**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 3](#_Toc139951749)

[Literature Review 4](#_Toc139951750)

[*Internet of Things* 4](#_Toc139951751)

[*IoT Architecture* 5](#_Toc139951752)

[*Smart stadiums* 8](#_Toc139951753)

[*IoT Technology and Cyber Security in sports* 13](#_Toc139951754)

[*Polling* 18](#_Toc139951755)

[Prevention and Detection Model 21](#_Toc139951756)

[Research Methodology 27](#_Toc139951757)

[Discussion 28](#_Toc139951758)

[Conclusion 29](#_Toc139951759)

[Lessons Learned, Evaluation, and Limitations 30](#_Toc139951760)

[Future Work 32](#_Toc139951761)

[References 33](#_Toc139951762)

# 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 into 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 exponential numbers of devices aimed at providing better functionality, however too often they are failing to sufficiently consider security. Therefore, the safeguarding of these devices, and ensuring the need for their accurate and consistent operation can ultimately be a matter of life and death.

# Research Question

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

# Aim

## To design and develop a prototype sports stadium management system which monitors Internet of Things devices in sports stadiums and provides pre-emptive detection and protection against DoS, Man in the Middle (MITM), sniffing, password cracking, vulnerability exploits, and identity theft cyber-attacks.

# Objectives

* To protect the IoT against DoS attacks and compromise within the sports stadium domain
* To create a prototype of the model, producing mitigations to the twelve risk examples listed in NCS4 and CISA’s integrated security considerations diagram
* To create a detailed report on the research findings

# 

# Literature Review

## *Internet of Things*

The Internet of Things (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 IoT is existential, 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).

The devices classed as IoT divides opinion, however it generally can be classified into one of two categories:

1. *Consumer IoT (CIoT)* – A connected system of physical and digital objects designed to be beneficial to the consumer’s lifestyle in some way. These smart devices usually include 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 seeing the benefit of IIoT, including energy, agriculture, manufacturing, transportation, and healthcare. Safety considerations are also paramount in IIoT, and so predictive maintenance is also of importance.

CIoT and IIoT can also overlap depending on use case. For example, wearable technology would normally be considered CIoT, however can also be worn by industrial engineers to monitor their location and radiation levels, making it suitable for IIoT.

## *IoT Architecture*

IoT architecture can be broken down into three basic fundamental layers (Alaba et al., 2017; Burhan et al., 2018; Abughazaleh et al., 2020; Mei et al., 2020).

* Perception / Sensing layer: comprising of sensors attached to physical devices that collect data, and actuators that act on it.
* Network / Transportation layer: connecting devices together, and responsible for the data transmissions between them, 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 layer: 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 level (MongoDB, N.D.) variations, as shown in Figure 1, and even seven layer models for providing higher IoT design granularity. Various other domain-specific models are discussed by Jamali et al. (2019).

In the four-layer model, a new Processing layer (often called Middleware layer) is introduced, above the Network layer, while the Network layer, often called Transport layer, continues to deal with messaging and connectivity. The Processing layer is responsible for any processing of the data from its raw form, performing data analytics to provide meaningful insights and aid decision making. In the five-layer model, a Business layer is introduced 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 also propose a six-layer architecture addressing security.



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.

This better describes how edge computing is incorporated into IoT. Sensors generate data, and actuators act on it. This can be analogous to the Perception layer in the three-layer model. Internet gateways are the proxy between the IoT network and the Internet, allowing the local IoT devices to effectively communicate with the outside world while keeping its own 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 can be incorporated to pre-process critical data, allowing decisions to be made in real time before data is offloaded in bulk to the cloud or local data centre for deeper analysis. By processing data on the edge of the network, local network devices receive feedback much quicker than if data were being sent to, and from the data centre. Furthermore, security is enhanced due to the limited network exposure available to untrusted actors. Finally, the Data Centre / Cloud stage allows heavy work to be done on the resultant big data, involving analytics to find insights and obtain meaningful results, 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), of which is reflected in IoT Analytics’s trends from Leuth (2020) and Hasan (2022).

IoT is already widespread in multiple sectors. For example, healthcare IoT (HIoT) is already prevalent, and is another area where human life is clearly paramount. Wearables monitoring heartbeats, blood pressure, and respiration provide telemetry-based health metrics, IoT can be used to predict or detect diseases which would previously have gone undiscovered and therefore enables them to become more treatable or preventable. IoT can assist those recovering, the elderly, or those with disabilities, with everyday life, relieving the workload of caregivers, and can also be used to support functions 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. Remote cameras can be deployed to monitor disease, and actuators can activate sprinklers on schedules or when specific criteria are met, increasing revenues for the farmer (Farooq et al., 2019).

The energy sector can benefit from smart meters in the home, making it easier for customers to monitor their 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. Predicted energy savings for smart cities are to reach $96 billion in 2026 (Juniper Research, 2022), and by moderating power supply across the city using intelligent devices, automated street lighting, traffic management, and wireless access points can be integrated to help it become truly connected. Smart cars can benefit from connected electric charging points, whilst their embedded systems pull latest traffic information and weather, preparing not only the driver for the journey ahead, moreover relaying the information directly to passing cars using Machine to Machine (M2M) communications and receiving real time updates on nearby accidents and road closures.

Smart homes are omnipresent with 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 can be leveraged to enable any mains powered device to have its power controlled by an app, turning mains-power enabled devices into somewhat intelligent ones. Common communication technology for smart homes include Zigbee and Z-Wave.

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.

Furthermore, sport is also highly affected by IoT. Athletes use wearables to monitor their performance such as smart vests containing Global Positioning System (GPS), heartrate and performance monitors, cameras are enabling on-field decisions with systems such as Hawkeye, goal line technology and Video Assistant Referee (VAR) (Harrod Sport, 2018), sensors can be inserted into balls to track spin, speed and trajectory, and fans are better engaged thanks to in-game updates sent to digital display monitors and advertising boards.

## *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 regeneration of cities or areas, such projects often include new shops, housing, and restaurants. These concepts bring numerous benefits to the local community and improves the well-being of local residents, showing the importance that sports stadiums have for cities.

Today’s elite stadiums are built with consumer convenience and experience enhancement in mind, as well as safety. Stadium IoT devices include a wide range of devices, from camera recognition technologies, to biometric entry, from automatic turnstiles, to digital advertising boards, big screens, automated lighting, Heating, Ventilation and Air Conditioning (HVAC) systems and retractable roofs. By introducing the IoT, sports stadiums can increase their automation, saving money and maximising convenience for the consumer. No longer do visitors solely benefit from viewing the event, moreover spectators can gain entry using ticketless entrance systems, order refreshments directly from their seat or 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 stages of development. 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 football 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, the recording of one’s face by 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. It may be difficult to expect 80,000 spectators to fill out a waiver upon entry, and perhaps unrealistic to expect them to read notices advising them of their recordings and data gathering. Brey, also highlights other specific issues of using FRT, including errors and function creep which have since been reduced through modern technology and the General Data Protection Regulation (GDPR), respectively.

*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 can cause threat to life when the cyber component either fails, or falls victim to cyber-attack. Either of these scenarios can be used as a precursor to launch a physical attack, for example locking smart turnstiles can pen people in one area, or a threatening message displayed on the big screen can cause people to panic and flee, subsequently maximising the effectiveness of a secondary physical attack on an area filled with people, leading to scenes similar to those witnessed at the Stade de France in 2015, and the Arianda Grande concert at the Manchester Arena in 2017 (Roberts, 2019).

IoT devices in stadiums can however, also positively contribute to security efforts. Devices can be deployed to 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 may be a useful method of assuring a healthy cybersecurity status amongst peers (Baker, 2020).

Melander (2020) also addresses privacy issues of collecting data from cameras, and remarks on several points of ethical use, 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, 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 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 Code of Practice (HM Government, 2018). This list of security requirements is aimed at providing an assurance baseline for IoT devices, aligning for product certification, and hopes to drive adoption of improved security measures 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, the act does not cover devices manufactured and deployed before its enactment in December 2022, meaning these devices may be 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 compromise*

The proliferation of cyber-attacks is growing due to the development and reliance of technology, especially following the increasing use of wireless communications such as cellular technology and Wi-Fi. The security of sports stadiums 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, they can be life threatening. Implantable Medical Devices (IMDs) 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 CPSs in today’s world, including those found in sports stadiums extends the threat of cyber-attacks to human life. Advance risk management of sporting events is imperative due to present threats to human life and the potential for financial and reputational damage for the organisation (Wan et al, 2022).

Mowafi et al. (2013) provided a useful framework for tracking the gathering of mass crowds 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 items of Personal Identifiable Information (PII) 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.

*Examples of historic compromise*

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 hundreds of thousands of devices across the world in its first twenty hours (Antonakakis et al., 2020). It 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 list of credentials. Likely evolving from a previous Trojan named Bashlight, Mirai produced multiple variants, and zombies from the resultant botnet 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.

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 success of the attack was clear to see with many vacant seats 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) showed how nation states can use sport as a way of showing their political prowess (Datta & Acton, 2022). A Russian state-sponsored cyber hacking group known as Fancy Bears were able to extract details of several athletes 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). The act caused embarrassment to WADA and the Olympics, and distrust amongst the public.

In 2021, a further example showed a hacktivist group were able to compromise 150,000 cameras, revealing footage of inside 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 a recent example (BBC, 2023).

## *IoT Technology and Cyber Security in sports*

A modern day smart stadium can include a network of generic laptops, desktops and networking equipment, and may be connected by wired or wireless means. They are also likely to include connected IoT devices such as CPSs 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. CPSs are hardware cyber-connected devices that incorporate software, and can 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 methods of networking, and making much networking equipment redundant. 5G was developed with IoT in mind with speeds 10 times faster than 4G, less latency, greater capacity, capable of coping with multiple device connections simultaneously, and allowing devices to connect directly with each other across geographic locations (Li et al., 2018). This will also eventually benefit those with devices in rural or remote locations previously without access to reliable broadband.

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 (SMEs), where hacktivism and nation states can see an opportunity to make their mark, this is an unrealistic possibility.

This has 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) also 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 problem (UN, 2021). The Open Web Application Security Project (OWASP) have also published an IoT top 10 (vulnerabilities) list as of 2018 (OWASP, 2018).

Organisations putting on major sporting events can also 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 continues 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 connected, using edge computing and artificial intelligence to facilitate information gathering at speed, and recreated digital twins to better understand events in real time (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.

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 may not be ideal for making detection decisions when human life is at stake, particularly if a learning dataset is contaminated by an attacker.

Li et al. (2018) 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 provide trust assurance through the IoT stack.

Most IoT attacks are also found in traditional cyber-attacks, owing to their dependency on the Internet as a backbone, while 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 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.

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

Vulnerable Internet-connected devices can be easily found using a website such as Shodan (N.D.), which also allows authentication attempts. Furthermore, details of devices, such as default credentials or radio frequencies, can be gleaned easily using open source intelligence. This can be 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.

An additional concern is that there is still no single provider that provides the hardware, software, communications, and application technology, holistically. This leaves difficulty in securely passing data up and down the IoT stack. Furthermore, components may also be designed and manufactured by other nation states. These countries may be allies upon purchase, however in a setting such as a sports stadium where devices may feasibly not be 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. Generally, in most commercial organisations, confidentiality is the tenet mainly focused on, closely followed by Integrity. However, within IoT, Availability is usually the most important.

# Methodology

This paper employed a cross-sectional, experimental study of IoT device attacks in the context of sport stadium IoT, and how a publisher / subscriber system can prevent and detect them, using the scientific method and a model-based approach to artefact creation.

Ethnography, or a case study at a specific football stadium would have made for an interesting spin on the research, however it was not appropriate in this case due to the time constraints limiting the opportunity to gain the required ethical approval.

The 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 is not dependent on future or archived results.

A comprehensive literature review of existing secondary research was first undertaken to understand the landscape of the topic in question.

The report then uses a quantitative research approach due the fact that the research should be objective in nature. Due to the lack of subjectivity, a positivist philosophy is used, meaning an interpretivist perspective would not be appropriate, and a qualitative approach would ultimately lead to inaccurate results due to its subjective nature.

Primary quantitative research was therefore conducted as the data gathering and testing method, with applied deductive reasoning to determine the results.

# Ethical considerations

Although the secondary research uncovered various ethical matters in IoT in sports stadiums, there were no ethical concerns for the primary research as it was based on a Proof of Concept (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 either would 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 IoT analysis, GDPR and Data Protection Act (DPA) regulations must be abided by, and a notice of consent would need to be sought from any 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 be catastrophic, and the omission of negative results leads to wasted time and resources (Mlinaríc et al, 2017).

If this model were to be developed into a prototype, it would need to do so with the GDPR, DPA, and ACM Code of Ethics and Professional Conduct in mind.

# Artefact Description

The artefact created for this project is in the form of a UML activity diagram and a spreadsheet using Microsoft Excel. The activity diagram shows the movement of data via notifications between the slave and master nodes. The spreadsheet contains four tabs:

**Threats**: This tab is informational and lists each threat discovered following the threat modelling stage. Threats are grouped by the IoT architecture layer it endangers. Each row lists an ID, the Threat, the Control Type (family of controls applicable to mitigate them: Administrative, Compensate, Detect, Prevent), and how it is mitigated by the model.

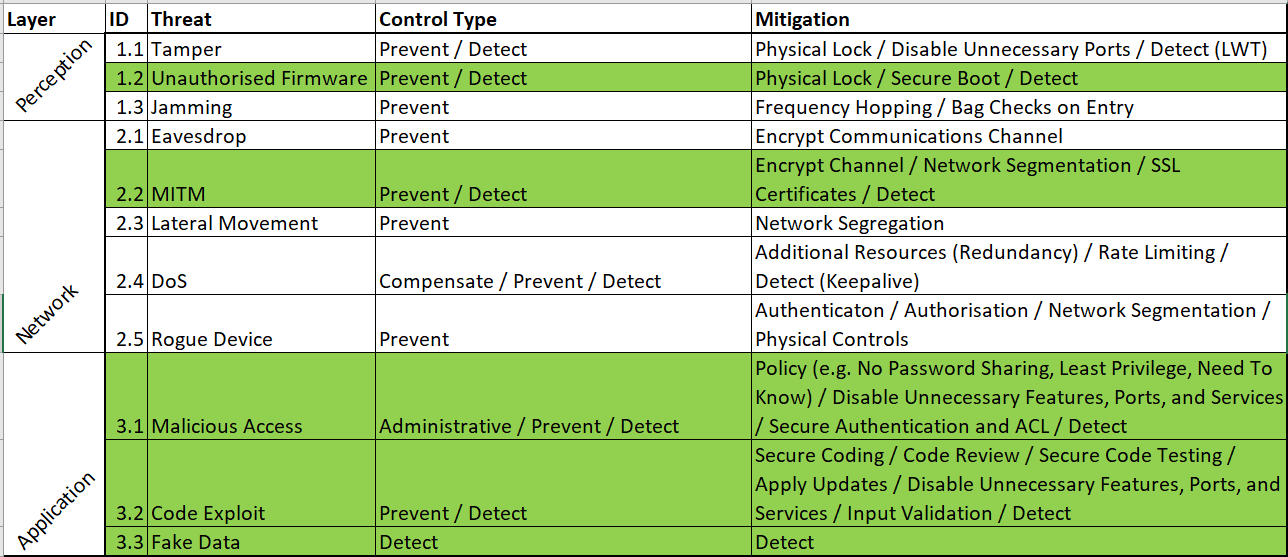


Figure 1: Threats

**IoCs**: Lists Indicators of Compromises (IoCs) that are typically found to contribute to each threat being realised. IoCs are listed by Event Code, together with the Event Name.

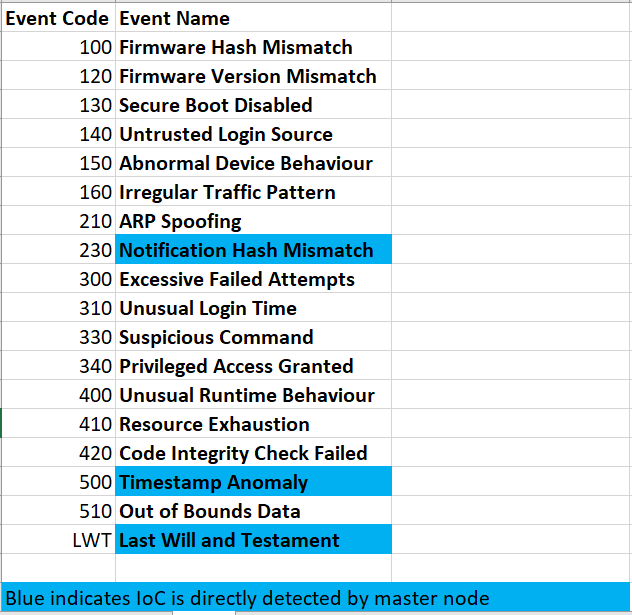


Figure 2: IoCs

**Weightings**: Some threats cannot be prevented alone and require supplementary detective controls to mitigate threats. Therefore, the Weightings and Score tabs use a scoring method to enable the system to detect threats using IoCs. Grouped by threat, the IoCs are listed with a name, a description, and a weighted score. The score for each IoC depends on the likelihood that a threat is present on a device when a notification of an event code is received by the master node. IoCs may be present in multiple threats, and their scores may vary depending on how important they are in that threat’s calculation.

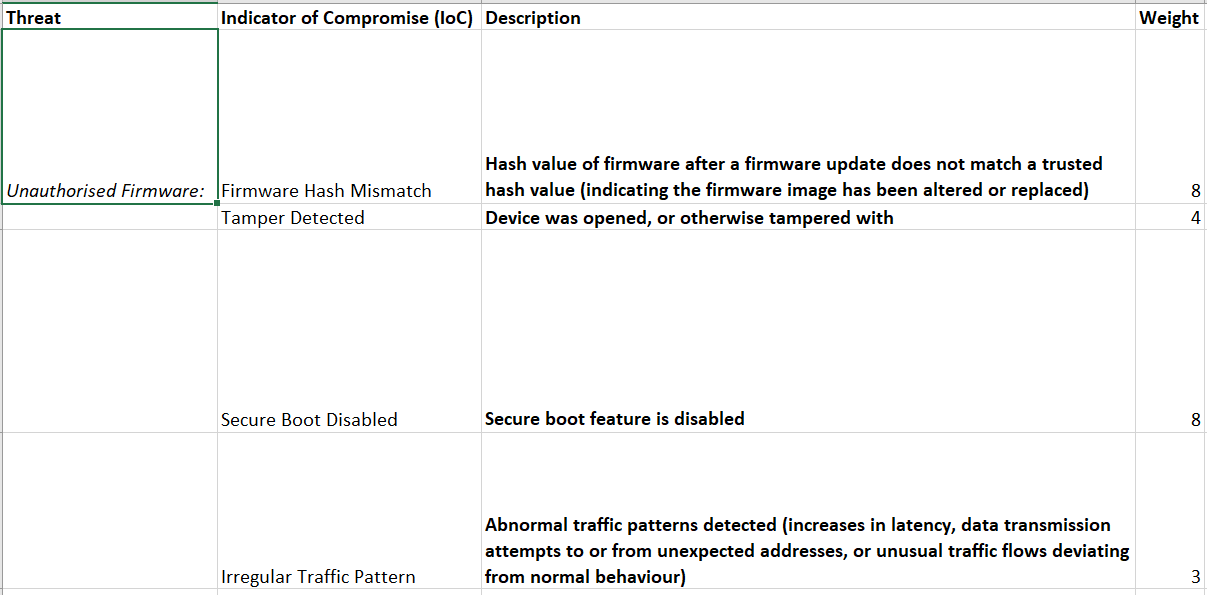


Figure 3: Weightings

**Score**: This tab uses formulas to simulate IoCs occurring in real time. As this is a PoC, the user enters IoC codes in the Code column. The Event Description field automatically populates with the corresponding Event Name. If the combine combined IoC weighted scores for a specific threat exceed a total of ten, an alarm will show. This simulates the master node detecting a score of ten in the real life system, triggering a response to automatically deactivate the compromised node, and failover to the backup IoT device.

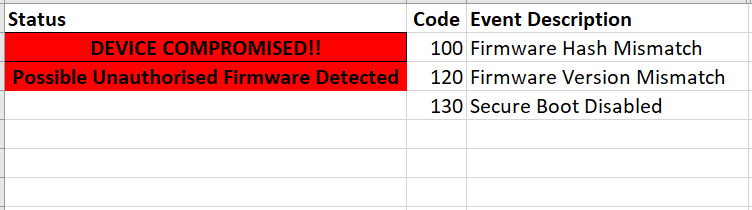


Figure 4: Score

**Timeline**

**Design**

There are several considerations to developing a system that can support IoT devices in a sports stadium. These include which communication architecture and messaging protocol should be used. The following discusses some options:

*Event-Driven*

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 to other devices. This architecture style uses asynchronous communication, meaning once the notification has left the producer, it is forgotten about.

One major advantage of EDA is that all producers and consumers are decoupled, meaning all nodes are independent of others and are not required to be available at the same time. If one device is down, others need not be affected. EDA is decentralised, and therefore scalable, and does not necessarily require a central node to move notifications along. Notifications in EDA are also deemed immutable and persistent, meaning they cannot be altered and can be used again after they have been used.

Depending on the implementation, EDA presents challenges, including the need for event notifications’ guaranteed delivery, ordering, and the concept of idempotency (Microsoft, N.D.). Guaranteed delivery may not be required in non-critical systems, however its use requires careful consideration for unreliable networks.

Furthermore, as devices may be dependent on notifications from others, reliability is often important, and is exacerbated when multiple devices send 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 the notifications to properly keep track.

Idempotency is the guarantee that if any event is processed more than once, it will not affect the intended end result (Wigmore, 2016). This is an additional concern in EDA, as receiving the same notification twice can result in the system crashing, or producing inconsistent results. Idempotency can occur when a broker goes down and has to return to a previous checkpoint. Here, a medium such as a database can be used to store notifications, with application logic applied to check against those previously received.

*Publish / Subscribe model*

The publish / subscribe model is a sub-type of EDA, where a broker proxies information sent between the producer (publisher) and the consumer (subscriber). Notifications are broadcast to consumers using topics. The main disadvantage of this architectre is that while any device can go offline, the broker is typically a single point of failure (SPoF) for the whole system, leaving Denial of Service (DoS) attacks possible.

The publish / subscribe model has numerous upsides. Including, if the consumer is down, notifications can still be retrieved when it eventually comes back online. EDA lends itself, when compared to polling, to processing high amounts of data such as those produced by multiple IoT devices, and consumers can act as soon as they arrive.

# *Polling*

Polling uses a client node to contact server nodes for messages that need processing. In what is known as short-polling, if the server does not have any data to transmit, it is ignored and the client moves to interrogate the next, or waits for an interval before polling again. Similar to EDA notifications, each polling request is independent, and does not rely on the last.

Polling is suitable for environments where long delays between network calls are acceptable. However, in systems comprising of multiple IoT devices, it may not be practicable, and if more regular requests are required, intervals need reducing, which adds to network load.

Polling implemented in systems where multiple servers send messages is inefficient. During the interval period, client resources are wasted creating needless handshakes and teardowns. Furthermore, all other devices have to wait for the client’s resources to be freed. Polling is also unsuitable for real time, or high volume applications for these reasons.

There are other sub-types of polling architecture including long-polling, in which clients poll resources for data, and in the event the server does not have any data, clients leave the connection open until either the response is given, or a timeout occurs. This, is preferred in scenarios containing small numbers of devices, as keeping the connection open ties up resources.

Long-polling can be more efficient than short polling, as servers can push data to the client whenever it becomes available, resulting in less handshakes and teardowns. However, this is still more network load intensive when compared with EDA.

The advantage long-polling has over EDA is that clients can maintain state of all the devices easier, and query each of the nodes on the network. However, polling may not be suitable in situations where notifications are waiting to be processed, while the client is busy polling other devices, especially when there are large numbers of systems involved. Polling may be better used when data does not need to be collected from devices quite so regularly.

*Request / Response Architecture*

A one-to-one model architecture, where the client is reliant on the server, meaning it is highly coupled. It can be thought of as one-way communication, as the server does not query the client. Devices connect to each other directly, without the use of a broker, and uses synchronous communications. When service A wants to query data from service B, service A waits for a response. Once ready, service B sends the data to service A, meaning all other devices cannot be contacted until completion. However, service A gets immediate acknowledgement through a response.

Lee et al. (2022) propose a power saving automatic IoT LED lighting system based on a master / slave architecture. The master LED node detects a signal, and subsequently triggers all other slave LEDs in the same zone to increase their brightness to the same level, thus saving power and cost in implementation wired infrastructure.

Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transport (MQTT) are two messaging protocols suitable for use with constrained devices, and supported over various protocols, furthermore Larmo et al. (2018) compare their performances over BLE and WiFi.

MQTT is an application layer communications protocol that transmits notifications between IoT devices using publish / subscribe architecture, and works over TCP that ensures reliable transmissions. MQTT can also leverage Transport Layer Security (TLS) to provide security if devices have sufficient resources. MQTT pushes notifications, rather than requiring clients to poll servers. Clients can also leverage unique MQTT properties such as Last Will and Testament (LWT), which identifies device failure in near real time, and retained notifications to hold last known good data in the event of a client outage.

CoAP is an HTTP-like communications protocol using RESTful standards, and was introduced to support constrained devices due to HTTPs large overheads. CoAP leverages UDP, meaning improved performance compared with TCP. While CoAP has properties which improve communications reliability, UDP is connectionless, and is therefore considered unreliable as packets may be lost or arrive in the incorrect order. UDP leverages DTLS in a similar way to TLS to provide authenticity, integrity and confidentiality.

Because CoAP clients rely on server responses, it is not useful for high network traffic loads.

**Threat Modelling**

Threat modelling allows detailed analysis to take place with the aim of detecting system threats. This paper used an attack-defence tree method to determine both abuse cases, and corresponding mitigations. The attack-defence tree can be found in Appendix A, and the threats are listed in Table 1:

Table 1: Threats

|  |  |  |
| --- | --- | --- |
| **Threat** | **Description** | **Layer** |
| Tamper | Malicious actor physically manipulates IoT devices or connections. This may be 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 actor replaces the known good firmware, with intentions of exploiting known vulnerabilities in the new software. | Perception |
| Jamming | Wireless Sensor Node (WSN) is interfered with by louder signals on the same frequency, leaving legitimate data collection impossible. | Perception |
| Eavesdrop | Attacker reads plain text communications in transit across the wire, or more commonly, over air. This is made possible due to 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 original destination (Conti et al., 2016). | Network |
| Lateral Movement | If an attacker successfully penetrates a device, they may use this as 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 can be exacerbated by 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, connect to the network, or broker via topics, with the intention to fool other clients to connect to them to intercept communications. | Network |
| Malicious Access | An unauthorised actor gains access to a device through one of its interfaces. This is likely to be following an initial reconnaissance stage whereby common credentials for that type of device are sought from open source intelligence (OSINT). | Application |
| Code Exploit | Attackers exploit vulnerabilities by entering malicious commands to the device's software. | Application |
| Fake Data | A compromised device is manipulated to send falsified data to create malicious situations, e.g. force open a door, or raise an unnecessary alarm. It may also be used to crash a device by sending invalid data | Application |

# Prevention and Detection Model

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 threat matrices using IoCs can also help determine zero day threats, or black swans. Therefore, a new model is proposed to prevent threats using preventative controls, and uses a supplement scoring algorithm based on weighted IoCs to detect threats.

As sports stadiums require detection of system threats in near real time to ensure human safety, the MQTT publish / subscribe model is most suitable, and this architecture is presented in Figure 1.

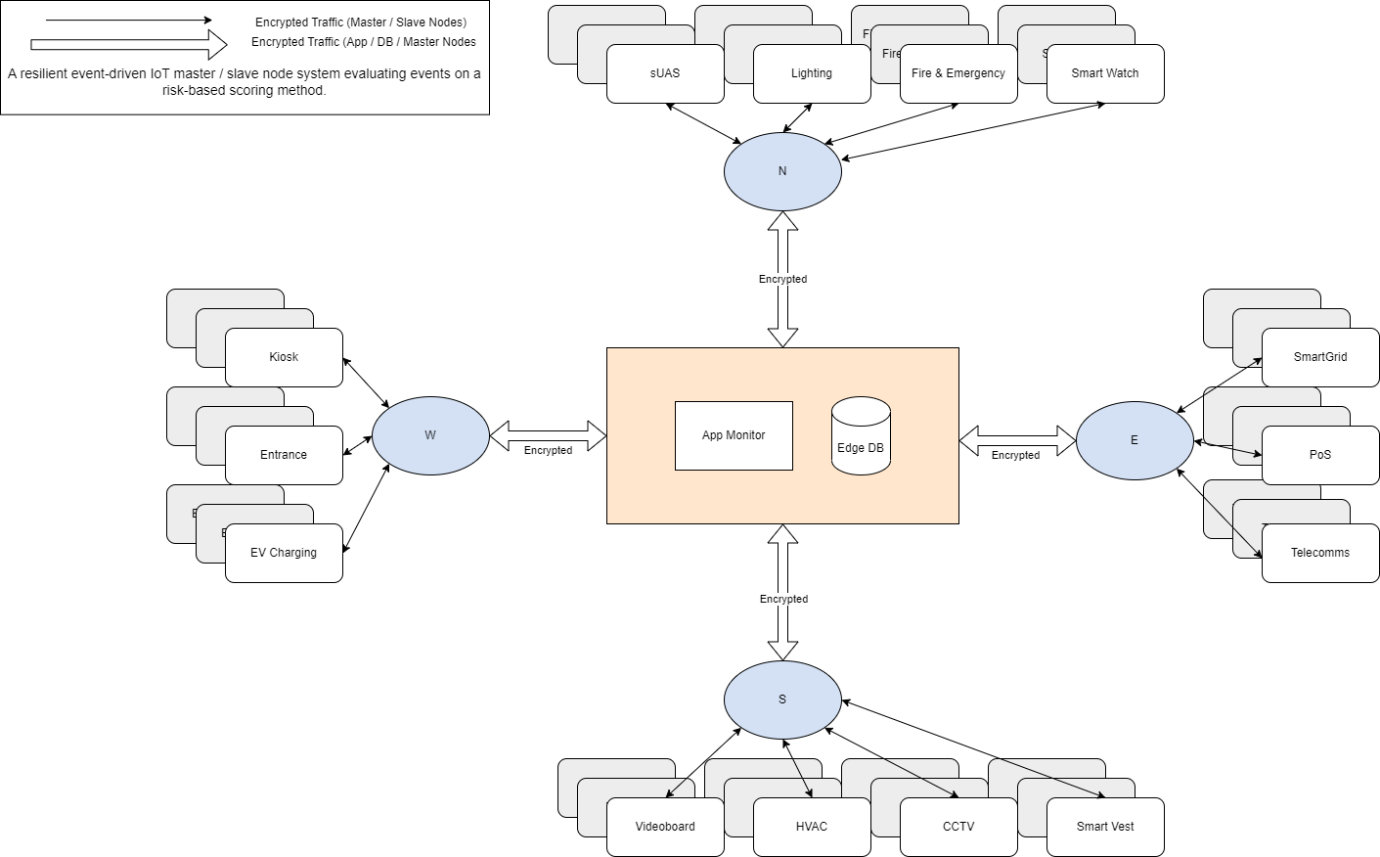


Figure 5: Stadium IoT Architecture

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 respective technologies, and the edge master nodes combine MQTT broker and IoT gateway capabilities. This enables them to accept notifications from multiple slave nodes, and make appropriate decisions.

*QoS*

MQTT uses a unique implementation of guaranteeing quality of service (QoS), and offers three levels: QoS 0: At most once, QoS 1: At least once, and QoS 2: Exactly once.

In sports stadiums, there may not be a need to expose devices to the public Internet. Therefore, security is improved using edge devices. By devices’ relatively close proximity, enhanced by the use of the cardinal nodes, the reliability of communications is already improved. However, because of the need to protect human life, the reliability of notifications is of paramount importance. MQTT uses TCP which is a reliable connection, and QoS 2 provides additional reliability at the application level. In sports stadiums, 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 (CONSIDER CITING THIS BLOG <https://cedalo.com/blog/understanding-mqtt-qos/>). By using a QoS 2 service level, the model is inherently idempotent. A keepalive period of four seconds is set. 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 the device fails over to a corresponding backup device.

A downside to using QoS 2 is increased notification delivery times due to a four step process needed to guarantee delivery between the producer and consumer. Additionally, using QoS 2 leaves the potential for DoS attacks if the publishing device is asked to send excessive data to the subscriber. This can cause backlogs and overload the broker, however this is mitigated in the model by using rate limiting, by taking a sample of data and sending event notifications exactly once per second. Similarly, a lockout method has been implemented to restrict brute force attacks overwhelming the system authentication attempts. The failover mechanism additionally provides redundancy in case of attack on, or malfunction of the devices.

To prevent rogue devices picking up notifications sent on the topic broadcast, authentication is required. Authentication to the broker must be enforced in the form of SSL certificates if the device has the resources, or alternatively using encrypted credentials sent in the MQTT CONNECT packet. Devices unable to authenticate cannot subscribe to topics.

Subscriptions may expire after a number of days of inactivity, this can be troublesome in sports stadiums during periods of inactivity, such as the close season. Stadiums may 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.

By throttling the publishing rate to once per second, the chances of overloading the broker are 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.

In an event-driven architecture, there is potential that more notifications will be sent than received. If the consumer gets overwhelmed or goes offline, then it is possible to add additional consumers, or include a broker cluster.

The database location is of lesser importance, as the master node makes decisions autonomously. If kept centrally, threats could compromise the network connection between the master node and the central database. Alternatively, each of the cardinal points keep its own cache database with transactions needing to be reliably synchronised back to the central database.

Additionally, the fact that cardinal 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 required to contain possible attacks more granularly.

For the scoring algorithm, it is still somewhat automated. IoCs are determined for each particular threat, with weightings given for each. If the combined score of the detected IoCs exceeds ten, the slave node is deactivated and and alarm is raised. The master node then activates a backup node.

Other solutions to this could be AI-based mechanisms, such as Naïve-Bayes classification, which use a pre-existing threat dataset to classify IoCs based on their previous involvement in genuine threats.

Each device is configured with a unique client ID. Therefore, if a backup is initiated, it connects to the broker using the same client ID, and the cleansession flag set to true, enabling it to seamlessly continue picking up notifications.

Due to its decoupled nature, EDA is poor for maintaining consistency, however as this model has only one consumer for each node in the chain, and uses QoS 2 for reliability, this problem is alleviated. The algorithm for this system can be found in Appendix B, with each swimlane individually shown below in Figures 2 - 4.

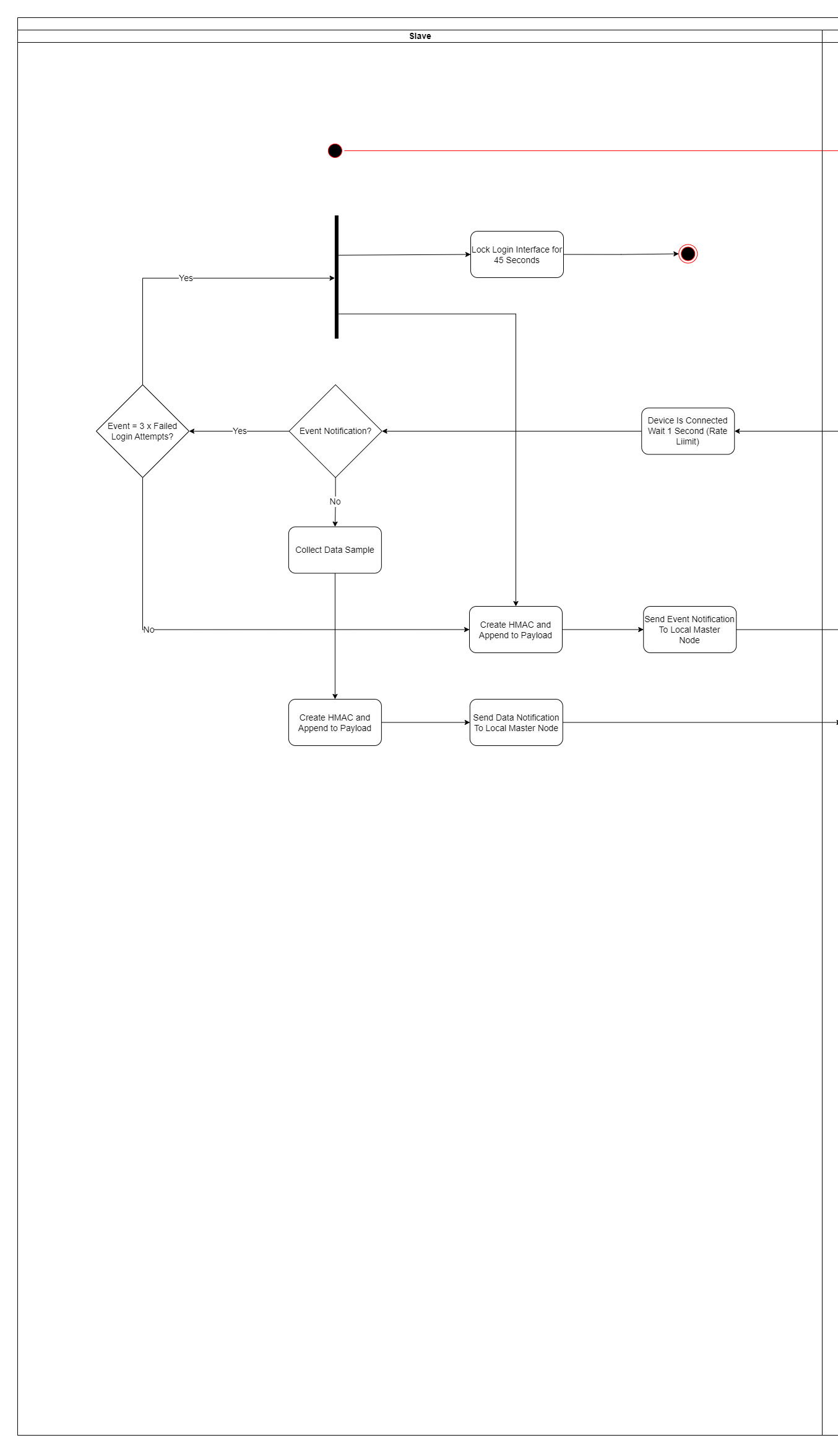


Figure 6: Slave swimlane

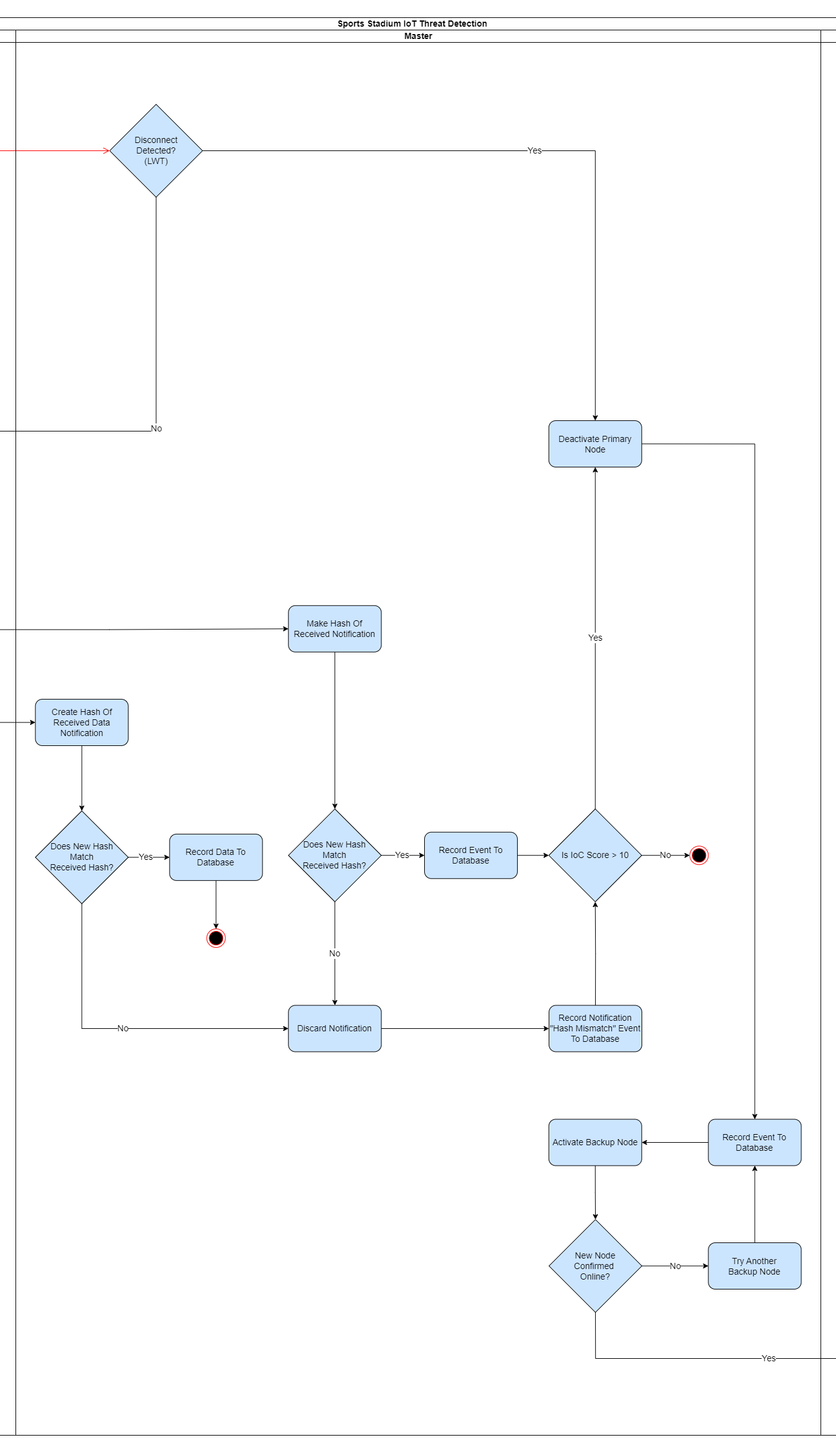


Figure 7: Master swimlane



Figure 8: Application swimlane

IoT Gateways / Master Nodes

Edge computing allows data to be processed at the edge of the local network, without sending data to the cloud. IoT gateways collect data from end nodes that are unable to communicate over the IP network. These gateways can therefore perform multiple functions as edge computing MQTT brokers for end devices to communicate with the rest of the system. This has several benefits, including less latency, higher network performance, and added security due to limited exposure over the public Internet.

Inside a sports stadium, many devices will be mains powered, and if using devices such as smart watches or smart sports equipment such as cricket balls, it may be possible to use a Wireless Personal Area Network (WPAN) technology such as BLE. Therefore, the use of long range mediums such as Low Power Wide Area Network (LPWAN) technologies, which preserve battery life are unnecessary. IoT gateways can accommodate these, and translate to IP for sending to the cloud, while making basic decisions regarding the end devices themselves.

A four second keepalive period was chosen, meaning notifications are forwarded to LWT topic consumers following a period of no communication after 150% of the set keepalive duration. Longer durations increase the risk to human life as problems may go undetected, and shorter durations increase false positive rates following increased sensitivity to minor network issues or device malfunctions.

Constrained nodes may not have the required resources to compute and leverage cryptographic algorithms used by digital certificates.

All data is therefore encrypted using private key encryption such as Advanced Encryption Standard (AES), in the absence of SSL certificates. Hashes are computed for messages and appended to the notification in the form of Hash-Based Message Authentication Codes (HMACs). Therefore, confidentiality and integrity is enforced. Authentication is provided by encrypting credentials and sent to the broker in the CONNECT packet. Authorisation is set per topic.

# Mitigating The Discovered Threats

* **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 can detect both purposeful tamper attacks and disruptive network issues (HiveMQ, 2015).
* **Unauthorised Firmware:** Preventative controls begin by disabling Over The Air (OTA) updates. These are inappropriate in a stadium, especially when reimaging already compromised devices, it is likely MITM attacks may be present which can replace the firmware. Firmware updates should can done manually, here unnecessary local connections may be disabled, such as JTAG and UART (Martinez, N.D.). Furthermore, it may also be possible detect modifications.
* **Jamming:** Difficult to avoid, however the best solutions are to make it difficult for attackers to find the correct frequency in which the data is sent.
  + Physical bag checks for patrons upon stadium entry can enable detection and confiscation of wireless jamming devices at source.
  + Spread Spectrum, e.g. Frequency Hopping or Direct Sequence (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 eavesdrop mitigation techniques, as detecting this kind of attack can be difficult (Stone, N.D.).
  + Network segmentation and firewalls prevent attackers gaining access to the network to sniff packets. It is particularly important to promote cyber security awareness amongst the stadium staff to ensure good cyber security habits are followed. Strong authentication is required in networks, as those which are openly available to connect to, provides a possibility for eavesdropping
  + Strong passwords
  + Most of all, encrypting data in transit can ensure that even if the attacker gains access to the packets, it would be unlikely to decrypt to read the plain text.
* **MITM:** If possible, Secure Sockets Layer (SSL) certificates should be used to mutually authenticate clients and servers on the network, with Transport Layer Security (TLS) used to protect data in transit.
* **Lateral Movement:** Attackers need to first compromise a device to then move around the network. To prevent this, as a defence in depth, network segregation must be used to limit what they can do if they are successful.
* **DoS:** QoS 2 level reliability. Redundant hardware. Rate limiting.
* **Rogue Device:** Employ firewalls to restrict data to inside the stadium network only. Edge devices employed to respond to client notifications, with minimal need to send data across the public Internet. This will ensure defence in depth as, attackers would need to breach the internal network, however would also then need to subscribe to topics to read the packets being sent by clients. Strict authentication and authorisation enforced at the broker ensures only those with a valid need to know are able to subscribe to topics.
* **Malicious Access:** Preventative measures include the changing of default credentials, as per the guidance in the Product Security and Telecommunications Infrastructure Act (2022). Strong passwords should be chosen, and only shared with those on a need to know and least privilege basis. Access Control Lists (ACL) should be leveraged to minimise functions running with elevated privileges, and prevent unauthorised access. Features, services and ports not necessary for its function, such as telnet, should be disabled or uninstalled. These weaknesses are common attack vectors, and enabled the Mirai botnet to be so effective.
* **Code Exploit**: Devices should be purchased from a known and trusted manufacturer, who adhere to the standards in the EN 303 645. The same due diligence should be taken for any distributors and installers, as backdoors or malicious components could be installed along the supply chain. Post install, security updates should be applied regularly and promptly. Features, services and ports unnecessary for its function, such as telnet, should be disabled or uninstalled. Input validation can be applied to ensure scripting attacks are not possible.
* **Fake Data:** Fabricated data may need to be relied upon using detection techniques.

**Investigation of what you’ve done**

**Excel**

# Discussion and Evaluation

Detection Scoring Algorithm:

Indicators of Compromise:

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, for example. Authorisation can also be enforced on the broker here to ensure clients are restricted to publishing, and cannot subscribe, for example. 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 can work in conjunction with TLS providing an additional layer of security, although this does come at the cost of performance.

As added protection, hashes are configured to ensure the notifications has been unaltered in transit. In constrained devices, HMAC is preferred as it is not as resource intensive as digital signatures, and uses the secret key to calculate the code proving that the payload has remained unchanged, and that only someone who knows the secret key was able to send it.

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

# Conclusion

# 

# Lessons Learned

This research contributes to the Infrastructure Security CyBOK Category and the associated Cyber-Physical Systems Security Knowledge Area (NCSC, 2019). However, the overall project was extremely challenging. In this process, vast amounts of time was spent determining and pinpointing the particular research problem, and project design. Although the topic remained the same, there was increasing pressure to find research gaps in order to find a path forward. This led to incessant reading at a broad level throughout the project, in a bid to find a novel problem.

The project also resulted in deep research to understand the technology holistically relating to the focus area, and examining various strategies to implement a suitable artefact. This led to attending multiple online boot-camps, followed by regular prototype creations to ensure the relevant skills were acquired, and ready to put into practice. Part of this problem was the attention given to the artefact, instead of determining an answer to the research problem at hand. The necessary inclusion of an artefact proved hugely distracting to focus on understanding the original problem. If such a project was to be revisited, it is clear that early diagnosis of the problem space is of paramount importance, leading to strong foundations for the project and a clear path forward. This could be eased by understanding project requirements in advance, and understanding that dedicated thinking during earlier modules may help in sculpting ideas for the ultimate deliverable.

However, this particular downfall did have some positives, namely the acquisition of several new skills for prototypes that were not pursued. Among these included new insight into containerisation technologies such as Docker, with further knowledge acquisition of Docker Swarm, and insight into tools such as Snyk to ensure container security. Further Linux skills were also acquired, in particular how packages are updated, implementing iptables, using Secure Copy (SCP), creating users, and establishing Secure Shell (SSH) tunnels.

Various new Python modules were also discovered, including Beautiful Soup, Requests, Colorama, Fabric, Pythonping, all of which were not used, however may prove useful for future work. Furthermore, new MQTT techniques such as the use of LWT notifications, QoS levels, cleansession flags, and keepalive intervals, were explored.

Naturally, as part of research for a capstone project around the subject of IoT, much content was digested regarding the different wireless sensor network (WSN) communication technologies, how they work, the various types of physical IoT devices available, how they are composed, and their various IoT attack vectors and techniques.

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

In terms of soft skills, much time was likely wasted reading entire research papers. In future, this would not be a recommended approach. Advice was offered on this, however there was always the temptation to cover all ground in the hope that nothing was missed. In future, it is likely more beneficial to scan papers paying particular attention to abstracts, and perhaps conclusions, before deciding whether it is worth delving in to the full content.

Limitations to the study included time constraints, exacerbated by an initial lack of understanding of requirements and technologies that might be used or needed to be understood. This pushed back the project milestones considerably. Additionally, working remotely proved very challenging, felt isolating and was amplified by having only sporadic email access and a limited allowance of video call time with supervisors.

More thorough IoCs could have been included in the model for testing, with more granular weightings if more time was available. However, this was a proof of concept model, and if time was not a restriction, other methods could have been pursued to create the threat matrix.

The project changed somewhat from the original research proposal.

The artefact changed like this…

The risks however did not change. Each risk stated in the research proposal was realised. In order to complete the project to a suitable standard, incessant reading to understand the various technologies involved was required, as was the need to find a research gap. This in turn led to the next risk being realised, with time quickly evaporating, this was very top heavy project following extensive research. There was difficulty at times understanding the requirements, and was likely due to having a non-academic background and miscommunication with supervisor’s. Time was taken at a critical point to take stock and re-evaluate, and this was one aspect in which remote study was beneficial due to reconstructing previous emails to find a way forward. This also meant being stuck at the literature review stage for some time, meaning the report was lacking for the most part. Finally, laptop malfunctions on two occasions meant that data loss occurred twice in the project. The advance consideration of these risks proved beneficial, as each predicted countermeasure paid dividends. Continuous research was practiced throughout, the project plan kept focus and aware of what was still required, and a work / study / life balance maintained stability. This was not helped by starting a new demanding job, but a continuous routine kept things balanced. Prior to this, during a time of unemployment, much additional research was performed during the slack time and this contributed to a good understanding of IoT technologies. The project resources and supervisors kept things heading in the right direction, and these were invaluable to the project’s success. Finally, the backed up data was required on two occasions. Would these not have been created in advance, the project would almost certainly have failed.

# Conclusion and Future Work

With more time, further IoCs and threats would have been sought. Thorough testing would have also been performed to ensure improved weighting accuracy, and improve detection sensitivity.

It may be beneficial to adapt the model to use other detection algorithms such as the Naïve Bayes classifier to classify IoCs. This may have produced more accurate results due to the engine being fed historical data.

The model also does not take into account Advanced Persistent Threats (APTs). These are threats that infiltrate the system long before the attack takes place, and so would not be detected by a real time IoCs algorithm. Therefore, another stage in scoring the threats may be used to include lurking threats, while still avoiding triggering false positives.

Any future work should be mindful of ethical issues involved in applying this to a real stadium.

# References

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

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

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>

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>

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.

Baker, P. (2020) The Rise of Cyberthreats in Sports. Available from: <https://professional.uchicago.edu/stories/master-science-threat-and-response-management/rise-cyberthreats-sports> [Accessed 12 April 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.

BBC. (2023) 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].

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].

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

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>

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].

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

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>

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.

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].

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

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].

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

HiveMQ. (2015) 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].

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].

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

Jamali, M. A. J., Bahrami, B., Heidari, A., Allahverdizadeh, P. & Norouzi, F. (2019) *Towards the Internet of Things*: *Architectures, Security, and Applications*. 1st ed. Cham, Switzerland: Springer International Publishing. Available from <https://link.springer.com/book/10.1007/978-3-030-18468-1>

Jazzar, M. & Hamad, M. (2022) ‘An Analysis Study of IoT and DoS Attack Perspective’, *Proceedings of International Conference on Intelligent Cyber-Physical Systems*. West Bengal, India, 4–26 June 2021. Singapore: Springer. 127–142.

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].

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.

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].

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.

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>

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].

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].

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):

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].

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.

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.

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].

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/s11948-018-0s033-5>

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>

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

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].

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

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

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].

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’, *14th International Conference on Trust, Privacy & Security in Digital Business.* Lyon, France, 30-31 August. Cham: Springer. 164–179.

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

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].

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].

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].

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

Cook, D. (2000) 'Developing franchised business in Scotland' Small firms: adding the spark: the 23rd ISBA national small firms policy and research conference. Robert Gordon University, Aberdeen, 15 17 November. Leeds: Institute for Small Business Affairs. 127-136.

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>

Wigmore, I. (2016) idempotence. Available from: <https://www.techtarget.com/whatis/definition/idempotence> [Accessed 04 June 2023].

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>

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

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>

**Bibliography**

# Appendices

**APPENDIX A: Detection Algorithm**

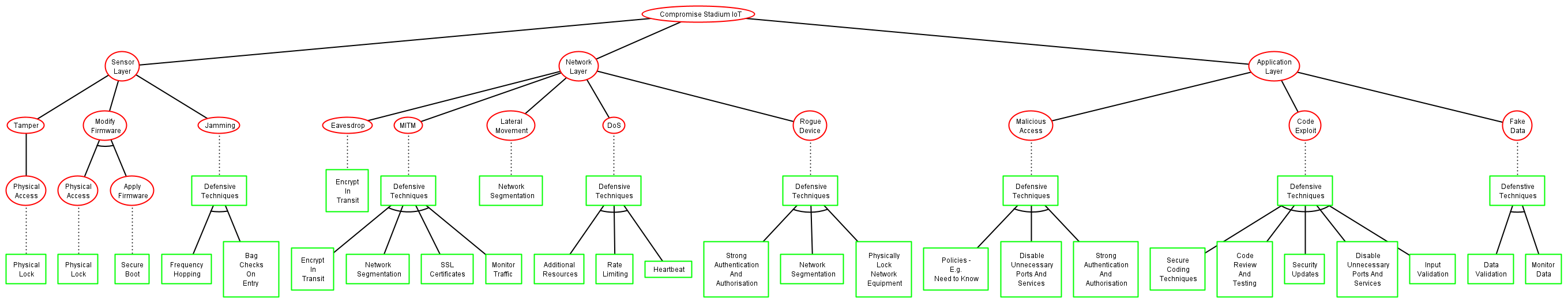
****

Figure 9: Attack-Defence Tree

**APPENDIX B: Detection Algorithm**

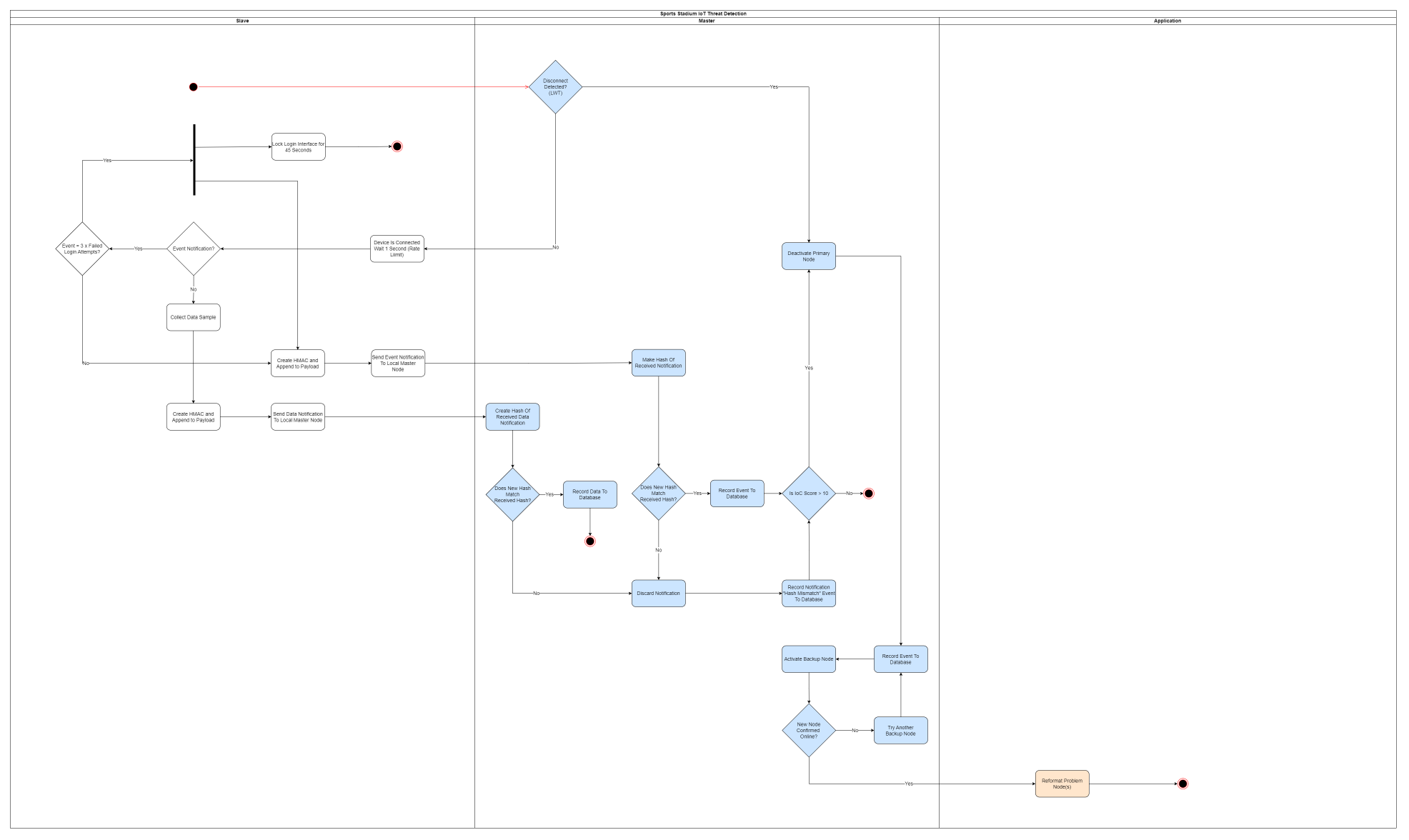


Figure 10: Algorithm Activity Diagrams