Privacy Concerns in Smart Indoor Environments in the Internet of Everything Era: A Smart University Campus Case Study

Andria Procopiou[1(✉)] and Eliana Stavrou[2]

[1] Department of Computing, School of Sciences, University of Central Lancashire Cyprus, Larnaca, Cyprus
aprocopiou@uclan.ac.uk

[2] Faculty of Pure and Applied Sciences, Open University of Cyprus, Nicosia, Cyprus
eliana.stavrou@ouc.ac.cy

Abstract. In the Internet of Everything era, indoor environment provides multiple benefits across different domains to their occupants such as improving their well-being and health, ensuring their safety, providing valuable assistance to their tasks and enhancing their experience using various types of intelligent sensors and devices. So far, we witnessed smart environments thriving in education, as they improve the overall experience, efficiency and education. One prominent example of is the smart university campus, empowered by IoE systems. Initially, such data is not considered sensitive, private and confidential to the occupants. However, through statistical analysis and machine learning, and in combination with heuristics and public information acquired, it can pose a significant risk to their privacy as it can directly leak personal information regarding their preferences, needs and interests. Unfortunately, the ICT systems of universities were targeted by numerous cyber attacks in the past. Therefore, it is only a matter of time before smart university campuses form the attack surface to novel privacy-leakage attacks. Hence, there is clear need for detailed and in-depth investigation. In this paper, we conduct a study on how the smart university campuses could leak sensitive information. We discuss how such information could threaten the occupants and their privacy, both in cyber and physical space, and the challenges related to their protection. Finally, we provide possible recommendations.

Keywords: Internet of Everything · Internet of Things · Smart Buildings · Smart Indoor Environments · Privacy · Security · Safety

1 Introduction

Technology forms a vital part of the society and the world, as of today. Various technologies such as smartphones, watches, thermostats, smart TVs, smart cars,

T. Pereira et al. (Eds.): IOECON 2023, LNICST 551, pp. 92–109, 2024.
https://doi.org/10.1007/978-3-031-51572-9_8

smart lighting systems and so on are becoming the norm, ultimately transforming our cities into smart intelligent entities of their own. This enhancement is mainly enabled by the Internet of Everything (IoE). IoE is denoted as a more holistic and complete set of technologies and concepts where computational devices, data, processes, AI and analytics come together with humans through the Internet for better decision-making, ultimately improving our lives [60].

IoT, a subset of IoE, denotes of all physical objects which have sensors and actuators embedded on them, have processing power, can be connected to the Internet and can communicate and directly exchange data with other similar entities without the need for a central authority through wireless communications [1,2]. IoT can be integrated into different types of indoor environments and transform them into smart entities of their own. Examples include residential homes, industrial and commercial buildings, stadiums, theatres, music venues, airports and universities, and schools.

IoT can also offer different types of services to the smart indoor environments and their occupants, such as providing assisted living, promoting sustainability and protecting the environment [5–7]. IoT sensors can monitor the indoor air and environment quality of the building, a vital part for the battle against Covid19. Furthermore, they can monitor the physical space and its occupants' behaviour and overall safety inside the building. They could also provide vital assistance and information to occupants with compromised health, special needs and/or disabilities. In certain smart buildings, the presence of smart appliances and devices in kitchens and dining areas can assist the occupants with their daily dietary and nutrition behaviour. Finally, the development of smart parking area spaces could help the occupants park their vehicles quickly and with minimum carbon emission and sound noise. Some examples of data collected through these services include room temperature, air quality, humidity, door locked/opened, visual presence, lights on/off, internal/external sounds, human motion and so on [6]. More information on the services smart indoor environments provide is presented in Sect. 2. Such data cannot be considered private, sensitive and confidential and directly related to the occupants.

Unfortunately, due to the IoT's weak security countermeasures, this data is relatively easy to be illegally obtained. The set of data compromised could indirectly reveal information and trends about the occupants' overall behaviour, interests, activities and preferences [3,4]. Using this data, the adversary can use machine learning and statistical analysis models to deduct private information of occupants as studies conducted [29,30] demonstrated.

More importantly, the illegally acquired data combined with heuristics, common knowledge, public timetables and building public information with regards to the smart indoor environment (e.g. wiring plans, floor plans) could possibly lead to the identification and possible profiling of individuals [6,9]. This could result in becoming a target in large-in-scale phishing campaigns or individual phishing campaigns. Furthermore, such an unfortunate scenario could threaten not only their privacy but also their physical safety.

Moreover, help of machine learning and statistical analysis models can deduct valuable information about the occupancy of spaces as studies conducted by

[29,30] showed. What is more concerning is that machine learning and statistical analysis in combination with heuristics, common sense, publicly available timetables social events and building-related public information can leak personal, private and sensitive information about the occupants.

In this paper, we conduct an in-depth investigation with regards to the privacy challenges in smart buildings, specifically smart university buildings, and the risk of its occupants private, sensitive and confidential information being revealed. Section 2 provides an introduction to the smart indoor environment definition and then focusing on the smart university campus and the different services it provides to its occupants. In Sect. 3, we present our case study with regards to smart university buildings and relevant privacy concerns that may arise from potential IoT-related data leakage. For every scenario considered, we present the impact that can have on individuals, their privacy and their safety. In Sect. 4, discuss on the impact caused on individual's privacy, consider possible challenges in ensuring privacy and briefly describe possible defence countermeasures, concluding that privacy is equally important as security. In the final section, we provide concluding remarks and what potential future work could be conducted.

2 Background Knowledge

2.1 Smart Indoor Environments

In general, any indoor environment is described as the indoor physical space that uses various technologies (e.g. IoT, analytics, artificial intelligence, the cloud, sensors/actuators and ubiquitous computing) to promote sustainability and protect the environment, provide assisted living to its occupants and enhance their experiences, ensure their safety and provide multiple services to them, monitor the indoor physical space and maintain its healthy state and ensure the availability of its services [5–7]. There are different categories of smart indoor environments depending on the services and type of occupants. Popular and notable types include but not limited to commercial and entertainment (e.g. shopping malls, stadiums, theatres, cinemas, music venues), corporate (e.g. companies and organisations), transportation (e.g. smart airports), health services (e.g. smart hospitals) and residential (e.g. smart homes). For the purpose of the study, we only consider a smart university campus.

2.2 Smart Services in Smart University Campuses

Indoor Air and Environment Monitoring: One of the most important benefits IoT technologies provided was the continuous monitoring of the indoor air quality. It has been the subject of numerous studies during the Covid19 era. Covid19 is transmitted through airborne particles and droplets. Infected individuals spread Covid19 by releasing particles and droplets contained in respiratory fluids into the air. Examples include breathing, speaking, singing, exercise,

coughing and sneezing. The risk of being infected with Covid19 is significantly increased when people are in close proximity and indoors [19]. Furthermore, air quality monitoring was also a subject of interest beforehand due to people spending more time indoors than outdoors during the winter months [20,21].

Air pollutant levels can be built up much faster due to less frequent exchange of air [22]. Sensors should be placed in strategic locations, monitoring various air quality metrics such as dust fine particulate matter (PM), Ozone (O3), Carbon Monoxide and Dioxide, Nitrogen Dioxide [7]. Furthermore, other environmental metrics should be monitored such as temperature, humidity and sound to ensure the well-being of individuals [6]. The efficient monitoring of the indoor environment extends beyond the assessment of air quality. It is important for the smart university campus to provide thermal comfort as well as appropriate lighting and acoustic control to individuals for assisted living purposes [3,21].

Physical Space/Individuals Monitoring: Most universities are open and accessible to the public. Hence, it should be ensured that appropriate security and safety measures are deployed. In detail, proper access control sensors (e.g. intelligent door locks, token-based authentication systems, CCTV) are placed so students and staff members are properly authenticated and authorised and any irregular behaviour is quickly and accurately detected [7,23]. Furthermore, through similar sensors and technologies, real-time monitoring and tracking of individuals in smart university campuses is possible. Tracking services can assist towards the physical safety and security of individuals by immediately notifying security staff on the event of criminal acts. In addition, tracking services can assist in ensuring any Covid19 social distance measures are correctly followed [7,23]. Another important aspect is to regularly monitor the physical grounds of the university to detect any environmental abnormalities and prevent any natural disasters such as fires and floods. Sensors that are responsible for this functionality are fire, gas and flood sensors [24].

Health and Well-Being of Individuals Monitoring and Assistance: One important benefit of a smart university campus is that it can provide valuable assistance to students, staff and visitors with disabilities and other health problems [26]. It is essential that everyone feels safe, confident and included and not by any means restricted. Hence, the smart university campus should be accessible and usable to everyone regardless of any disabilities and/or health problems they might face and make their visit a pleasant one [18]. Firstly, the smart university campus should be able to consist of disabled access entrances, lifts, stairways, escalators and ramps in all the key orientation points to accommodate people with movement disabilities [10] as well as automatic door openings [13].

Secondly, the smart university campus should make relevant campus information and university services available in different video and/or audio formats. Furthermore, these information services should be able to make adjustments in their explanation provided to people with different abilities and needs. Specifically, dedicated sensors and technologies should be able to describe objects and

places and help them navigate through them [11]. Finally, appropriate communication channels should be available to people so they can communicate with staff members in case they require additional help and assistance.

Moreover, any mobile smart medical equipment individuals carry with them (e.g. asthma inhalers, blood pressure monitors, blood glucose and diabetes monitors and other types of health and wellness trackers) should communicate with dedicated services of the smart university campus [17]. Through them, properly trained personnel can interfere and provide immediate help in case of a medical emergency [12]. We also have to note that all individuals exhibiting health problems and/or disabilities can carry a tracker sensor so the dedicated personnel can keep track of their movements inside the smart university campus and be ready to provide them immediate help without wasting any valuable time.

Finally, through the assistive environments the smart campus university offers the opportunity to its occupants to adjust a room's settings according to their needs and preferences. Examples include automated adjustment of lights, temperature and sounds to ease symptoms of anxiety, depression and other mental heath issues [3,12,14–16].

Smart Appliances/devices Monitoring: In dedicated kitchen facilities, which are most likely to only be accessed by staff members, there will be various smart appliances and devices available. Examples include smart fridges, microwaves, ovens, hobs, coffee machines and kettles [42]. These appliances will be able to assist individuals in their food and drink preparation [42]. Furthermore, staff members could potentially set up the dedicated fridges to inform them on possible food run-outs and could automatically place an order upon a run-out [43] through dedicated smart cameras and other sensors.

Smart Parking Services: University campuses, especially large ones in urban areas, consist of large parking spaces since not everyone is likely to live close to the university premises or able to use public transport to accommodate incoming drivers, cyclists and motorcyclists. A smart parking is bound to benefit the university staff, students and visitors, the environment as well as the ecosystem. The services deployed will be able to inform drivers, cyclists and motorcyclists on the parking availability and where it is located in the parking lots through, smart weight and measure sensors. Specifically, the weight and measure sensor at the entrance would check the incoming vehicle and guide the driver to the nearest available parking space [7]. In addition, special zones for emergency vehicles, loading vehicles and parking spaces for people with disabilities will be available as well as electric vehicle recharging points [7].

3 Smart University Buildings Privacy Concerns Case Study

In this section, we present the different use case scenarios where the privacy of individuals can be leaked using occupant and/or environment-related data from

Table 1. Privacy Leakage Scenarios Summary

Smart Service	Non-Private Data Acquired	Direct Private Data Leaked	Indirect Private Data Leaked
Air Qual	Indoor Pollut	Human Pres., Occupants No.	Role, Breaks, Locat., Sens. Info
Air Qual	Air Qual. Metr.	Human Pres., Occupants No.	Role, Breaks, Locat., Sens. Info
Air Qual	Temp./Humid	Human Pres., Occupants No.	Role, Breaks, Locat., Sens. Info
Phys. Space	Door Locks	Human Pres., Occupants No.	Durat., Entry/Exit, Breaks, Sleep ,Sens. Info
Phys. Space	Authen. Mechan	Human Pres., Occupants No.	Durat., Entry/Exit, Breaks, Sleep, Sens. Info
Phys. Space	CCTV log	Human Pres., Occupants No.	Durat., Entry/Exit, Breaks, Sleep, Sens. Info
Health	Heart rate	Heart Diseas. (e.g. arrhythmia)	Routes, Sens. Info
Health	Oxygen level	Respir. Diseas. (e.g. asthma, copd)	Routes, Sens. Info
Health	Blood Pres	Blood Pres. (hypertension 1, 2)	Routes, Sens. Info
Health	Disab. Ramps, Lifts Interact	Disab. Status	SRoutes, Sens. Info
Health	Help. Points Interact	Disab. Status	Routes, Sens. Info
Health	Lights Interact	Mental Healh Stat	Sens. Info
Health	Sounds Interact	Mental Healh Stat	Sens. Info
Health	Thermal Interact	Mental Healh Stat	Sens. Info
Smart Appl	Smart Appl. Data	Human Pres.	Durat., Breaks, Purpose, Sleep Patt., Sens. Info
Smart Parking	Vehicle weight, Dur., Model	Individ. Role, Disab. Stat	n/a

compromised IoT devices and sensors as well as accessible types of information, summarising them in Table 1. For space constraints reasons, we define sensitive data as the set of personal data to the individuals. This data includes age, gender, sexual orientation, marital status, medical and biological data, disability status, political views, interests and activities, religion, ethnic race, cultural background and financial information.

As highlighted in the paper so far, and previously argued by related studies [6], different types of IoT devices and sensors that collect environment-related data can reveal private-related information regarding the occupants, their movements and overall behaviour inside the environment and overall preferences [25].

As a result, adversaries can illegally acquire such data and use them for malicious purposes. The risk explained above in combination with other accessible types of information can lead to the identification and profiling of individuals [6,9], conduction of phishing campaigns and even threatening the physical safety of them. We define accessible types of information as the following:

- Heuristics and Common Sense: In a smart university campus, different types of occupants are likely to be located at the university's premises at different times. Examples include deducting that it is more likely that students will be present at the university late at night (e.g. studying, submitting coursework) and non-faculty members come before 7 am and leave no later than 5pm [9].
- Publicly available timetables and social events: Every university has a dedicated website which contains information regarding the faculty members and their expertise, the modules/course taught and even their calendars. It also contains publicly available information regarding the non-staff members, their

job roles within the university and where their offices are located. Furthermore, the website is likely to include information regarding the societies of the university currently established (e.g. description, meeting dates, boarding members) as well as events that are open to the public (e.g. open days) [9].
– Building-related public information: The university consists of multiple buildings. These buildings consist of wiring and floor plans as well as dedicated building information models. The buildings' classrooms, labs, lecture theatres and any room is likely to consist of a number and possibly a name if it is large enough. Therefore, every room in the university's buildings is likely to have dedicated sensors and devices which even if they cannot be accessed physically, their location can be revealed using building-related public information [9].

Indoor Air and Environment Monitoring Privacy Leakage Scenarios: The compromise of air quality monitoring sensors could reveal the presence of occupants inside a room and possibly for how long they stayed. Specifically, this can be achieved by monitoring the different levels of air quality metrics and indoor pollutants (e.g. Ozone, Carbon Monoxide, Carbon Dioxide, Air Velocity, Air Pressure) as well as other metrics such as indoor lights, temperature and humidity. [26,27]. If there is someone present in the room, the lights are likely to be turned on and then turned off when they leave the room. The temperature could indicate the presence of occupants, and possibly the number of them. Humans live by breathing. Their respiration releases energy as heat and therefore, the room temperature will rise as occupants will release heat energy. Similarly, the carbon dioxide levels are elevated due to the occupants exhaling CO2 [59]. Using this information, the adversary can work out how long the occupants stayed in a room(s), the possible route taken, possible entry/exit points and break sessions.

The illegally data acquired presented in combination with different types of accessible of information can in further reveal personal and sensitive information about the occupants of the smart university campus.

Combining the presence and number of occupants with heuristics and common sense data could reveal their role inside the university (e.g. student/academic staff member/non-academic staff member). It is more likely for students to be inside the smart university campus during the evening/late night hours and for non-academic staff members to be in early in the morning. In addition, if there are occupants located in different buildings of the smart university campus, the adversary could potentially work out if they had any social interactions or met in a common room.

Combining the presence and number of occupants with publicly available timetables, social events information and building-related public information can reveal personal information about the occupants' identity, interests and activities. Specifically, using names and room numbers and publicly acquired timetables the adversary could possibly find out about staff and non-staff members currently being at their office desks, specific students and staff members

being in certain lectures theatres and/or labs at specific times. The academics' office room numbers are publicly available from the university website and the students' timetable could be relatively easily acquired from the university website. In addition, the smart university's societies and clubs tend to advertise their social events in the smart campus which is a public space and anyone can witness such information. Therefore, by combining human presence and this information, the adversary can make plausible assumptions about the individuals. For example, if the music society is hosting a concert, the adversary can deduct that the occupants are likely to be music students or have a strong interest in music.

Beyond the occupants' personal interests and activities, other more personal and sensitive information can be revealed. Examples include meetings of past alcoholics, victims of domestic violence, LGBT+ individuals, societies of various religions, faiths and ethnicity's, and cancer and other deadly diseases patients and survivors.

Physical Space/Individuals Monitoring Privacy Leakage Scenarios: The compromise of physical space and authentication mechanisms (intelligent door locks, token-based authentication systems) could initially reveal occupancy in rooms and number of occupants, provided that each occupants uses their personal token to enter a room. Every time an individual wants to enter a room using their personal token (e.g. campus card), the token-based authentication mechanism is activated upon and produces a signal. Therefore, the adversary will know if there is human presence in the room and possibly how many individuals are currently in the room.

Proceeding, the adversary can work out how long individuals stayed in a room, the entry/exit points they used and the possible route taken to enter a room. Furthermore, they could make plausible assumptions about the purpose of visit for example, if the card-authentication system of the library is activated, the individual (possibly a student) wants to enter the library.

In addition, other types of personal data can be revealed to the adversary such as sleep patterns. For example, if certain staff-members and/or students are more frequently present during the night it is possible their sleep patterns are shifted. Once again, similarly to the air quality data argument presented in the previous section, combining the presence and number of occupants with publicly available timetables, social events information and building-related public information can reveal personal information about the occupants' identity, interests and activities.

We also need to note that with the compromise of CCTV data, the identity of individuals can be revealed more accurately. This illegally acquired data in combination with the academic term timetables, the university's clubs and societies events timetables and other social events can give a more clear view of who exactly these individuals are. Bringing back the music society hosting a concert example, the adversary now has visual evidence of who these individuals are. Using image/video processing tools and software they can map specific individuals to their interests, activities and personal information. This can be proved

particularly dangerous when it comes to sensitive data such as meetings of past alcoholics, victims of domestic violence, LGBT+ individuals, societies of various religions, faiths and ethnicity's, and cancer and other deadly diseases patients and survivors.

Health and Well-Being of Individuals Monitoring and Assistance Privacy Leakage Scenarios: Through the compromise of medical devices the occupants own (e.g. asthma inhalers, blood pressure monitors, blood glucose and diabetes monitors, fitness trackers), the adversary could obtain information about their health such heart rate, oxygen level, blood pressure and activity levels (step counting). Using this information, the adversary could work out on which potential diseases the individuals suffer from [8,17].

For example, if the medical device owner produces between an oxygen level rate between 88% and 92% oxygen they are likely to suffer from a mild chronic obstructive pulmonary disease [51]. On the other hand, an oxygen level of 97% or above indicates of a case of mild asthma, 92–97% indicates moderate asthma, and less than 92% is a strong indication of a severe asthma [56]. Another example consists monitoring the heartbeats of individuals. A pulse higher than 100 beats/second indicates tachycardia [52]. Statistically, it is more likely for women to have tachycardia than men as well as heavy smokers, people who have high blood pressure, diabetes and people suffering from anxiety [52].

In addition, by monitoring the blood pressure, the adversary can work out if the patient is suffering from various blood pressure conditions such as elevated blood pressure, hypertension stage or hypertension stage 2. In elevated blood pressure, readings consistently range between 120–129 systolic and less than 80 mm Hg diastolic. In hypertension stage 1, readings consistently range from 130–139 systolic or 80–89 mm Hg diastolic. Finally, in hypertension stage 2, readings range at 140/90 mm Hg or higher [53]. Using these simple rules, the adversary could assume from what kind of hypertension disease the individual suffers from. Moreover, the adversary could use simple statistics to determine other sensitive information about the individuals such as age, gender, family medical history and ethnic race. In detail, the probability of having blood pressure problems increases with age. With regards to gender, men before the age of 55 have a higher probability of demonstrating blood pressure problems while women after menopause. Blood pressure problems also tend to run in families. Finally, it is statistically observed that African Americans are at increased risk for showing blood pressure issues [53].

Furthermore, the adversaries could learn more about an occupant's disability status by monitoring the interactions of an individual with the dedicated spaces. For example, if an individual has used the dedicated disabled ramps and/or lifts, then the adversary will know that the said individual exhibits mobility problems.

On the other hand, through the occupants' interaction with the dedicated IoT sensors and devices offering information in different formats (e.g. video, audio, alternative explanations), the adversary can obtain information about the occupants' abilities and needs such as occupants exhibiting visual, auditory

impairments or being neurodivergent (e.g. autism, adhd). Specifically, an individual with visual impairment will choose to interact with auditory information and an individual with auditory impairment will choose to interact with visual information. Individuals who are classified as neurodivergent could choose to be presented with information in alternative formats according to their needs.

Regarding individuals exhibiting different health problems and/or disabilities, their overall movement inside the smart university campus can be acquired as they could carry a tracker sensor with them to gain immediate help from personnel in case of emergency.

In addition, through compromising a room's visual and acoustic settings based on occupants' personal preferences and needs, the adversary could make plausible assumptions regarding their mental health and well-being [45]. People who suffer seasonal affective disorder, depression and sleep disorders may choose specific light settings (e.g. light therapy lamps) to ease their symptoms [54]. According to [46], visual comfort at work is directly related to the occupants' performance, after-work hours as well as sleep quality.

Another impact aspect is that through the room's thermal acoustic settings, gender, age and possible metabolic rates could be plausibly assumed. Older people are more likely to get cold easily and women have lower metabolic rates than men [47–49]. Finally, through the acoustic settings of a room, the adversary could make assumptions about the individuals' anxiety levels as binaural beats have been used to ease anxiety [55].

Smart Appliances/devices Monitoring Privacy Leakage Scenarios: Illegally smart appliances/devices monitoring acquired data can immediately reveal human presence, as an individual directly interacts with them. Using the acquired data, the adversary can work out the dietary customs of individuals for example, the adversary can work out when and how often individuals drink coffee/tea by monitoring their interactions with the smart coffee/tea machine. Another example would include on when the individuals are having lunch/dinner/snack by monitoring their interactions with the smart oven/microwave/fridge. In addition, by working out the specific timestamps of the interactions, the adversary could learn more about the individuals' sleep patterns. For example, if an individual regularly interacts with the smart appliances during the night, it is possible they sleep during the day. Using the same timestamps, the adversary could work out how long the individuals stayed in the kitchen and if they had any interactions with each other, depending on the duration they stayed in. Finally, by compromising the cameras and sensors inside the smart fridge, the adversary could gain information about their food preferences, possible allergies and diseases the occupants might have and store chains preferences.

Smart Parking Services Privacy Leakage Scenarios: Illegally smart parking services data acquired could reveal private information on the occupants' vehicle. Specifically, through compromising the dedicated weight sensors, the

vehicle's model could be leaked as each vehicle has its own specific weight [7]. In addition, based on the parking space the vehicle is parked, the adversary could deduct on whether the vehicle is an emergency, loading, disabled-assistive or electric. Furthermore, if the smart university campus consists of dedicated parking areas based on the driver's role at the university, the driver's university role could be leaked. In addition, using the weight sensors, the adversary can possibly work out how long the driver has stayed in.

4 Discussion, Challenges and Possible Countermeasures

4.1 Discussion on Privacy Leakage Impact

Undoubtedly, privacy should be of equal focus to security in a smart university campus since, as presented in this paper, the risk of privacy leakage of individuals even through non-personal data is exceptionally high [8,28]. The fact that IoT devices and sensors are not able to accommodate sophisticated and complex security countermeasure due to lack of hardware resources makes their compromise a relatively easy and straightforward task [8].

Furthermore, as also demonstrated in the paper, simple yet valuable assumptions based on the information gained about individuals can lead to successful phishing campaigns. The adversary can use all the private, sensitive and personal information gathered to either target specific people (most likely in key positions) within the university in a spear phishing attack.

A spear phishing example could target individual people such as the rector of a university. The rector is likely to have their own dedicated parking space (if they drive a vehicle). After gaining the necessary information about their vehicle model, the adversary could send a phishing email with regards to their vehicle such as service is needed and they need to provide their credit card information to authorise the payment. Since a rector's personal details (e.g. name, profession) is likely to be listed in the university's website, the adversary could make the phishing email more personal (e.g. personal greeting) and therefore more believable to the victim. Another example would consist of a person high in status inside the university (e.g. head of the department, dean, head of finance, HR manager). These people are likely to have their own offices with smart appliances facilities (e.g. smart fridge, smart coffee machine) for their own usage. A spear phishing attack would consist of the food chain the individual buys food/coffee from informing them that they need to re-enter their credit card bank details otherwise their order will not be placed.

On the other hand, the adversary could target large groups of people in general phishing campaigns. An example could consist of the adversary targeting students with disabilities to sign up for extra assistive services by giving personal information about them such as date of birth, gender, telephone number, address and additional information regarding their disability status. Another example would consist of all the students to re-register for the new academic year in their course due to a "system malfunction". On the event of a successfully completing a phishing campaign (either general or spear type), the adversary could use the

newly acquired personal information to threaten the individuals in further in multiple ways both in physical and cyber space. In detail, the adversary could:

- Physically threaten the individual's physical safety provided that they acquire their corresponding address. Examples could include the adversaries illegally entering their house to perform an act of burglary or threaten the individual and/or their family, stalking the individuals or vandalising the victim's residential premises.
- Perform malicious acts of social engineering to illegally obtain more sensitive information about the victim. Using personal information already obtained through the compromise of the IoT sensors and/or a successful phishing campaign, the adversary could deceive the victim in further. This could happen by disguising themselves as a familiar service the victim uses. Examples include, the adversary pretending to be a bank staff member, calling to "confirm the victim's personal information" or "re-authorising a payment due to a malfunction". Credit card details could be obtained from a successful phishing campaign. Another example would consist of the adversary disguising themselves as a staff member from the food chain the victim shops groceries from to "confirm the victim's personal and bank details for an order placed". Such data could be obtained from compromising the victim's food and its associated data placed in the smart fridge.
- Blackmail individuals through extortion in exchange of not revealing sensitive information about them. Examples could include extortionists threatening individuals with exposing data about their sexual orientation, gender identification, religion, ethnic race, cultural background, political views, health and genetics and financial data.
- Steal an individual's identity. Since the adversary acquired a plethora of different personal information about the victim, they can illegally authenticate themselves as the victim to gain access to other services the victim has. An example would be to "regain access to a bank account after losing the card" by answering relevant security questions. If the security questions have to do with acquired information the adversary has (e.g. mother's maiden name, favourite sports team, first car, city grew up, university attended) they can easily bypass them and gain access to the account so they can deposit funds to their own.

4.2 Challenges in Ensuring Privacy

IoT networks, such as the smart university campus, comes with its own set of network and device requirements. An IoT network includes a massive number of IoT sensors and devices [57] that can be deployed with a considerable distance to each other. Specifically, it is estimated that a typical a smart IoT environment contains 1000 s of devices [58]. We also have to consider that in a smart university campus, there is a great chance of a dynamic number of IoT devices entering and leaving the network. In addition, these devices can also be mobile (e.g. medical devices) [36]. Unarguably, a large-scale network produces an even greater

traffic size that takes more time to properly monitor for malicious behaviour. In addition, the mobility and the dynamic nature of the IoT devices connected to the network is challenging, as they can join and leave the network from anywhere in the smart university campus. Therefore, it is easier for them to bring external threats right to the network. An IoT device entering the network may already be compromised and cause further issues to the network such as trying to spread malware and then exit the network immediately to avoid detection.

Another important issue to consider is that each IoT device comes with its own set of protocols, standards and functionality [36]. Many of the IoT devices use non IP-based protocols and other IoT-based protocols such as CoAP, MQTT, XMPP, AMQP and so on. Each of them have their own headers, commands and payload sizes. Therefore, the traffic generated is heterogeneous, and it could be potentially harder to monitor as it is more difficult to define a distinct baseline of what traffic is considered legitimate and which is considered malicious.

Furthermore, we should address that IoT devices and sensors are low in resources, specifically memory, processing power and storage. Therefore, they are unable to accommodate any sophisticated and complex security countermeasures [8] such as intrusion detection systems, robust authentication protocols and complex encryption schemes. As a result, adversaries can easily compromise a large number of them and acquire a plethora of different data to expose the individuals' privacy as demonstrated in this paper.

Moreover, we should highlight that confidentiality is not equivalent to privacy [31]. Confidentiality is defined as cyber security principle that ensures that information is protected from unauthorised disclosure. In practice, data and information either stored or exchanged between users remains secure from eavesdroppers through the usage of appropriate encryption techniques. However, this does not guarantee that the privacy of the data will remain intact. Privacy (in cyberspace) gives the freedom to users to control their own personal information. Hence, even if users' data is encrypted, it could still be shared with third-parties and other organisations due to insufficient security policies in place [50]. Not all users are familiar with appropriately handling the access rights to their data. Therefore, misconfigurations can occur without the user's knowledge.

4.3 Possible Countermeasures to Ensure Privacy

Encryption might not fully guarantee the privacy of individuals but it certainly ensures confidentiality, where the information and data exchanged between different nodes is encrypted and secure. However, sophisticated and complex encryption can cause a computational overhead which is unacceptable to IoT devices and senors from a resources perspective [8,41]. Therefore, there is need for lightweight encryption schemes which are potentially equally accurate as their more complex equivalents. Exceptional proposed systems have been proposed so far however, more work needs to be conducted [32–35]. Proceeding, the deployment of zero-knowledge proofs could be a strong solution towards ensuring the privacy of the occupants. Zero-knowledge proofs denote the techniques which the cloud server can verify a response to a query sent by a device without actually

seeing the data. Previous work involving smart meter data [37] demonstrated reassuring results. Since data is significantly related to the privacy issues in our case, defence countermeasures that are directly related to data will pose a set of effective solutions. One popular solution is data obfuscation, where the data is substantially modified by adding noise to the data. In that way, statistical analysis is made harder to be successfully conducted. Previous work conducted in [38] demonstrated that data obfuscation can defend against occupancy detection using smart meter data.

Another important solution is the anonymisation of data. Anonymisation is where the data is significantly changed so the identity of individuals is hard to be leaked. Appropriate anonymisation techniques could be integrated on data so no indication about the occupants' lives is leaked [39,40]. Furthermore, another suggestion would be to keep the data stored locally and not sent to any third parties and/or cloud servers. If the data is stored locally, it cannot be compromised through any communication channel attacks and therefore, the attack vectors are decreased [3]. In addition, even if the data is not directly related to the occupant, appropriate security policies could be introduced for each individual. In that way, the occupants will be able to have a clear view of the security policies in place and will have more control of the data generated from their interaction with the smart university campus and its services [3].

5 Future Work and Concluding Remarks

In this paper, we performed an in-depth investigation of the privacy concerns a smart university campus could pose to its occupants. We highlighted that data collected from the environment and interactions with the university's occupants could eventually reveal personal and confidential information about the occupants even though are not directly related to them cannot be classified as private on its own. This could have serious consequences to the privacy of individuals, from leakage of sensitive information to profiling of them, to successful phishing campaigns, stealing their identities and even their lives being threatened. Hence, it is essential that appropriate handling of such data is conducted through the effective deployment of privacy enhancing technologies. In terms of future work, we aim to practically evaluate our assumptions with regards to the privacy risk posed on individuals in smart university campuses by deploying the appropriate IoT technologies and ultimately investigating and developing appropriate privacy enhancing solutions.

References

1. Mattern, F., Floerkemeier, C.: From the internet of computers to the internet of things. In: Sachs, K., Petrov, I., Guerrero, P. (eds.) From Active Data Management to Event-Based Systems and More. LNCS, vol. 6462, pp. 242–259. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-17226-7_15

2. Procopiou, A., Chen, T.M.: Security challenges and solutions in IoT networks for the smart cities. In: Internet of Things, 1st edn., pp. 161–204. CRC Press, Boca Raton (2022)
3. Chen, D., Bovornkeeratiroj, P., Irwin, D., Shenoy, P.: Private memoirs of IoT devices: safeguarding user privacy in the IoT era. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), pp. 1327–1336 (2018). https://doi.org/10.1109/ICDCS.2018.00133
4. Weinberg, B.D., Milne, G.R., Andonova, Y.G., Hajjat, F.M.: Internet of things: convenience vs. privacy and secrecy. Bus. Horizons **58**(6), 615–624 (2015). https://doi.org/10.1016/j.bushor.2015.06.005
5. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Sensing as a service model for smart cities supported by internet of things. Trans. Emerg. Telecommun. Technol. **25**(1), 81–93 (2014)
6. Mace, J.C., Morisset, C., Pierce, K., Gamble, C., Maple, C., Fitzgerald, J.: A multi-modelling based approach to assessing the security of smart buildings. In: Living in the Internet of Things: Cybersecurity of the IoT - 2018, pp. 1–10 (2018). https://doi.org/10.1049/cp.2018.0031
7. Righetti, F., Vallati, C., Anastasi, G.: IoT Applications in Smart Cities: A Perspective Into Social and Ethical Issues. In: 2018 IEEE International Conference on Smart Computing (SMARTCOMP), pp. 387–392 (2018). https://doi.org/10.1109/SMARTCOMP.2018.00034
8. Alami, A., Benhlima, L., Bah, S.: An overview of privacy preserving techniques in smart home wireless sensor networks. In: 2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA), pp. 1–4 (2015). https://doi.org/10.1109/SITA.2015.7358409
9. Pappachan, P., et al.: Towards privacy-aware smart buildings: capturing, communicating, and enforcing privacy policies and preferences. In: 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 193–198 (2017). https://doi.org/10.1109/ICDCSW.2017.52
10. Kalikova, J., Krcal, J., Sterba, M.: Use of iBeacon technology for safe movement of disabled people. In: 2021 Smart City Symposium Prague (SCSP) (2021). https://doi.org/10.1109/SCSP52043.2021.9447392
11. Orza, O., Constantin, F., Negoita, A., Bosoc, S.C., Balaceanu, C., Suciu, G.: Indoor air quality monitoring for improvement of the environment in smart toilets. In: 2021 16th International Conference on Engineering of Modern Electric Systems (EMES), pp. 1–4 (2021). https://doi.org/10.1109/EMES52337.2021.9484146
12. Marques, G., Pitarma, R.: An indoor monitoring system for ambient assisted living based on internet of things architecture. Int. J. Environ. Res. Public Health **13**(11), 1152 (2016)
13. Lymperopoulos, P., Meade, K.: PathPass: opening doors for people with disabilities. In: 2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH), pp. 32–35 (2014). https://doi.org/10.1109/MOBIHEALTH.2014.7015902
14. McColl, S.L., Veitch, J.A.: Full-spectrum fluorescent lighting: a review of its effects on physiology and health. Psychol. Med. **31**(6), 949–964 (2001)
15. Rejeh, N., Heravi-Karimooi, M., Tadrisi, S.D., Jahani, A., Vaismoradi, M., Jordan, S.: The impact of listening to pleasant natural sounds on anxiety and physiologic parameters in patients undergoing coronary angiography: A pragmatic quasi-randomized-controlled trial. Complement. Therap. Clin. Pract. **25**, 42–51 (2016). https://doi.org/10.1016/j.ctcp.2016.08.001. ISSN 1744-3881

16. Ashkenazy, T., Einat, H., Kronfeld-Schor, N.: Effects of bright light treatment on depression- and anxiety-like behaviors of diurnal rodents maintained on a short daylight schedule. Behav. Brain Res. **201**(2), 343–346 (2009). https://doi.org/10.1016/j.bbr.2009.03.005. ISSN 0166-4328
17. Keshavarz, M., Anwar, M.: Towards improving privacy control for smart homes: a privacy decision framework. In: 2018 16th Annual Conference on Privacy, Security and Trust (PST), pp. 1–3 (2018). https://doi.org/10.1109/PST.2018.8514198
18. Salha, R.A., Jawabrah, M.Q., Badawy, U.I., Jarada, A., Alastal, A.I.: Towards smart, sustainable, accessible and inclusive city for persons with disability by taking into account checklists tools. J. Geogr. Inf. Syst. **12**(04), 348–371 (2020)
19. Chao, C.: Transport phenomena of human exhaled droplets due to respiratory action in ventilated indoor environments. Hong Kong Med. J. **14**(5 Suppl), 19–22 (2008)
20. Raysoni, A.U., Stock, T.H., Sarnat, J.A., et al.: Characterization of traffic-related air pollutant metrics at four schools in El Paso, Texas, USA: implications for exposure assessment and siting schools in urban areas. Atmos. Environ. **80**, 140–151 (2013)
21. Saini, J., Dutta, M., Marques, G.: A comprehensive review on indoor air quality monitoring systems for enhanced public health. Sustain. Environ. Res. **30**(1), 1–12 (2020)
22. Rawi, N.A.M.N., Jalaludin, J., Chua, P.C.: Indoor air quality and respiratory health among Malay preschool children in Selangor. Biomed. Res. Int. **2015**, 248178 (2015)
23. Gupta, D., Bhatt, S., Gupta, M., Tosun, A.S.: Future smart connected communities to fight COVID-19 outbreak. Internet Things **13**(100342), 100342 (2021)
24. Ramapatruni, S., Narayanan, S.N., Mittal, S., Joshi, A., Joshi, K.: Anomaly detection models for smart home security. In: 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), pp. 19–24 (2019). https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00015
25. Mace, J.C., Morisset, C., Smith, L.: A socio-technical ethical process for managing access to smart building data. In: Living in the Internet of Things (IoT 2019) (2019). https://doi.org/10.1049/cp.2019.0135
26. Zhang, W., Wu, Y., Calautit, J.K.: A review on occupancy prediction through machine learning for enhancing energy efficiency, air quality and thermal comfort in the built environment. Renew. Sustain. Energy Rev. **167**(112704), 112704 (2022)
27. Bakó-Biró, Z., Wargocki, P., Weschler, C.J., Fanger, P.O.: Effects of pollution from personal computers on perceived air quality, SBS symptoms and productivity in offices. Indoor Air **14**(3), 178–187 (2004)
28. Bugeja, J., Jacobsson, A., Davidsson, P.: On privacy and security challenges in smart connected homes. In: 2016 European Intelligence and Security Informatics Conference (EISIC), pp. 172–175 (2016). https://doi.org/10.1109/EISIC.2016.044
29. Jin, M., Bekiaris-Liberis, N., Weekly, K., Spanos, C., Bayen, A.: Sensing by proxy: occupancy detection based on indoor CO2 concentration. Berkeley.edu (2015)
30. Jin, M., Bekiaris-Liberis, N., Weekly, K., Spanos, C.J., Bayen, A.M.: Occupancy detection via environmental sensing. IEEE Trans. Autom. Sci. Eng. **15**(2), 443–455 (2018). https://doi.org/10.1109/TASE.2016.2619720
31. Jin, R., He, X., Dai, H.: On the security-privacy tradeoff in collaborative security: a quantitative information flow game perspective. IEEE Trans. Inf. Forensics Secur. **14**(12), 3273–3286 (2019). https://doi.org/10.1109/TIFS.2019.2914358

32. Khashan, O.A.: Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment. IEEE Access **8**, 66878–66887 (2020). https://doi.org/10.1109/ACCESS.2020.298431
33. Roy, S., Rawat, U., Karjee, J.: A lightweight cellular automata based encryption technique for IoT applications. IEEE Access **7**, 39782–39793 (2019). https://doi.org/10.1109/ACCESS.2019.2906326
34. Fotovvat, A., Rahman, G.M.E., Vedaei, S.S., Wahid, K.A.: Comparative performance analysis of lightweight cryptography algorithms for IoT sensor nodes. IEEE Internet Things J. **8**(10), 8279–8290 (2021). https://doi.org/10.1109/JIOT.2020.3044526
35. Camtepe, S., et al.: Compcrypt-lightweight ANS-based compression and encryption. IEEE Trans. Inf. Forensics Secur. **16**, 3859–3873 (2021). https://doi.org/10.1109/TIFS.2021.3096026
36. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Future Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
37. Molina-Markham, A., Danezis, G., Fu, K., Shenoy, P., Irwin, D.: Designing privacy-preserving smart meters with low-cost microcontrollers. In: Keromytis, A.D. (ed.) FC 2012. LNCS, vol. 7397, pp. 239–253. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32946-3_18
38. Chen, D., Irwin, D., Shenoy, P., Albrecht, J.: Combined heat and privacy: preventing occupancy detection from smart meters. In: 2014 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 208–215 (2014). https://doi.org/10.1109/PerCom.2014.6813962
39. Bordel, B., Alcarria, R., Robles, T., Iglesias, M.S.: Data authentication and anonymization in IoT scenarios and future 5G networks using chaotic digital watermarking. IEEE Access **9**, 22378–22398 (2021). https://doi.org/10.1109/ACCESS.2021.3055771
40. Attaullah, H., et al.: Fuzzy-logic-based privacy-aware dynamic release of IoT-enabled healthcare data. IEEE Internet Things J. **9**(6), 4411–4420 (2022). https://doi.org/10.1109/JIOT.2021.3103939
41. Ghali, C., Tsudik, G., Wood, C.A.: When encryption is not enough: privacy attacks in content-centric networking. In: Proceedings of the 4th ACM Conference on Information-Centric Networking (2017)
42. Ständer, M., Hadjakos, A., Lochschmidt, N., Klos, C., Renner, B., Mühlhäuser, M.: A Smart Kitchen Infrastructure. In: 2012 IEEE International Symposium on Multimedia, pp. 96–99 (2012). https://doi.org/10.1109/ISM.2012.27
43. Edward, M., Karyono, K., Meidia, H.: Smart fridge design using NodeMCU and home server based on Raspberry Pi 3. In: 2017 4th International Conference on New Media Studies (CONMEDIA), pp. 148–151 (2017). https://doi.org/10.1109/CONMEDIA.2017.8266047
44. Ukil, A., Bandyopadhyay, S., Pal, A.: IoT-privacy: to be private or not to be private. In: 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 123–124 (2014). https://doi.org/10.1109/INFCOMW.2014.6849186
45. Serghides, D.K., Chatzinikola, C.K., Katafygiotou, M.C.: Comparative studies of the occupants' behaviour in a university building during winter and summer time. Int. J. Sustain. Energy **34**(8), 528–551 (2015)
46. Chang, C.Y., Chen, P.-K.: Human response to window views and indoor plants in the workplace. HortScience **40**(5), 1354–1359 (2005)

47. Katafygiotou, M.C., Serghides, D.K.: Bioclimatic chart analysis in three climate zones in Cyprus. Indoor Built Environ. **24**(6), 746–760 (2015)
48. Nicol, J.F., Humphreys, M.A.: Adaptive thermal comfort and sustainable thermal standards for buildings. Energy Build. **34**(6), 563–572 (2002)
49. Smolander, J.: Effect of cold exposure on older humans. Int. J. Sports Med. **23**(2), 86–92 (2002)
50. Stavrou, E.: Guidelines to develop consumers cyber resilience capabilities in The IoE ecosystem. In: Pereira, T., Impagliazzo, J., Santos, H. (eds.) IoECon 2022. LNICST, vol. 458, pp. 18–28. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-25222-8_2
51. NICE. Quality statement 6: Emergency oxygen during an exacerbation, Chronic obstructive pulmonary disease in adults Quality standards (2011)
52. Tachycardia. Cleveland Clinic. https://my.clevelandclinic.org/health/diseases/22108-tachycardia. Accessed 03 Sept 2022
53. High blood pressure and older adults. National Institute on Aging. https://www.nia.nih.gov/health/high-blood-pressure-and-older-adults. Accessed 03 Sept 2022
54. Terman, M., Terman, J.S.: Light therapy. Health Prog. **4**(3), 5 (1998)
55. Binaural beats are being used as sound wave therapy for anxiety, but does it really help? Prevention (2021). https://www.prevention.com/health/mental-health/a35782370/binaural-beats-for-anxiety/. Accessed 03 Sept 2022
56. Asthma workup. Medscape.com (2022). https://emedicine.medscape.com/article/296301-workup. Accessed 03 Sept 2022
57. Abdul-Qawy, A.S., Pramod, P., Magesh, E., Srinivasulu, T.: The internet of things (IoT): an overview. Int. J. Eng. Res. Appl. **1**(5), 71–82 (2015)
58. Pekar, A., Mocnej, J., Seah, W.K.G., Zolotova, I.: Application domain-based overview of IoT network traffic characteristics. ACM Comput. Surv. **53**(4), 1–33 (2021). https://doi.org/10.1145/3399669. Article 87
59. Carbon dioxide in indoor air. Ncceh.ca. https://ncceh.ca/documents/field-inquiry/carbon-dioxide-indoor-air. Accessed 03 Sept 2022
60. Kiesler, N., Impagliazzo, J.: Perspectives on the internet of everything. In: Pereira, T., Impagliazzo, J., Santos, H. (eds.) IoECon 2022. LNICST, vol. 458, pp. 3–17. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-25222-8_1