**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](#_Toc138504630)

[Literature Review 4](#_Toc138504631)

[*Internet of Things* 4](#_Toc138504632)

[*IoT Architecture* 5](#_Toc138504633)

[*Smart stadiums* 8](#_Toc138504634)

[*IoT Technology and Cyber Security in sports* 13](#_Toc138504635)

[Polling 17](#_Toc138504636)

[Methodology 17](#_Toc138504637)

[Results 18](#_Toc138504638)

[Discussion 18](#_Toc138504639)

[Conclusion 18](#_Toc138504640)

[References 19](#_Toc138504641)

# 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.

# 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).

Which devices are 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, used 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, as well lacking in security (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. By breaking the IoT architecture into more levels, security can be thought of more granularly and specific to each of them. 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, introduce predictive maintenance, maintain quality assurance, and maintain 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, thus 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 very difficult to expect 80,000 spectators to fill out a waiver upon entry, and perhaps unrealistic for them to read a notice mounted on a wall advising them of their recordings and data gathering. Brey also highlights other specific issues of using FRT, including errors and function creep, which are now however, 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 the very 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).

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.).

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, while 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 EN303645, 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 such vulnerabilities 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*

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 to be compromised 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 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. Also, tags are vulnerable to cloning, and readers would be affected by many thousands of people passing by, with potential for collisions, manipulation, and jamming attacks.

*Examples of historic compromise*

The Mirai botnet of 2016 showed how inept the IoT world was in detecting and preventing 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 a retaliation for banning Russian athletes from the 2016 Summer Paralympic games in Brasil, 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 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. There 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), and the Open Web Application Security Project (OWASP) have published an IoT top 10 (vulnerabilities) list as of 2018 (OWASP, 2018).

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 how to 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 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, 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.

**Architecture Types**

*Event-Driven architecture*

IoT devices in an event-driven architecture (EDA) communicate by publishing messages and commands to each other in the form of notifications. These notifications may be triggered by events that occur on devices (indicating a change in state), or be sent on a schedule. The device transmits the notification to appropriate endpoints on the network, who then can publish their own reactive notifications to other devices. This architecture style works using asynchronous communication, where once the notification has left the device, it is forgotten about, and the device is ready to process with the next event.

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

Depending on the implementation and its requirements, EDA can present 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 may be a complex consideration for use over unreliable networks. Consideration should be taken over whether guaranteed delivery is required, or whether send and forget is sufficient.

Devices are typically dependent on notifications from others. This is exacerbated when multiple devices are sending simultaneous notifications that need to be processed in the correct order. Ordering is a well-known issue in this architecture, which often needs to be resolved by appending identification numbers, versions or timestamps to the notifications themselves 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, as receiving the same notification twice can result in the system crashing, or leaving inconsistent results. This can happen if the broker goes down and has to return to a previous checkpoint. Here, a medium such as a database can used to store notifications, with controller logic applied to check against previously received notifications.

*Publish / Subscribe model*

The publish / subscribe (pub / sub) model is a sub-type of EDA, where a broker proxies the information sent between the producer (publisher) and the consumer (subscriber). Messages are broadcast to consumers using topics. The disadvantage of the pub / sub model is that while any device can go offline, the broker is typically a single point of failure for the whole system, meaning a Denial of Service (DoS) is possible, with a successful attack resulting in an outage of the entire system.

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

# 

# *Polling*

Polling uses a client node to contact server nodes (IoT devices) to check 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 notifications in EDA, each polling request is independent, and does not rely on the last.

This may be suitable for environments where long delays between network calls is acceptable, however in a system comprising multiple IoT devices, each with information to send, this may not be practicable, and if more regular requests are required to be sent to the servers, then the interval needs to be reduced, adding to network load.

Polling in systems where multiple servers are sending messages is inefficient. During and interval period, resources on the client side are wasted by creating handshakes and teardowns, when continuously polling devices which have no data to transmit. Furthermore, while the client polls the server for messages, all other devices have to wait while the client’s resources are consumed. Polling is unsuitable for real time, or high volume applications due to these reasons.

There are also other sub-types of polling architecture including long-polling, in which a client will poll the resource for data, however if the server does not have any data, the client leaves the connection open until the response is given, or a timeout occurs. This, is preferred in implementations containing minimal devices, as it only makes the one connection, however is less efficient in some ways than short-polling as keeping the connection open each time until it receives a response ties up both the client and the server for that duration.

Long-polling can also be more efficient than short polling, as the server can push data to the client whenever it becomes available, meaning handshakes and teardowns are not required so often. However, is still more network load intensive when compared with EDA.

The advantage it has over EDA is that the client can maintain state of all the devices easier, and can query each of the nodes on the network. However, polling may not be suitable in situations where messages 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.

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.

*Request / Response Architecture*

1 to 1 model architecture, where the client is reliant on the server, meaning it is highly coupled.

**Which one?**

HTTP cannot be used as the overhead is too great for constrained devices.

Because of the importance of receiving data in near real time to detect threats to systems that have the ability to compromise human safety, an EDA has been chosen.

MQTT is an application layer communications protocol often used to transmit messages between IoT devices using a publish / subscribe architecture, and works on top of TCP to ensure reliable connections. MQTT can also leverage TLS if the devices have the resources to support it. has been chosen because…

Constrained Application Protocol (CoAP) is an HTTP-like communications protocol using RESTful standards, designed for constrained devices. CoAP leverages UDP, meaning performance may be improved compared with TCP. However, although CoAP has properties which can be used to ensure reliable communications, it still uses UDP and is considered connectionless and therefore an unreliable protocol. This may mean that packets can be lost or arrive in the incorrect order. As UDP cannot leverage TLS, it uses DTLS to provide authenticity, integrity and confidentiality.

Because CoAP clients rely on server responses, it is not useful in situations where there is high network traffic load. CoAP’s mechanisms for reliability are also not as robust as MQTT which uses TCP for transmitting packets.

Sports stadiums will usually operate an internal network, meaning a reliable network is present. However, even though this is the case, because of the potential for human life to be affected by the system malfunctioning, or not detecting a message (notification), QoS2 has been chosen. QoS2 ensures guaranteed delivery of each message exactly once. This is important to ensure that every notification reaches its destination, as well as ensuring that messages do not arrive more than once. This is important to inherently guarantee the notion of idempotence. As there is only one device consuming the published messages, with QoS2 service level, the system is inherently idempotent. If a device should fail, or not report back for five seconds, the system failsover to the backup device. Another way to implement this is to implement three devices collecting the data as part of a broadcast. However, this could lead to a mismatch in states.

Downsides to using the QoS2 service level include increased message delivery times due to the four step process needed to guarantee delivery between the producer and consumer. Additionally, using QoS2 does have the potential to cause DoS attacks if a publishing device is asked to send excessive data to the subscriber. This can cause a backlog and overload the broker, this is mitigated using rate limiting by taking a sample of data, and sending error messages once per second in the model. Similarly, a lockout method has been implemented to restrict brute force attacks overwhelming the system with credential requests and notifications. The failover mechanism additionally provides redundancy in case of attack on, or malfunction of a system.

# Methodology

This paper therefore employs a comparison-style cross-sectional study of the pub/sub and polling architectures in the context of sport stadium IoT, and how they may respond to DoS attacks on the network.

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 method, with applied deductive reasoning to determine the results.

There were no ethical concerns for this study as it did not involve any human participants, or include and real organisational data.

# Results

# Discussion

# Conclusion

# 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].

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].

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].

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>

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].

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].

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].

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. (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/s11948-018-0033-5

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

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

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

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].

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>

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].

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

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].

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**

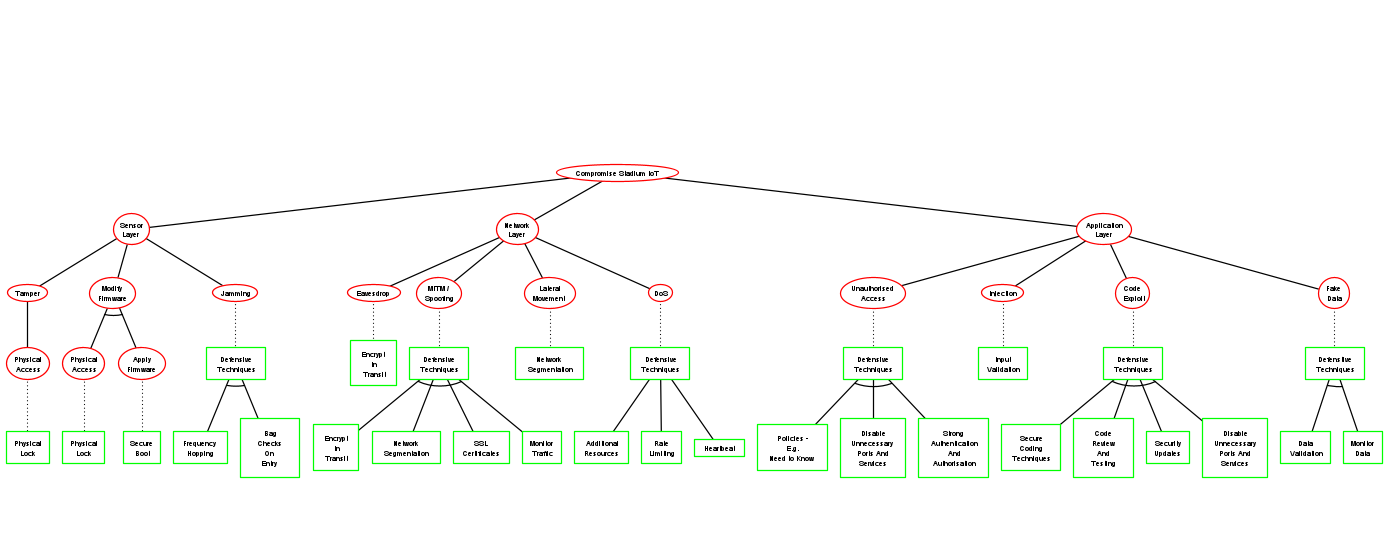
****

Figure 1: Attack-Defence Tree