IOT IN PRACTICE: INVESTIGATING THE BENEFITS AND CHALLENGES OF IOT ADOPTION FOR THE SUSTAINABILITYOF THE HOSPITALITY SECTOR

Nick Kalsi, Fiona Carroll, Kasha Minor and Jon Platts

[1]Cardiff School of Technologies, Cardiff Metropolitan University, Llandaff Campus, Western Avenue, Cardiff, CF52YB

ABSTRACT

Enhancing the sustainability of the hospitality sector with technology is essential to achieving growth whilstalso reducing the hotel's impact on the environment. Indeed, the Internet of Things (IoT) concept has recently gained popularity as a new research topic in various industrial disciplines, including the hospitality industry. IoT is being seen and used to transform the hospitality industry for the newly desired sustainable growth. However, it is not all 'smooth sailing' as multiple challenges must be addressed by organisations in the hospitality industry when installing IoT. These challenges include cost, security, infrastructure and IoT protocols. Considering the diversity of IoT applications, the paper will examine IoT's use in hotels whilst also highlighting the challenges hotels face when using IoT. In particular, it will cover the effect of cyber security, including IoT's protocol layers, potential monitoring and sensor technologies.

KEYWORDS

Hotel, Internet of Things (IoT), Sensors, IoT Security, Cloud, compliance, privacy, safety, standard, communication, information.

1. INTRODUCTION

Technology has evolved significantly, with businesses in different industries worldwide relying on technological innovations to accomplish their new green and smart objectives [1]. These technological innovations have specifically impacted the tourism, aviation and hospitality industries, with the Internet of Things (IoT) becoming an essential aspect of businesses operating in this industry, with a projected 95 per cent of companies projected to adopt this technology by the end of 2022 [2] In particular, research [3]indicates that IoT has gained even more popularity since the Covid-19 pandemic due to the need to avoid social interactions and human contact. This has increased the need for remote interaction and, in turn, has enabled providers to access vital information from society through remote approaches supported by IoT. While the pandemic has accelerated IoT adoption, implementing these technologies has been a progressive process to improve the 'greenness' of the hotel (e.g. enhance the customer eco-experience, cut down the cost of hotel operations, and enhance security)[4]. Unsurprisingly, the future has already arrived, but new changes are needed to improve the hotel's sustainable operations further as technology evolves. IoT technological innovations are changing the landscape of the hospitality industry. Asa result, hotels must understand the challenges of using IoT. The following sections of this paper will discuss the compliance issues that come with the use of IoT, their relevance in hotels, and

David C. Wyld et al. (Eds): ICDIPV, CBIoT, ICAIT, WIMO, NC, CRYPIS, ITCSE, NLCA, CAIML -2023
pp. 143-158, 2023. CS & IT - CSCP 2023 DOI: 10.5121/csit.2023.131311

their benefits in conjunction with the associated costs. Importantly, it will highlight, the knowledge of IoT's current usage problems, issues around General Data Protection Regulation (GDPR) privacy, and data storage that are relevant when implementing or determining IoT types to afford a more sustainable hotel.

2. What Does IoT Mean for Hotels?

As defined by [3] 'IoT is an advanced technology that links intelligent devices with the internet to trigger an action, automate a process, and collect data by eliminating overreliance on human involvement [3]. Moreover, Verma et al. describe 'IoT as the technology that connects different devices through the cloud or internet services through sensors fitting into these devices to facilitate data collection and distribution and ease the analysis of such data in an accurate and real-time manner'[5]. The standard terms encapsulating the concept are the internet, automation, and data. This implies that IoT is a technological device that intends to automate specific tasks and processes through intelligent devices interconnected through the internet to enhance data collection, analysis, and distribution.

While IoT was initially focused on enhancing supply chain management, its usefulness has extended beyond its initial focus, with different industries capitalising on them to identify, track, collect, and authenticate data used to enforce service or product delivery to customers. [6]. recognise 'the role of IoT in shaping marketing actions adopted by businesses by enabling them to acquire a holistic and comprehensive understanding of their customer's behaviours and needs' [6]. By 2025, 75 billion devices worldwide are expected to be Internet-connected, providing information to consumers, manufacturers and utility providers [7]. The rise of the IoT goes hand in hand with the rise of artificial intelligence powered by big data. These technological innovations are effectively set up to ensure the easy, accurate, and real-time flow of information. And this is without the need for human involvement, which often results in significant errors in data collection and analysis. From a hotel perspective, this has huge potential benefits, with IoT being defined as: 'A network of digital devices and machines interrelated through the internet for enhanced guest experience and optimized expenses' [8].

3. What other Hotels are doing using IoT and their Benefits

IoT has gained popularity across different industries, and the hospitality industry has leveraged these applications to improve its performance. Hotels have incorporated IoT into their business for the associated benefits, including saving energy costs, enhancing customer experience, reducing employee workload, and reducing operational costs [10], [11]. As such, the hospitality sector benefits from enhancing the guest experience and monitoring energy expenditure within a facility. For example, *Starwood Hotels and Resorts* implements 'daylight harvesting', an energy-saving scheme that saves energy and increases indoor lighting consistency by automatically adjusting the energy-efficient LED lighting based on the natural light detected in the hotel room [12]. Moreover, studies have demonstrated that by using daylight harvesting technologies, owners can see an average annual energy savings of 24% [13]. Another example is the *Marriott Hotels* which have a mobile app catering to its mobile-savvy guests. They provide guests with a pre-programmed key card. Additionally, the app will automatically notify guests when their room is ready. According to the consulting firm Hudson Crossing, 80 percent of emerging travellers in the U.S. own smartphones [14]. As technology and its usage evolves this figure increases. From a hotel perspective, it means that smartphones can pro- vide current and future guests with enhanced flexibility and convenience across their travels and stay in hotels.

3.1. Smart hotel operation using IoT devices

IoT in hotels reaches far beyond having only lavish hotel guest rooms. An intelligent hotel represents disruptive technologies such as the Internet of Things and Artificial Intelligence. Moreover, to improve management, access to information can be given at anytime and anywhere as long as cloud management platforms are used. Efficiency and control from the hotel management can result in a better service to the guests. It considers the whole facility of integration, such as energy efficiency improvements, including renewable energy sources, environmentally green policy and treatment towards all waste products in the business, such as waste food, waste and sewage water treatment, energy recuperation, etc. Therefore, the smart hotel concept is instead an integrated concept which includes an automation control system based on modern information technology, a sophisticated set of sensors and actuators, optical or any other source of speedy communication facilities and protocols such as Wi-Fi, LoRa WAN, ZigBee wireless technology, integrated renewable energy sources. An example of a Smart Hotel being monitored using IoT devices in real time is presented in figure 1.

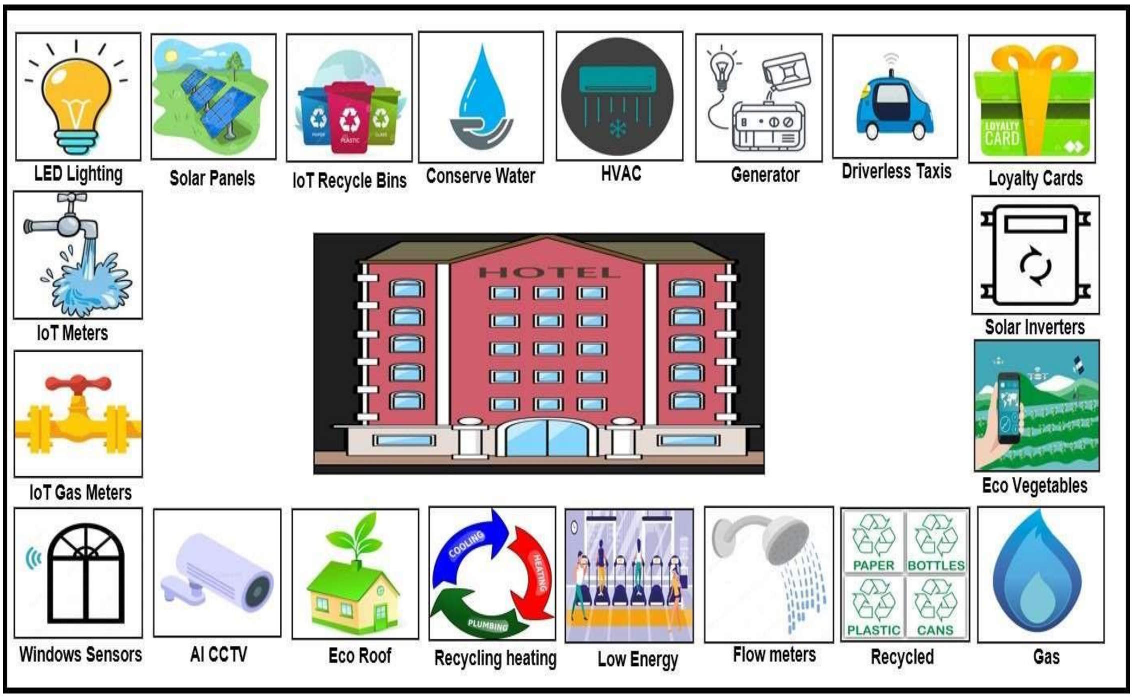

Figure 1: Functions of IoT devices and applications in a hotel

This includes

- IoT Recycle bins: Should a bin become full in public areas, an alarm can be sent to the local cleaner. Alarms can be grouped to alert specific staff.
- Led Lighting: The ability to conserve energy during the day, allowing remote control and management through mobile or web applications.
- Solar Panels inverters: As electricity has become an essential part of life and hotels use more, the power usage of every hotel has increased three- fold compared to the energy resources. To accommodate these surging needs, hotels are switching to a sustainable source of solar energy tobecome energy efficient.
- Conserving water: By having a water management system, a hotel can use aggregate and correlated data from an existing array of intelligent water sensors allowing to detect water leaks and detection and generate alerts that enable the hotel to quickly pinpoint problem areas and manage system pressure before leaks become extreme or a pipe burst.

- HVAC: By scheduling air conditioning, cooling can be controlled from the hotel property management system before the guest arrives at the room. Voice-activated controls for air conditioning are now a commonly used feature.
- Generator: Monitoring of Powered Gas or diesel generator for fuel levels, notification of electricity generated for a hotel, weekly self-tests. Driverless Taxis: As the communication capabilities between connected, intelligent devices grow, car manufacturers are taking advantageof new technologies designed to enhance passenger comfort and safety.
- Loyalty cards: Hotel guests are more likely to become loyal to hotels that share their concern for the global environment and actively look for solutions. Loyalty Cards and global warming tothe hotels they frequented. For hoteliers who listen to their guests, there is more than the added Reward Program for Hotel Membership is essential to push guest fidelity.
- Eco Vegetables: With the support of soil moisture sensors, results to good irrigation management gives better vegetables and uses fewer inputs.
- Gas: Sensors are designed to monitor the surroundings for any leakage continuously and will send the alert to the user via email or a dashboard. Furthermore, it alerts the user about environmental conditions like the temperature of that location and the gas level.
- Recycled: Separate compartments for materials that you can recycle include: glass bottles, cardboard, plastic bottles, food and drink cans, printer cartridges, electrical items
- A shower head flow sensor: A IoT sensor connected allowing to control of the flow of water and monitoring how many litres of water was consumed by the guest when having a shower; thisdata can then be sent to the guest after their stay to gain loyalty points
- Low energy Gym machines: Running machines generating electricity when used by guests, data is logged in lifestyle data.
- Recycling Energy: Sensors deployed to gather and transmit data in real-time. The main aim is to produce, transmit and distribute green energy so that energy optimisation and load management can be made in real-time.
- Green Roofs: Green roofs can be built on hotel buildings with soil depths less than 30 cm and low management frequency allowing shrubs, flowers, grass, and turf to be grown on those above.It helps to conserve heat for a hotel.
- AI CCTV: AI cameras detect and classify people, vehicles, faces, license plates and more in real time. The cameras’ deep-learning algorithms can reliably identify multiple distinct objects with various available resolutions from 2MP to 4K. Analytics become a reliable second pair of eyes to operators, helping them know where to look for critical real-time events while making post-event forensic searches highly efficient. Window contact sensors: When the guest opens a bedroom window, the HVAC (heating, ventilation, and air conditioning) stops to prevent the wastage of electrical energy.
- IoT Gas Meters: The ability to monitor the hotel Gas consumption to manage their operations and demand and efficiently invoice customers. IoT Water meters: Smart water metering allows efficient water demand and supply balance, reducing costs and contributing to sustainability requirements. Smart meters automate and help reduce water loss, such as leaks, throughout the entire water distribution network of the hotel.

3.1.1. IoT Guest room management system (GRMS)

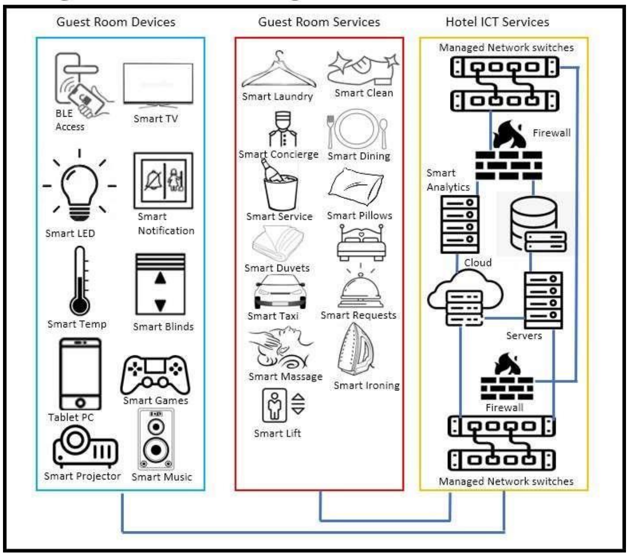

Figure 2: Smart Hotel Using GRMS

Guest Room Management System (GRMS) is a commonly used application in smart hotels. The Intelligent Hotel Room delivers personalised intelligent services to clients by monitoring their locations, activities, and smart objects within their rooms. GRMS provides guests convenience and enhances the hotel operator's control by providing efficient and intelligent management. The typical functions provided include Room status monitoring such as Do-not-Disturb, Make-up Room, Laundry, Guest occupancy and many more as per the customer specifications. HVAC/ AC Control, Access Control, Dimming Control, Lighting Control, Curtain/Blind Control Integration with PMS, BMS other 3rd party systems. The entire system in the room can be controlled via customised bedside panels and Smart Tablet PCs/devices. An example is the GRMS presented in figure 2.

Besides enhancing service delivery, IoT is actively useful in improving hotel accessibility as it automates check-in and entry into hotels. These applications help make emergency alerts on specific issues that require emergency attention [3]. In hotels, applications such as *Social Monitoring* and *Stop Corona* are actively used during the pandemic to reduce the individual guest risk for Covid 19. Other applications, such as cameras, are essentially used to monitor the hotel, including employees and guests, enhancing their safety and improving response time on their calls. Furthermore, IoT through temperature sensors is used in everyday operations to improve food storage and reduce energy and food wastage [10].

Generally, IoT devices and applications are widely used to support efficient service delivery in the hospitality industry. Hotels like Hilton leverage these innovations to enhance performance and improve guest experiences. Led by The American Hotel Lodging Association (AHLA) and the 5-Star Promise, hoteliers continue to make strong commitments to safety and security standards for the industry For instance; the Hilton has a 'Digital Key', a technology that is currently operational in 80% of the hotel's portfolio used to reduce plastic waste by 125 tons and open more than 235 million guestroom doors [15]. This technology works by allowing primary guests to share their active Digital Key with four additional people from the Hilton Honors App, allowing them to gain access to the room throughout the duration.

3.1.2. GRMS challenges and implications

Overall, GRMS solutions are costly for hotels taking into account maintenance service contracts with 24-hour monitoring services. Should any failures occur, specialist engineering knowledge is required for diagnoses leading to downtime. IoT devices have different integration standards, which can cause compatibility issues with GRMS applications communicating effectively.

However, guests can experience challenges using over-engineered technology in hotel guest rooms. For example, a guest wishes to close the bedroom curtains using a smart tablet pc. The smart application user interface should be presented clearly to the guest so that this will lead to frustration and a bad experience. Most hotels use system integrators (SIs) for GRMS solutions; these solutions are generally complex by design and need maintenance at all times, furthermore cost implications. The other challenging point is when backend systems services fail to communicate; for example, a typical guest requests a bottle of wine using room services using the Smart tablet pc. Suppose the interface between the IoT applications has stopped for some unknown reason. In that case, the room services department will not receive the order, resultingin a failed order and leading to a loss of revenue for the hotel.

3.1.3. Four layers of the IoT architecture

The Internet of Things (IoT) is an enhancement of the Internet that can be described as things in our environment being connected over the Internet, so as to give seamless communications and external services [16]. Every IoT Ecosystem is different, despite the many variations, all follow the same basic structure and flow. There are four IoT architecture layers that are required, each having a specific function (see figure 3)

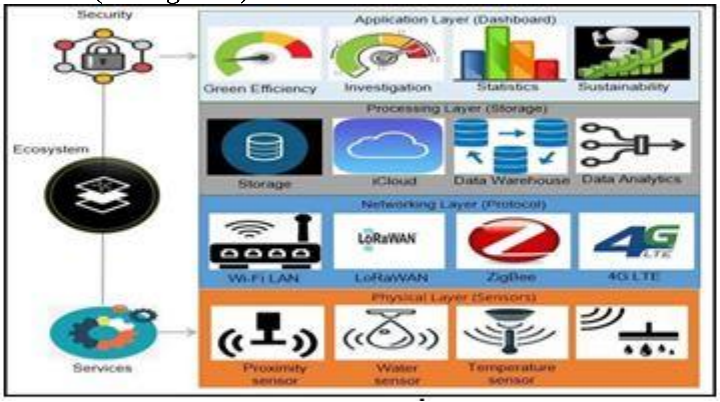

Figure 3: Four layers of IoT

The first layer of IoT architecture is sensing layer that includes devices, sensors, and actuators that collect data from their surroundings and control things at the edge. Devices that sense or control things in the real world are the foundation layer for an IoT ecosystem; these can be classified as proximity, water, humidity sensors. The second layer is a network layer that transports data from the device Layer to the Internet, often via a Gateway that performs additional switching or routing and often aggregates communications with edge devices. Security functionality, including authentication, and encryption, is typically managed here. Protocols such as Wi-Fi LAN, TCP/IP, Lora WAN, and ZigBee are some standard protocols. The third layer is a processing layer structured to handle data analysis and pre-processing. This layer is either located in the gateway or the cloud. Here, applications can access data for edge analytics in use cases like autonomous vehicles where real-time data is necessary. Data is monitored and managed while the processing is completed. The fourth layer is located in the cloud; data is used by end-user applications. This is true even in the case of edge computing, which generally still interacts with the cloud for data that isn't required in real-time. Once the data is processed in the cloud, it is used for applications like monitoring building heating and ventilation to monitor system performance and identify problems.

Communication is critical for IoT use, among its primary functions. A network protocol is a set of communication procedures and rules to exchange information and data over the network' [17]. Several groups formed by the Internet Engineering Task Force have developed and continue developing key IoT protocols. According to research [18] 'IoT's standard protocol stack is divided into IEEE 902.15.4, 6LoWPAN, CoAP, and RPL. IEEE 802.15.4 lays down communication guidelines at the physical layer and requires low energy for communication, while 6LoWPAN enables IPv6 packet transmission at higher layers using low-energy protocols'. In addition, CoAP is used in the application layer communication, ensuring interoperation ability between heterogeneous networks. In meeting IoT requirements regarding small device capacity and low power consumption, 'the application layer protocols such as CoAP, Advanced Queuing Protocol, and Message Queuing Telemetry Transport are essential' [19]. The network layer involves several protocols, including Ethernet, Wi-Fi, LTE, Bluetooth, 5G, and ZigBee. These protocols are essential in facilitating data communication between different layers of the IoT infrastructure.

4. Challenges using the IoT in Hospitality

For hotels to implement IoT, they need to understand how these devices work and the areas where they are best applied without violating customer privacy and well-being or employment terms. Like most other technologies to facilitate business processes, IoT leverages available data to enhance operations, which is a significant issue with their adoption in the hospitality industry. An array of challenges associated with using IoT in hospitality impedes rapid adoption of their application and reliability. Indeed, IoT brings big data to the network infrastructure regarding administration, operations, and performance, with security concerns standing out [20].

4.1. Security Concerns

These security concerns include weak passwords, insecure interfaces, poor IoT device management, IoT skills gap, insufficient data protection, and lack of regular patches and updates [21]. Unlike information technology companies which invest intensively in technological infrastructure, hotels are end users of IoT and are less likely to have a better technical infrastructure. For example, the Hotel group *Marriott International* has recently confirmed another data breach, with hackers claiming to have stolen twenty gigabytes of sensitive data, including guests' credit card information [22]. As described, IoT generates big data that limits conventional computing frameworks from their intended purpose of providing speed and storage capacities depending on the growth rate of the data generated [20]. Such a challenge adversely affects IoT's functionality and objectivity as hospitality businesses are less likely to invest in technological infrastructure to capture this challenge. The inability to invest extensively in this infrastructure creates a challenge leading to lags, delays, and crashes that affect the overall purpose of IoT in enhancing efficiency. Ultimately overloading the technological infrastructure with big data streams.

5. SECURITY DATA BREACH

IoT has also been linked to security data issues. Technology has been identified as a pathway to addressing security concerns regarding information management. For instance, research has identified authentication, access control, encryption, and password security as tools used to enhance information security [23]. However, they are still susceptible to security breaches. For instance, between 2016 and 2017, an Austrian hotel was hacked four times, with hotel keys becoming unusable after clicking a link sent to the owner [24]. According to research, IoT is one of the enabling technologies for smart grid networks [25]. However, they connect different devices through online platforms, making these smart grids vulnerable to significant attacks. Due to its interconnection nature, if one device is compromised, the whole grid immediately becomes susceptible to an attack as they all work as a single unit. In fact, due to security reasons, [26]. IoT adoption has been hindered as many businesses, and their customers have become cautious about the potential for attacks and the associated consequences [26]. Multiple forms of attack present a challenge to adopting IoT in hospitality [26]. identifies ransomware, denial of services, exploitation of integrated systems, interoperability and heterogeneity, and physical attacks as possible ways to compromise the security of information in IoT [26].

As IoT data advances, *Trend Micro* notes that threats' attack surface is expanded. Information security has therefore been a significant issue when using IoT [27]. Other than the issue of security, privacy concerns have been a significant challenge in the use of IoT in the hospitality industry. For IoT to facilitate real-data collection, analysis, and distribution, they must always be present. Therefore, [26]. emphasise that IoT devices and ultra-connectivity are omnipresent, providing qualitative and quantitative private information about an in- dividual ([26]).

People are mostly unaware of the information being collected by IoT as these devices collect data in a passive and non-intrusive way through seamless interactions with individuals. Devices such as drones, wearables, robots, IoT buttons, smartphones, smartwatches, and remote cameras are commonly integrated and used in hospitality and other industries [3]. These devices facilitate accurate and real-time tracking, profiling, identification, and traffic information, violating people's privacy. As described in research [28], users must be assured of their safety and privacy,a complex issue to guarantee when using IoT. Therefore, the implementation and use of IoT are widely impeded by privacy concerns as people tend to treasure their privacy and protect their personal information, which a third party might misuse.

5.1. Planning IoT for hotels

Considering this desire to defend oneself, hotels can- not install and effectively use IoT across all their customers due to their distinct needs and concerns. While IoT offers an easier way of effectively collecting, analysing and using diverse information in the hospitality industry to promote service delivery, its use is not as easy as serving a client some food. There are safety, security, privacy, and infrastructural concerns that a business in this industry must account for and address before using these devices. Among the goals of IoT are increasing customers' experiences to gain their loyalty and promoting efficiency and sustainability [4]. However, the inability to guarantee safety and privacy, the associated collection of big data, and the technological infrastructure overload significantly affect these devices' adoption, implementation, and use. Hotels must analyse the risks of implementing IoT and the costs involved before enactment to limit ethical and legal consequences.

One of the essential considerations when using technology is its capacity to protect data. While

IoT can offer enhanced operations, reduce time wastage, and promote communication between entities. Safety and security concerns must be considered when using these devices. Data can be misused or maliciously accessed by unauthorised users via multiple devices, the network connecting them, and the end user level. Therefore, securing the entire IoT infrastructure is a priority in protecting users and maintaining the quality and integrity of the system and data within it. Cybersecurity ensures that ‘an organisation’s assets and technologies are protected and that the cyber environment is safe for sharing and communicating important information that supports operations’ [29]. Therefore, committing resources and measures to enhance cyber security is vital for IoT implementation, adoption, and use. Like any other technological innovation, malicious actions constantly threaten data safety in the system. Due to the associated risks of use, including breaches and attacks on the system, cyber security has gained relevance.

Cyber security ‘is the collection of policies, tools, security safeguards, guidelines, actions, security concepts, best practices, and risk management approaches that help protect cyber environments, including user and organisational assets; cyber security is the actual process and methods or protecting data in technological devices’ [29]. Therefore, it involves applying techniques and technologies to advance networks, systems, data, devices, and attack protection. Protecting data and access to these devices is, therefore, essential. One strategy to enhance IoT security is having wireless sensor network measures such as secret key algorithm, security routing protocol, key management, physical security design, and authentication and access control [30]. The strategy ensures limited access to devices and that only a few authorised individuals can access the devices and data through passwords and other measures. Device encryption is essential in promoting IoT safety, as an attack on a single device may affect all other devices in the system.

5.2. RFID Connectivity

Besides having wireless sensor network measures, RFID-based authentication measures are essential in securing data and the entire system. RFID is a commonly used IoT technology that facilitates identification information transmission through a microchip via a wireless network [31]. RFID devices, therefore, allow users to identify, track and monitor RFID tags. While RFID and related technologies make IoT riskier, especially on authentication, specific measures are relevant in protecting data. These measures include a cryptography technology scheme, an IPSec-based security channel, data encryption, and access control [31].

Also, physical cybersecurity schemes fall under these measures. RFID-based authentication measures aim to prevent the misuse of RFID devices and the stealing of data by attackers. Moreover, to prevent eavesdropping and tampering with data during transfer, perform encryption and authentication over IoT, and mask and hide the IoT system from attackers. It eliminates data dependencies and randomises encryption values in IoT devices [31]. Cybersecurity is critical when using these devices because the IoT is primarily focused on remote data collection, analysis, and sharing. Given the nature of the data collected by these devices, failure to assure proper security will have ethical, legal, and operational consequences for an organisation. Taking these measures ensures that the system or the instruments used in IoT are adequately safeguarded and that the data processing and sharing processes are free of any vulnerability that may make it easier for malicious access to affect the data quality.

6. TYPES OF IOT SENSORS

IoT facilitates data collection, analysis, processing, and management from different aspects of a business. Some operate remotely, while others collect data passively as a device is used. Therefore, sensors are essential for the interaction of IoT with the environment. These sensors collect and process data to detect changes in physical objects. The IoT operates because different devices are interconnected through the cloud or the internet to facilitate information flow [32]. Further, they are not limited to one sector, making the available sensor diverse in their use and application. While available sensors can be placed at any position to facilitate data collection, which can be retrieved remotely or physically, sensors used in IoT are different as they facilitate real-time data collection and sharing. Common types of sensors used in IoT include proximity sensors, temperature, pressure, light, smoke, alcohol, gas, humidity, accelerometer, position, touch, sound, and weight [33], [34],[35].

These sensors play a central role in remote data collection and sharing, facilitating the operational ability of the IoT system. Each sensor is used for a specific purpose, focusing on collecting data of a defined parameter within the environment or selected setting.

6.1. Temperature Sensors

Hotel temperature sensors actively monitor temperatures, facilitating appropriate food storage and avoiding wastage [10]. With the *European Council and Parliament* assigning hotel guidelines on temperature control to food products in fridges and freezers, the IoT temperature sensor has become helpful in ensuring compliance and preventing food wastage.

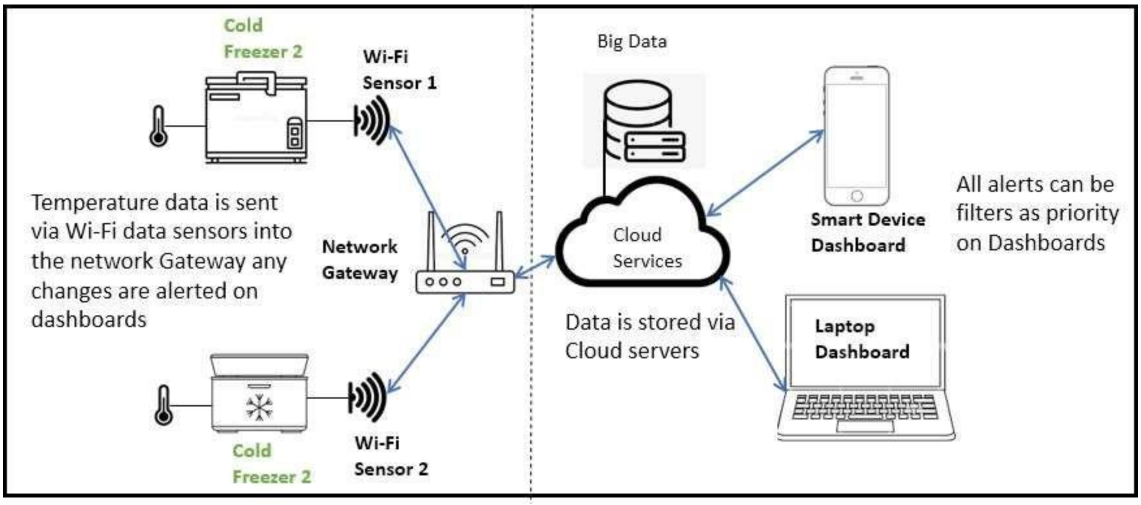
Cold
Freezer 2
Wi-Fi
Sensor 1
Temperature data is sent via Wi-Fi data sensors into the network Gateway any changes are alerted on dashboards
Network
Gateway
Cold
Freezer 2
Wi-Fi
Sensor 2
Big Data
Cloud
Services
Data is stored via Cloud servers
Smart Device
Dashboard
All alerts can be filters as priority on Dashboards
Laptop
Dashboard

Figure 4: IoT Temperature Sensor

Figure 4 above outlines the layout of an IoT temperature sensor and its integration with other devices connecting the fridge to a user's control device. The sensor limits energy wastage while appropriately storing the foods under the required temperature. Measuring temperature in real-time, the first sensor communicates to sensor two in the refrigerator via the gateway, which transmits Wastage information to the cloud through the internet for storage. From the cloud, the users of the devices can view data with emergency alerts being made via text messages. Such integration improves food storage management and increases the user's capacity to regulate power usage and monitor food storage to reduce wastage. Another area of importance is controlling the quality of water used in hotels. Water contamination is common, and it is vital to ensure that the water used in hostels in food preparation and served to the customers is free of contamination. Research [36]described continuous monitoring of biological and non-biological contaminants are essential but remain a challenge.

6.2. Waterflow Sensors

Real-time water flow, conductivity, temperature, turbidity, pH, and ORP, as shown in figure 5, are essential in detecting chemical and biological contaminants and reducing the risk of using contaminated water [36].

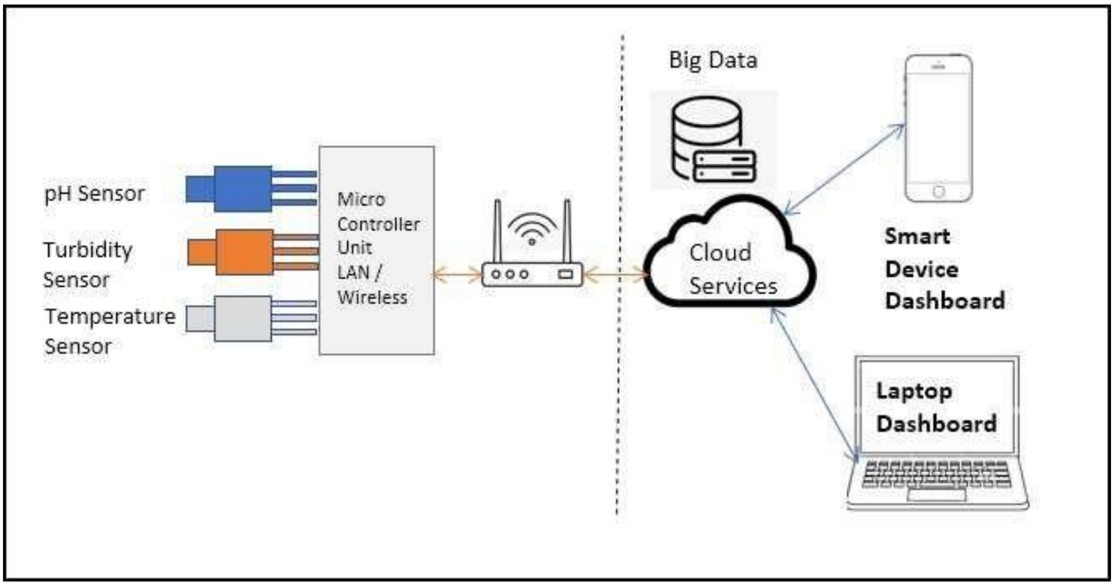

Figure 5: Water Contamination IoT sensor system

These systems ensure that a hotel is actively involved in the monitoring and controlling the quality of water being supplied and used in its operations. These sensors are essential in an organisation's operations as they provide required data on specific operations areas that enhance efficiency and effectiveness. While different industries may use the same devices to collect detailed data, their use is specified for an organisation's operations. Wearable sensors such as pressure and electromyography sensors are actively used in healthcare settings to detect and prevent falls [35], while wearable robot controllers control some practices and processes in hotels remotely [37]. Hotels and other business organisations have a responsibility to their clients, and in meeting these responsibilities, they need to provide top-notch services. IoT sensors limit human interactions and improve service delivery by enabling these organisations to detect and monitor critical parameters in their operations. By reducing human interactions, these devices enhance overall client experiences and the overall performance of an organisation in terms of cost-reduction, improved efficiencies, limited errors, and quality services.

7. IoT Compliance

While IoT security is one of the significant standards and considerations for use, other factors must be considered when using IoT, and compliance is essential. As research [38] highlights next to IoT security and protection issues, liability, ethics, responsibility, autonomy, insurance, and accountability are among other problems that must be accounted for when using these applications. Compliance aims at incorporating measures imposed by law to fulfil regulations and support interoperability across IoT devices. A standardised approach to IoT use is essential in reducing ethical, security, functional, and operational issues. In under- standing the concept of IoT compliance, identifying compliance standards is vital. As described by [39], compliance standards can be classified as those in the healthcare, application domain, aerospace, automotive, production, telecommunication, and energy. While categorised by industry, these standards can also be classified as safety, security, and process management. These standards de- fine how organisations use IoT and focus on ensuring their user's safety. Research indicates that violating these standards can result in fines, lawsuits, and loss of licenses [39]. Therefore, they standardise the use of IoT in different industries and the general safety and security standards that limit the abuse of these applications.

7.1. GDPR Privacy Concerns

A significant consideration for compliance and security standards is the General Data Protection Regulation (GDPR). According to research [40]GDPR is a valid and mandatory regulation for states in the European Union to protect individuals' data and enhance compliance with data privacy by organisations. GDPR is a compliance regulation that enhances data safety, privacy, and security when distributing data via IoT applications. While it is important, research indicates that compliance requires handling complex issues like collecting, processing, storage, security, deletion, and transmission of personal data, proof of consent, and enforcing policies for data retention [41]. Hotels are especially vulnerable because they deal with a large amount of personal information from guests and customers [42]. Therefore, all these procedures discussed must be extensively documented to comply with GDPR.

8. Data Storage

IoT creates data that is shared with the main application for consumption. Data can be stored remotely or physically depending on the network, the organisation's capacity, and power consumption [43]. While data is temporarily stored in the devices and sensors, it is transferred to appropriate processing applications, which transfer it to us- ability applications or storage applications and hardware. Physical storage is possible within a hotel but requires extensive infrastructural investment.

The cloud has become a vital storage system for IoT for ease and effectiveness. According to research [44], while on-premise storage is used, cloud storage is a noticeable choice as it providesa direct connection between IoT devices and the cloud allowing faster data storage and retrieval. Therefore, nowadays, cloud storage is the most preferred for most organisations as it enhances IoT efficiency.

9. Conclusion

The current research has focused on IoT, its use in hotels and the associated challenges. While it explores pertinent issues related to IoT, future research aims to focus on the effects or significance of IoT on hotels as this may help measure the value of IoT investment based on performance outcomes. Furthermore, exploring the ethical, privacy, confidentiality and safety issues related to IoT use is an area of interest as IoT, like other technologies, has safety, ethical, legal, and privacy implications. With IoT using the cloud as the main storage platform, future research on developinga secure cloud storage system is also important to further understand the nature of IoT and the storage capabilities provided by the cloud.

The evolution of technology has changed how businesses and hotels operate, with IoT providinga new pathway to hotel processes and activities. The concept of intelligent hotels has received increased attention and adoption. Saying that adopting these technologies has been marked by extensive challenges, including the safety and security of data. Using smart technologies linked together through automated or manned approaches helps hotels and other organisations in the hospitality industry enhance their performance. This, as presented in this paper, is possible through continuous process monitoring, automation of specific activities, re-modifying hotels to client specifications, and installing sensors and devices that help detect inappropriate changes and take affirmative action. While this is possible, users, in this case, hotels, must also adhere to specific standards and protocols that define how these devices can and should be used, limiting ethical, privacy, and legal issues that may arise with these applications. As the authors of this paper conclude, IoT has huge potential for the efficiency and effectiveness of the hotel sector, but it is not all ‘smooth sailing’ yet.

REFERENCES

[1] F. K. Shaikh, S. Zeadally, and E. Exposito, ‘Enabling technologies for green internet of things’, *IEEE Syst J*, vol. 11, no. 2, pp. 983–994, Jun. 2017, doi: 10.1109/JSYST.2015.2415194.

[2] ‘The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution’, 2016.

[3] M. Nasajpour, S. Pouriyeh, R. M. Parizi, M. Dorodchi, M. Valero, and H. R. Arabnia, ‘Internet of Things for Current COVID-19 and Future Pandemics: an Exploratory Study’, *J Healthc Inform Res*, vol. 4, no. 4, pp. 325–364, Dec. 2020, doi: 10.1007/s41666-020-00080-6.

[4] P. Eskerod, S. Hollensen, M. F. Morales-Contreras, and J. Arteaga-Ortiz, ‘Drivers for pursuing sustainability through IoT technology within high-end hotels-An exploratory study’, *Sustainability (Switzerland)*, vol. 11, no. 19, Oct. 2019, doi: 10.3390/su11195372.

[5] A. Verma, V. K. Shukla, and R. Sharma, ‘Convergence of IOT in tourism industry: A pragmatic analysis’, in *Journal of Physics: Conference Series*, Jan. 2021, vol. 1714, no. 1. doi: 10.1088/1742-6596/1714/1/012037.

[6] S. Gupta, A. Leszkiewicz, V. Kumar, T. Bijmolt, and D. Potapov, ‘Digital Analytics: Modeling for Insights and New Methods’, *Journal of Interactive Marketing*, vol. 51, pp. 26–43, Aug. 2020, doi: 10.1016/j.intmar.2020.04.003.

[7] T. International Renewable Energy Agency, *Internet of Things – Innovation landscape brief*. 2019. [Online]. Available: www.irena.org

[8] ‘Mistry’.

[9] 2022 September 28, ‘How Can IoT in Hospitality Industry Grow Your Hotel Business?’, Sep. 2022.

[10] S. Mercier, S. Villeneuve, M. Mondor, and I. Uysal, ‘Time–Temperature Management Along the Food Cold Chain: A Review of Recent Developments’, *Compr Rev Food Sci Food Saf*, vol. 16, no.4, pp. 647–667, Jul. 2017, doi: 10.1111/1541-4337.12269.

[11] Sri Venkateshwara College of Engineering. Department of Electronics and Communication Engineering, Institute of Electrical and Electronics Engineers. Bangalore Section, IEEE Computer Society, and Institute of Electrical and Electronics Engineers, *RTEICT-2017 : 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology : proceedings : 19-20 May 2017*.

[12] P. Kansakar, A. Munir, and N. Shabani, ‘Technology in the Hospitality Industry: Prospects and Challenges’, *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 60–65, May 2019, doi: 10.1109/MCE.2019.2892245.

[13] D. Katz, ‘Daylight_Harvesting_Technologies’, *Daylight Harvesting Technologies*, vol. 102, no. 1,pp. 40–48, 2005.

[14] Debbie Carson, ‘Marriott International Commits to Continued Innovation in Hotel Guest-facing Technologies’, *https://hoteltechnologynews.com/2019/07/marriott-international-commits-to-continued-innovation-in-hotel-guest-facing-technologies/*, 2019, Accessed: Mar. 10, 2023. [Online]. Available: https://hoteltechnologynews.com/2019/07/marriott-international-commits-to- continued-innovation-in-hotel-guest-facing-technologies/

[15] Michal Christine Escobar, ‘Hilton Introduces Tech Enhancements to Improve Guest Experience’, *Hilton Introduces Tech Enhancements to Improve Guest Experience*, 2021, Accessed: Mar. 10, 2023. [Online]. Available: https://hospitalitytech.com/hilton-introduces-tech-enhancements- improve-guest-experience

[16] S. G. Tzafestas, ‘The Internet of Things: A Conceptual Guided Tour’, 2018.

[17] S. Elhadi, ‘Comparative study of IoT protocols’. [Online]. Available: https://ssrn.com/abstract=3186315

[18] A. Tewari and B. B. Gupta, ‘Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework’, *Future Generation Computer Systems*, vol. 108, pp. 909–920, Jul. 2020, doi:10.1016/j.future.2018.04.027.

[19] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, ‘A survey of IoT security based on a layered architecture of sensing and data analysis’, *Sensors (Switzerland)*, vol. 20, no. 13. MDPI AG, pp. 1–20, Jul. 01, 2020. doi: 10.3390/s20133625.

[20] S. Nadkarni, F. Kriechbaumer, M. Rothenberger, and N. Christodoulidou, ‘The path to the Hotel of Things: Internet of Things and Big Data converging in hospitality’, *Journal of Hospitality and Tourism Technology*, vol. 11, no. 1, pp. 93–107, May 2020, doi: 10.1108/JHTT-12-2018-0120.

[21] Thales, ‘Thales Iot security issues in 2022’, *https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats*, 2022, Accessed: Mar. 10, 2023. [Online]. Available: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats

[22] J Tidy, ‘Marriott Hotels fined £18.4m for data breach that hit millions’, Accessed: Mar. 10, 2023. [Online]. Available: https://www.bbc.co.uk/news/technology-54748843

[23] D. T. Bourgeois, ‘Information Systems for Business and Beyond’, *Published by The SaylorAcademy*, 2014, Accessed: Mar. 10, 2023. [Online]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2014/02/Information-Systems-for-Business-and-Beyond.pdf

[24] Padraig Belton, ‘The Austrian hotel that was hacked four times’, *Lock out: The Austrian hotel thatwas hacked four times*, Dec. 2017, Accessed: Mar. 10, 2023. [Online]. Available: https://www.bbc.co.uk/news/business-42352326

[25] K. Kimani, V. Oduol, and K. Langat, ‘Cyber security challenges for IoT-based smart grid networks’, *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, Jun. 2019, doi: 10.1016/j.ijcip.2019.01.001.

[26] S. Mercan, K. Akkaya, L. Cain, J. H. Thomas, and J. Thomas, ‘Security, Privacy and Ethical Concerns of IoT Implementations in Hospitality Domain Privacy-Perserving In AMI Network View project Machine Learning In Cybersecurity: Challenges and Opportunities View project Security, Privacy and Ethical Concerns of IoT Implementations in Hospitality Domain’, 2020. [Online]. Available: https://www.researchgate.net/publication/344347630

[27] Vit Sembera and Jakub Urbanec, ‘IoT Security Issues, Threats, and Defenses’, Accessed: Mar. 10, 2023. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/internet-of- things/iot-security-101-threats-issues-and-defenses

[28] A. Infante-Moro, J. C. Infante-Moro, J. Gallardo-Pérez, and F. J. Martínez-López, ‘Key Factors inthe Implementation of E-Proctoring in the Spanish University System’, *Sustainability (Switzerland)*, vol. 14, no. 13, Jul. 2022, doi: 10.3390/su14138112.

[29] R. Von Solms and J. Van Niekerk, ‘From information security to cyber security’, *Comput Secur*,vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[30] Y. Lu and L. Da Xu, ‘Internet of things (IoT) cybersecurity research: A review of current research topics’, *IEEE Internet Things J*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019, doi: 10.1109/JIOT.2018.2869847.

[31] L. Wang, T. Liu, J. Siden, and G. Wang, ‘Design of Chipless RFID Tag by Using Miniaturized Open-Loop Resonators’, *IEEE Trans Antennas Propag*, vol. 66, no. 2, pp. 618–626, Feb. 2018, doi: 10.1109/TAP.2017.2782262.

[32] R. Von Solms and J. Van Niekerk, ‘From information security to cyber security’, *Comput Secur*,vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.

[33] SCAD College of Engineering and Technology and Institute of Electrical and Electronics Engineers, *Proceedings of the International Conference on Trends in Electronics and Informatics (ICOEI 2019) : 23-25, April 2019*.

[34] H. Hayat, H. Hayat, B. Francis, D. M. Gudi, J. O. Bishop, and P. Wang, ‘A concise review: The role of stem cells in cancer progression and therapy’, *OncoTargets and Therapy*, vol. 14. Dove Medical Press Ltd, pp. 2761–2772, 2021. doi: 10.2147/OTT.S260391.

[35] R. Rucco *et al.*, ‘Erratum: Correction: Rucco, R.; et al. Type and Location of Wearable Sensors for Monitoring Falls during Static and Dynamic Tasks in Healthy Elderly: A Review. Sensors 2018, 18, 1613 (Sensors (Basel, Switzerland) (2018) 18 5 PII: E2462)’, *Sensors (Basel, Switzerland)*, vol.18, no. 8. NLM (Medline), Jul. 30, 2018. doi: 10.3390/s18082462.

[36] S. N. Zulkifli, H. A. Rahim, and W. J. Lau, ‘Detection of contaminants in water supply: A review on state-of-the-art monitoring technologies and their applications’, *Sensors and Actuators, B: Chemical*, vol. 255. Elsevier B.V., pp. 2657–2689, Feb. 01, 2018. doi: 10.1016/j.snb.2017.09.078.

[37] IEEE Staff, *2017 14th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI)*. IEEE, 2017.

[38] K. Stuurman and I. Kamara, ‘IoT standardization-The approach in the field of data protection as a model for ensuring compliance of IoT applications?’, in *Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016*, Oct. 2016, pp. 336–341. doi: 10.1109/W-FiCloud.2016.74.

[39] A. Bicaku, M. Tauber, and J. Delsing, ‘Security standard compliance and continuous verification for Industrial Internet of Things’, *Int J Distrib Sens Netw*, vol. 16, no. 6, Jun. 2020, doi: 10.1177/1550147720922731.

[40] C. K. Metallidou, K. E. Psannis, and E. A. Egyptiadou, ‘Energy Efficiency in Smart Buildings: IoT Approaches’, *IEEE Access*, vol. 8, pp. 63679–63699, 2020, doi: 10.1109/ACCESS.2020.2984461.

[41] C. K. Kaneen and E. G. M. Petrakis, ‘Towards evaluating GDPR compliance in IoT applications’, in *Procedia Computer Science*, 2020, vol. 176, pp. 2989–2998. doi: 10.1016/j.procs.2020.09.204.

[42] SiteMinder, ‘What independent hoteliers need to know about data security’, *https://www.siteminder.com/r/hotel-data-breaches/*, Accessed: Mar. 10, 2023. [Online]. Available: https://www.siteminder.com/r/hotel-data-breaches/

[43] M. Amer and A. Alqhtani, ‘IoT applications in Smart Hotels’. [Online]. Available: http://www.iaras.org/iaras/journals/ijitws

[44] J. D. Bokefode, A. S. Bhise, P. A. Satarkar, and D. G. Modani, ‘Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based Encryption’, in *Procedia Computer Science*, 2016, vol. 89, pp. 43–50. doi: 10.1016/j.procs.2016.06.007.

AUTHORS

Nick Kalsi, a part-time PhD Research student at Cardiff Metropolitan University, studying the Internet of Things (IoT) within the Department of Cardiff School of Technologies.I am passionate about exploring the potential of IoT technologies to improve and optimise various aspects of modern hotels. One area where IoT can improve hotel operations is through smart building management systems using IoT sensors and devices. To monitor energy consumption, reduce energy waste, and save costs. Additionally, IoT can enhance the guest experience through personalised services such as voice activated room controls, smart lighting, and in-room entertainment systems.I have also worked as a Network Consultant for the last 22 years for Edwardian Hotels based in Central London, specialising in Network infrastructure and IoT technologies. Able to manage large projects hotel projects, and Research new technology in hospitality

Skills & Management:
Deployment of Cisco Meraki Wi-Fi solutions for 13 hotels, a single dashboard platform.R&D with Google Chromecast creating a home-to-home experience for hotel guests.Collaboration with Samsung Korea R&D to deploy over 2000 CCTV IP cameras using smart analytics.The rollout of digital wayfinding signage systems for hotel guests.The rollout of 350 innovative guest room management systems (GRMS) lighting, AirConditioning, Door locking, guest requests, and room service.Understanding guest behaviour during the COVID pandemic in quarantine hotels using CCTV AI, Wi-Fi usage, Location-based services,Design and build data centres for medium-large hotels.

Dr Fiona Carroll is a reader with the Cardiff School of Technologies (CST), Cardiff Met University, Wales. Her research over the past seventeen years has focused on the fast-changing relations between humans and digital technologies. It is inter-disciplinary and shows a substantial contribution to scholarship in the fields of Human Computer Interaction. As an accomplished academic, she has successfully won more than twenty research grant applications and has more than fifty peer-reviewed publications. At CST, she currently co-leads the Creative ComputingResearch Centre (CCRC).

Dr Kasha Minor is a senior lecturer in Hospitality at Cardiff School of Management, Cardiff Metropolitan University. Her research relates to hospitality and tourism management with a focus on digital technologies. Kasha's PhD investigated the impacts of daily deal websites, such as Groupon, on the hotel industry in Wales. She continues this work through a collaborative project with researchers at the University of Ljubljana, Slovenia and Krems University, Austria with the aim of mapping daily deal websites usage in the Mediterranean region using data-led methodologies. She currently leads a project which focuses on mobile travel apps and their accessibility to visually impaired travellers. She is a vice president of the International Federation for Information Technologies in Travel and Tourism, the leading independent global community for the discussion, exchange and development of knowledge about the use and impact of new information and communication technologies in the travel and tourism industry and experience (eTourism).

Professor Jon Platts is the Dean of Cardiff School of Technologies at Cardiff Metropolitan University and Professor of Autonomous Systems. Jon took up this role following careers in the UK Royal Air Force and industry research and development. He has had commercial success with his own company Muretex, winning significant, nationally competed, research grant funding; including Innovate UK funding for Robotics and Autonomous Systems. He has international contacts and reach, having proposed and chaired 2 European research action groups over 8 years and been invited to deliver a NATO lecture series on autonomy. Jon was the Head of Autonomy for QinetiQ for 13 years, shaping the direction of research programmes and co-ordinating multi-organisation teams (from QinetiQ, Dstl, BAE Systems, Thales UK, the Military and Academia) and multi-disciplinary teams. In his current role Jon leads the ambitious multi-million pound Cardiff School of Technologies development, to further establish Cardiff Metropolitan University as a world leader within the tech industry. Teaching and research will focus on areas such as data science, cyber security, mobile computing, artificial intelligence and autonomous systems engineering. Jon holds a BEng in Electrical and Electronic Engineering from the University of Bradford, an MSc in Aerosystems Engineering and a PhD in Self organising fuzzy logic, both from Loughborough University. He is a Chartered Engineer and Fellow of both the Institution of Engineering and Technology the Institution of Measurement and Control.