 2018).

## Smart Stadiums

Sports stadiums are important for the area they are located in, attracting visitors willing to contribute to the local economy in return for entertainment. They are among the top tourist attractions in the most frequently visited cities, forming the concept of venues as a destination (Baroncelli & Ruberti, 2022). Their infrastructures serve as a catalyst for the regeneration of cities or areas, and such projects often include new shops, housing, and restaurants. These concepts bring benefits to the local community and improves local residents’ well-being, showing the importance that sports stadiums have for cities.

Today’s elite stadiums are built with convenience, functionality and safety in mind (Roberts, 2019; University of Chicago Professional Education, 2020). Stadium IoT devices are wide ranging, from camera recognition technologies, to biometric entry, from automatic turnstiles, to digital advertising boards, big screens, automated lighting, retractable roofs, and heating, ventilation and air conditioning (HVAC) systems. By adopting the IoT, sports stadiums increase their automation, saving money and energy, while maximising convenience for the consumer (Li, 2022). No longer do visitors solely benefit from viewing the event, moreover spectators gain entry using ticketless entrance systems, order refreshments directly from their seat, pay with convenience using NFC, and get in-game stats on the live event itself (PWC, N.D.). Smart stadiums in particular are often used as testbeds for developing IoT prior to deployment in smart cities and other real world scenarios (O’Brolcháin et al., 2019; Hutchins & Andrejevic, 2021; Van Heck et al., 2021).

Organisations are also working to introduce new technology, such as with FIFA using cameras secured within stadiums to track players’ limbs, and the ball, to virtually recreate plays on the field for spectators, as well as aiding on-field decisions (FIFA, 2022).

Van Heck et al. (2021) provide a review of various smart devices in the Johan Cruijff Arena in Amsterdam, a forerunning smart-focused stadium with a particular goal of becoming the world’s most innovative stadium, and discusses the problem of combatting the ever-increasing lure of watching sport at home. Nine smart devices in the stadium were discovered, including an innovative smart turf monitoring system, however only four were operational at the time, with the others in various deployment stages. Most of the discovered devices were for improving customer service, such as payment systems and ticketing check ins, where interestingly none were there to directly enhance the experience. The study found that further smart enhancements to the stadium would improve fan experience, including stadium guides, and facial recognition technology (FRT) which was subsequently used in magnitude with 15,000 cameras being deployed at the 2022 Qatar football world cup, which itself raises privacy concerns (Seals, 2022).

Automated FRT is such a hotly disputed topic that the British Security Industry Association (BSIA) have published a set of guidelines to navigate the ethical and legal issues that this technology brings (BSIA, 2021). Super Bowl XXXV caused uproar in 2001 after it became known that police had deviously used FRT to scan 100,000 visitor faces looking for known criminals (Brey, 2004), whereas conversely, Norstrom (2021) advocates FRT could have prevented the Euro 2020 final disaster by using it for verification on entry. Brey, discusses the advantages and disadvantages of using facial recognition in public places, noting that security often comes at the cost of privacy. Furthermore, recording one’s face using IoT-operated cameras directly contradicts principle 1.6 of the Association of Computer Machinery’s (ACM) Code of Ethics and Professional Conduct (ACM, N.D.), and this opens up more questions as to who owns such data. Moreover, it is difficult to expect 80,000 spectators to fill out waivers upon entry, and perhaps unrealistic to expect them to read notices advising them of recordings and data gathering. Brey, also highlights other specific FRT issues, including errors and function creep which have since been reduced through modern technology and the General Data Protection Regulation (GDPR), respectively.

## Cyber Security Challenges in Sports Stadiums

Roberts (2019), discusses example threats present within sports stadiums in parallel with the maritime transport industry, conducting example risk assessment approaches, and comparing them with traditional physical-only attacks. Roberts, highlights that physical security has traditionally been at the forefront of discussions, however indicates an increasing interest on how CPS causes threat to life when the cyber component either fails, or falls victim to cyber-attack. Either scenario can be used as a precursor to launch a physical attack, for example locking smart turnstiles can pen people in one area, or threatening messages displayed on the big screen can cause people to panic and flee, subsequently maximising secondary attack effectiveness in an area filled with people, leading to scenes similar to those at the Stade de France in 2015, or the Arianda Grande concert at the Manchester Arena in 2017 (Roberts, 2019).

IoT devices in stadiums however, also positively contribute to security efforts. For instance, deployed devices assist with crowd control, surveillance, and logistics (O’Brolcháin et al., 2019).

Alhadad & Abood (2018) discuss the importance of making improvements to stadiums, in a desperate bid to keep alluring spectators back, speculating that organisers are competing amongst themselves off the field, just as their sporting subjects are on it. Interestingly, according to Nate Evans, a lecturer from Argonne National Laboratory, competition is a useful method of assuring a healthy cybersecurity status amongst peers (University of Chicago Professional Education, 2020).

Melander (2020), also addresses data collection privacy issues from camera use, and remarks on several ethical points and the need for strict regulation, a more extensive ethical study in this respect was conducted by O’Brolcháin et al. (2019).

Any organisation in the UK that collects and stores data from customers, including data acquired by IoT devices, is subject to the Data Protection Act (2018) and GDPR, meaning data must be protected by secure means, stored only for required purposes, and as long as necessary, whilst preserving the data subjects’ rights to their own data (GDPR, 2022).

Melander (2020), also comments on the need for a uniform security protocol standard for all devices to mitigate a large proportion of IoT security threats.

Regulation in the IoT has longed been campaigned for, and until recently UK businesses in the IoT production lifecycle had only voluntary guidelines. The European Telecommunications Standards Institute (ETSI) released EN303 645, the first IoT standard in June 2020 (ETSI, 2020), and follows the UK’s lead with its 13 requirements closely matching the pioneering Code of Practice (HM Government, 2018). This list of security requirements aims to provide an assurance baseline for IoT devices, aligning for product certification, and hopes to drive improved security measure adoption worldwide**.** Moreover, the Product Security and Telecommunications Infrastructure Act (2022) was recently introduced, enforcing the first three foremost practices from the former Code of Practice and EN 303 645 into UK law. The act carries harsh penalties, synonymous with that of the GDPR (2022). While addressing vulnerabilities such as the use of default credentials, which facilitated the 2016 Mirai attack (Margolis et al., 2017), the act does not cover devices manufactured and deployed before its enactment in December 2022, meaning many devices will remain forever insecure in the wild, notwithstanding further important omissions such as secure communications, unnecessary port closure, or input validation. Perhaps most prominently in regards to this paper, it does not cover industrial IoT devices, nor those used by businesses, as those are to be superseded by other regulations (UK Parliament, 2021).

Consequences of IoT Compromise

Cyber-attack proliferation is growing due to technology development and reliance, especially following the increasing use of wireless communications such as cellular technology and Wi-Fi. Sports stadium security is something that cannot be taken lightly, with 70% of sports institutions annually subjected to a cyber-incident (NCSC, 2020).

Compromise of one device, can mean compromise of an entire network, as demonstrated in 2018 where an IoT fish tank was breached, allowing attackers to move laterally to penetrate a casino’s internal network (Wilner, 2018). Furthermore, this can be life threatening. Implantable medical devices (IMD) such as pacemakers come with the possibility of compromise from outside the body, making assassination possible. Reportedly, former US vice-president Dick Cheney was concerned enough about this threat, that he asked for its wireless functions to be disabled as a countermeasure (Pycroft & Aziz, 2018).

Compromise can lead to financial losses, reputational damage, financial penalties, and most importantly in the IoT’s case, loss of life.

The very fact that the IoT comprises of CPS in today’s world, including those found in sports stadiums extends the threat of cyber-attacks to human life. Advance sporting event risk management is imperative due to present threats to human life and the potential for financial and reputational damage for the organisation (Wan et al, 2022).

## IoT Technology and Cyber Security in Sports

The Mirai botnet of 2016 showed how inept the world was in detecting and preventing IoT cyber-attacks. Preying on the multitude of smart devices lacking rigidly secure defences, the botnet was able to infect almost sixty-five thousand devices across the world in its first twenty hours (Antonakakis et al., 2017). Mirai, propagated as a worm using each new zombie to scan for further devices with open SSH or Telnet ports, and attempted authentication using a pre-determined credentials list. Likely evolving from a previous Trojan named Bashlight, Mirai produced multiple variants, and zombies from the resultant botnets, comprising of nearly half a million zombies were eventually used to target Dyn, a hosting company providing DNS services (Kambourakis et al., 2017), rendering several well-known sites unavailable.

A modern day smart stadium includes a network of generic laptops, desktops and networking equipment, connected by wired or wireless means. They are also likely to include connected IoT devices such as sensors, CPS and embedded systems. Embedded systems often include a user interface and are generally software-based, static control systems instilled in a physical platform to perform a specific function. CPS are hardware cyber-connected devices that incorporate software, and often include many more capabilities than embedded systems (Wan et al., 2022), to interact with the real world.

With the gradual introduction of 5G, IoT is destined to become Massive IoT, eliminating the need for human interaction, simplifying traditional networking methods, and making much networking equipment redundant. 5G was developed with IoT in mind with speeds 10 times faster than 4G, less latency, greater capacity, handling multiple device connections simultaneously, and allowing devices to connect directly with each other across geographic locations (Li et al., 2018). This will eventually benefit those with devices in rural or remote locations previously without access to reliable broadband, and therefore will benefit sports stadiums too, whatever the setting (Fang, 2022).

Often in the outside world, it is enough to secure your defences so that attackers will give up to seek easier targets. Unfortunately, when hosting sports mega events (SME), where hacktivism and nation states see opportunities to make their mark, this is an unrealistic possibility.

The 2018 Winter Olympics opening ceremony suffered an attack on IT systems causing display monitors to shut down, and paralysed the Wi-Fi and the website leaving attendees unable to print tickets or access information.  The attack’s success was clear to see with many seats left vacant during the celebration. This attack was perfectly timed and successfully gained the world’s attention through the media (Kaspersky, 2018). In 2016, an attack on the World Anti-Doping Agency (WADA) revealed how nation states use sport to showcase their political prowess (Datta & Acton, 2022). A Russian state-sponsored cyber hacking group known as Fancy Bears were able to extract several athletes’ details taking legitimately approved drugs by using credentials gleaned from a phishing attack, and posted them to their website (Pitsiladis et al., 2017). This according to WADA was in retaliation to banning Russian athletes from the 2016 Summer Paralympic games in Brazil after they had been accused of submitting doctored samples during the 2014 Winter games testing (Pingue, 2016). This seemingly political act caused embarrassment to WADA and the Olympics, and distrust amongst the public.

In 2021, a further hacktivism example saw a group able to compromise 150,000 cameras, revealing inside footage of prisons, hospitals, and schools. The attackers exploited insecure configurations, and again leveraged leaked admin credentials (Scroxton, 2021). Hacktivism is a real threat to sporting events, with Just Stop Oil providing recent examples of protesters targeting sport (BBC, 2023a; BBC, 2023b).

Threats like these have led to the development of the National Centre for Spectator Sports Safety and Security (NCS4), an academic centre at the University of Southern Mississippi dedicated to furthering spectator sport safety and security (NCS4, N.D). The NCS4 conduct research, and inform sporting organisations on best practices for the safety and security of their operations.

NCS4 have, in partnership with the Cybersecurity & Infrastructure Security Agency (CISA), provided an example diagram of a typical connected stadium with key vulnerabilities, consequences, and suitable mitigations (CISA, N.D.).

The United Nations (UN) produced a guide for securing SMEs, identifying operational, legal, and reputational risks as three key cyber risk categories for consideration when preparing for cyber-attacks, and highlighting IoT as a particular concern (UN, 2021). The Open Web Application Security Project (OWASP) also published an IoT top 10 (vulnerabilities) list in 2018 (OWASP, 2018).

Organisations arranging SMEs can further benefit from the input of global experts in cyber security, physical security, and sporting legislation by participating in international efforts such as Project Stadia (INTERPOL, N.D.).

Qatar continued the trend for modern cyber intelligence enhancements, learning from previous SMEs. Helped by its close proximity, the eight stadiums used in the 2022 world cup were inter-connected, leveraging edge computing and artificial intelligence to facilitate information gathering at speed, and recreated digital twins for better real time understanding of event security (Seals, 2022).

Literature on sports stadium IoT security is thin, however many IoT security-based problems have been discussed, as the potential disasters are well-known and feared. Melander (2020) gives an example of a sensor failing to report a fire, with disastrous consequences.

Phanish et al. (2015) provide a solution to assess an American Football stadium’s structural health using wireless sensor networks, however do not focus on the security on the devices themselves.

Wan et al. (2022) proposed a cost-effective AI model to determine cyber-attacks to CPS which enhanced prediction and accuracy on abnormal network traffic, with improved latency, delay and packet loss compared to other methods. While this model was successful, an artificial intelligence method alone is not ideal for making detection decisions when human life is at stake, particularly if a learning dataset is contaminated by attackers (Swinhoe, 2018).

Mowafi et al. (2013) provided a useful framework for tracking the mass crowd gatherings using Radio Frequency Identification (RFID) tags, and enables guidance information for patrons, while providing decision support for crowd managers. Whilst this has obvious benefits to human safety, it does not consider cybersecurity. Older RFID tags can also be read by anyone with an RFID reader, and with many personal identifiable information (PII) items stored in this example, there are also significant privacy risks. Furthermore, tags are vulnerable to cloning, and readers would be affected by many thousands of people passing by, with high potential for collisions, manipulation, and jamming attacks (Rieback et al., 2006).

Most IoT attacks are also found in traditional cyber-attacks, owing to their dependency on the Internet as a backbone, however IoT devices are less equipped to defend against them due to their limited resources (Deogirikar & Vidhate, 2017). Deogirikar & Vidhate (2017) provide a taxonomy of various attacks on IoT, classifying them into four categories: physical, network, software, and encryption based, while Akram Abdul-Ghani et al. (2018) provide a similar, however somewhat more comprehensive, classification using the following categories: physical, protocol, data (at rest), and software based. Li et al. (2018) further highlighted some security challenges with the introduction of 5G technology, including how to secure communications through cryptographic means and at the device level, how to provide energy-efficient security for resource-constrained devices, and how to provide trust assurance through the IoT stack.

Vulnerable Internet-connected devices can be easily found using a website such as Shodan (N.D.), which also facilitates authentication attempts. Furthermore, device details, such as default credentials or radio frequencies, can be gleaned using open source intelligence. This is a cocktail for disaster, and makes it reasonably easy to exploit insecure devices from afar. Someone with physical access might be able to do much more damage, extracting the firmware using UART or JTAG for reverse engineering, flashing their own firmware (Shepherd et al., 2017), or by simply disconnecting the device.

Security is challenging when IoT devices are constructed from many components, each by manufactures with differing security perspectives and implementations (Li & Xu, 2017). This leaves difficulty in securely passing data up and down the IoT stack. Furthermore, components re often designed and manufactured by nation states which may be allies upon purchase, however in a setting such as a sports stadium where devices are feasibly not upgraded for decades, this is a high risk that stadiums take on political security.

Information security is primarily focused on the confidentiality, integrity and availability (CIA) of data (Samonas & Coss, 2014), and in most organisations, information security concerns focus on the confidentiality and integrity tenets. However, within IoT, Availability is usually the most important (Li & Xu, 2017).

After reviewing available literature, there are still clear research gaps in adequately protecting and detecting threats with current techniques. IoT increases functionality, moreover expands the attack surface in sports stadiums, with security left lagging behind. Furthermore, the relative ease of attacks currently means this is more urgent than ever. This research therefore focuses on designing an improved method of preventing and detecting threats.

# Methodology

This study aims to investigate how sports stadium IoT threat prevention and detection can be improved by integrating a management system. Due to the subjectivity required to answer this research question, and because qualitative data was used for data collection, an interpretivist epistemology was preferred, in contrast to an objective positivist approach which generally uses qualitative data and hard evidence (Abramson & Sánchez-Jankowski, 2020). Through evidence gathering, it is still subjective as to whether the evidence proves that the preventative or detective control mitigates the problem.

The scientific method was used (Science Notes, 2023), and following the research question, this began with a comprehensive literature review of existing secondary research to understand the topic landscape. This led to finding a research gap, identifying a lack of current sufficient sports stadium IoT safety and security measures.

Data collection was limited to secondary research mainly through acquiring threat IoC evidence from historical research papers, and primary applied research to create a simulation of a rudimentary arithmetic detection algorithm. This algorithm was created in the form of a spreadsheet, and using a model-based approach, combines with architecture and UML diagrams to form a PoC prevention and detection model artefact. The IoCs were used to provide inputs for the identification of cyber threats in real time, with weightings given for each IoC depending on the threat they indicate.

It is worth noting that the weightings given in the algorithm were subject to bias, due to the study following an interpretivist epistemology (Farquhar, 2012), and are used to demonstrate a PoC, and therefore did not affect the findings.

Although the research uses qualitative data, which is usually associated with inductive reasoning, deductive reasoning was then used to prove the hypothesis (McCombes, 2022; Miessler, N.D.).

Ethnography, or a case study at a specific football stadium would have allowed stadium-specific analysis in a social, legal and ethical context. This may have led to more accurate IoCs and threats relating to the particular setting, however this research subsequently uses secondary research to gather data from stadium IoT in general. Furthermore, these research methods would also benefit if conducted as a group research project due to a likely further reduction in bias (Runeson & Höst, 2008). However, as ethical approval would need to be sought for these research types, it would have left less time to perform data gathering and analysis, and so it was decided to concentrate on data collection methods from an earlier point.

This study is cross-sectional, due to the results being taken from a state in time. A longitudinal study would not be useful here as the study was not dependent on future or archived results (Dawson, 2015: 29).

As the data required was not statistical or numerical, secondary qualitative data in the form of evidence supporting cyber security measures to defend against IoT threats in a sports stadium was used for analysis (BRM, N.D.). This used a non-probabilistic sampling strategy, as it would have been difficult to obtain sources of IoCs matching threats randomly.

Content analysis was used to classify and summarise the data. Discourse and narrative analysis was not useful due to the evidence gathered being text based, and not involving human responses or stories. Furthermore, grounded theory and thematic analysis were not useful as evidence needed to be gathered from multiple different sources to determine categories relating to each threat, and so were not used to build upon a theory or discover a pattern or theme (BRM, N.D.). Quantitative data analysis was not applicable due to the data not being numerical or statistical in nature. However, should this model be taken forward in further research, quantitative analysis could be performed on real statistical data. Furthermore, this study aims to further research by providing a PoC model. Content analysis was very time consuming.

# Ethical Considerations

Although the secondary research uncovered various ethical matters in IoT in sports stadiums, there were no ethical concerns concerning the primary research as it was based on a PoC and did not involve any human participants or any real organisational data. If the project were to be performed as a case study, or involved ethnography, approval would have been required from the University of Essex Online’s Ethics Committee due to the risk to organisational reputation (social) or exposure to genuine cyber, legal or physical threats following assessment of their security posture and practices. Any identifiable data collected would either need to be anonymous at source, or have confidentiality and pseudonyms applied before submission, to avoid any potential for harm (Bhandari, 2022; Runeson & Höst, 2008). For this reason, the paper also does not include any organisational or personally identifiable images. Furthermore, if real data were being collected on humans as part of the IoT analysis, GDPR and Data Protection Act (DPA) regulations must be abided by, and a notice of consent would need to be sought from affected individuals (O’Connor et al., 2017).

It was also important to provide accurate data in this report so not to mislead readers with inaccurate results caused by an increasing positive bias trend. Misleading results in the context of protecting human life in sports stadiums could have catastrophic consequences, and the omission of negative results leads to wasted time and resources (Mlinaríc et al, 2017).

Furthermore, if this model were to be developed into a prototype or used to determine real time threats in a stadium setting, it would need to do so while exercising due care to spectators, athletes, and staff, ensuring compliance with the ACM Code of Ethics and Professional Conduct, GDPR, and DPA, and the following legislation: Safety of Sports Grounds Act (1975), Fire Safety and Safety of Places of Sports Act (1987), Football Spectators Act (1989), Sports Grounds Safety Authority Act (2011), Health and Safety at Work etc. Act (1974), and Corporate Manslaughter and Corporate Homicide Act 2007 (Sports Grounds Safety Authority, N.D.).

# Timeline

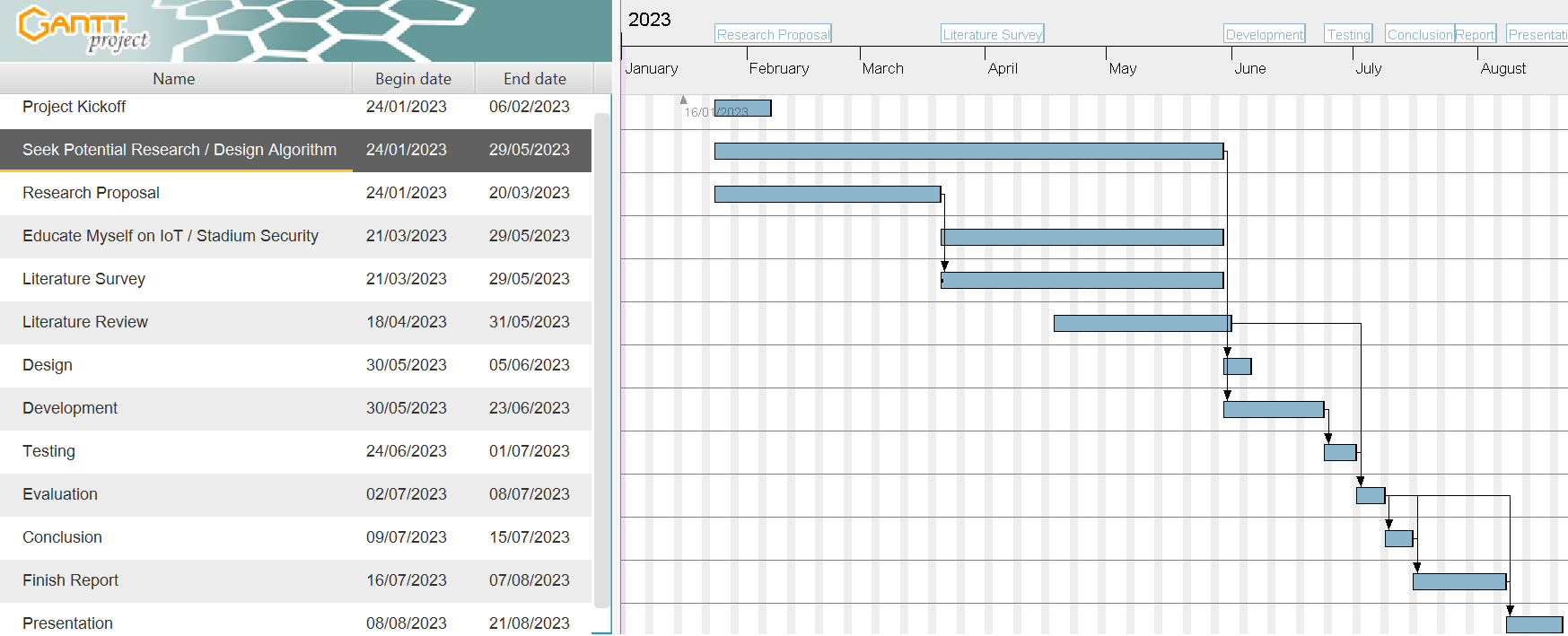


Figure 2: Project Timeline

# Design

There are several considerations to developing a model to protect and detect threats to sports stadium IoT devices. These include which network and communication architecture, and which messaging protocol should be used. The following discusses some options.

## Network Architecture

*Edge Computing*

Edge computing allows for data processing at the local network’s edge, without sending data to the cloud. This has several benefits, including less latency and bandwidth usage, and added security, privacy, and reliability due to limited exposure over the public Internet (Carvalho et al., 2021).

*IoT Gateways*

IoT gateways collect data from end nodes using various technologies, and allow them to communicate over the IP network. These gateways can also perform multiple additional functions, for example, as edge computing MQTT brokers (Koziolek et al., 2020). IoT edge gateways accommodate these, and translate to IP for sending to the cloud for backend processing, while making basic decisions regarding the end devices themselves, thus merging the Internet Gateway and Edge Computing IoT architecture stages.

Inside a sports stadium, many devices will be mains powered and subsequently use resource hungry communication methods such as Ethernet or WiFi, and if using smart wearables or smart sports equipment (Abdelrasoul, et al., 2015), it is possible to use a Wireless Personal Area Network (WPAN) technology such as BLE. Due to a stadium’s relatively small size, long range mediums such as low-power wide-area network (LPWAN) technologies which preserve battery life, are unnecessary (De Carvalho Silva et al., 2017).

## Communication Architecture

*Event-Driven Architecture*

Devices in event-driven architecture (EDA) communicate by publishing messages and commands to each other through notifications. These notifications are either triggered by events that occur on devices (indicating a change in state), or sent on a schedule. Devices transmit notifications to appropriate endpoints on the network, who can then act accordingly, or publish their own reactive notifications in response or to other devices. EDA uses asynchronous communication, meaning once the notification has left the producer, it is forgotten (Richards, 2015).

A major EDA advantage is that all producers and consumers are decoupled, meaning all nodes are independent, and are not required to be available at the same time. EDA is scalable, and does not necessarily require a central node to move notifications along (Richards, 2015). Furthermore, notifications are deemed immutable and persistent, meaning they cannot be altered and can be used again after they have been used (A Dev’ Story, 2021).

Depending on its implementation, EDA presents challenges, including the guaranteeing notification delivery, ordering, and the concept of idempotency (Microsoft, N.D.). Guaranteed delivery is not required in non-critical systems, however requires careful consideration when used for critical system communication over unreliable networks (Jiang et al., 2011).

Furthermore, where devices are dependent on notifications from others, reliability is often important, and is exacerbated when multiple devices are sending simultaneous notifications needing to be processed in the correct order. Ordering is a well-known issue in EDA, and often requires mitigation by either appending identification numbers, versions, or timestamps to notifications to properly keep track (CockroachDB, 2021).

Idempotency is the guarantee that if any event is processed more than once, it will not affect the end result (Macero García, 2020). This is an additional consideration in EDA, as receiving the same notification twice in a non-idempotent system can result in the system crashing, or producing inconsistent results (Sun et al., 2019). Inconsistencies would spell disaster in a sports stadium, and can occur when there’s a failure on the event channel, broker or consumer and the notifications are sent again. Here, a medium such as a database can be used to store events, with application logic applied to check against those previously received (Sen, 2018).

EDA lends itself to processing high amounts of data such as those produced by multiple IoT devices, and as brokers push notifications to, they can act as soon as they arrive (Jansen & Saladas, 2020).

*Publish-Subscribe*

The publish-subscribe model is an EDA sub-type which uses the broker topology. Brokers proxy information sent from the producer (publisher) to the consumer (subscriber), and notifications are broadcast to consumers using event channels known as topics (Gorton, 2022).

The architecture’s main disadvantage, in addition to those suffered by EDA in general, is that while it can survive devices going offline, the broker is typically a single point of failure (SPoF), leaving DoS attack vulnerabilities.

There are further considerations with ensuring reliability, including how to manage idempotency and lost messages, at the expense of performance (Gorton, 2022).

However, the publish-subscribe model has numerous upsides. Including scalability, and the option to store notifications for disconnected consumers until they come back online (Gorton, 2022).

*Request-Driven Architecture*

Request driven architecture (RDA), is a one-to-one model architecture following the request-response model, and uses one-way communication, with the client querying a server. Devices connect to each other synchronously without the requiring a broker, meaning it is tightly coupled. When a client queries a server, it sends a request and gets an immediate response, meaning other devices cannot be contacted until completion. It is easier to implement, and troubleshoot than EDA, however due to its tight coupling, it is less resilient and less scalable (Ihuman, N.D.; Tammadge, 2021).

*Polling*

Polling is similar to RDA, as it also follows the request-response model. However, the client makes requests to the server at intervals for data that need processing (Raj et al., 2017a). If the server does not have any data to transmit, it closes the connection and waits for before polling again. In addition, the server cannot push information until the client initiates a request (Stratmann et al., 2011).

Therefore, polling is suitable for environments where long delays between network calls are tolerated. For example, it is ineffective in systems sending regular data as client resources are wasted creating needless handshakes and teardowns, meaning it is not practicable, and if more regular requests are required, intervals need to be reduced, which adds to network load and also the potential for lost events (Kannan et al., 2014; Stratmann, 2011).

Polling also means potentially long execution times, and relatively large messaging overheads, especially when transmitting small-sized messages. Because of this, and the fact that clients must repetitively poll the resource, polling results in increased network load and latency, and therefore is inappropriate for real time applications (Westerholt & Bernd Resch, 2015).

A polling sub-type, known as long-polling, enables the client to open a connection with the server and wait until data is available. This saves resources compared with short-polling, however is still synchronous, meaning nodes are tightly coupled (Stratmann, 2011). This, is preferred in scenarios containing small numbers of devices, as keeping the connection open ties up resources. Long-polling is more efficient than short polling, as servers push data to the client whenever it becomes available, resulting in less handshakes and teardowns, however it requires nodes to be tied up for longer periods (Stratmann, 2011).

Polling architecture therefore, is not be suitable in situations where notifications are waiting to be processed, especially when there are many systems involved.

## Messaging Protocols

Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT) are two application layer messaging protocols designed for use with constrained devices, and they are both supported over various communication technologies. Larmo et al. (2018) compare their performances over BLE and WiFi, and Thangaval et al. (2014) compared their performances over varying network conditions.

*MQTT*

MQTT transmits notifications between IoT devices using publish-subscribe architecture, and works over TCP to ensure reliable transmissions (Thangavel et al., 2014). MQTT also leverages Transport Layer Security (TLS) to provide security if devices have sufficient resources (Karagiannis et al., 2015). MQTT pushes notifications, rather than requiring clients to poll servers (Soni & Makwana, 2017), and clients can leverage unique MQTT properties such as Last Will and Testament (LWT) to identify device failure in near real time, while brokers can retain notifications to store last known good data following a client outage (Wagle, 2016).

*CoAP*

CoAP is an HTTP-like communications protocol using RESTful standards, and was introduced to support constrained devices by reducing overheads (Khattak et al., 2014). CoAP leverages UDP, meaning improved performance compared with TCP (Khattak et al., 2014). However, while CoAP has properties which improve communications reliability, UDP is connectionless, and is therefore considered unreliable (Bansal & Priya, 2020; Naik, 2017). UDP leverages DTLS in a similar way to TLS to provide authenticity, integrity and confidentiality (Naik, 2017).

**Threat Modelling**

Threat modelling allows detailed analysis to take place with the aim of detecting system threats. This paper performed threat modelling using an attack-defence tree to determine both abuse cases, and corresponding mitigations to sports stadium IoT. The attack-defence tree was created using ADTree (Université Du Luxembourg, N.D.) and is found in Appendix A, with the identified threats listed in Table 1:

Table 1: Threats

|  |  |  |
| --- | --- | --- |
| **Threat** | **Description** | **Layer** |
| Tamper | Malicious actor physically manipulates IoT devices or connections by accessing hardware components, modifying or accessing details through local ports, or simply disconnecting the device’s power (Varga et al, 2017). | Perception |
| Unauthorised Firmware | Malicious actors look to replace known good firmware, with intentions of exploiting known vulnerabilities in the new malicious software (Bettayeb et al., 2019). Kvarda et al (2016) noted an increase in recent IoT firmware attacks due to detection difficulties at a sub-operating system level. Barcena & Wueest (2015) conducted tests on multiple smart home devices which showed most were not using cryptographic techniques to sign firmware updates, leaving unauthorised firmware installation possible. | Perception |
| Jamming | Specifically related to wireless sensors, attackers send signals to interfere with wireless transmissions on the same frequency leaving legitimate data collection impossible. Jamming is a form of DoS and can be categorised as a network layer attack, however here it is classed as a perception layer threat to illustrate that sensor nodes using open wireless technologies to glean data, such as HVAC or RFID sensors, are vulnerable (Akram Abdul-Ghani et al., 2018; Deogirikar & Vidhate, 2017; Uke et al, 2013). | Perception |
| Eavesdrop | Attacker reads plain text communications in transit across the wire, or more commonly, over air. This is made possible due to physical exposure, vulnerabilities in equipment or applications, or in the absence of encrypted communication channels (Stone, N.D.). | Network |
| MITM | Occur when attackers position themselves between two or more communicating network nodes. By falsifying identity, legitimates node are fooled into believing they are still communicating with each other. However, the MITM intercepts or alters each packet, before forwarding to the intended destination (Conti et al., 2016). | Network |
| Lateral Movement | If an attacker successfully penetrates a device, they establish a foothold to search for further devices on the same network (SentinelOne, N.D.). | Network |
| DoS | Seeks to overwhelm devices until they are unable to respond to legitimate requests. This attack violates the availability tenet of the CIA, and is exacerbated when introducing multiple sources of malicious requests resulting in distributed denial of service (DDoS) (Jazzar & Hamad, 2022). | Network |
| Rogue Device | Unauthorised devices, operating under the guise of legitimate devices (Javaid et al, 2020). Rogue devices may also attempt to subscribe to MQTT topics (Arseni et al., 2021). Rogue devices could be classified as a perception layer threat, however is included here in the Network layer due to its threat of picking up transmissions. | Network |
| Malicious Access | An unauthorised actor gains access to a device through one of its interfaces, leading to further threats such as information being stolen, and services and devices being deactivated (Firdous et al., 2017). | Application |
| Code Exploit | Device software often has vulnerabilities which go unnoticed unless there is a comprehensive vulnerability disclosure and management program in place (UL, 2019). Furthermore, if the device model is known, exploitation details are easily found online (Rytel et al., 2020). Therefore, preventative controls, and both known and zero day threat detection is required. Code exploits allow attackers to enter malicious commands to manipulate device behaviour (Gupta, 2019; Msgna, 2022; UL, 2019). | Application |
| False Data Injection | A compromise allows manipulated data to be sent from the device. These attacks create dangerous situations, e.g. force open doors, raise unnecessary alarms, or crash devices. Swinhoe (2018) discusses several consequences. | Application |

# Prevention and Detection Model

As sports stadiums require system threat prevention and detection in near real time to ensure human safety, the artefact uses the MQTT publish-subscribe for the communication protocol due to its unique capabilities and higher reliability. The communication architecture employs a master-slave pattern (Figure 3) which delegates data collection work to the end devices, known as slaves, to return data to the master to perform calculations (Raj et al., 2017b). This architecture pattern has been used in IoT designs in other sectors, and is employed in this design for a sports stadium.

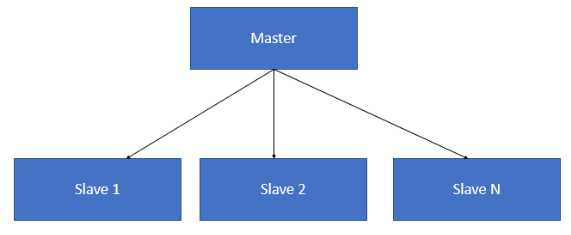


Figure 3: Master-Slave Pattern

Lee et al. (2022) proposed a power saving automatic IoT LED lighting system based on a master-slave architecture. The master LED node detects a signal, and subsequently triggers other slave LEDs in the same zone to increase their brightness to the same level, thus saving power and cost in implementation wired infrastructure. Jan et al. (2021) designed a novel routing protocol for optimising energy consumption for underwater wireless sensors, based on master-slave architecture.

The architecture design is presented in Figure 5:

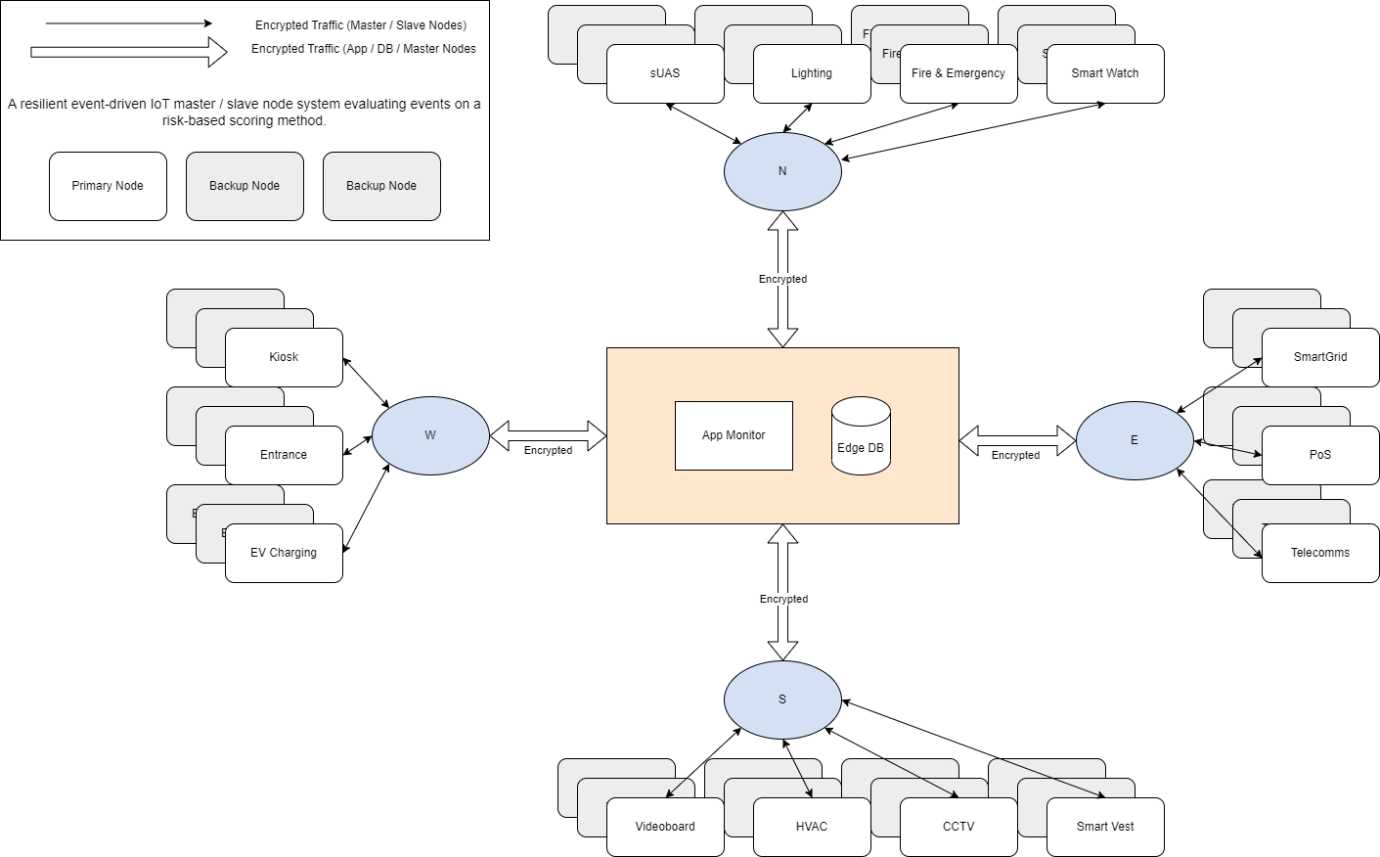


Figure 4: Stadium IoT Architecture

Each side of the stadium is divided into four, with one master node being responsible for multiple slave nodes (IoT endpoint devices) in each side. Slave nodes communicate with their respective master nodes through their various communication protocols (e.g. Ethernet, WiFi, BLE), and edge master nodes combine MQTT broker and IoT gateway capabilities. This enables them to subscribe to notifications from multiple slave nodes, and make appropriate decisions without needing to communicate to the cloud.

Each slave node each has two backup nodes in an active-passive setup in case of malfunction or attack on the primary node. These backup nodes are located on separate virtual networks (VLAN) to ensure any incidents are contained. Should a problem with the slave node be detected by the master node, the problem node is deactivated and a backup node takes its place.

The application layer in the centre of the diagram, contains a monitor, and database to store data and event notifications send from the slave nodes.

The artefact created for this project is a PoC described by an architecture diagram, UML activity and misuse case diagrams, and a spreadsheet created in Microsoft Excel. The activity diagram shows data and event code notifications moving between slave and master nodes. The misuse case diagram shows the detectable ways attackers will attack the IoT devices. The spreadsheet represents the detection algorithm, and contains four tabs. Shepherd et al. (2017) identified IoT risks using a risk matrix calculated from asset value, threat and vulnerability combinations. Risk matrices are commonplace in assessing risk, however a threat matrix leverages IoC to help determine threats, and is applied automatically in real time. Therefore, the proposed model prevents threats using preventative controls, and is supplemented by the scoring algorithm, to detect threats based on weighted IoC.

**Threats**: this tab (Figure 5) is informational and lists each threat discovered following the threat modelling stage. Threats are categorised by the layer it endangers, based on the three-layer IoT architecture model. Each row lists a Threat, its countermeasure Control Type (Prevent/Detect), and how it is mitigated by the model.

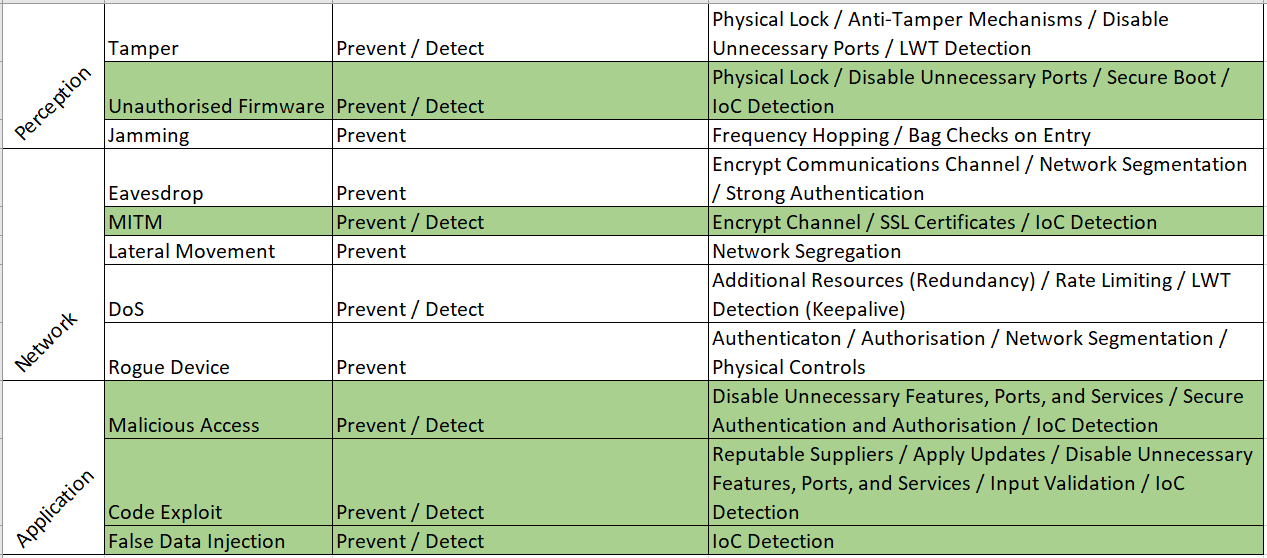


Figure 5: Threats

**IoCs**: lists indicators of compromise (IoC) that are typically found to contribute to each threat being realised. IoC are used by the detection algorithm and are listed by Event Code, together with the Event Name (Figure 6).

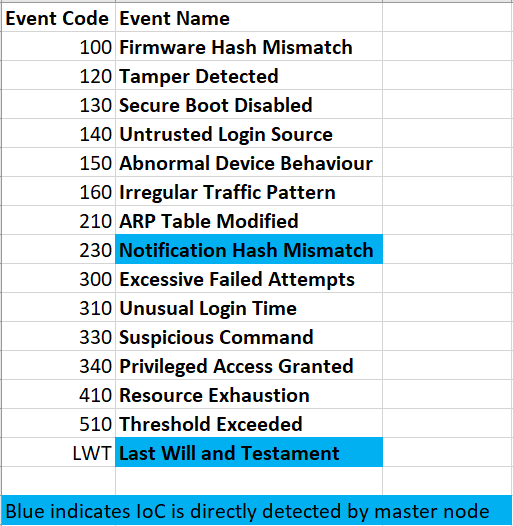


Figure 6: IoCs

**Weightings**: some threats cannot be prevented alone, and require supplementary detective measures to mitigate threats. Therefore, the Weightings (Figure 7) and Score (Figure 8) tabs use a scoring method to enable the system to detect threats using IoCs. Grouped by Threat, IoCs are listed with a Description, and Weight. The weight for each IoC depends on the likelihood a threat is typically present on a device when a notification of that event is received by the master node. IoCs may be present in multiple threats, with varying scores depending on how applicable they are to that threat’s calculation.

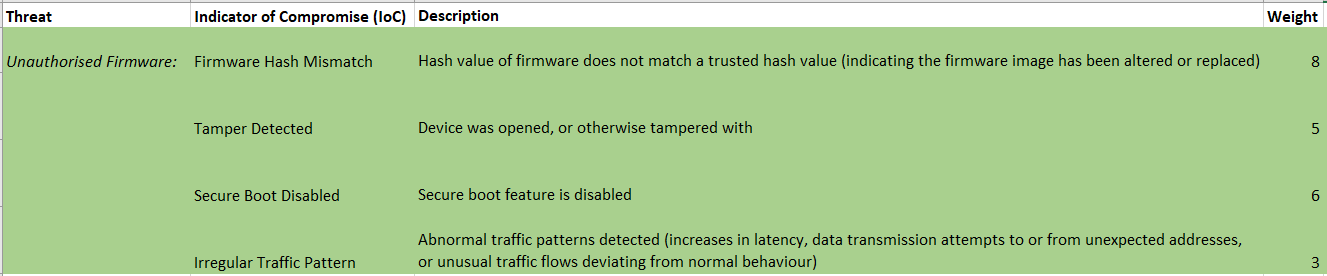


Figure 7: Weightings

**Score**: this interactive tab uses formulas to simulate events occurring in real time. As this is a PoC, the user enters IoC codes in the Code column. The Event Description field then automatically populates with the corresponding Event Name. If the combined IoC weighted scores for a particular threat exceed a total of ten, an alarm will be displayed in red. This simulates the master node detecting a threat in the real world sports stadium scenario and raising the alarm. This alarm automatically triggers a response to deactivate the compromised node, fail over to the backup slave node, and send an alert to a monitor for human response to attend to the problem device.

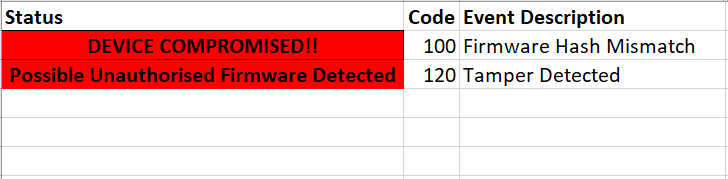


Figure 8: Score

The threats to IoT relevant to the detection algorithm are found in Figure 9.

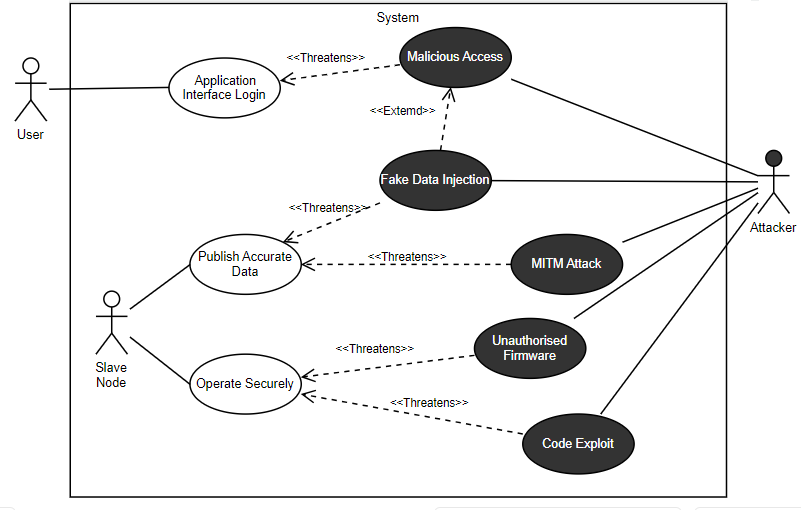


Figure 9: Misuse Case Diagram (Relating To Detection Controls)

*Quality of Service*

MQTT uses a unique implementation of reliability, offering three quality of service (QoS) levels: QoS 0 - At most once, QoS 1 - At least once, and QoS 2 - Exactly once (Safaei et al., 2017).

In sports stadiums, there may be no need to expose IoT devices to the public Internet, and therefore, security is improved by employing edge devices. By the devices’ relatively close proximity, enhanced by the use of the master edge nodes, communications reliability is already improved through short range communication protocols such as WiFi, Ethernet, and BLE. However, because of the need to protect human life, notification reliability is of paramount importance. MQTT uses TCP which is a reliable transport protocol, and QoS 2 provides additional reliability at the application level (Safaei et al., 2017). As human life is at stake, it is important to ensure every notification reaches its destination, as well as ensuring notifications do not arrive multiple times, and so QoS 2 inherently guarantees idempotence (Cheong, 2022). MQTT clients register a four second keepalive period upon connecting with the broker. If a device should either fail or not report back for more than six seconds, determined by one and a half times the keepalive period, the keepalive is exceeded, and an LWT event notification is triggered by the broker. The broker then deactivates the problem device, and again fails over to a corresponding backup device.

Four seconds was deemed optimal, as longer durations increase the risk to human life due to problems going undetected, and shorter durations increase false positive rates following increased sensitivity to minor network issues or device malfunctions. QoS 2 increases notification delivery times due to a four step process needed to guarantee delivery exactly once. Additionally, using QoS 2 increases the potential for DoS attacks if the publishing devices are send excessive data to the broker (Chifor et al., 2017). However, this is mitigated in the model using rate limiting, by taking a data sample, and sending data and event notifications exactly once per second. By throttling the publishing rate, the broker overload potential is minimised, and thus the notifications flow is constant. Considering there are backup devices, one second would likely not have a huge effect on the risk to human life, say if the temperature was getting too high in a HVAC facility, or the entrance gates were stuck shut.

Similarly, an interface lockout method is implemented to restrict brute force attacks overwhelming the system with excessive authentication attempts (Barcena & Wueest, 2015). If credentials are entered incorrectly three times, the interface is locked for forty-five seconds before returning to the log in screen. The failover mechanism explained earlier, additionally provides redundancy in case slave device malfunction or attacks. Backup device sets are isolated on separate VLANs, meaning they are less likely to be affected by an attack that compromised the primary node.

Constrained nodes may not have the required resources to compute and leverage cryptographic algorithms used by asymmetric cryptography (Iqbal et al., 2016). Therefore, they must authenticate by sending encrypted credentials in the MQTT CONNECT packet. Timestamps and hashes are computed for messages, and appended to the notification using hash-based message authentication codes (HMACs). Data is sent encrypted using a symmetric encryption algorithm such as Advanced Encryption Standard (AES). Therefore, notification authentication, confidentiality and integrity remains enforced. Devices are authorised to publish at a topic level, and any device that is unauthorised, or unable to authenticate, therefore is denied the ability publish or subscribe to topics.

Topic subscriptions may expire after several inactive days, this is troublesome in sports stadiums during periods of inactivity, such as the close season. In this case, stadiums need to begin running operations early to keep this issue at bay, and perform running tests to ensure the data is flowing correctly in preparation of the returning masses.

In an event-driven architecture, there is potential that more notifications will be sent than received. In a real world scenario, if the master node gets overwhelmed or goes offline, then additional consumers can either be introduced, or a broker cluster can be implemented.

The database location is therefore less important, as the master node makes decisions autonomously, and ordering is mitigated by using singular event channels with QoS 2, and MQTT brokers processing notifications on a First In, First Out (FIFO) basis (Bauer & Aschenbruck, 2017). If kept centrally, threats could compromise the network connection between the master node and the central database. Alternatively, each master node keeps its own cache database, with transactions needing to be reliably synchronised back to the central database.

Additionally, the fact that master nodes are implemented in the architecture, addresses network segmentation further. Any compromised device is contained within a stadium section, easing incident response and containing attacks. This could be segregated further, if developed into a prototype model, to contain possible attacks more granularly.

Each slave node transmits data on its own topic. Due to its decoupled nature, publish-subscribe models have difficulties maintaining consistency, however as this model has only one producer sending data per topic at any one time, and uses QoS 2 for reliability, this problem is alleviated. Each slave node set is configured with a client ID, with the backup nodes as replicas using the same client ID. Therefore, if a backup is initiated, it connects to the broker using the same ID, with the cleansession flag set to true, enabling subscriptions to continue seamlessly.

The activity diagram is shown below in Figure 10, with each swimlane individually shown in Figures 11 – 13.

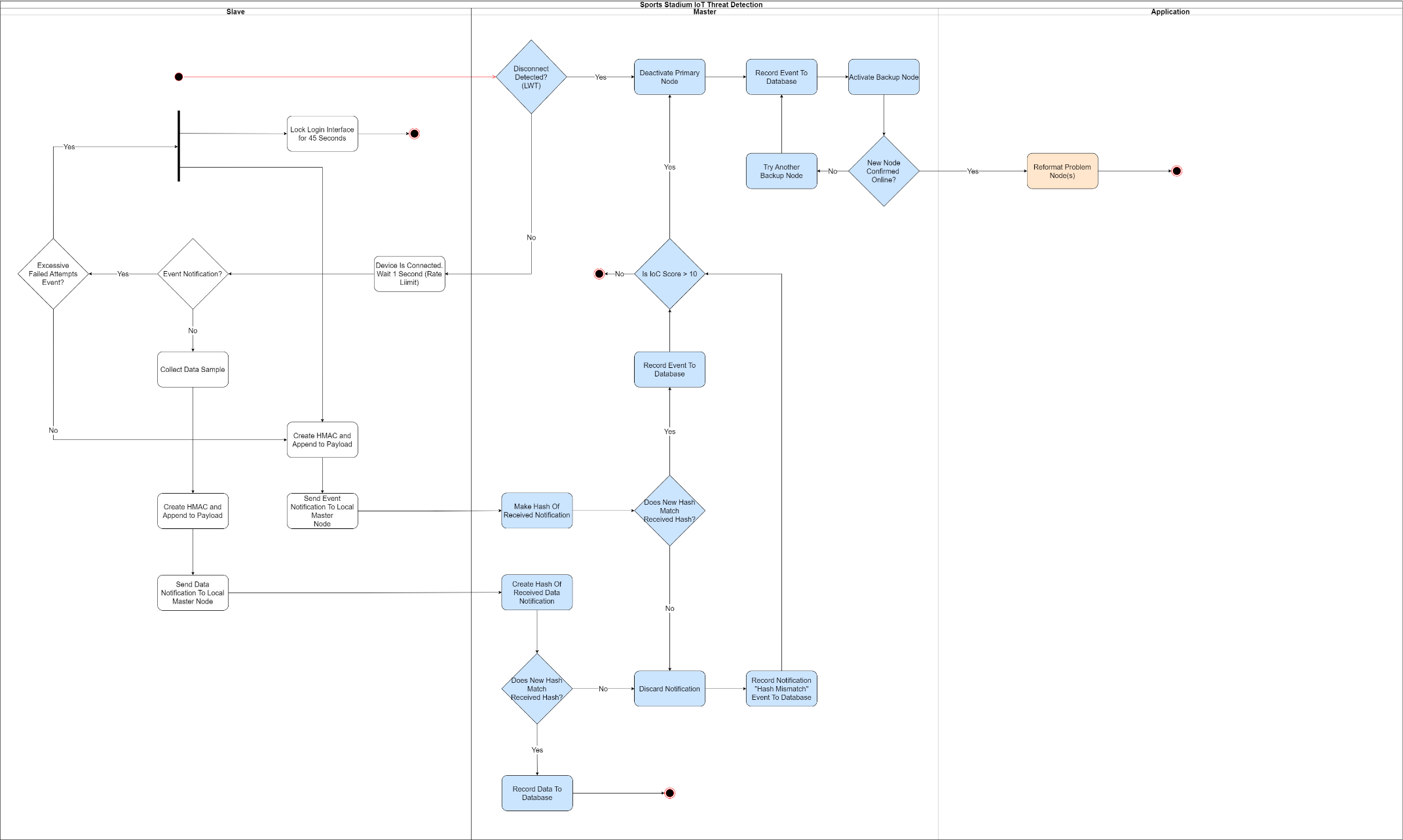


Figure 10: Activity Diagram

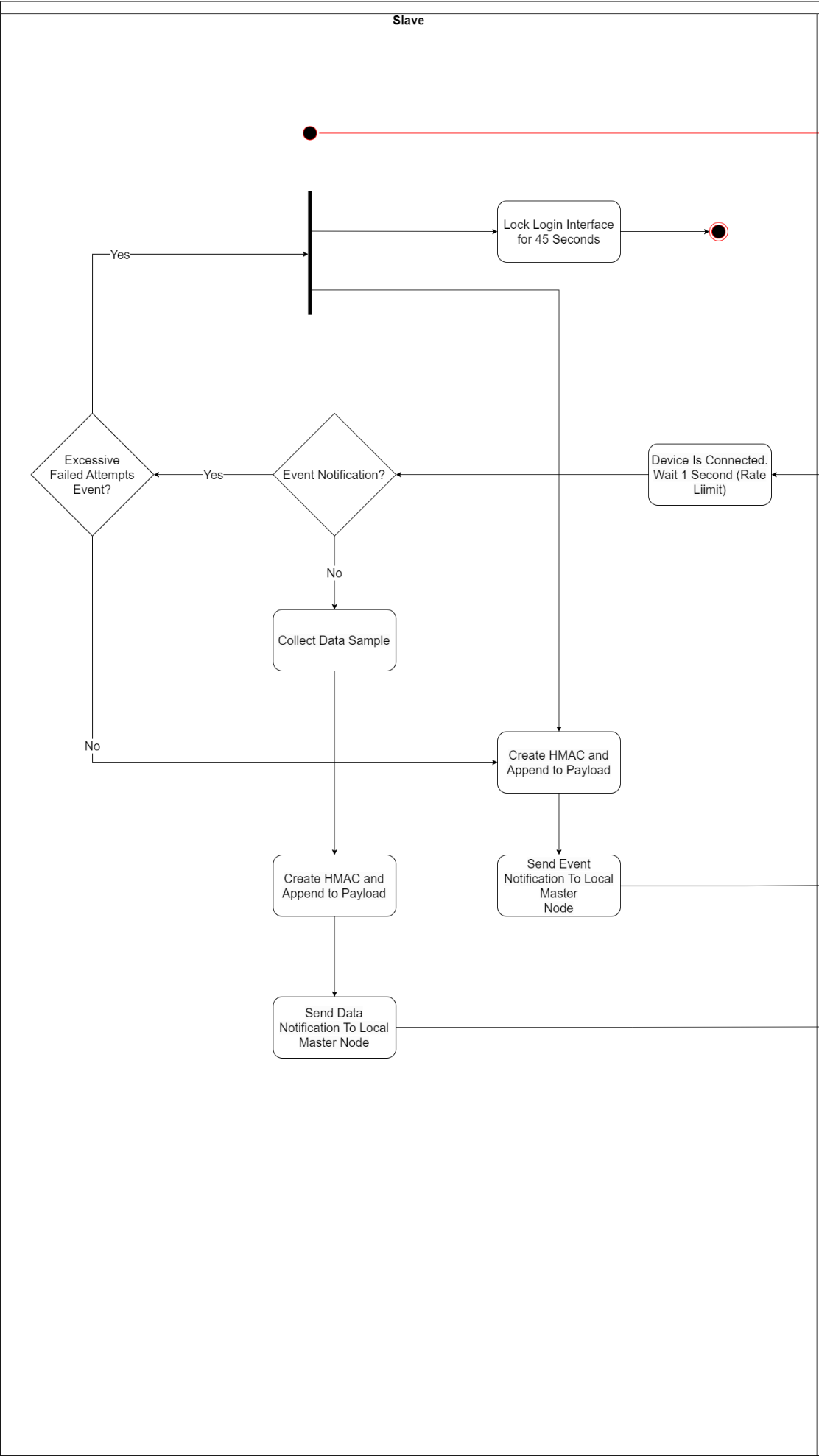


Figure 11: Slave Node Swimlane

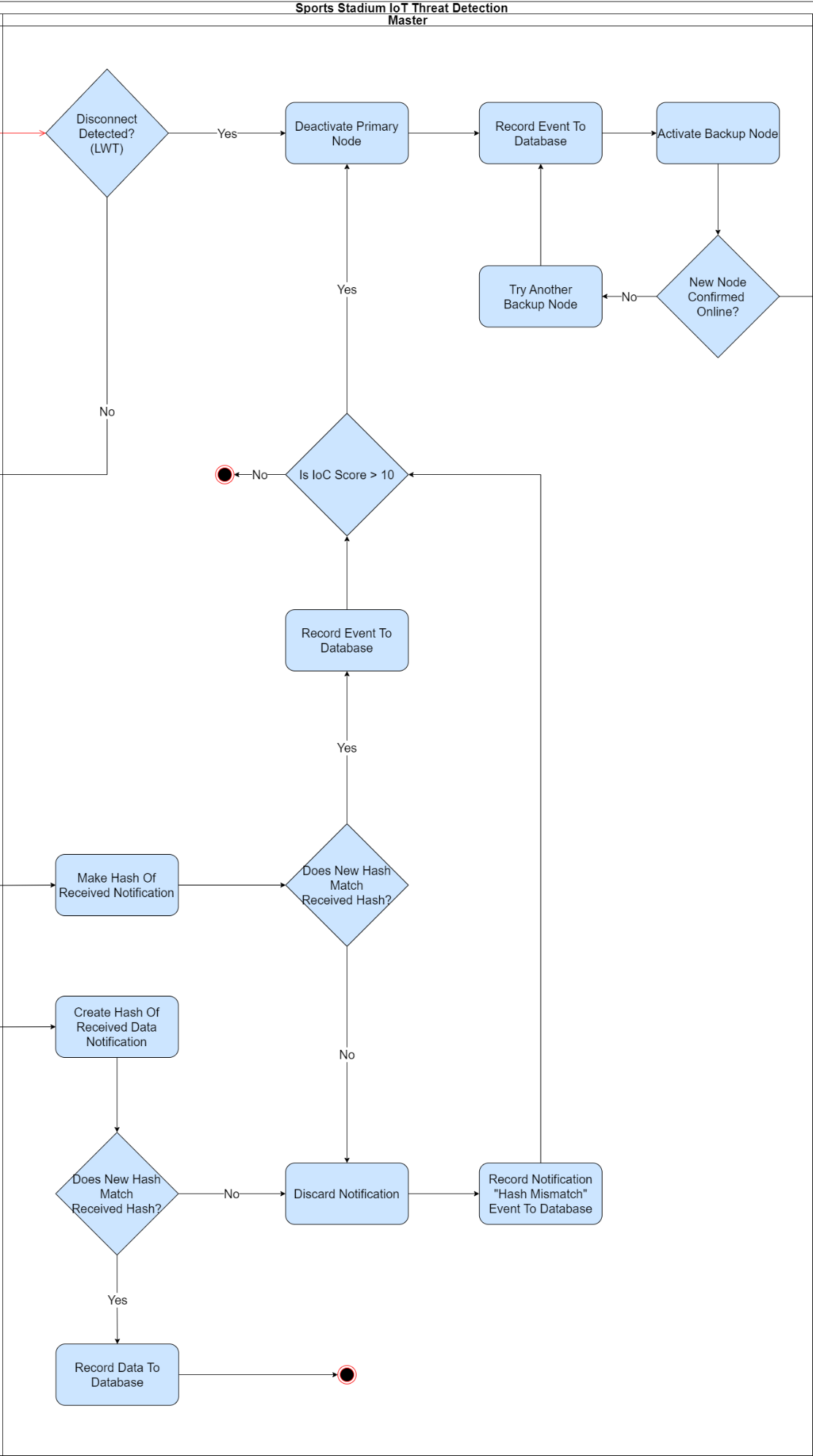


Figure 12: Master Node Swimlane



Figure 13: Application Node Swimlane

# Results

The research question stated “How can the safety and security of IoT systems in sports stadiums be improved through the integration of a management system”. Therefore, evidence has been sought to support mitigation provision for each threat identified using the ADTree using preventative and detective cyber security controls, with IoC examples being used in the detection algorithm implementation figures, including formula evidence used in implementing.

## Mitigations

Table 2: Mitigations

|  |  |
| --- | --- |
| **Threat** | **Mitigating Controls** |
| Tampering | Physical protections such as locks and tamper-resistant packaging (Varga, 2017). Brokers send LWT notifications when clients disconnect or are unable to communicate within a specified keepalive period. Following receipt of this notification, the system detects both purposeful tamper attacks and disruptive network issues (HiveMQ, 2015a). Unnecessary local connections must be disabled, such as JTAG and UART (Pearson et al., 2019), and tamper detection mechanisms should be employed (Msgna, 2022). |
| Unauthorised Firmware | Preventative controls begin by disabling Over-the-air (OTA) updates for compromised devices (Makhdoom et al., 2019), as malicious actors may still be present and can intercept the firmware. Unnecessary local connections disabled such as JTAG and UART (Martinez, N.D.; Pearson et al., 2019).  Furthermore, detection measures are employed using the following IoC:   * **Firmware Hash Mismatch:** can be a firmware manipulation indicator (He et al., 2019). * **Tamper Detected:** anti-tamper techniques can detect physical device tampering, and excessive power surges and temperatures (STMicroelectronics, 2023). * **Secure Boot Disabled:** secure boot guarantees firmware integrity and authenticity, and is able to detect modifications (Srihith et al., 2023). * **Irregular Traffic Pattern:** irregular traffic patterns can be a sign of compromised firmware (Srihith et al., 2023). |
| Jamming | The best anti-jamming solutions are to make it difficult for attackers to find the frequency in which the data is sent. Therefore, the following should be used:   * Physical bag checks for patrons upon stadium entry enables detection and confiscation of wireless jamming devices, such as the one designed by Yunan et al. (2021), at source. * Spread Spectrum, e.g. Frequency Hopping or Direct Sequence (Akram Abdul-Ghani et al., 2018; Varga et al., 2017) is a common technique to make it difficult for jammers to find the correct frequency. |
| Eavesdrop | Preventative controls are the most effective in mitigating eavesdropping, as detecting this attack is difficult (Stone, N.D.).   * Network segmentation and firewalls prevent attackers gaining access to the network to sniff packets, and strong authentication is enforced (Akram Abdul-Ghani et al., 2018; Islam & Aktheruzzaman, 2020). * Most importantly, encrypting data in transit ensures that even if the attacker gains access to packets, decryption to read the plain text is unlikely (Akram Abdul-Ghani et al., 2018; Islam & Aktheruzzaman, 2020). |
| MITM | Preventative controls include using Secure Sockets Layer (SSL) certificates to mutually authenticate clients and servers on the network, while enforcing TLS to further protect data integrity and confidentiality in transit (Gayathri et al., 2022; IBM, 2023). However, in constrained devices, this is not always possible and the following measures should be used:   * Symmetric encryption to protect payload data in transit (Akram Abdul-Ghani et al., 2018). * Strong authentication must accompany encryption techniques where certificates cannot be used (Gayathri et al., 2022).   Furthermore, modifications are detected using the following IoC:   * **Irregular Traffic Pattern:** MITM attacks can be indicated by unusual network activity (Lahmadi et al., 2020). * **Firmware Hash Mismatch:** firmware modifications are indicators of a precursor to, or result of, MITM attacks (Li et al., 2017; He et al., 2019). * **ARP Table Modified:** Address Resolution Protocol (ARP) poisoning alters the mapping between media access control (MAC) addresses to IP addresses, allowing attackers to redirect traffic (Petrović et al., 2021). * **Notification Hash Mismatch:** appending a HMAC stamp to notifications, prevents data from being modified in transit. If these do not match, the packet may have been modified by a MITM attack (Salem, 2022). |
| Lateral Movement | Attackers need to first compromise a device to then move around the network. To prevent this, as a defence in depth technique, network segregation is used to limit damage following a successful attack (Arifeen et al., 2021). Each end of the stadium has its own master node and slave nodes, and is segregated from others using a VLAN (Tomar, 2020). In addition to this, the backup slave nodes are kept on different network VLANs. |
| DoS | Using QoS 2 level reliability increases network load, and therefore rate limiting is applied to control data flows publishing once per second, preventing flooding attacks (Bhunia & Gurusamy, 2017. If a compromised or faulty slave node is detected, it is deactivated and replaced with a backup in a controlled client takeover, therefore allowing redundancy to maintain availability (Samaila et al., 2018). For wireless devices, the protections against jamming attacks also apply (Deogirikar & Vidhate, 2017). |
| Rogue Device | VLANs restrict data between nodes to inside the stadium network, and edge devices respond to client notifications, reducing the need to send data across the public Internet. This ensures defence in depth, as attackers would need to join the internal network to transmit data, moreover they also need to subscribe to topics to read packets being sent by clients. Strict authentication and authorisation requirements enforced by the broker ensures only those with a valid need to know publish and subscribe to topics (Arseni et al., 2021). |
| Malicious Access | Preventative measures include the changing of default credentials, following guidance in the Product Security and Telecommunications Infrastructure Act (2022). Strong local authentication and authorisation mechanisms prevent easy access to devices and data, and features, services and ports not necessary for its function, such as telnet, should be disabled or uninstalled (Vignau et al., 2019). These weaknesses are common attack vectors, and enabled the Mirai botnet to be so effective.  Furthermore, it is possible to detect:   * **Excessive Failed Attempts:** this can be an indicator of a malicious user attempting to gain unauthorised access (Asiri et al., 2023). * **Unusual Login Time:** unusual login times can be a malicious authentication attempt indicator (Exameam, N.D.). * **Untrusted Login Source:** unusual access attempts can be a malicious access indicator (Asiri et al., 2023; Exabeam, N.D.). * **Abnormal Device Behaviour:** abnormal behaviour can indicate malicious access, as seen in the Mirai botnet (Antonakakis, 2017). * **Privileged Access Granted:** stadium organisations should always be alert when privilege escalation is detected, as attackers will swiftly look to upgrade their access (Jullian et al., 2023; Rizvi et al., 2020). |
| Code Exploit | Devices should be purchased from known and trusted manufacturers, who adhere to the standards in the EN 303 645. The same due diligence should be taken for any distributors and installers, as vulnerabilities could be introduced along the supply chain, moreover can be detected during design stages (Omitola & Wills, 2018). Post install, security updates should be applied regularly and promptly (UL, 2019). Features, services and ports unnecessary for its function, such as telnet, should be disabled or uninstalled (Vignau et al., 2019). Input validation must be applied to prevent scripting attacks (Song & García-Valls, 2022).  Furthermore, it is possible to detect:   * **Abnormal Device Behaviour:** IoT devices generally exhibit relatively predictable behaviour, with abnormal activity a possible code exploit indicator (Wang & Lu, 2020). * **Privileged Access Granted:** a device running in privileged access mode may be a injected malicious code indicator (Noman, H.A. & Abu-Sharkh, 2023). * **Resource Exhaustion:** injection attacks, or exploits of other vulnerabilities in code, can lead to excessive use of device resources (Roohi et al., 2019; Masood & Java, 2015; Rauf et al., 2021). * **Suspicious Command:** malicious or suspicious commands can indicate a code exploit (Ding et al., 2020). |
| False Data Injection | In addition to the measures preventing rogue devices publishing their own fake data, legitimate devices employ encryption, timestamps and hashing methods to data in transit (Swinhoe, 2018).  Furthermore, fabricated data is detected using IoCs:   * **Irregular Traffic Pattern:** change in data transmission rate can be a false data indicator (Song et al., 2017). * **Threshold Exceeded:** falsified data can manifest itself as data values exceeding thresholds (Song et al., 2017). * **Resource Exhaustion:** false data injection attacks can result in power depletion, especially relevant for battery powered devices (Ye et al., 2005). * **Abnormal Device Behaviour:** false data injection is usually due to an already compromised device (Ye et al., 2005). Therefore, a device exhibiting other abnormal behaviour can be evidence of a false data injection attack. |

* **Tampering:** physical protections such as locks and tamper-resistant packaging (Varga, 2017). Brokers send LWT notifications when clients disconnect or are unable to communicate within a specified keepalive period. Following receipt of this notification, the system detects both purposeful tamper attacks and disruptive network issues (HiveMQ, 2015a). Unnecessary local connections must be disabled, such as JTAG and UART (Pearson et al., 2019), and tamper detection mechanisms should be employed (Msgna, 2022).
* **Unauthorised Firmware**: preventative controls begin by disabling Over-the-air (OTA) updates for compromised devices (Makhdoom et al., 2019), as malicious actors may still be present and can intercept the firmware. Unnecessary local connections disabled such as JTAG and UART (Martinez, N.D.; Pearson et al., 2019). Furthermore, detection measures are employed using the following IoC:
  + **Firmware Hash Mismatch:** can be a firmware manipulation indicator (He et al., 2019).
  + **Tamper Detected:** anti-tamper techniques can detect physical device tampering, and excessive power surges and temperatures (STMicroelectronics, 2023).
  + **Secure Boot Disabled:** secure boot guarantees firmware integrity and authenticity, and is able to detect modifications (Srihith et al., 2023).
  + **Irregular Traffic Pattern:** irregular traffic patterns can be a sign of compromised firmware (Srihith et al., 2023).
* **Jamming:** the best anti-jamming solutions are to make it difficult for attackers to find the frequency in which the data is sent. Therefore, the following should be used:
  + Physical bag checks for patrons upon stadium entry enables detection and confiscation of wireless jamming devices, such as the one designed by Yunan et al. (2021), at source.
  + Spread Spectrum, e.g. Frequency Hopping or Direct Sequence (Akram Abdul-Ghani et al., 2018; Varga et al., 2017) is a common technique to make it difficult for jammers to find the correct frequency.
* **Eavesdrop:** preventative controls are the most effective in mitigating eavesdropping, as detecting this attack is difficult (Stone, N.D.).
  + Network segmentation and firewalls prevent attackers gaining access to the network to sniff packets, and strong authentication is enforced (Akram Abdul-Ghani et al., 2018; Islam & Aktheruzzaman, 2020).
  + Most importantly, encrypting data in transit ensures that even if the attacker gains access to packets, decryption to read the plain text is unlikely (Akram Abdul-Ghani et al., 2018; Islam & Aktheruzzaman, 2020).
* **MITM:** preventative controls include using Secure Sockets Layer (SSL) certificates to mutually authenticate clients and servers on the network, while enforcing TLS to further protect data integrity and confidentiality in transit (Gayathri et al., 2022; IBM, 2023). However, in constrained devices, this is not always possible and the following measures should be used:
  + Symmetric encryption to protect payload data in transit (Akram Abdul-Ghani et al., 2018).
  + Strong authentication must accompany encryption techniques where certificates cannot be used (Gayathri et al., 2022).

Furthermore, modifications are detected using the following IoC:

* + **Irregular Traffic Pattern:** MITM attacks can be indicated by unusual network activity (Lahmadi et al., 2020).
  + **Firmware Hash Mismatch:** firmware modifications are indicators of a precursor to, or result of, MITM attacks (Li et al., 2017; He et al., 2019).
  + **ARP Table Modified:** Address Resolution Protocol (ARP) poisoning alters the mapping between media access control (MAC) addresses to IP addresses, allowing attackers to redirect traffic (Petrović et al., 2021).
  + **Notification Hash Mismatch:** appending a HMAC stamp to notifications, prevents data from being modified in transit. If these do not match, the packet may have been modified by a MITM attack (Salem, 2022).
* **Lateral Movement:** attackers need to first compromise a device to then move around the network. To prevent this, as a defence in depth technique, network segregation is used to limit damage following a successful attack (Arifeen et al., 2021). Each end of the stadium has its own master node and slave nodes, and is segregated from others using a VLAN (Tomar, 2020). In addition to this, the backup slave nodes are kept on different network VLANs.
* **DoS:** using QoS 2 level reliability increases network load, and therefore rate limiting is applied to control data flows publishing once per second, preventing flooding attacks (Bhunia & Gurusamy, 2017. If a compromised or faulty slave node is detected, it is deactivated and replaced with a backup in a controlled client takeover, therefore allowing redundancy to maintain availability (Samaila et al., 2018). For wireless devices, the protections against jamming attacks also apply (Deogirikar & Vidhate, 2017).
* **Rogue Device:** VLANs restrict data between nodes to inside the stadium network, and edge devices respond to client notifications, reducing the need to send data across the public Internet. This ensures defence in depth, as attackers would need to join the internal network to transmit data, moreover they also need to subscribe to topics to read packets being sent by clients. Strict authentication and authorisation requirements enforced by the broker ensures only those with a valid need to know publish and subscribe to topics (Arseni et al., 2021).
* **Malicious Access:** preventative measures include the changing of default credentials, following guidance in the Product Security and Telecommunications Infrastructure Act (2022). Strong local authentication and authorisation mechanisms prevent easy access to devices and data, and features, services and ports not necessary for its function, such as telnet, should be disabled or uninstalled (Vignau et al., 2019). These weaknesses are common attack vectors, and enabled the Mirai botnet to be so effective. Furthermore, it is possible to detect:
  + **Excessive Failed Attempts:** this can be an indicator of a malicious user attempting to gain unauthorised access (Asiri et al., 2023).
  + **Unusual Login Time:** unusual login times can be a malicious authentication attempt indicator (Exameam, N.D.).
  + **Untrusted Login Source:** unusual access attempts can be a malicious access indicator (Asiri et al., 2023; Exabeam, N.D.).
  + **Abnormal Device Behaviour:** abnormal behaviour can indicate malicious access, as seen in the Mirai botnet (Antonakakis, 2017).
  + **Privileged Access Granted:** stadium organisations should always be alert when privilege escalation is detected, as attackers will swiftly look to upgrade their access (Jullian et al., 2023; Rizvi et al., 2020).
* **Code Exploit:** devices should be purchased from known and trusted manufacturers, who adhere to the standards in the EN 303 645. The same due diligence should be taken for any distributors and installers, as vulnerabilities could be introduced along the supply chain, moreover can be detected during design stages (Omitola & Wills, 2018). Post install, security updates should be applied regularly and promptly (UL, 2019). Features, services and ports unnecessary for its function, such as telnet, should be disabled or uninstalled (Vignau et al., 2019). Input validation must be applied to prevent scripting attacks (Song & García-Valls, 2022). Furthermore, it is possible to detect:
  + **Abnormal Device Behaviour:** IoT devices generally exhibit relatively predictable behaviour, with abnormal activity a possible code exploit indicator (Wang & Lu, 2020).
  + **Privileged Access Granted:** a device running in privileged access mode may be a injected malicious code indicator (Noman, H.A. & Abu-Sharkh, 2023).
  + **Resource Exhaustion:** injection attacks, or exploits of other vulnerabilities in code, can lead to excessive use of device resources (Roohi et al., 2019; Masood & Java, 2015; Rauf et al., 2021).
  + **Suspicious Command:** malicious or suspicious commands can indicate a code exploit (Ding et al., 2020).
* **False Data Injection:** in addition to the measures preventing rogue devices publishing their own fake data, legitimate devices employ encryption, timestamps and hashing methods to data in transit (Swinhoe, 2018). Furthermore, fabricated data is detected using IoCs:
  + **Abnormal Device Behaviour**: false data injection is usually due to an already compromised device (Ye et al., 2005). Therefore, a device exhibiting other abnormal behaviour can be evidence of a false data injection attack.
  + **Irregular Traffic Pattern:** change in data transmission rate can be a false data indicator (Song et al., 2017).
  + **Threshold Exceeded:** falsified data can manifest itself as data values exceeding thresholds (Song et al., 2017).
  + **Resource Exhaustion**: false data injection attacks can result in power depletion, especially relevant for battery powered devices (Ye et al., 2005).

## Detection Algorithm Implementation

Evidence of the detection algorithm simulation is found in Figures 14-25, with Figure 26 and 27 showing hidden calculation fields:

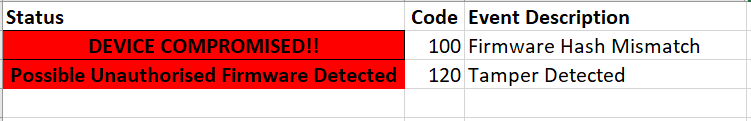


Figure 14: Successful Unauthorised Firmware Trigger 1

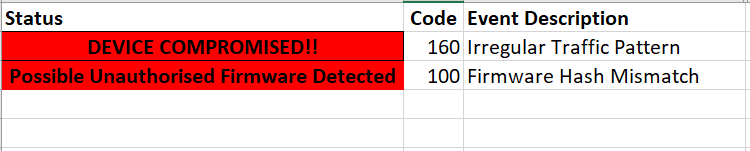


Figure 15: Successful Unauthorised Firmware Trigger 2

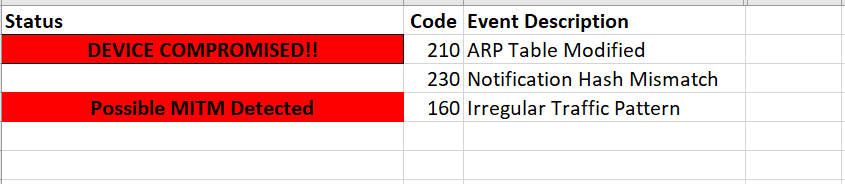


Figure 16: Successful MITM Trigger 1

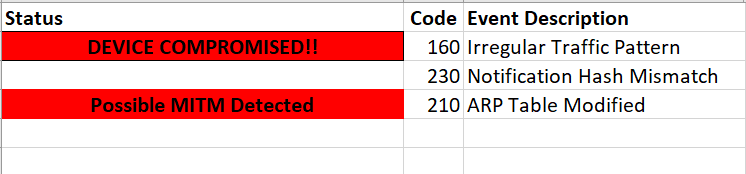


Figure 17: Successful MITM Trigger 2

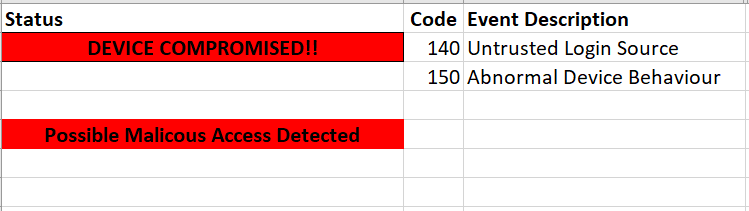


Figure 18: Successful Malicious Access Trigger 1

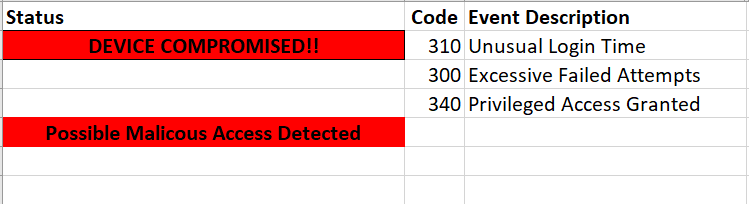


Figure 19: Successful Malicious Access Trigger 2

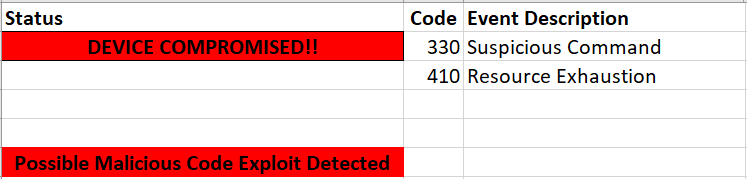


Figure 20: Successful Code Exploit Trigger 1

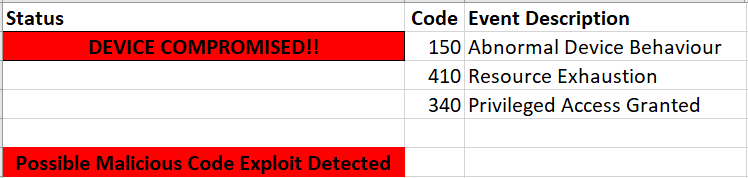


Figure 21: Successful Code Exploit Trigger 2

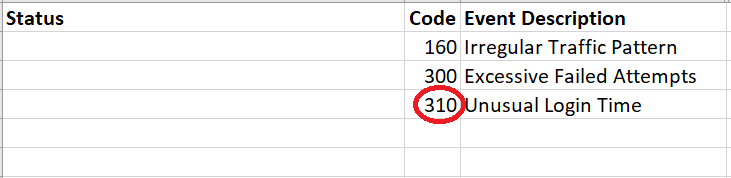


Figure 22: No Trigger - Event Code 310 not an IoC for False Data Injection

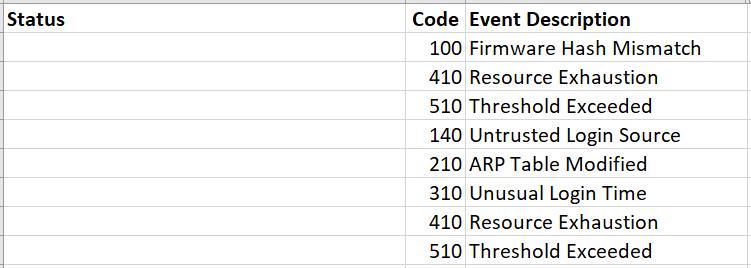


Figure 23: No Trigger (All Threat Scores Remain < 10)

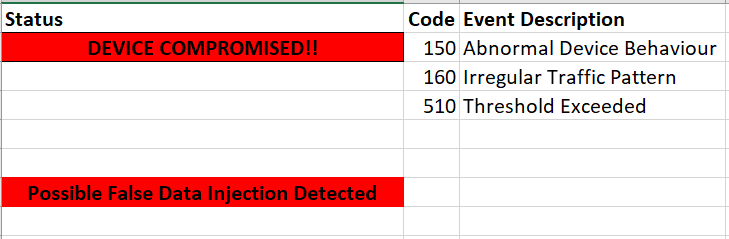


Figure 24: Successful False Data Injection Trigger 1

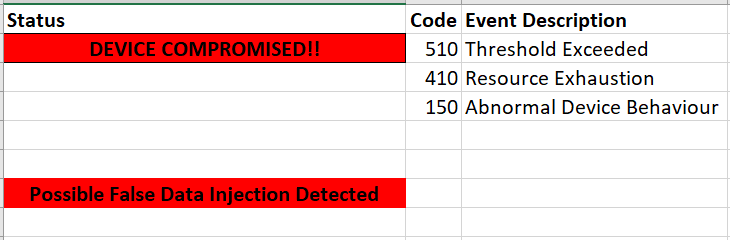


Figure 25: Successful False Data Injection Trigger 2

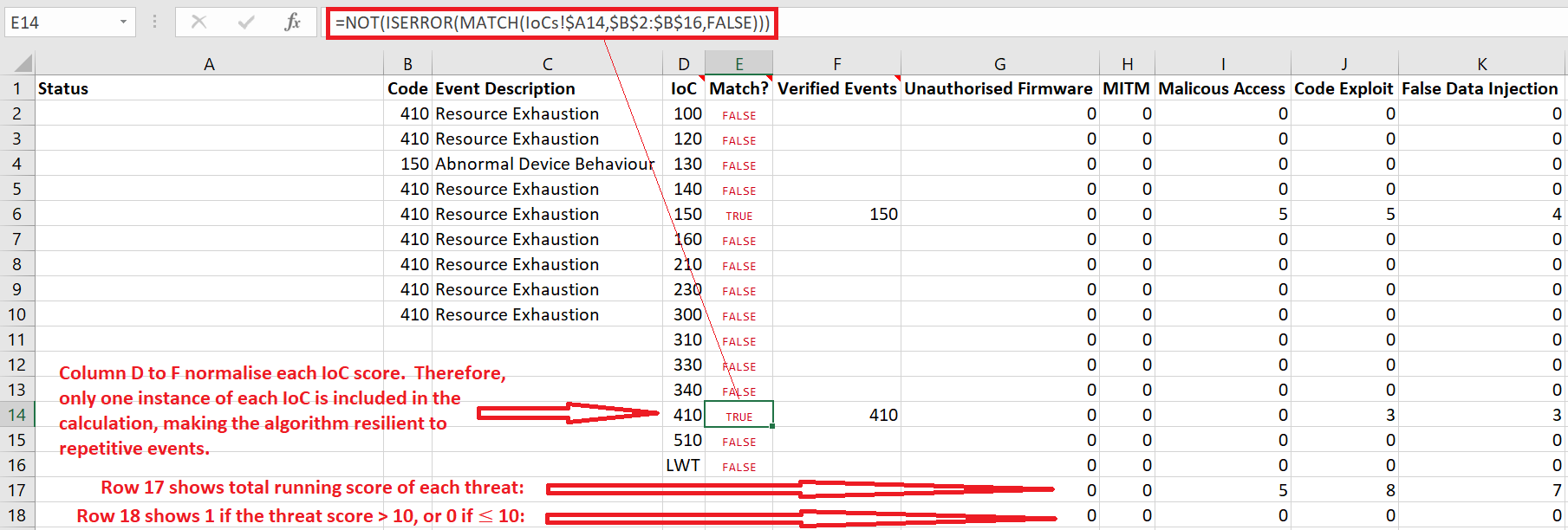


Figure 26: IoC Score Normalisation

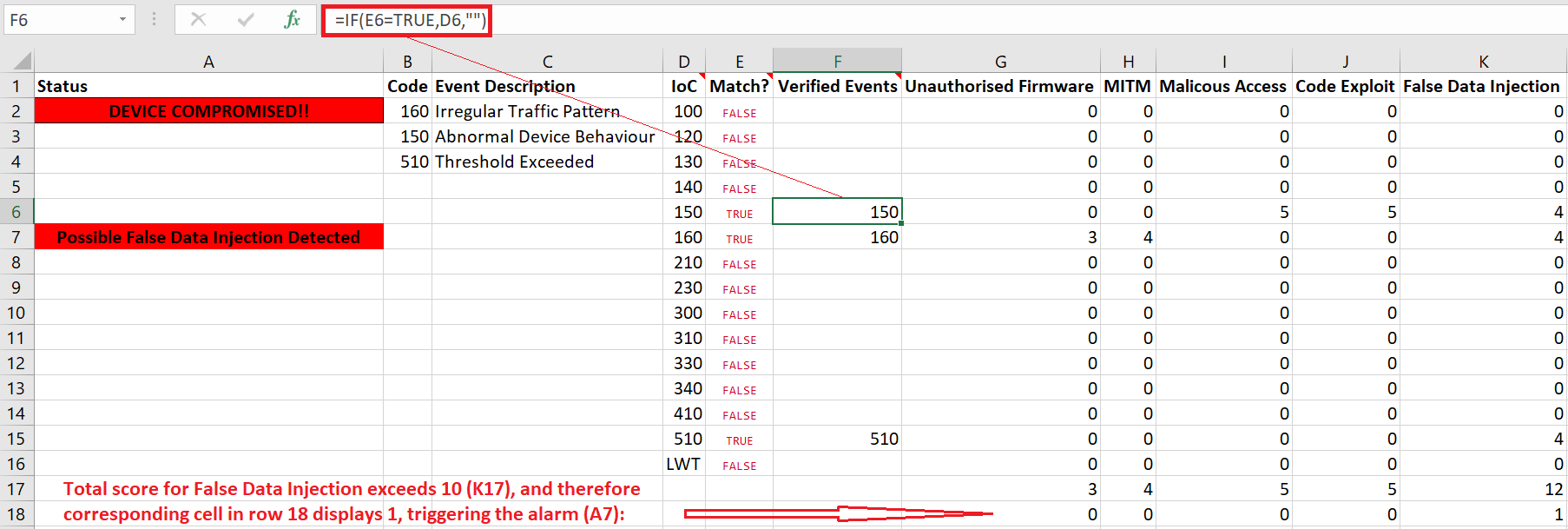


Figure 27: Hidden Score Fields Showing Alarm Triggered

# Discussion and Evaluation

The above figures show examples of threats detected using the defined IoCs, true positives. The figures also include examples of true negatives, where a threat was correctly undiagnosed due to IoCs present in the device’s operation not being sufficiently indicative of a realised threat, meaning the score had not exceeded ten.

Due to IoCs having to be present to indicate threats, the system inherently does not suffer from false positives. However, false negatives were encountered in the results. While no evidence was found of IoCs contributing to threats in the data collection, it is likely that these IoCs would be present in a production environment. For example, many of these threats are present as a secondary threat due to another being realised earlier in the cyber kill chain (Lockheed Martin, N.D.). As demonstrated in Figure 22, event code 310 is present in the device simulation, however no threat was detected. However, while no evidence was found, in a real life scenario, unusual time event code notifications could indicate an unauthorised attacker accessing the device as a precursor to executing a significant attack such as false data injection.

The figures show that threats to sports stadium IoT can be prevented and detected using the management system, with evidence found for threat. The alternative hypothesis is therefore proven, as it proves that threats can be detected using cost effective methods.

MITM: In order to prevent MITM attacks, it is preferable that SSL certificates are used which provide both authentication as well as confidentiality and integrity protection. This, however is sometimes impossible in constrained devices, and so payload encryption would be used in conjunction with authentication on topics. Authorisation can also be enforced on the broker here to ensure clients are restricted to publishing, and cannot subscribe. As symmetric encryption cannot prove the sender identity, MITM attacks are not prevented when not also using authentication.

As payload encryption works on the application layer, it works in conjunction with TLS providing an additional security layer, although this does come at a performance cost (HiveMQ, 2015b).

As added protection, hashes are configured to ensure the notifications has been unaltered in transit. In constrained devices, HMAC are used, as symmetric encryption is less computationally expensive as digital signatures, to calculate a stamp proving that the payload has remained unchanged, and that only someone who knows the secret key was able to send it (HiveMQ, 2015b).

ARP: Changes in ARP tables are a clear indicator or MITM attacks. Modifications on ARP tables map MAC addresses to IP addresses, making it possible for attackers to redirect packets to themselves without legitimate nodes suspecting.

# Research Limitations

Although sufficient time was allocated to create a PoC model, additional time would have permitted more thorough IoC investigations, resulting in a more granular model, larger sample size, and therefore potentially more accurate results (Asiamah et al., 2017). Further investigation into threats and additional technologies would also have been possible, culminating in an improved threat matrix.

Furthermore, ethical approval could have been sought to apply such a matrix to a real sports stadium which would have dual benefits for academia, and the stadium management themselves in the ever long pursuit of improved security. For example, performing real data analysis on sports stadium IoT attacks would likely result in more accurate IoC weightings based on their relevancy to threats, and therefore the validity, reliability, and generalisability of the findings would also be improved (University of Essex Online, N.D.).

To improve data collection, AI models could have been used, however the time required to acquire and understand relevant datasets, and to implement AI learning would have made it challenging to finish the project in time.

The literature review was also limited due to the sparse secondary research available for sports stadium IoT cyber security, however this meant the project was open to cover new ground.

One major limitation of the model itself is that it does not take into account advanced persistent threats (APT). APTs are threats that infiltrate the system long before the attack takes place, and so would not be detected by a real time IoC algorithm. It is also possibly prone to false positives.

Another limitation is the lack of analysis involving attacks on the broker. Brokers are a SPoF in publish-subscribe architecture and if attacks are successful, the whole model fails. Therefore, clustering or failover approaches should be used, however inclusion of analysis to identify threats to them would also be beneficial.

# Conclusion and Future Work

In this paper, an algorithm was designed to prevent and detect cyber-related threats to a sports stadium. The algorithm was based on a master-slave architecture, using the MQTT publish-subscribe communication protocol, and the research contributes to the Infrastructure Security CyBOK Category and the associated Cyber-Physical Systems Security Knowledge Area (NCSC, 2019).

Many ethical concerns regarding IoT device usage in sports stadiums were discovered, including using CCTV to record supporters and staff, as was regulation to ensure responsible IoT design, implementation, and usage. The particular use of SME to make political points by hacktivist or nation states make them a particular target.

Need to write more here…

General cybersecurity best practices should be followed to supplement the preventative and detective algorithm and controls mentioned in this report. All equipment, including non-IoT devices should be purchased and maintained by reputable manufacturers and installers. The stadium should run a regularly updated and comprehensive employee security awareness program. Policies and procedures should be followed at all times. Firmware and application updates should be applied promptly as part of an update cycle program, with non-critical pilot groups for testing. This includes network equipment and the local area network hosting typical IT devices.

A vulnerability assessment program should also be enforced, with external penetration testing included to proactively seek vulnerabilities in the network. Supplementing these controls, with those described in this paper leads to a comprehensive defence in depth approach to keeping humans safe from existential threats, allowing them to continue to enjoy the live sport experience that only sports stadiums provide.

For future work, further analysis into the available technologies should be explored, such as those mentioned by Naik (2017). Moreover, a greater IoC and threat catalogue should be sought. Thorough testing and refinement would should be performed to ensure improved weighting accuracy, and improved detection sensitivity.

It may be beneficial to adapt the model to use AI-based detection algorithms such as the Naïve Bayes classifier to classify IoCs using a pre-existing datasets. This may produce more accurate results due to the engine being fed historical data. This PoC may also be expanded to support more complex stadium systems, whereby an EDA orchestration topology model may be beneficial, rather than the simpler broker topology.

Any future work should consider the ethical issues involved in applying this to a real stadium. Another step in threat scoring should be explored, while still avoiding triggering false positives, to incorporate lurking APT indicators.

# Lessons Learned

This research extends on a topic researched in the Research Methods and Professional Practice module, and in similar fashion, the capstone project proved extremely challenging. During the process, much time was spent determining and pinpointing a particular research problem, and suitable project design. Although the topic remained consistent throughout, there was increasing pressure to find a narrow focus, which led to incessant reading at a broad level throughout most of the project.

The project required deep research to understand the technology holistically in relation to the focus area, and various strategies for implementing a suitable artefact were examined. This resulted in attending multiple online boot-camps, reading, and creating regular prototype artefacts to ensure sufficient and relevant skills were acquired and ready to put into practice. This included reading about various wireless sensor communication technologies, how they work, the available physical IoT device types available, how they are composed, and IoT attack vectors, techniques and how to defend against them. This proved a challenging learning curve due to minimal existing IoT knowledge, however much was learned in the module that will help in future work, and this has additional fuelled an appetite for continued future learning.

The necessary inclusion of an artefact proved hugely distracting from focusing on a research problem identification, and led to several unsuccessful ideas including multiple discarded plans, and the building of an unused containerised solution, see Appendix B. However, once an algorithm was finally agreed upon, there was a huge relief, and there was an instant motivation to push forward, and thankfully much ground was covered in the final few weeks.

This particular downfall did have positives, namely the acquisition of several new skills from the creating various unused prototypes. These included insight into containerisation technologies such as Docker Desktop (Docker, N.D.), with a further understanding of Docker Swarm, and associated tools such as Snyk to ensure container security. Further Linux skills were also acquired, including how packages are updated, how to use iptables and secure copy (SCP), and how to create users, and establish Secure Shell (SSH) tunnels. There were all skills relevant to the workplace, and would have been useful in former placements. Malware detection APIs were also investigated (VirusTotal, 2023), as well as various new Python libraries, including Beautiful Soup, Requests, and Fabric, all of which were unused in the final project, however may prove useful for future work.

Additionally, working remotely proved very challenging and felt isolating, which was amplified by limited video call time with supervisors, and asymmetric email correspondence resulting in long periods of frustration.

The project focus changed somewhat from the original research proposal, which was to find twelve solutions to twelve vulnerabilities identified by CISA (N.D.), see Appendix C. However, after discussions with supervisors, it was clear the plan did not meet project requirements and was quickly abandoned. This was difficult to concede due to an artefact already having been created, causing much panic, and significant delays to the project, see Appendix D.

This was caused by an initial lack of understanding of project requirements and the technologies that might be used or needed to be understood. It was concluded that this was caused by a combination of the difficulties experienced in the previous module, a non-academic background, miscommunication with supervisors, and that the capstone project gives much freedom for creativity, leading to difficulties in understanding what is required and expected.

Knowledge from previous course material proved helpful as a base for creating the artefact. This manifested as an attack-defence tree, UML diagrams, and the publish-subscribe model, which used newly learned MQTT attributes such LWT notifications, QoS levels, cleansession flags, and keepalive intervals. An in depth understanding of CoAP, and various communication architectures were also explored.

In terms of soft skills, much time was wasted reading entire research papers. In future, this could be streamlined by scanning papers, paying particular attention to abstracts and conclusions, before deciding whether to invest time reading the full content. Advice was offered on this, however there was always temptation to cover all ground ensuring nothing was missed.

Each risk stated in the research proposal were realised, and therefore the planned countermeasures proved useful when facing them. Firstly, it was clear that to complete the project, incessant reading to understand relevant technologies was required, and be to find a research gap. This in turn led to the next risk being realised, and with time quickly evaporating, the project stalled at the literature review stage and became very top heavy. There was often difficulty understanding requirements, and so regular interaction with the supervisors was vital. Time was therefore taken at a critical point to take stock and re-evaluate. This proved pivotal, and was one aspect in which remote study was beneficial due to the ability to reconstruct previous emails looking for patterns to find a way forward. Finally, laptop malfunctions on two occasions meant that the data loss risk occurred twice in the project. The advance consideration of these risks therefore proved beneficial, as each predicted countermeasure paid dividends. Continuous iterative research was practiced throughout, the project plan maintained focus and awareness of what was still required, and a work/study/life balance maintained stability. This was not helped by starting a new demanding job, however a continuous routine kept things balanced. Prior to this, during a time of unemployment, it was crucial to be proactive in conducting research during slack time, and this contributed to a good base understanding of IoT technologies. The project resources and supervisors kept things heading in the right direction, and these were invaluable finishing the project. Finally, restoring data from backups was required on two occasions. Would these not have been created in advance, the project would almost certainly have failed.

It was interesting on reflection, to see similarities in difficulties experienced with this and the previous module, in comparison with the rest of the course, see Figure 28.

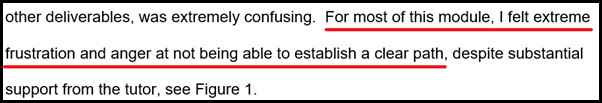


Figure 28: Research Methods and Professional Practice Individual Reflection Excerpt

If such a project was revisited, it is clear that early problem space diagnosis is of paramount importance, leading to strong project foundations, with dedicated thinking during earlier modules helping to sculpt ideas for the ultimate deliverable. Furthermore, project requirements should also be understood as clearly as possible in advance, allowing to focus on a clear path forward.

# References

Abate, F., Carrat[ù](https://ieeexplore.ieee.org/author/37086101131), M., Liguori, C., Ferro, M. & Paciello, V. (2018) ‘Smart meter for the IoT’, *2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*. Houston, United States, 14-17 May 2018. IEEE. 1-6.

A Dev’ Story. (2021) What is Event Driven Archsitecture? (EDA - part 1). Available from: <https://www.youtube.com/watch?v=DQ5Cbt8DQbM> [Accessed 14 July 2023].

Abdelrasoul, E., Mahmoud, I., Stergiou, P. & Katz, L. (2015) The accuracy of a real time sensor in an instrumented basketball. *Procedia Engineering* 112: 202-206. DOI: https://doi.org/10.1016/j.proeng.2015.07.200

Abramson, C. M. & Sánchez-Jankowski, M. (2020) ‘Conducting Comparative Participant Observation: Behavioralist Procedures and Techniques’, in: Abramson, C. M. & Neil Gong (eds) *Beyond the Case: The Logics and Practices of Comparative Ethnography*. Oxford: Oxford University Press. 57-87.

Abughazaleh, N., Bin Jabal, R., Btish, M. & Mahalingham, H. (2020) DoS Attacks in IoT Systems and Proposed Solutions. *International Journal of Computer Applications* 176(33): 16-19. DOI: <https://doi.org/10.5120/ijca2020920397>

ACM. (2018) ACM Code of Ethics and Professional Conduct. Available from: https://www.acm.org/code-of-ethics [Accessed 14 April 2023].

Akram Abdul-Ghani, H., Konstantas, D. & Mahyoub, M. (2018) A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *International Journal of Advanced Computer Science and Applications (IJACSA)* 9(3): 355-373. DOI: https://dx.doi.org/10.14569/IJACSA.2018.090349

Alaba, F. A., Othman, M., Hashem, I. A. T. & Alotaibi, F. (2017) Internet of Things security: A survey. *Journal of Network and Computer Applications* 88: 10-28. DOI: <https://doi.org/10.1016/j.jnca.2017.04.002>

Alahmadi, S., Rojas, P., Idriss, H & Bayoumi, M. (2023) ‘Taxonomy of Consumer and Industrial IoT’, [*SoutheastCon 2023*](https://ieeexplore.ieee.org/xpl/conhome/10115054/proceeding). Orlando, United States, 1-16 April. IEEE. 418-424.

Alhadad, S. A. & Abood, O. G. (2018). Enhancing smart sport management based on information technology. *IOSR Journal of Sports and Physical Education (IOSR-JSPE)* 5(5): 19-26. DOI: <https://doi.org/10.9790/6737-05051926>

Antonakakis, M. et al. (2017) ‘Understanding the Mirai Botnet’, *SEC'17: Proceedings of the 26th USENIX Conference on Security Symposium*. Vancouver, 16-18 August. United States: USENIX Association. 1093-1110. Available from: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf [Accessed 19 July 2023].

Arifeen, M., Petrovski, A. & Petrovski, S. (2021) ‘Automated Microsegmentation for Lateral Movement Prevention in Industrial Internet of Things (IIoT)’, *2021 14th International Conference on Security of Information and Networks (SIN)*. 15-17 December 2021. Piscataway: IEEE. 1-6. DOI: https://doi.org/10.1109/SIN54109.2021.9699232. [Accessed 19 July 2023].

Aroganam, G., Manivannan, N. & Harrison, D. (2019) Review on Wearable Technology Sensors Used in Consumer Sport Applications. *Sensors* 19(0): 1983. DOI: https://doi.org/10.3390/s19091983

Arseni, S., Chifor, B., Coca, M., Medvei, M., Bica, I. & Matei, I. (2021) RESFIT: A Reputation and Security Monitoring Platform for IoT Applications. *Electronics* 10(15): 1840. DOI: https://doi.org/[10.3390/electronics10151840](http://dx.doi.org/10.3390/electronics10151840)

Asiamah, N., Mensah, H.K. & Oteng-Abayte, E.F. (2017) Do Larger Samples Really Lead to More Precise Estimates? A Simulation Study. *American Journal of Educational Research* 5(1): 9-17. Available from: https://www.researchgate.net/publication/312174643\_Do\_Larger\_Samples\_Really\_Lead\_to\_More\_Precise\_Estimates\_A\_Simulation\_Study

Asiri, M., Saxena, N., Gjomemo, R. & Burnap, P. (2023) ‘Understanding Indicators of Compromise against Cyber-Attacks in Industrial Control Systems: A Security Perspective’, *ACM transactions on cyber-physical systems* 7(2): 1-33. DOI: https://doi.org/ 10.1145/3587255 [Accessed 20 July 2023].

Bansal, M. & Priya (2021). Performance Comparison of MQTT and CoAP Protocols in Different Simulation Environments. In: Ranganathan, G., Chen, J. & Rocha, Á. (eds) *Inventive Communication and Computational Technologies*. Lecture Notes in Networks and Systems, vol 145. Springer, Singapore. DOI: <https://doi.org/10.1007/978-981-15-7345-3_47>

Barcena, M. B. & Wueest, C. (2015) *Insecurity in the Internet of Things*. Symantec. Available from: <https://docs.broadcom.com/doc/insecurity-in-the-internet-of-things-en> [Accessed 13 July 2023].

Baroncelli, A. & Ruberti, M. (2022) ‘Smart Sport Arenas Make Cities Smarter’, in: Visvizi, A. & Troisi, O. (eds) *Managing Smart Cities: Sustainability and Resilience Through Effective Management*. Cham: Springer. 89–104.

Bauer, J. & Aschenbruck, N. (2017) ‘Measuring and Adapting MQTT in Cellular

Networks for Collaborative Smart Farming’, *IEEE 42nd Conference on Local Computer Networks (LCN)*. Singapore, 9-12 October. IEEE. 294-302. DOI: https://doi.org/ 10.1109/LCN.2017.81 [Accessed 19 July 2023].

BBC. (2023a) London Marathon 2023: Just Stop Oil 'will continue disrupting sporting events'. Available from: <https://www.bbc.co.uk/sport/athletics/65335724> [Accessed 27 May 2023].

BBC. (2023b) Wimbledon 2023: Just Stop Oil protesters interrupt play twice, jigsaws taken off sale. Available from: <https://www.bbc.co.uk/sport/tennis/66041547> [Accessed 28 July 2023].

Benslimane, K. (2022) Protecting global stadiums and events with Self-Learning AI. 03 March 2022. Available from: <https://darktrace.com/blog/protecting-global-stadiums-and-events-with-self-learning-ai> [Accessed 08 April 2023].

Bettayeb, M., Nasir, Q. & Abu Talib, M. (2019) ‘Firmware Update Attacks and Security for IoT Devices: Survey’, *Proceedings of the ArabWIC 6th Annual International Conference Research Track*. Rabat, Morocco, 7 – 9 March. New York: Association for Computing Machinery. 1-6. DOI: <https://doi.org/10.1145/3333165.3333169> [Accessed 19 July 2023].

Bhandari, P. (2022) Ethical Considerations in Research | Types & Examples. Available from: <https://www.scribbr.co.uk/research-methods/ethical-considerations> [Accessed 12 July 2023].

Bhunia, S.S. & Gurusamy, M. (2017) ‘Dynamic Attack Detection and Mitigation

in IoT using SDN’, *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*. Melbourne, Australia, 22-24 November. IEEE. 1-6. DOI: https://10.1109/ATNAC.2017.8215418 [Accessed 19 July 2023].

Brey, P. (2004) Ethical Aspects of Facial Recognition Systems in Public Places. *Journal of information, communication and ethics in society* 2(2): 97-109. DOI: <https://doi.org/10.1108/14779960480000246>

BRM. (N.D.) Qualitative Data Analysis. Available from: <https://research-methodology.net/research-methods/data-analysis/qualitative-data-analysis> [Accessed 27 July 2023].

BSIA. (2021) BSIA launches industry-first ethical Automated Facial Recognition (AFR) framework. Available from: <https://www.bsia.co.uk/blogs/152/bsia-launches-industry-first-ethical-aut> [Accessed 14 April 2023].

Burhan, M., Rehman, R.A., Khan, B. & Kim, B. (2018) IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors* 18(9): DOI: <https://doi.org/10.3390/s18092796>

Carvalho, G., Cabral , B., Periera, V. & Bernardino, J. (2021) Edge computing: current trends, research challenges and future directions. *Computing* 103(5): 993-1023. DOI: <https://doi.org/10.1007/s00607-020-00896-5>

Cheong, S. (2022) Understanding MQTT Quality of Service or also known as MQTT QoS. 6 October 2022. *MQTT basics*. Available from: <https://cedalo.com/blog/understanding-mqtt-qos> [Accessed 18 July 2023].

Chifor, B., Bica, I. & Patriciu, V. (2017) ‘Mitigating DoS attacks in publish-subscribe

IoT networks’, *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI).* Targoviste, Romania, 29 June-01 July. IEEE. 1-6. DOI: https://doi.org/ 10.1109/ECAI.2017.8166463 [Accessed 19 July 2023].

CISA. (N.D.) Stadium Spotlight: Connected Devices and Integrated Security Considerations. <https://www.cisa.gov/resources-tools/resources/stadium-spotlight-connected-devices-and-integrated-security-considerations> [Accessed 19 April 2023].

CockroachDB. (2021) Idempotency and Ordering. Available from: <https://www.youtube.com/watch?v=ZOZ8LuVS8VY> [Accessed 14 July 2023].

Conti, M., Dragoni, N. & Lesyk, V. (2016) A Survey of Man In The Middle Attacks. *IEEE Communications Surveys & Tutorials* 18(3): 2027–2051. DOI: <https://doi.org/10.1109/COMST.2016.2548426>

Danbatta, S.J. & Varol, A. (2019) ‘Comparison of Zigbee, Z-Wave, Wi-Fi, and

Bluetooth Wireless Technologies Used in Home Automation’, *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. Barcelos, Portugal, 10-12 June.IEEE. 1-5. DOI: <https://doi.org/10.1109/ISDFS.2019.8757472> [Accessed 19 July 2023].

Data Protection Act 2018, United Kingdom. Available from: <https://www.legislation.gov.uk/ukpga/2018/12/enacted> [Accessed 13 April 2023].

Datta, P. M. & Acton, T. (2022) From disruption to ransomware: Lessons From hackers. *Journal of Information Technology Teaching Cases* 0(0): DOI: <https://doi.org/10.1177/204388692211102>

Dawson, C. W. (2015) *Projects in Computing and Information Systems: A Student's Guide*. Harlow: Pearson Education. Available from: <https://ebookcentral-proquest-com.uniessexlib.idm.oclc.org/lib/universityofessex-ebooks/detail.action?docID=5176771> [Accessed 18 July 2023].

De Carvalho Silva, J., Rodrigues, J., Alberti, A.M., Šolić, P. & Aquino, A. L. L. (2017) LoRaWAN — ‘A low power WAN protocol for Internet of Things: A review and opportunities’, 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech). Split, Croatia, 2017. 1-6. Available from: <https://ieeexplore.ieee.org/abstract/document/8019271> [Accessed 19 July 2023].

Deogirikar, J. & Vidhate, A. (2017) ‘Security Attacks in IoT: A Survey’, *International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. Palladam, India, 10-11 February. IEEE. 32-37.

Ding, F. et al. (2020) DeepPower: Non-intrusive and Deep Learning-based Detection of IoT Malware Using Power Side Channels, *Proceedings of the 15th ACM Asia conference on computer and communications security*. Taipai, Taiwan, 5-9 October. New York: Association for Computing Machinery. 33-46. <http://dx.doi.org/10.1145/3320269.3384727> [Accessed 21 July 2023].

Docker. (N.D.) Docker Desktop. Available from: <https://www.docker.com/products/docker-desktop> [Accessed 22 July 2023].

ETSI. (2020) ETSI EN 303 645. Available from: <https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf> [Accessed 12 April 2023].

Exabeam. (N.D.) Abnormal Authentication. Available from: <https://www.exabeam.com/wp-content/uploads/EXA-Solution-Brief-Abnormal-Authentication-2021-05.pdf> [Accessed 20 July 2023].

Fang, L. (2022) The deployment of smart sharing stadium based on 5G and mobile edge computing. *Wireless Networks* 1-11.DOI: https://doi.org/10.1007/s11276-021-02855-0

Farooq, M.S., Riaz, S., Abid, A., Abid, K. & Naeem, M.A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. *IEEE Access* 7: 156237–156271. DOI: <https://doi.org/10.1109/access.2019.2949703>

Farquhar, J.D. (2012) *Case Study Research for Business.* London: SAGE Publications Ltd. Available from: https://methods-sagepub-com.uniessexlib.idm.oclc.org/book/case-study-research-for-business/n3.xml [Accessed 23 July 2023].

FIFA. (2022) Limb-tracking technology offers new array of possibilities. Available from: <https://www.fifa.com/technical/football-technology/news/limb-tracking-technology-offers-new-array-of-possibilities> [Accessed 10 April 2023].

Gayathri, R. et al. (2022) Detection and Mitigation of IoT-Based Attacks Using SNMP and Moving Target Defense Techniques. *Sensors* 23(3): 1708. DOI: https://doi.org/10.3390/s23031708

GDPR. (2022) General Data Protection Regulation (GDPR). Available from: https://gdpr.eu/tag/gdpr [Accessed 13 April 2023].

Gorton, I. (2022) *Foundations of Scalable Systems: Designing Distributed Architectures*. Sebastopol, United States. O’Reilly Media Inc. Available from: <https://learning.oreilly.com/library/view/foundations-of-scalable/9781098106058> [Accessed 14 July 2023].

Gowda, M., Dhekne, A., Shen, S., Choudhury, R. R., Yang, S. X., Yang, L., Golwalkar, S. & Essanian, A. (2018) IoT Platforms for Sports Analytics. *GetMobile Mobile Computing and Communications* 21(4): 8-14. DOI: https://doi.org/10.1145/3191789.3191793

Gupta, A. (2019) *The IoT Hacker’s Handbook: A Practical Guide to Hacking the Internet of Things*. Berkeley, United States: Apress. Available from: https://learning.oreilly.com/library/view/the-iot-hackers/9781484243008/html/473264\_1\_En\_1\_Chapter.xhtml [Accessed 14 July 2023].

Harrod Sport. (2018) Hawk-Eye - Technology in Sport. Available from: <https://www.harrodsport.com/advice-and-guides/hawkeye-technology-in-sport> [Accessed 16 April 2023].

Hasan, M. (2022) State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. Available from: <https://iot-analytics.com/number-connected-iot-devices> [Accessed 31 March 2023].

He, X., Algahtani, S., Gamble, R. & Papa, M. (2019) ‘Securing Over-The-Air IoT Firmware Updates using Blockchain’, *COINS '19: Proceedings of the International Conference on Omni-Layer Intelligent Systems*. Crete, Greece, 5-7 May 2019. New York, United States. 164-171. DOI: <https://doi.org/10.1145/3312614.3312649> [Accessed 20 July 2023].

HiveMQ. (2015a) What is MQTT Last Will and Testament (LWT)? – MQTT Essentials: Part 9. 9 March 2015. *MQTT Essentials.* Available from: <https://www.hivemq.com/blog/mqtt-essentials-part-9-last-will-and-testament> [Accessed 02 July 2023].

HiveMQ. (2015b) MQTT Message Data Integrity - MQTT Security Fundamentals. *MQTT Security Fundamentals.* Available from: https://www.hivemq.com/blog/mqtt-security-fundamentals-mqtt-message-data-integrity [Accessed 19 July 2023].

HM Government. (2018) Code of Practice for consumer IoT security. Available from: <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security> [Accessed 12 April 2023].

Hutchins, B. & Andrejevic, M. (2021) Olympian Surveillance:

Sports Stadiums and the Normalization of Biometric Monitoring. *International Journal of Communication* 15(2021): 363–382.Available from: <https://ijoc.org/index.php/ijoc/article/view/16377/3323> [Accessed 16 April 2023].

Iberdrola. (N.D.) Industry 4.0: which technologies will mark the Fourth Industrial Revolution? Available from: <https://www.iberdrola.com/innovation/fourth-industrial-revolution#:~:text=The%20concept%20of%20the%20Fourth,book%20of%20the%20same%20name>. [Accessed 31 March 2023].

IBM. (2023) How TLS provides identification, authentication, confidentiality, and integrity. Available from: <https://www.ibm.com/docs/en/ibm-mq/9.1?topic=tls-how-provides-identification-authentication-confidentiality-integrity> [Accessed 26 July 2023].

Ihuman, A. (N.D.) Request-Driven (RESTful) vs Event-Driven in Microservices. Available from: <https://blog.getambassador.io/request-driven-restful-vs-event-driven-in-microservices-82798cba80d5> [Accessed 19 July 2023].

INTERPOL. (N.D.) Project Stadia. Available from: <https://www.interpol.int/en/How-we-work/Project-Stadia> [Accessed 16 April 2023].

Iqbal, M. A., Olaleye, O.G. & Bayoumi, M.A. (2016) A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches. *Global journal of computer science and technology* 16(7): 1-10. Available from: <https://globaljournals.org/GJCST_Volume16/1-A-Review-on-Internet-of-Things.pdf> [Accessed 16 July 2023].

Islam, M. R. & Aktheruzzaman, K.M. (2020) An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions. *Journal of Computer and Communications* 8(4): 11-25. DOI: http://dx.doi.org/10.4236/jcc.2020.84002

Jabraeil Jamali, M. A., Bahrami, B., Heidari, A., Allahverdizadeh, P. & Norouzi, F. (2020) *Towards the Internet of Things: Architectures, Security, and Applications*. Cham: Springer. Available from: <https://doi.org/10.1007/978-3-030-18468-1_2> [Accessed 26 July 2023].

Jan, S., Yafi, E., Hafeez, A., Khatana, H. W., Hussain, S., Akhtar, R. & Wadud, Z. (2021) Investigating Master–Slave Architecture for Underwater Wireless Sensor Network. *Sensors* 21(9): 3000. DOI: https://doi.org/10.3390/s21093000

Jansen, G. & Saladas, J. (2020) Advantages of the event-driven architecture pattern. Available from: <https://developer.ibm.com/articles/advantages-of-an-event-driven-architecture> [Accessed 14 July 2023].

Javaid, U., Furqan, J., Javaid, U., Khan, M. T. R. & Jäntti, R. (2020) Rogue Device Mitigation in the Internet of Things: A Blockchain-Based Access Control Approach. *Mobile Information Systems* 2020. DOI: https://doi.org/10.1155/2020/8831976

Jazzar, M. & Hamad, M. (2022) ‘An Analysis Study of IoT and DoS Attack Perspective’, in: Agarwal, B., Rahman, A., Patnaik, S. & Poonia, R.C. (eds) *Proceedings of International Conference on Intelligent Cyber-Physical Systems*. Singapore: Springer. 127–142.

Jiang, W., Zhan, J., Chang, Z. & Sang, N. (2011) Energy-Efficient and Reliable Wireless Message Scheduling for Mission-Critical Cyber Physical Systems. *Journal of Control Engineering and Applied Informatics* 13(3): 95-100. Available from: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=cb75f490d7c972619374ebe7ea3cc3534dad0bac>

Jullian, O., Otero, B., Rodriguez, E., Gutierrez, N., Antona, H. & Canal, R. (2023) Deep‑Learning Based Detection for Cyber‑Attacks in IoT Networks: A Distributed Attack Detection Framework. *Journal of Network and Systems Management* 31(33): DOI: https://doi.org/10.1007/s10922-023-09722-7

Juniper Research. (2022) SMART CITIES: MARKET FORECASTS, KEY TECHNOLOGIES & ENVIRONMENTAL IMPACT 2022-2026. Available from: <https://www.juniperresearch.com/researchstore/sustainability-technology-iot/smart-cities-research-report> [Accessed 19 April 2023].

Kalsoom, T. et al. (2021) Impact of IoT on Manufacturing Industry 4.0: A New Triangular Systematic Review. *Sustainability* 13(22): 12506. DOI: https://doi.org/10.3390/su132212506

Kambourakis, G., Kolias, C. & Stavrou, A. (2017) ‘The Mirai Botnet and the IoT Zombie Armies’, *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*. Baltimore, MD, USA, 23-25 October. IEEE. 267-272. DOI: <https://doi.org/10.1109/MILCOM.2017.8170867> [Accessed 19 July 2023].

Kannan, R., Jo, J. & Go, H.S. (2014) ‘Improved event driven architecture for tizen sensor framework’, *Proceedings of the 1st International Conference on Mobile Software Engineering and Systems*. Hyderabad, India. 2-3 June. New York: Association for Computing Machinery. 75-78. DOI: <https://doi.org/10.1145/2593902.2593922> [Accessed 19 July 2023].

Karagiannis, V., Chatzimisios, P., Vázquez-Gallego, F. & Alonso-Zarate, J. (2015) A Survey on Application Layer Protocols for the Internet of Things, *Transaction on IoT and Cloud computing* 3(1): 11-17. Available from: <https://www.researchgate.net/publication/303192188_A_survey_on_application_layer_protocols_for_the_Internet_of_Things> [Accessed 15 July 2023].

Kaspersky. (2018) OlympicDestroyer is here to trick the industry. Available from: <https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295> [Accessed 10 April 2023].

Khattak, H.A., Ruta, M. & Di Sciascio. (2014) ‘CoAP-based Healthcare Sensor Networks: a survey’, *11th International Bhurban Conference on Applied Sciences & Technology* (IBCAST). Islamabad, 14-18 January. 499-503. DOI: <https://doi.org/10.1109/IBCAST.2014.6778196> [Accessed 19 July 2023].

Koziolek, H., Grüner, S. & Rückert, J. (2020). A Comparison of MQTT Brokers for Distributed IoT Edge Computing. In: Jansen, A., Malavolta, I., Muccini, H., Ozkaya, I.& Zimmermann, O. (eds) Software Architecture. ECSA 2020. Lecture Notes in Computer Science, vol 12292. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-58923-3\_23

Kvarda, L., Hynk, P., Vojtech, L., Lokaj, Z., Neruda, M. & Zitta, T. (2016) Software Implementation of a Secure Firmware Update Solution in an IOT Context. *Advances in Electrical and Electronic Engineering* 14(4): 389-396.DOI: <https://doi.org/10.15598/aeee.v14i4.1858>

Lahmadi, A., Duque, A., Heraief, N. & Francq, J. (2020) MitM Attack Detection in BLE Networks Using Reconstruction and Classification Machine Learning Techniques. In: Koprinska, I., *et al.* (eds) *ECML PKDD 2020 Workshops. ECML PKDD 2020*. Communications in Computer and Information Science, vol 1323. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-65965-3\_10

Larmo, A., Del Carpio, F., Arvidson, P. & Chirikov, R. (2018) ‘Comparison of CoAP and MQTT Performance Over Capillary Radios’, *2018 Global Internet of Things Summit (GIoTS)*. Bilbao, 04-07 June. IEEE. 1-6. DOI: <https://doi.org/10.1109/GIOTS.2018.8534576> [Accessed 19 July 2023].

Li, C., Qin, Z., Novak, E. & Li, Q. (2017) Securing SDN Infrastructure of IoT–Fog Networks From MitM Attacks. *IEEE Internet of Things Journal* 4(5): 1156 – 1164. DOI: https://doi.org/10.1109/JIOT.2017.2685596

Li, S. (2022) ‘Development of Intelligent Sports Stadium System Based on Internet of Things Technology’, 2022 *2nd International Conference on Computer Technology and Media Convergence Design (CTMCD 2022)*. 2022. Atlantis Press. 570-576.

Li, S. & Xu, L.D. (2017) *Securing the Internet of Things*. Cambridge, United States : Syngress. Available from: https://learning.oreilly.com/library/view/securing-the-internet/9780128045053/xhtml/chp002.xhtml#st0070 [Accessed 13 July 2023].

Li, S., Xu, L.D. & Zhao, S. (2018) 5G Internet of Things: A survey. *Journal of Industrial Information Integration* 10: 1-9. DOI: <https://doi.org/10.1016/j.jii.2018.01.005>

Lockheed Martin. (N.D.) Cyber Kill Chain. Available from: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html> [Accessed 28 July 2023].

Lueth, K. L. (2020) State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. Available from: <https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time> [Accessed 31 March 2023].

Macero García, M. (2020) *Learn Microservices with Spring Boot: A Practical Approach to RESTful Services Using an Event-Driven Architecture, Cloud-Native Patterns, and Containerization.* 2nd ed. Berkeley: Apress. Available from: https://learning.oreilly.com/library/view/learn-microservices-with/9781484261316/html/458480\_2\_En\_7\_Chapter.xhtml [Accessed 14 July 2023].

Makhdoom, I., Abolhasan, M., Lipman, J., Lui, R.P. & Ni, W. (2019) Anatomy of Threats to the Internet of Things. [*IEEE Communications Surveys & Tutorials*](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9739)21(2): 1636-1675. DOI: https://doi.org/10.1109/COMST.2018.2874978

Margolis, J., Oh, T.T., Jadhav, S., Kim, Y.H. & Kim, J.N. (2017) ‘An In-Depth Analysis of the Mirai Botnet’, *2017 International Conference on Software Security and Assurance (ICSSA)*. Altoona, United States, 24-25 July. IEEE. 6-12. DOI: https://doi.org/10.1109/ICSSA.2017.12 [Accessed 19 July 2023].

Martinez, I. C. (N.D.) The key to everything: Firmware on IoT devices. Available from: <https://www.puffinsecurity.com/the-key-to-everything-firmware-on-iot-devices> [Accessed 02 July 2023].

Masood, A. & Java, J. (2015) ‘Static analysis for web service security - Tools & techniques for a secure development life cycle’, *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*. Waltham, United States, 14-16 April. IEEE. 1-6. DOI: <https://doi.org/10.1109/THS.2015.7225337> [Accessed 21 July 2023].

McCombes, S. (2022) Types of Research Designs Compared | Examples. Available from: <https://www.scribbr.co.uk/research-methods/types-of-research-designs> [Accessed 18 July 2023].

Mei, G., Xu, N., Qin, J., Wang, B. & Qi, P. (2020) A Survey of Internet of Things (IoT) for Geohazard Prevention: Applications, Technologies, and Challenges. *IEEE Internet of Things Journal* 7(5): 4371 – 4386. DOI: https://doi.org/10.1109/JIOT.2019.2952593

Melander, B.A. (2020) SMART STADIUMS: AN ILLUSTRATION OF HOW THE “INTERNET OF THINGS” IS REVOLUTIONIZING THE WORLD. *SPORTS & ENTERTAINMENT LAW JOURNAL ARIZONA STATE UNIVERSITY* 6(2): Available from: https://asuselj.org/wp-content/uploads/2017/08/Melander-Smart-Stadiums.pdf [Accessed 15 July 2023].

Microsoft. (N.D.) Event-driven architecture style. Available from: <https://learn.microsoft.com/en-us/azure/architecture/guide/architecture-styles/event-driven> [Accessed 24th June 2023].

Miessler, D. (N.D.) The Difference Between Deductive and Inductive Reasoning. Available from: <https://danielmiessler.com/blog/the-difference-between-deductive-and-inductive-reasoning> [Accessed 18 July 2023].

Mlinarić, A., Horvat, M. & Smolčić, V. S. (2017) Dealing with the Positive Publication Bias: Why You Should Really Publish Your Negative Results. *Biochemia Medica* 27(3): 447-452. DOI: <https://doi.org/10.11613/BM.2017.030201>

MongoDB. (N.D.) What is IoT Architecture? Available from: <https://www.mongodb.com/cloud-explained/iot-architecture> [Accessed 02 April 2023].

Mowafi, Y., Zmily, A., AbouTair, D. & Abu-Saymeh, D. (2013) ‘Tracking Human Mobility at Mass Gathering Events Using WISP’, *Second International Conference on Future Generation Communication Technologies (FGCT 2013)*. London, 12-14 November. IEEE. 157-162. DOI: https://doi.org/10.1109/FGCT.2013.6767212 [Accessed 19 July 2023].

Msgna, M. (2022) Anatomy of attacks on IoT systems: review of attacks, impacts and countermeasures. *Journal of Surveillance, Security and Safety* 3(4): 150-173. DOI: <https://doi.org/10.20517/jsss.2022.07>

Naik, N. (2017) ‘Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP’, *2017 IEEE International Systems Engineering Symposium (ISSE)*. Vienna, Austria, 2017. IEEE. 1-7. DOI: <https://doi.org/10.1109/SysEng.2017.8088251> [Accessed 19 July 2023].

Navarro, E., Costa, N. & Pereira, A. (2020) A Systematic Review of IoT Solutions for Smart Farming. *Sensors* 20(15): 4231. DOI: <https://doi.org/10.3390/s20154231>

Naveen, S. (2016) ‘Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges’, *International Conference on Innovations in Computing & Networking (ICICN16).* Bangalore, 12-13 May. International Journal of Advanced Networking and Applications IJANA. 477-482. Available from: <https://www.researchgate.net/publication/330501274_Study_of_IoT_Understanding_IoT_Architecture_Applications_Issues_and_Challenges> [Accessed 19 July 2023].

NCS4. (N.D.) National Center for Spectator Sports Safety and Security. Available from: <https://ncs4.usm.edu> [Accessed 19 April 2023].

NCSC. (2019) CyBOK The Cyber Security Body of Knowledge. Available from: <https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf> [Accessed 11 July 2023].

NCSC. (2020) The Cyber Threat to Sports Organisations. Available from: <https://www.ncsc.gov.uk/files/Cyber-threat-to-sports-organisations.pdf> [Accessed 10 April 2023].

Noman, H.A. & Abu-Sharkh, O.M.F. (2023) Code Injection Attacks in Wireless-Based Internet of Things(IoT): A Comprehensive Review and Practical Implementations. *Sensors* 23(13): 6067. DOI: https://doi.org/10.3390/s23136067

O’Brolcháin, F., de Colle, S. & Gordijn, B. (2019) The Ethics of Smart Stadia: A Stakeholder Analysis of the Croke Park Project. *Science and Engineering Ethics* 25(3): 737-769. DOI: <https://doi.org/10.1007/s11948-018-0033-5>

O’Connor, Y., Rowan, W., Lynch, L & Heavin, C. (2017) Privacy by Design: Informed Consent and Internet of Things for Smart Health. *Procedia Computer Science* 113*.* 653-658. DOI: <https://doi.org/10.1016/j.procs.2017.08.329>

Omitola, T. & Wills, G. (2018) Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain*. Procedia Computer Science* 126(2018): 441-450. DOI: http://dx.doi.org/10.1016/j.procS.2018.07.278

Onag, G. (2021) Chip shortage will hinder IoT growth by 10% to 15% in 2022. Available from: <https://futureiot.tech/chip-shortage-will-hinder-iot-growth-by-10-to-15-in-2022> [Accessed 05 April 2023].

OWASP. (2018) OWASP INTERNET OF THINGS TOP 10 2018. Available from: <https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf> [Accessed 20 April 2023].

Panish, D. et al. (2015) ‘A wireless sensor network for monitoring the structural health of a football stadium’, *Conference: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT).* Milan, 6-8 December. IEEE. 471-477. DOI: <https://doi.org/10.1109/WF-IoT.2015.7389100> [Accessed 19 July 2023].

Pearson et al. (2019) ‘On Misconception of Hardware and Cost in IoT Security and Privacy’, *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. Shanghai, 20-24 May. IEEE. DOI: <https://doi.org/10.1109/ICC.2019.8761062> [Accessed 25 July 2023].

Petrović, R., Simić, D., Stanković., S. & Perić, M. (2021) ‘Man-In-The-Middle Attack Based on ARP Spoofing in IoT Educational Platform’, *2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*. Nis, Serbia, 22 November. IEEE. 307-310. DOI: <https://doi.org/10.1109/TELSIKS52058.2021.9606392> [Accessed 20 July 2023].

Pingue, F. (2016) WADA says hackers released another batch of athlete data. Available from: <https://www.reuters.com/article/uk-doping-wada-cyber-idUKKCN11L079> [Accessed 16 April 2023].

Pitsiladis, Y. et al. (2017) Make Sport Great Again: The Use and Abuse of the Therapeutic Use Exemptions Process. *Current Sports Medicine Reports* 16(3): 123-125. DOI: https://doi.org/10.1249/JSR.0000000000000364

Product Security and Telecommunications Infrastructure 2022. United Kingdom. Available from: https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted [Accessed 11 April 2023].

PWC. (N.D.) Stadiums of the future – How can technology transform stadiums? Available from: <https://www.pwc.co.uk/industries/hospitality-leisure/insights/can-technology-transform-future-stadiums.html> [Accessed 10 April 2023].

Qadri, Y.A., Nauman, A., Zikria, Y.B., Vasilakos, A.V. & Kim, S.W. (2020) The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. *IEEE Communications Surveys & Tutorials* 22(2): 1121-1167. DOI: https://doi.org/10.1109/COMST.2020.2973314.

Raj, P., Raman, A. & Subramanian, H. (2017a) *Architectural Patterns.* Packt Publishing. Available from: https://learning.oreilly.com/library/view/architectural-patterns/9781787287495/ceecb40b-550e-4c91-9d71-e6d48c4bff65.xhtml [Accessed 17 July 2023].

Raj, P., Raman, A. & Subramanian, H. (2017b) *Architectural Patterns.* Packt Publishing. Available from: https://learning.oreilly.com/library/view/architectural-patterns/9781787287495/cab8e24d-5814-49ac-8514-2f3a0f1d9076.xhtml [Accessed 17 July 2023].

Rauf, B. et al. (2021) Application Threats to Exploit Northbound Interface Vulnerabilities in Software Defined Networks. *ACM Computing Surveys* 54(6): 1-36. DOI: https://doi.org/10.1145/3453648

Richards, M. (2015) *Software Architecture Patterns.* Sebastopol, United States: O’Reilly Media Inc. Available from: https://learning.oreilly.com/library/view/software-architecture-patterns/9781491971437/ch02.html [Accessed 14 July 2023].

Rieback, M.R., Crispo, B. & Tanenbaum, A.S. (2006) The evolution of RFID security. EEE Pervasive Computing 5(1): 62-69. DOI: 10.1109/MPRV.2006.17

Rizvi, S., Orr, R.J., Cox, A., Ashokkumar, P. & Rizvi, M.R. (2020) Identifying the attack surface for IoT network. *Internet of Things* 9: DOI: https://doi.org/10.1016/j.iot.2020.100162

Roberts, F.S. (2019) From Football to Oil Rigs: Risk Assessment for Combined Cyber and Physical Attacks. *Journal of Benefit-Cost Analysis* 10(2): 251-273. DOI: <https://doi.org/10.1017/bca.2019.15>

Roohi, A., Adeel, M. & Ali Shah, M. ‘DDoS in IoT: A Roadmap Towards Security & Countermeasures’, *2019 25th International Conference on Automation and Computing (ICAC)*. Lancaster, United Kingdom, 5-7 September. IEEE. 1-6. <https://doi.org/10.23919/IConAC.2019.8895034> [Accessed 21 July 2023].

Runeson, P. & Höst, M. (2008) Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering* 14(2): 131-164. DOI: <https://doi.org/10.1007/s10664-008-9102-8>

Rytel, M., Felkner, A. & Janiszewski, M. (2020) Towards a Safer Internet of Things—A Survey of IoT Vulnerability Data Sources. Se*nsors* 20(21): 5969 DOI: <https://doi.org/10.3390/s20215969>

Safaei, B., Monazzah, A. M. H., Bafroei, M.B. & Ejlali, A. (2017) ‘Reliability Side-Effects in Internet of Things Application Layer Protocols’, *2017 2nd International Conference on System Reliability and Safety (ICSRS)*. Milan, Italy, 20-22 December 2017. IEEE. 207-212. DOI: <https://doi.org/10.1109/ICSRS.2017.8272822> [Accessed 19 July 2023].

Salem, O., Alsubhi, K., Shaafi, A., Gheryani, M., Mehaoua, A. & Boutaba, R. (2022) Man-in-the-Middle Attack Mitigation in Internet of Medical Things. *IEEE Transactions on Industrial Informatics* 18(3): 2053-2062. DOI: https://doi.org/10.1109/TII.2021.3089462

Samaila, M.G., Neto, M., Fernandes, D.A.B., Freire, M.M. & Inácio, P.R.M. (2018) Challenges of securing Internet of Things devices: A survey. *Security and Privacy Journal* 1(2): 1-32. DOI: http://dx.doi.org/10.1002/spy2.20

Samonas, S. & Coss, D. (2014) The CIA strikes back: Redefining confidentiality, integrity and availability in security*.* *Journal of Information System Security* 10(3): 21–45. Available from: https://www.proso.com/dl/Samonas.pdf

Science Notes. (2023) Steps of the Scientific Method. Available from: <https://sciencenotes.org/steps-scientific-method> [Accessed 27 July 2023].

Scroxton, A. (2021) Attack on surveillance cameras a warning over security, ethics. Available from: https://www.computerweekly.com/news/252497593/Attack-on-surveillance-cameras-a-warning-over-security-ethics [Accessed 19 April 2023].

Seals, T. (2022) Cyber Threats Loom as 5B People Prepare to Watch World Cup Final. Available from: <https://www.darkreading.com/attacks-breaches/cyberthreats-loom-5b-people-watch-world-cup-final> [Accessed 10 April 2023].

Sen, G. (2018) What is a Message Queue and Where is it used? Available from: <https://www.youtube.com/watch?v=oUJbuFMyBDk> [Accessed 5 July 2023].

SentinelOne. (N.D.) What Is Lateral Movement? Definition & Examples. Available from: <https://www.sentinelone.com/cybersecurity-101/lateral-movement/#:~:text=Lateral%20movement%20is%20a%20tactic,attacker%20reaches%20their%20ultimate%20target> [Accessed 02 July 2023].

Sethi, P. & Sarangi, S. R. (2017) Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering* 2017(1) 1-25. DOI: <https://doi.org/10.1155/2017/9324035>

Shepherd, C., Petitcolas, F. A. P., Akram, R. N. & Markantonakis, K. (2017) ‘An Exploratory Analysis of the Security Risks of the Internet of Things in Finance’, in: Lopez, J., Fischer-Hübner, S. & Lambrinoudakis, C. (eds) *Trust, Privacy and Security in Digital Business*. Cham: Springer. 164–179.

Shodan. (N.D.) Search Engine for the Internet of Everything. Available from: <https://www.shodan.io> [Accessed 18 May 2023].

Song, H., Fink, G.A. & Jeschke, S. (2017) *Security and Privacy in Cyber-Physical Systems*. Wiley-IEEE Press.Available from: https://learning.oreilly.com/library/view/security-and-privacy/9781119226048/c14.xhtml [Accessed 21 July 2023].

Song, L. & García-Valls, M. (2022) Improving Security of Web Servers in Critical IoT Systems through Self-Monitoring of Vulnerabilities. *Sensors* 22(13): 5004. DOI: 10.3390/s22135004

Soni, D. & Makwana, A. (2017) ‘A SURVEY ON MQTT: A PROTOCOL OF INTERNET OF THINGS(IOT)’, *INTERNATIONAL CONFERENCE ON TELECOMMUNICATION, POWER ANALYSIS AND COMPUTING TECHNIQUES (ICTPACT - 2017)*. Bharath Institute of Higher Education and Research, Chennai, India, April 2017. 173-177. Available from: <https://www.researchgate.net/publication/316018571_A_SURVEY_ON_MQTT_A_PROTOCOL_OF_INTERNET_OF_THINGSIOT> [Accessed 19 July 2023].

Sports Grounds Safety Authority. (N.D.) Legislation. Available from: <https://sgsa.org.uk/legislation/#:~:text=Under%20the%20Health%20and%20Safety,punishable%20by%20an%20unlimited%20fine> [Accessed 27 July 2023].

Srihith, I. D., Donald, A.D., Srinivas, T.A.S., Anjali, D. & Chandana, A. (2023) Firmware Attacks: The Silent Threat to Your IoT Connected Devices. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)* 3(2): 145-154. DOI: 10.48175/IJARSCT-9104

Statista. (2023) Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030. Available from: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide> [Accessed 05 April 2023].

STMicroelectronics. (2023) Introduction to STM32 microcontrollers security. Available from: <https://www.st.com/resource/en/application_note/an5156-introduction-to-stm32-microcontrollers-security-stmicroelectronics.pdf> [Accessed 20 July 2023].

Stone, M. (N.D.) What are eavesdropping attacks? Available from: <https://www.verizon.com/business/en-gb/resources/articles/s/what-are-eavesdropping-attacks> [Accessed 02 July 2023].

Stratmann, E., Ousterhout, J. & Madan, S. (2011) ‘Integrating long polling with an mvc web framework’, *2nd USENIX conference on Web application development*. Portland, United States, 15-16 June. 113-124. Available from: <https://www.semanticscholar.org/paper/Integrating-Long-Polling-with-an-MVC-Web-Framework-Stratmann-Ousterhout/77b04a81b09f686d33aab3d1fdbea1fbe7cc187f#citing-papers> [Accessed 19 July 2023].

Sun, F. et al. (2019) ‘Recovery-oriented Big Data Computing for Exactly

Once Message Processing’, 2019 IEEE International Conference on Big Data (Big Data). Los Angeles, 9-12 December 2019. IEEE. 2923-2930. DOI: <https://doi.org/10.1109/BigData47090.2019.9006585> [Accessed 19 July 2023].

Swinhoe, D. (2018) Why fake data is a serious IoT security concern. Available from: <https://www.csoonline.com/article/566517/why-fake-data-is-a-serious-iot-security-concern.html> [Accessed 14 July 2023].

Tammadge, D. (2021) Event-Driven VS Request-Driven Architecture: The Pros & Cons and Trade-offs of event driven systems. Available from: https://danieltammadge.com/2021/01/event-driven-vs-request-driven-architecture-trade-offs

Thangavel, D., Ma, X., Valera, A., Tan, H. & Tan, C. K. (2014) ‘Performance Evaluation of MQTT and CoAP via a Common Middleware’, *2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*. IEEE. 1-6. DOI: <https://doi.org/10.1109/ISSNIP.2014.6827678> [Accessed 19 July 2023].

Tomar, D. (2020) A Network Architecture for secure traffic management for the Internet of Things using Virtual Local Area Network. *International Journal of Computer Trends and Technology* 68(12): 11-14. DOI: <https://doi.org/10.14445/22312803/IJCTT-V68I12P103>

University of Essex Online. (N.D.) Validity and Generalisability. Available from: <https://www.my-course.co.uk/Computing/Computer%20Science/RMPP/RMPP%20Lecturecast%204/content/index.html> [Accessed 23 July 2023].

UK Parliament. (2021) Regulation of consumer connectable product cyber security. Available from: <https://bills.parliament.uk/publications/43916/documents/1025> [Accessed 12 April 2023].

Uke, S.N., Mahajan, A. R. & Thool, R. C. (2013) UML Modeling of Physical and Data Link Layer Security Attacks in WSN. *International Journal of Computer Applications* 70(11): 25-28. DOI: <https://doi.org/10.5120/12006-7132>

UL. (2019) IoT Security Top 20 Design Principles. Available from: https://www.ul.com/sites/g/files/qbfpbp251/files/2021-08/IoT%20Security%20Top%2020%20Design%20Principles%20whitepaper.pdf [Accessed 14 July 2023].

UN. (2021) GUIDE ON THE SECURITY OF MAJOR SPORTING EVENTS. Available from: <https://theicss.org/wp-content/uploads/2021/10/2112787-OCT-Sports-web.pdf> [Accessed 10 April 2023].

Université Du Luxembourg. (N.D.) ADTool. Available From: https://satoss.uni.lu/members/piotr/adtool [Accessed 17 July 2023].

University of Chicago Professional Education. (2020) Growing Threats of Cybersecurity Attacks in Sports. Available from: https://www.youtube.com/watch?v=Lf4VNjSb9h8 [Accessed 27 July 2023].

Van Heck, S.G.J., Valks, B. & Den Heijer, A.C. (2021) The added value of smart stadiums A case study at Johan Cruijff Arena. *Journal of Corporate Real Estate* 23(2): 130-148. DOI: <https://doi.org/10.1108/JCRE-09-2020-0033>

Varga, P., Plósz, S., Soos, G. & Hegedus, C. (2017) ‘Security Threats and Issues in Automation IoT’, *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS).* Trondheim, Norway, 31 May - 02 June. IEEE. 1-6. DOI: <https://doi.org/10.1109/WFCS.2017.7991968> [Accessed 19 July 2023].

Vignau, B., Khoury, R. & Hallé, S. (2019) ‘10 Years of IoT Malware: A Feature-Based

Taxonomy’, *2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. Sofia, Bulgaria, 22-26 July. IEEE. 458-465. DOI: <https://doi.org/10.1109/QRS-C.2019.00088> [Accessed 19 July 2023].

VirusTotal. (2023) VirusTotal API v3 Overview. Available from: https://developers.virustotal.com/reference/overview [Accessed 22 July 2023].

Wagle, S. (2016) ‘Semantic Data Extraction over MQTT for IoTcentric

Wireless Sensor Networks’, *2016 International Conference on Internet of Things and Applications (IOTA)*. Maharashtra Institute of Technology, Pune, India, 22-24 January. IEEE. 227-232. DOI: <https://doi.org/10.1109/IOTA.2016.7562727> [Accessed 19 July 2023].

Wan, B., Xu, C., Prasad Mahapatra, R. & Selvaraj, P. (2022) Understanding the Cyber‑Physical System in International Stadiums for Security in the Network from Cyber‑Attacks and Adversaries using AI. *Wireless Personal Communications* 127: 1207-1224. DOI: <https://doi.org/10.1007/s11277-021-08573-2>

Wang, X. & Lu, X. (2020) A Host-Based Anomaly Detection Framework Using XGBoost and LSTM for IoT Devices. *Wireless Communications and Mobile Computing* 2020.1-13. DOI: https://doi.org/10.1155/2020/8838571

Westerholt, R. & Resch, B. (2015) Asynchronous Geospatial Processing: An Event-Driven Push-Based Architecture for the OGC Web Processing Service. *Transactions in GIS* 19(3): 455-479. DOI: http://dx.doi.org/10.1111/tgis.12104

Wiler, A. S. (2018) Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation. *International Journal* 73(2): 308–316. DOI: https://doi.org/10.1177/002070201878249

Woodall, M. (2021) The Most Popular Smart Home Devices 2022. Available from: <https://www.reviews.org/home-security/most-popular-smart-home-device-statistics/#:~:text=Smart%20speakers%20take%20the%20cake,at%20least%20one%20smart%20speaker> [Accessed 07 April 2023].

Yang, S., Shiue, Y., Su, Z., Liu, I & Lui, C. (2020) An Authentication Information Exchange

Scheme in WSN for IoT Applications. *IEEE Access* 8: 9728-9738. DOI: <https://doi.org/10.1109/ACCESS.2020.2964815>

Ye, F., Luo, H., Lu, S. & Zhang, L. (2005) Statistical En-Route Filtering of Injected False Data in Sensor Networks. *IEEE Journal on selected areas in communications* 23(4): 839-850. DOI: 10.1109/INFCOM.2004.1354666

Yin, Y., Zeng, Y., Chen, X. & Fan, Y. (2016) The internet of things in healthcare: An overview. *Journal of Industrial Information Integration* 1(1):3-13. DOI:

https://doi.org/10.1016/j.jii.2016.03.004

Yunan, A., Satria, E., Ilham, D.N., Anugrenia, F., Khairuman, K. & Sandra, S. (2021) ‘Signal jammer reduces wireless fidelity network and global system in local environment’, *IOP Conference Series: Earth and Environmental Science*. Banda Aceh, Indonesia, 21-22 September 2020. IOP Publishing Ltd. 644. DOI: <https://doi.org/10.1088/1755-1315/644/1/012022> [Accessed 19 July 2023].

Zubaydi, H. D., Varga, P. & Molnár, S. (2023) Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors* 23(2): 788.DOI: <https://doi.org/10.3390/s23020788>

# Appendices

**APPENDIX A: Detection Algorithm**

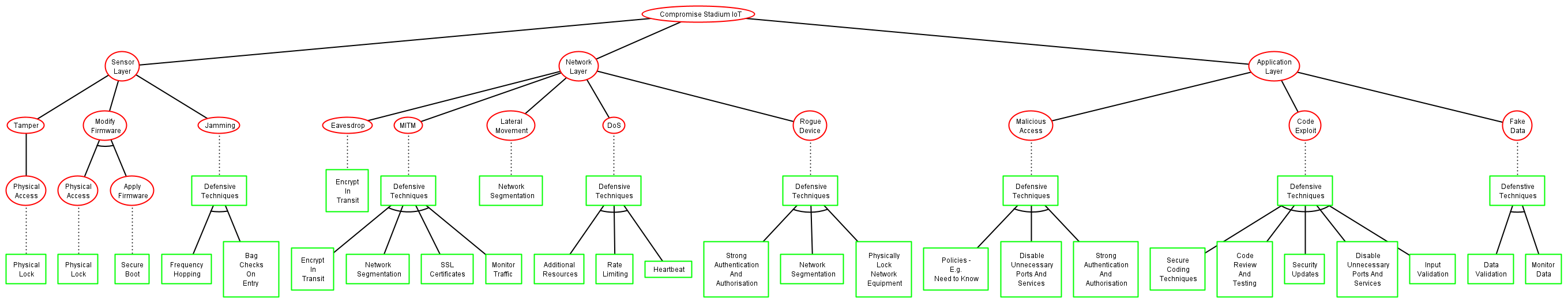
****

Figure 29: Attack-Defence Tree

**APPENDIX B: Abandoned Plans**

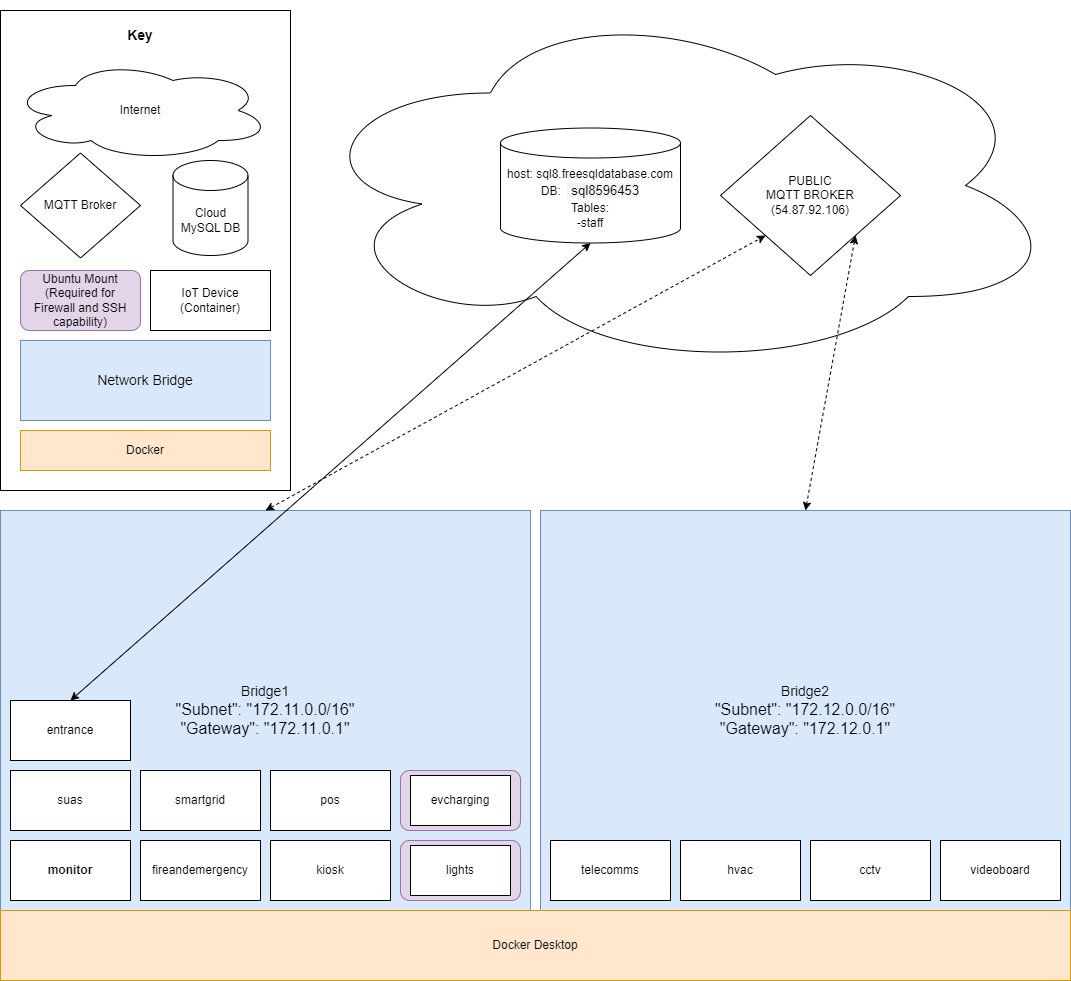


Figure 30: Original Artefact

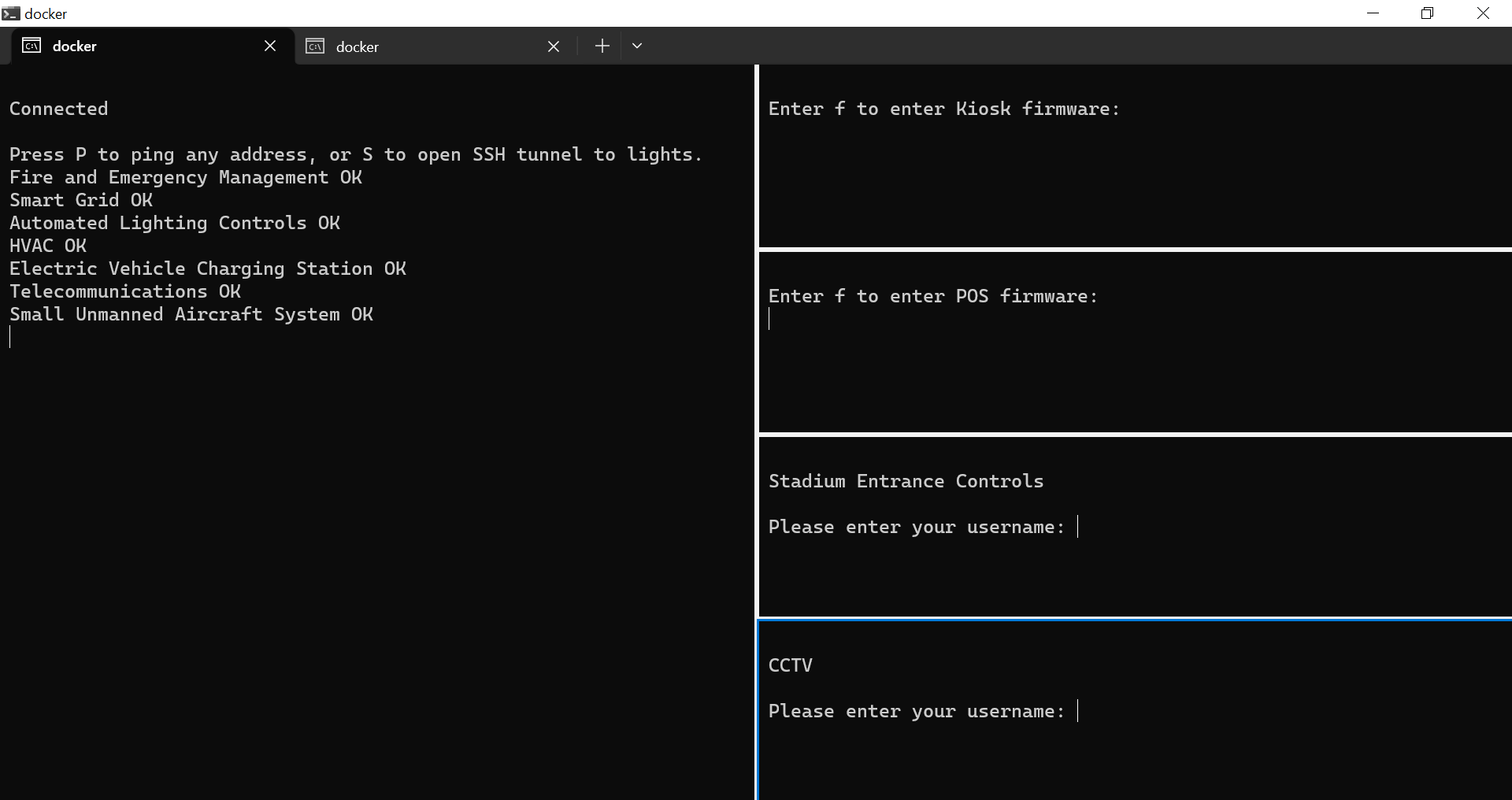


Figure 31: Original Artefact Screen A

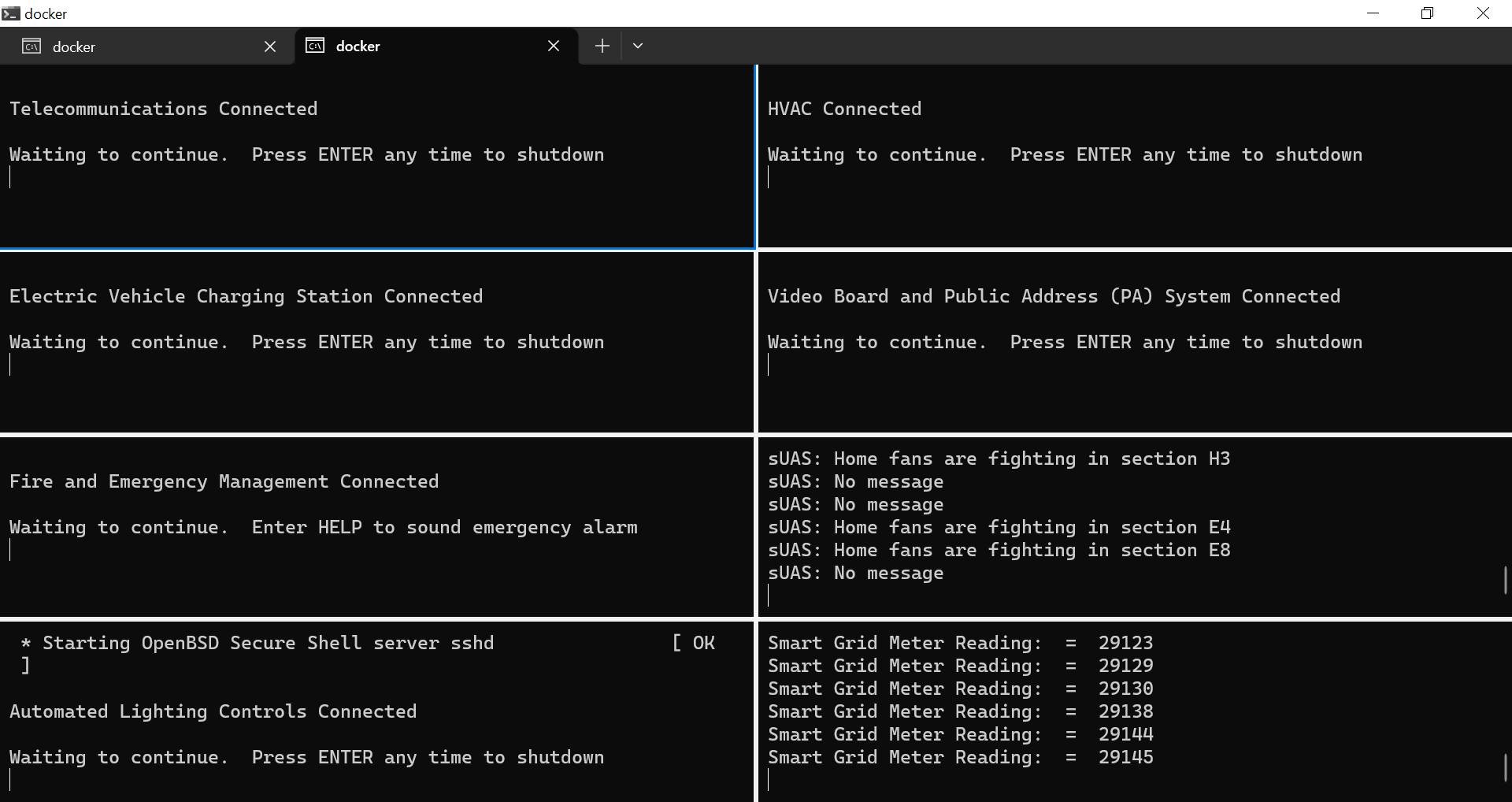


Figure 32: Original Artefact Screen B

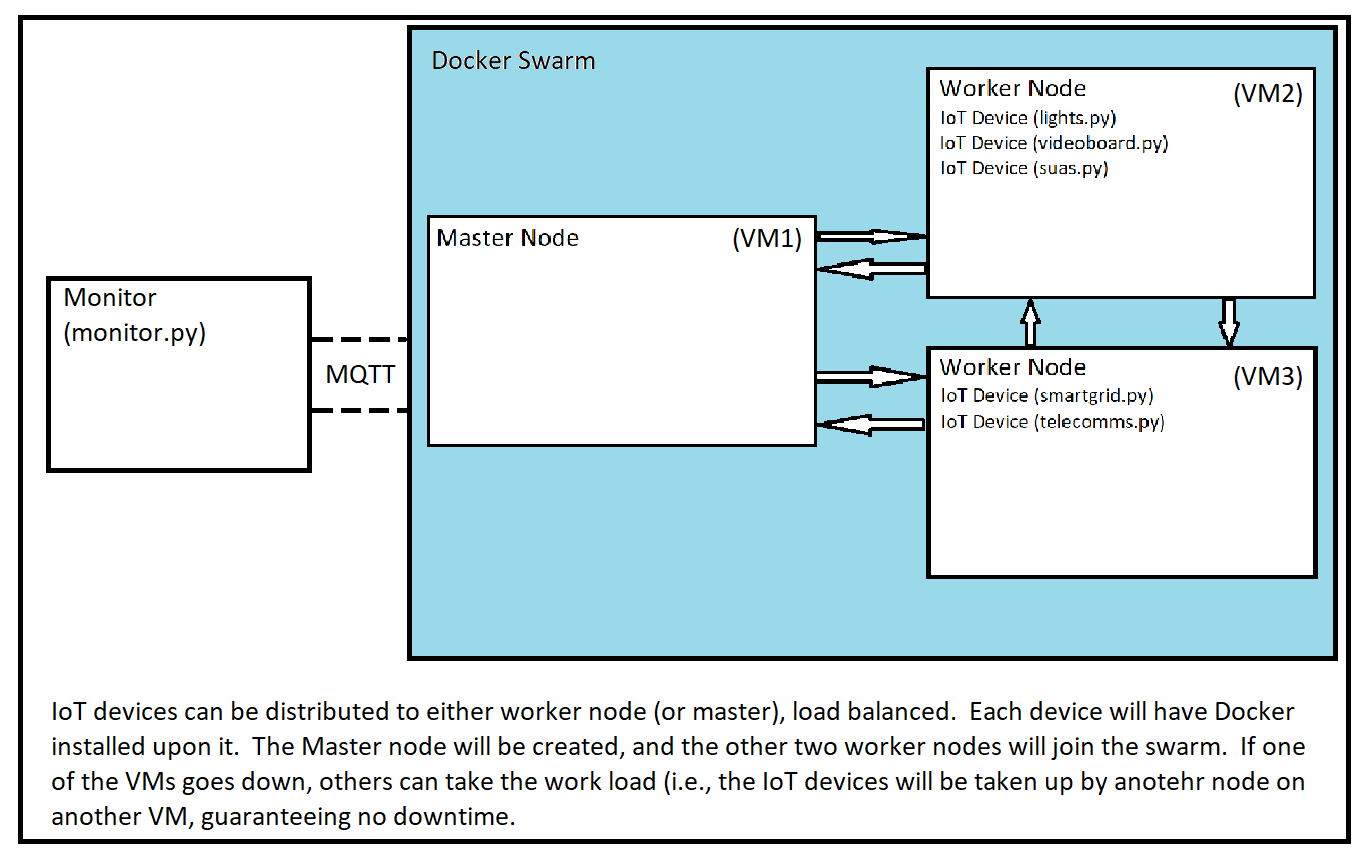
****

Figure 33: Docker Swarm Proposal

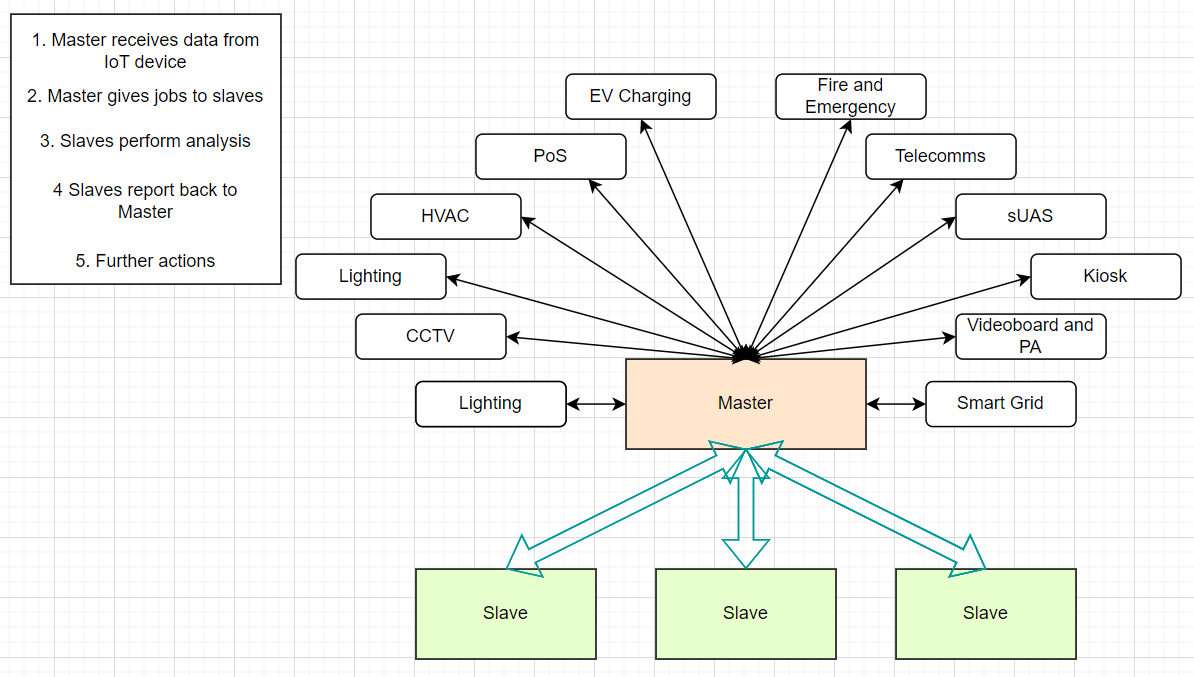
****

Figure 34: Master-Slave Architecture First Attempt

**APPENDIX C: Original Research Proposal Idea**

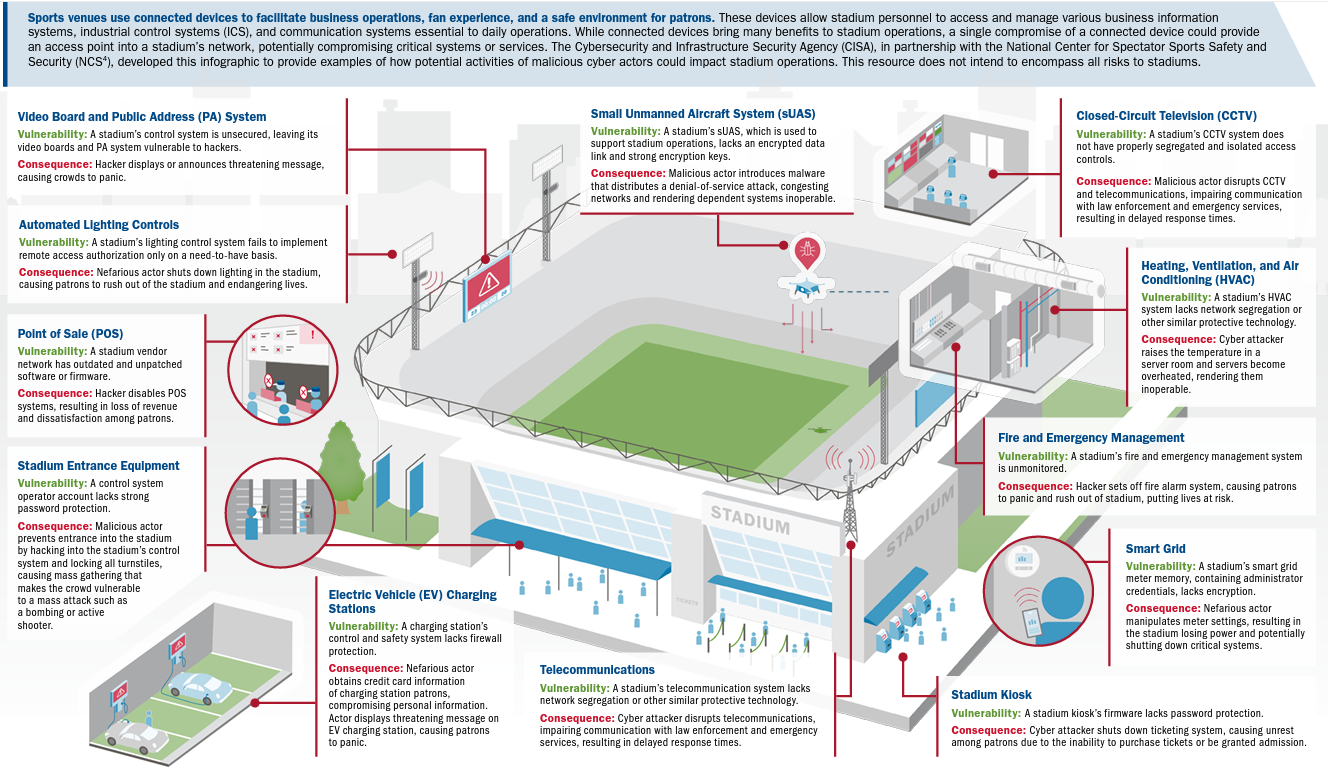


Figure 35: Twelve Mitigations To Twelve Vulnerabilities In Sports Stadium IoT (CISA, N.D.)

**APPENDIX D: Original Project Timeline**

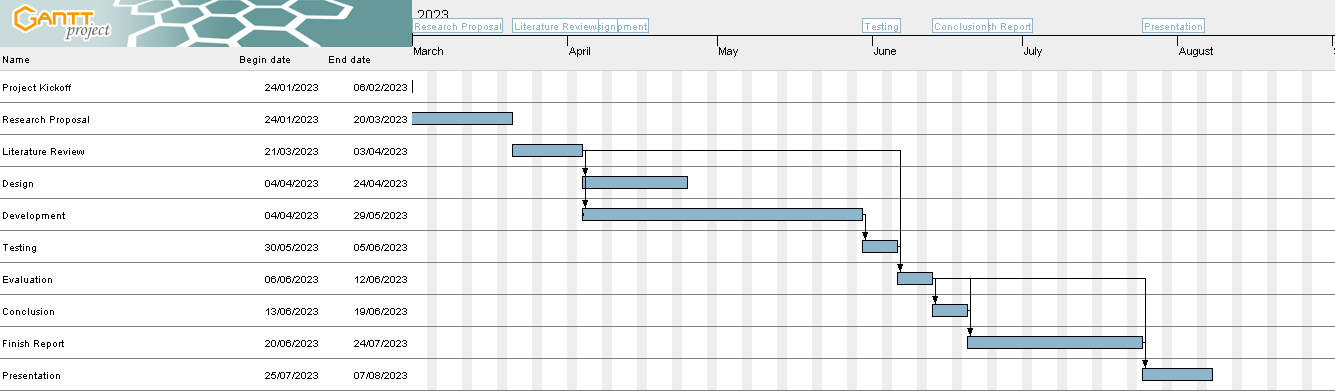


Figure 36: Original Project Timeline