National College of Ireland

Framework to assess cyber security maturity of smart buildings

MSc Internship
CyberSecurity

Siddhant
Student ID: x18203884

School of Computing
National College of Ireland

Supervisor: Mr Vikas Sahni

National College of Ireland
Project Submission Sheet
School of Computing

National College of Ireland

Student Name:	Siddhant
Student ID:	x18203884
Programme:	CyberSecurity
Year:	2020
Module:	MSc Internship
Supervisor:	Mr Vikas Sahni
Submission Due Date:	07/09/2020
Project Title:	Framework to assess cyber security maturity of smart buildings
Word Count:	4421
Page Count:	17

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature:	siddhant
Date:	6th September 2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Framework to assess cyber security maturity of smart buildings

Siddhant
x18203884

Abstract

Smart buildings are increasing at a high rate because it provides utilities like cooling, lighting, gas, hot water, heating, electricity, safety, and comfort of occupants in an efficient way which is eco-friendly as well. Cybersecurity of smart buildings is becoming a major concern nowadays, because if the smart buildings are not secure then it can impact the life of an organization as well as the life of employees working in that organization. This report presents a framework to assess the cyber security majority based on the threats and vulnerabilities present in smart buildings, the impact of threats according to their levels. Moreover, it also describes design parameters and methodology to mitigate vulnerabilities of smart buildings and make smart buildings cyber secure. Overall this paper gives better understanding of the security of smart buildings and what are all the measures that should be taken while making smart buildings cyber secure.

1 Introduction

There is no single set of rules which makes smart buildings smart. Smart buildings are an integration of different smart components which makes it smart. Smart buildings process starts by linking smart technologies such as smart temperature meter, water meter, power meter, pumps, lighting, heating, control systems, fire alarms, and other smart sensors. Moreover, at more advanced stage entry, exit (of unknown person), and elevator access to building become smart with the help of smart systems [1].

Smart buildings control the operations automatically with the help of automated processes which makes it smart and for that building uses different components such as an actuator, sensors, and microchips for managing and collecting data [2]. This also helps in increasing the reliability and performance of the organization by decreasing the consumption cost smartly.

As smart buildings are getting smarter, cybersecurity is becoming an important aspect in protecting connected smart buildings and people present in that building from online cyber threats [3]. One research estimates that smart buildings will generate global revenue of 8.5 Bn dollars in 2020 which is increasing at a rate of 15.9 percent every year from 4.7 Bn dollars in 2016. Moreover in 2021 expected revenue of smart buildings is almost three times the 2020 revenue which is 24.7 Bn dollars. Figure 1 shows smart buildings components which make smart buildings smart.

Smart buildings are beneficial from the employee's point of view as well as the owner's point of view because it saves energy and productivity of an organization and in addition

Figure 1: smart buildings components [4]

to that it also provides comfort to employees by doing automatic processes. Figure 2 highlights some key benefits of smart buildings.

Smart buildings reduce the cost of an organization by providing different solutions [5] like improvement in building operation, reduce energy usage by automatic sensors, increase the productivity of staff, enhance in the decision making process, and support sustainability efforts.

The energy efficiency of an organization is increased by smart buildings by using optimal start and stop, which helps the automation system to understand the process of on/off of the air conditioning system for a particular zone [6]. In addition to this practical loads are also categorized in groups from critical to the high priority of essentials and when building load rises then automatically low priority loads turn off's as compare to high priority loads.

Safety also increases with the help of smart buildings with inbuilt systems like fire detection, water, and gas leak. Smart buildings contain diagnostics systems that alert when something is faulty or when there is a decrease in performance [7] . It also decreases time by doing automatic daily processes.

Here is the list of some components used in smart buildings.

Network: Network should be secure because it is a nervous system of a building that helps hardware and software to communicate and sends information between them, which drives the building. If smart buildings network has loopholes [8] then anyone can hack it and send the malicious request in between the network which can lead to dangerous harm on employees and buildings.

Software: Artificial intelligence of a building depends upon your software type and efficiency. Smart buildings learn from the information given by the software and make decisions and future predictions based on that information [9]. So if your software is

Figure 2: Smart buildings Benefits [4]

faulty then it may lead to wrong information which can cause disaster.

Hardware: Hardware acts like human senses for smart buildings so that buildings can think for its benefits with the help of sensors and meters [10]. It also helps in determining light, temperature, gas leak, noise level, carbon dioxide level, and so on.

After observing all the scenario's smart buildings can also contribute to changing its temperature from air conditioning, smart lighting, smart heating effect and so on, by giving command with the help of devices and actuators.

2 Related Work

Till now a lot of researches were carried out on smart buildings, In 2012 Pradeep and Singh carried out a design on a three-way authentication approach [11] for computing devices in smart buildings. Whereas in 2013 research was carried out on lightweight key establishment protocol by Li(2013) [12] which establish a connection between network nodes in a building. Furthermore in 2015 research was proposed by Santoso and Vun (2015) [13] in which they were using ECC for smart homes, by using the center node of a network as a mutual node in wifi gateway.

In this report, a literature review was carried out, based on different techniques to understand the security areas of smart buildings [9] and how it can be enhanced. This was divided into different parts like smart buildings considerations, threats of smart buildings, and mitigation plans for it. A study was also carried out on different components used in smart buildings for analyzing loopholes and mitigation plans. A further literature review was carried out on studying security objectives, attacks, and issues in smart buildings to get the complete cyber understanding of the building. The study was further extended

to survey from people working in organizations on smart buildings in Ireland.

There are a lot of papers on smart buildings [14] and about the types of components present in smart buildings with security measures in those components, but the weakness is there is no paper which defines "How to secure existing smart buildings" and this is a very important aspect because as smartness of devices is increasing with that cyber threats are also increasing. That's why all smart buildings should be cyber secure otherwise in addition to organization it can also impact human life's as well present in those buildings. So this paper will define that how anyone can secure their existing smart buildings by securing their components from different types of attacks. Note that here there are 2 subsections subsection 2.1 and subsection 2.2.

2.1 Smart buildings security issues

Smart buildings are moving towards the Internet of things (IoT) devices which also contain state of converging to Operational technology systems and Information technology systems in buildings [15]. New elements are changing the usage and operation of the building environment by using data sharing and analytics, cloud remote access, and connected shared networks.

Moreover, buildings are facing more and more new threat which are undervalued from a long time, and as digitization is increasing threats are increasing. After observing recent cyber attacks on smart buildings stakeholders are recognizing potential cyber threats that can impact businesses and working on their security [16].

2.2 Smart buildings integration network

Integration networks are virtually connected to other aspects of building with the help of BAS, In which smart software is open for extreme vulnerabilities [17] and can be hacked by a skilled hacker easily to get access at any point of building [18]. Figure 3 shows some vulnerabilities present in an integrated network of smart buildings.

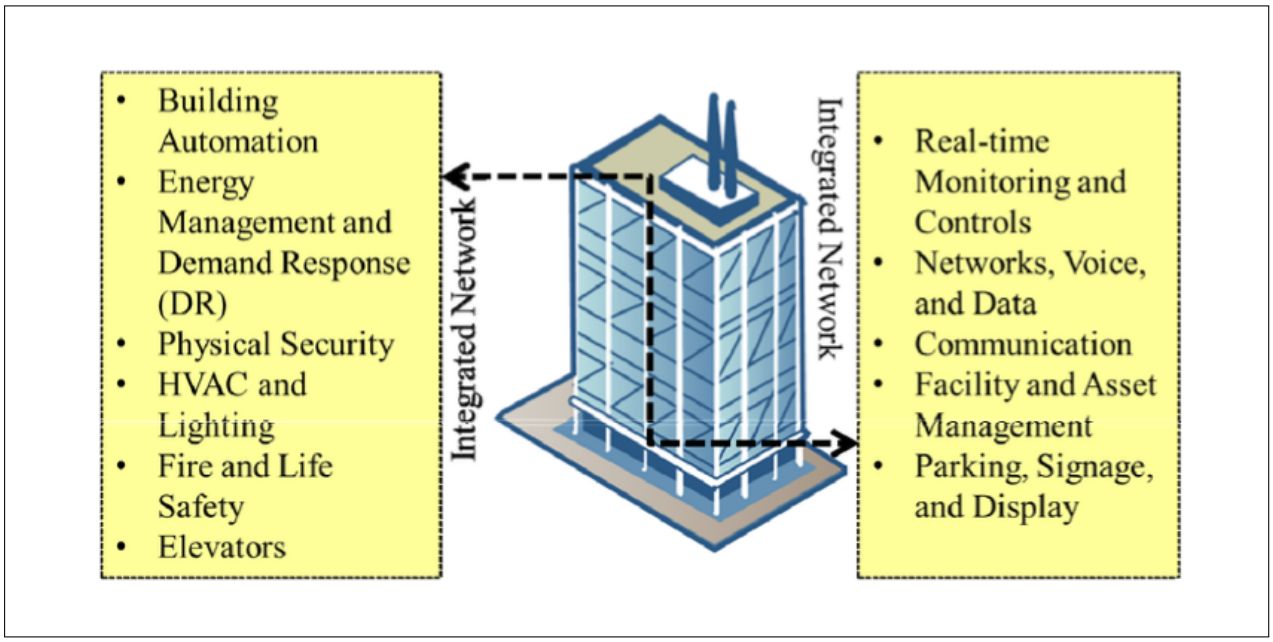

Figure 3: Integrated network vulnerabilities [19]

In Figure 4 attackers can get access through physical building or the internet and after bypassing that attacker can get access to IoT devices, workstation, and programmable logic controller (PLC). After getting access to a PLC attacker can control the sensor and actuator and with that hackers can get the whole access of the building which can lead to dangerous disasters.

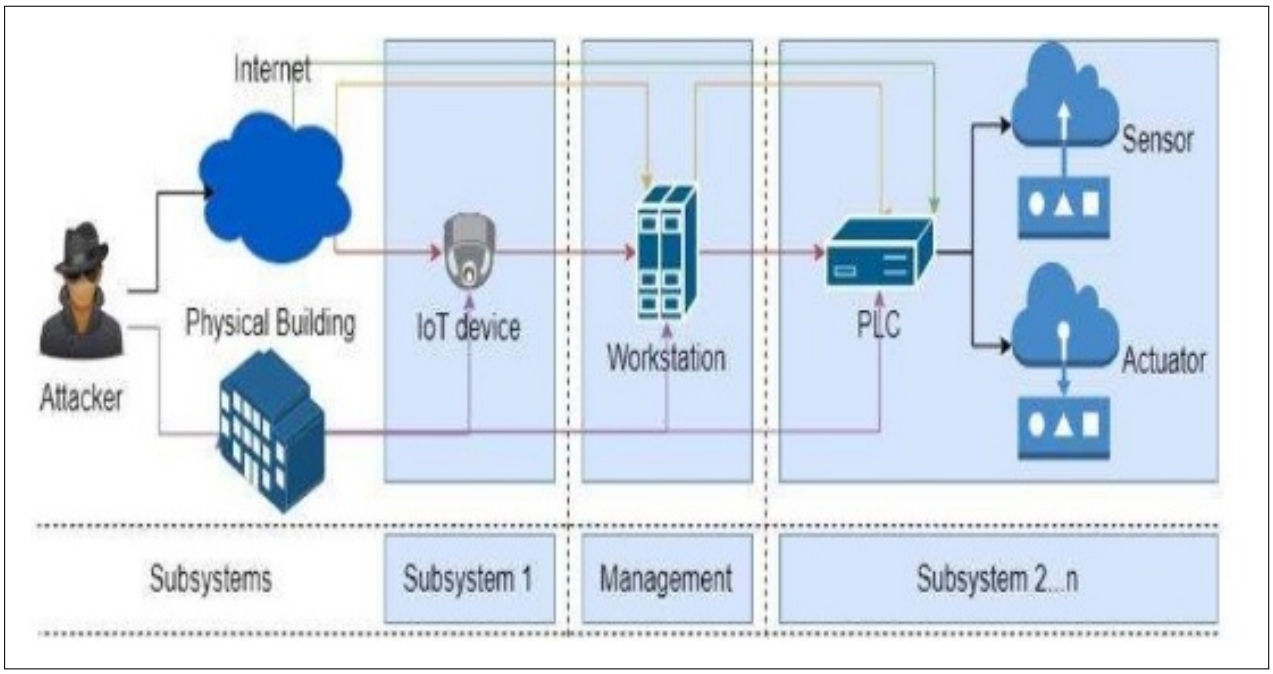

Figure 4: Attack methodology in smart buildings [4]

2.3 Smart buildings past live hacks

In 2016, Penetration testing team of IBM hack into multiple smart buildings via building automation system. In 2014, an ethical hacker wrested control of black hat HVAC, lightning and entertainment system in hotel in China. In 2013 "State government facility" got hijacked by a hacker and hacker makes it "unusually warm". Ethical hacker hacked into google Sydney HQ in 2013 through building management system. Millions of customer credit card data were traced from US retailer target to ventilation system.

3 Methodology

The proposed solution is to prevent smart buildings from increasing cyber threats [20]. It also describes the loopholes in smart buildings and patching techniques for them. According to research predicted that the market for smart buildings will increase from 5.73 billion dollars in 2016 to 24.73 billion dollars by 2021. So cybersecurity will be a big concern for smart buildings that's why this report is putting all the security measures for securing existing smart buildings.

3.1 Physical cyber threats

In smart buildings complex threats, rages are increasing rapidly day by day. These threats have scopes which present area like, side channel, software control, communication me-

dium, sensory channel, and supply chain [21]. Smart buildings threats can come from various actors like malicious outsider (hacker, cybercriminal, and terrorist) and malicious insider(employee) [22]. Table 1 shows the threat description and the corresponding examples for every threat.

Table 1: Threat descriptions of smart buildings with corresponding example

Threat description	Corresponding example
Software control: Software controls refers to softwares which are used for monitoring, operating and configuring smart buildings traffic and information.	Nick hacked into the smart TV on smart buildings by exploring weak authentication system in cloud application and able to populate sensitive information over multimedia.
Communication medium: Wireless and wired Protocol: bluetooth, digitalStorm, Wifi, ZigBee etc	In 2014, chapman obtains network configuration with the help of LIFX smart bulb because of insecure IPV6 wireless personal area network
Sensory channel : By exploiting physical weakness of sensors(voice sensors, infrared sensors, and ultrasonic sensors), attackers can manipulate the process of data collection with the help of malicious codes.	Dolphin attack was carried out in which ultrasonic sensors of smart buildings were compromised by sending voice at 20KHz which sounds similar to human voice.
Supply chain: In this process attacker embeds malware into the software or hardware before delivery to customer.	On installation these softwares additionally access web history and change network configuration over android device.

3.2 Impact of threats

Smart buildings threats impact on two different categories which are businesses and smart homes. For businesses, Smart buildings threats an impact business digitally and physically as well which also impacts the lives of employees [23]. There are security researches companies analysis as well which shows that how poor security of smart buildings puts employee lives at risk [24]. Wired published in one of the reports that more than 10 billion dollar attack damage on white house assessment is caused by NotPetya malware.

Smart homes threat can be further categorized into two parts, cyber impacts, and physical impacts [25]. For cyberthreats, buildings must follow the cyber triad of (CIA) confidentiality, integrity, and availability. Wherever physical threats can further be broken down into various types, unauthorized actuation, delayed actuation, prevented actuation, incorrect actuation, and physical privacy breach.

3.3 Components of smart buildings

Analytical Softwares: Software components help in understanding data collected by sensors and also help in converting that information into actions. In addition to sensors, soft-wares also collects data [26] from sources like, utility rated and weather data to determine the building temperature and saving in electricity usage [27]. For example by collecting weather data software only switch on the air conditioning system for 2-3

hours a day, if the temperature is already cool outside which also leads to the saving of electricity cost of an organization.

User interface: User interface is the interface that makes it easy to interact and communicate between user and software for example icons, computer screen, etc. It also represents a huge bunch of data in an easy way in front of the user which makes it easy to understand and make the whole process efficient. This seems to be a less important component of smart buildings but this component helps users in accessing resources more efficiently.

IOT sensors: Sensors are used to monitor the building's data and then data is sent to access point which further travels from gateway [28]. Then gateway combines the data altogether and sends that to cloud [29]. There is a wide variety of sensors for smart buildings like temperature, light, vibration, motion, air quality, location, etc.

Connectivity: Now after gathering all the data organizations need to communicate with the internet and for that connectivity is required. For connectivity, there are two different ways cellular-based and wifi based. Cellular based is the best technique which can be used over a wide range but it is expensive. Whereas wifi is a local area network with a good coverage area but it is risky to allow a third party IoT device on your network for security purposes.

4 Design Specification

Smart buildings interact with both the internal and external environment for better performance and with the best energy-saving solutions. In the external environment, every single entity is responsible for the performance of smart buildings by connecting it with the smart grid. Whereas the internal environment contains all devices relate to smart buildings controlled by a central entity. The external and internal environments both have specific entities within smart buildings.In Figure 5 energy service interface (ESI) represent the external environment whereas the Energy management system (EMS) represents the internal environment. ESI is used to enable remote control devices within smart buildings and grid whereas EMS is used for the management of various devices.

4.1 Smart buildings security objective

Smart buildings security depends upon 6 pillars of the building which are:

Confidentiality: Only authorized person can access the data.

Integrity: Assurance of accuracy of data that no unauthorized person can modify the data in between while transmitting or at any point in time.

Availability: Assurance of availability of data that any authorized person can access the data at any point in time.

Authorization: Access control for every user in an organization should be defined according to their purpose of access.

Authentication: Assurance of validation that received message is sent by the right person whom they claim they are in the communication.

Non repudiation: Nonrepudiation assures that no one can deny after sending something or can not deny about the signature on a document.

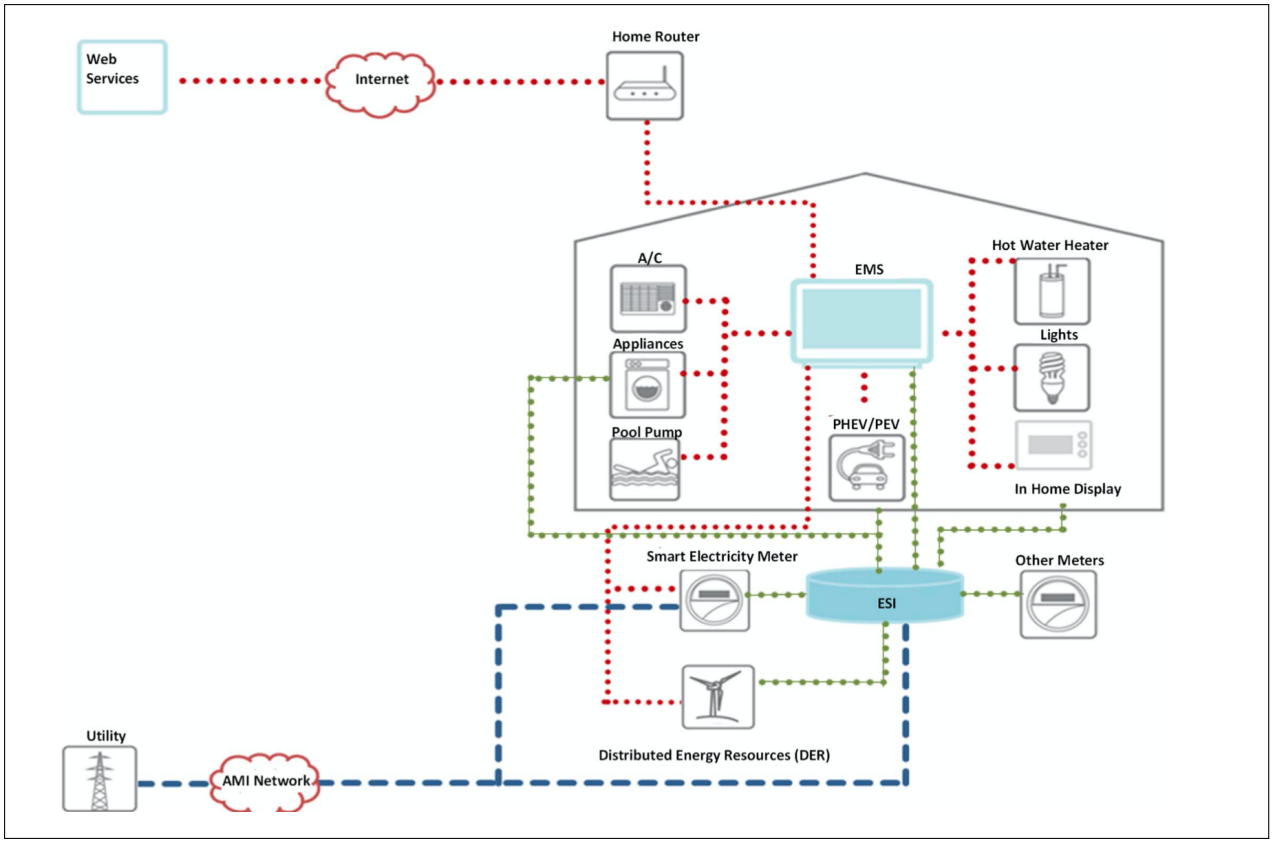

Figure 5: Smart buildings internal and external environment [23]

4.2 Smart buildings security attacks

Security attacks take place by the threats by compromising the security goals we just described. Threats are further divided into two "active attack" and "passive attack". Active attacks include data modification and also affect the operations of the affected organization. Here are some examples of active attacks like denial of service, masquerading, replay, and malicious software. Whereas Passive attacks are used to gather information on an organization without modifying it. It is also more dangerous than an active attack because a compromised person does not even know that someone has access to data.

4.3 Smart buildings impact evaluation

The criticality of a vulnerability is described by the impact assessment in which the level of threats are pre-defined with low, medium, and high criticality. FIPS 199 criteria are adopted for impact assessment. FIPS 199 defines impact in three criteria which are low, medium, and high. In addition to this Table 2 defines a matrix for checking smartness and security impacts of smart buildings with low, medium, and high criteria.

Low: Low criticality explains that the effect on security goals is a limited adverse effect which will affect the smart buildings but not that much. Limited adverse effects mean minor degradation in smart buildings in entities' performance like primary functions, minor facial loss, or loss to individuals.

Moderate: Medium criticality explains that the effect on security goals is a significant adverse effect that will affect the smart buildings on a medium scale. Significant adverse effect means medium degradation in smart buildings in entities performance like primary

function, significant loss to assets, significant financial loss, and individual loss.

High: High criticality explains that the effect on security goal is a severe adverse effect which affects smart buildings severely. Severe adverse effect means high degradation in smart buildings in entities performance like primary functions, severe loss to assets, severe financial loss, and individual loss.

Table 2: Matrix for checking smartness of smart buildings

Smart components	Impact level on smartness	Security impact
Fire Detection devices	High (Fire detection deal with human life)	High (False alarm can evacuate whole building and attackers can attack in that specific time)
CCTV	High (It can help in backtracking)	High (If CCTV is compromised than attacker can monitor all your activities and it will be difficult to backtrack)
Access control	High (Only allow authentic persons)	High (Attacker can easily get into you infrastructure if access control gets compromised)
Command and control system	Medium (System transform actionable data into real time)	Medium (False public announcement can be made if system is compromised)
Lightning control systems	High (Helps to save energy)	Low (Impact is low because lightning can impact the work in night only and that for few minutes only)
Elevator	Low (Fast mode of travelling between different floors inside building)	Low
Databases	High(Helps to maintain the data of an organization in an systematic way)	High (Data is the main asset for every organization because it includes all the information about the organization)
Generator	High (Backup device for providing energy to an organization)	High (Organization can go under DDOS attack if energy supply cut down and generator also stops working)
Heating, Ventilation, Air conditioning (HVAC)	High (Helps in maintaining temperature of an organization)	High (If air conditioning of data server room stops working than organization can face huge loss and can also lead to ddos attack)
Network monitoring devices	High (Helps in monitoring different activities)	High (Looks for malicious activities in an organisation and beeps alarm if anything suspicious)

5 Implementation

5.1 Defence mechanism of cyber security

The challenges of securing the cyber-physical security of smart buildings are becoming complex. In smart buildings, various attributes are present everywhere and its connectivity varies from machine to machine and human to machine. In addition to this attributes also forms a powerful threat landscape by combing actuator, electronics, networking, mechanical device, and sensors together. Therefore, ordinary threat landscape attacks can also apply in the same. Table 3 shows a matrix for checking the cyber maturity of smart buildings. Moreover, after the table here are some mitigation steps for threat landscape attacks of smart buildings.

Table 3: Matrix for checking cyber maturity of a smart buildings

Impact areas	Cyber Breach incidents	Cyber defence components	Preventative aspects
Users	failure in Systems	Identity validation	Access to fire system (False alarm to evacuate building)
Third party remote access	Nuisance techniques to life threatening damage	Security for end point devices	Access to security system (Unauthorized access)
Physical access to apps, networks and connected devices	Malicious softwares and virus infections	Network security	Access to communication network
Integration platforms	Attack by unauthorized outsider or fraud by staff	Data security	Access to utility-installed device
Communication gateway	Unintentional damage by third part access because there infrastructure got compromised	Multi layer security	Hijack BAS for ransomware

Denial of service defense: Wireless sensor network should employ for security measures in layer approach. At the different layers of the TCP/IP layer model, a defense mechanism should be placed. Moreover, a genetic algorithm should also be introduced and implemented for the betterment in defense mechanisms.

Two-factor authentication: Two-factor authentication is a highly recommended feature for every organization because it provides an extra layer of security which always asks for the consent of the real owner of that asset by sending a security code on provided email or contact number.

Defence for cryptography: Software encryption and authentication should be implemented in the context of wireless sensor networks for cybersecurity measures. Moreover, for the defense in cryptography, various defenses should be used like key exchange management, role-based access control, encryption, and authentication. In addition to this for ensuring data transmission reliability and secure cryptographic tools should be used.

Defence for improper access control: Improper access control can lead to information modification, disclosure, and destruction of data. So access control should be restricted for all the users according to their roles and requirements. By default, functionality access should not be there for users. It should allow users to access functions according to their requirements and roles, don't just hide functions. Role-based access control and access control lists should be used for granting access.

Intrusion detection and prevention: Machine learning algorithm should be implemented for the detection of abnormalities or intrusion in sensor reading. In addition to this for BACnet protocol mitigation and intrusion detection tools should be used.

Defence for protocols: Lot's of the test takes place everywhere on KNX/IP protocol but one research carries out by KNX comes across that through VPN, KNX/IP could not outperform connections. Whereas other researches carried out that the use of elliptic curve cryptography and the online key server can improve the security of KNX. In addition to this security data analysis has also been proposed in the BACnet protocol.

Defence for transit network and data: Security of data while transmission ensured by analysis of information flow in smart buildings and security model. Whereas smart buildings compromising security communication by compromising, authorization, authenticating, confidentiality, availability, and data integrity.

Best practices guidelines: In addition to technical discussions and experiment, best practice guideline's also proposed. Smart buildings should be pointed out in potentially disastrous consequences and advice on best practice and countermeasures proposed. Moreover paper also suggests that list of vulnerabilities should also be sent to the customer which makes the manufacturer responsible.

6 Evaluation

Evaluation of the model and presented solutions in the report are evaluated by the industry specialist who are currently working in smart buildings cybersecurity in Ireland in the real world for better understanding and for a better working model which helps for real-world problems.

So here are some graphs from a survey filled by industry specialists of smart buildings security.

6.1 Case Study 1: smart buildings components

The first question (Figure 6) of the survey is to understand which building is considered as a smart buildings. In which sensors and Energy saving devices are on the top with 87.9 percent whereas monitoring device are on the second with 84.8 percent which is just 1.1 percent less than the sensors and energy devices. Moreover, access control is on third with 69.7 percent and manual door lock system with 27.3 percent. In addition to all these options, there was an option of manual text filling in which we got the input of personalized spaces, secure data transmission, automation, and connected devices in the building each with 3 percent.

6.2 Case Study 2: smart buildings threats

The second survey question (Figure 7) is on threats of smart buildings which gives an idea of practical world threats of buildings by industry experts. In which improper access

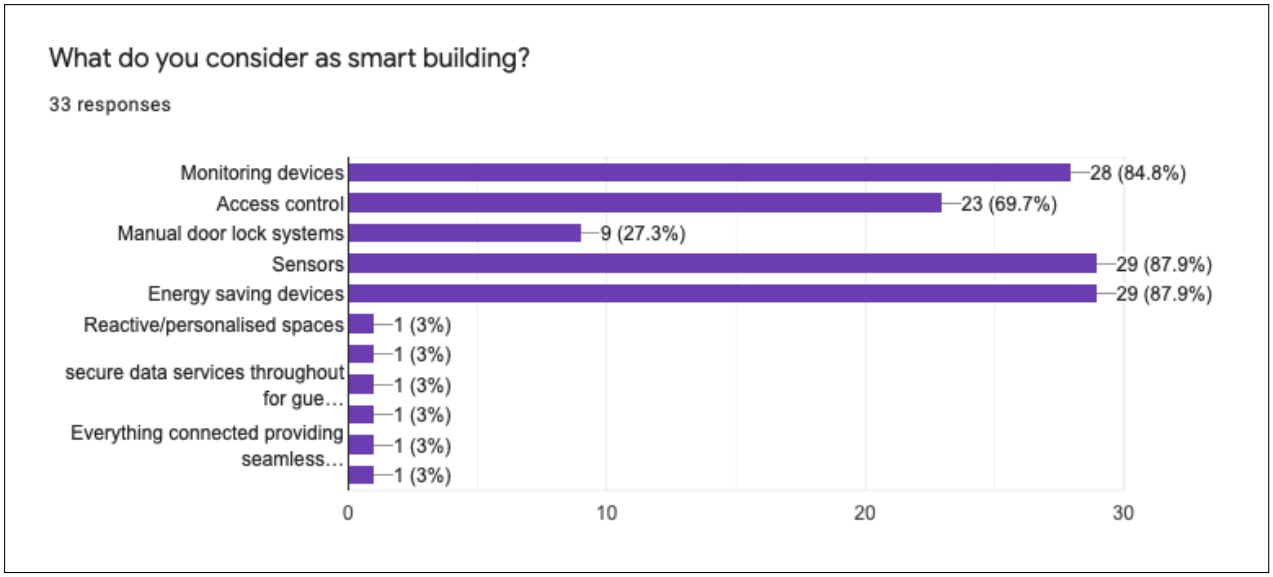

Figure 6: smart buildings considerations survey

control is on the top with 78.8 percent than on second its harvesting people data with 63.6 percent. Whereas bad infrastructure and phishing emails have the same vote and are on third with 54.5 percent. Bad internet is on fourth with 39.4 percent and manual text entry by people on outdated soft wares and human compromising systems with 3 percent each.

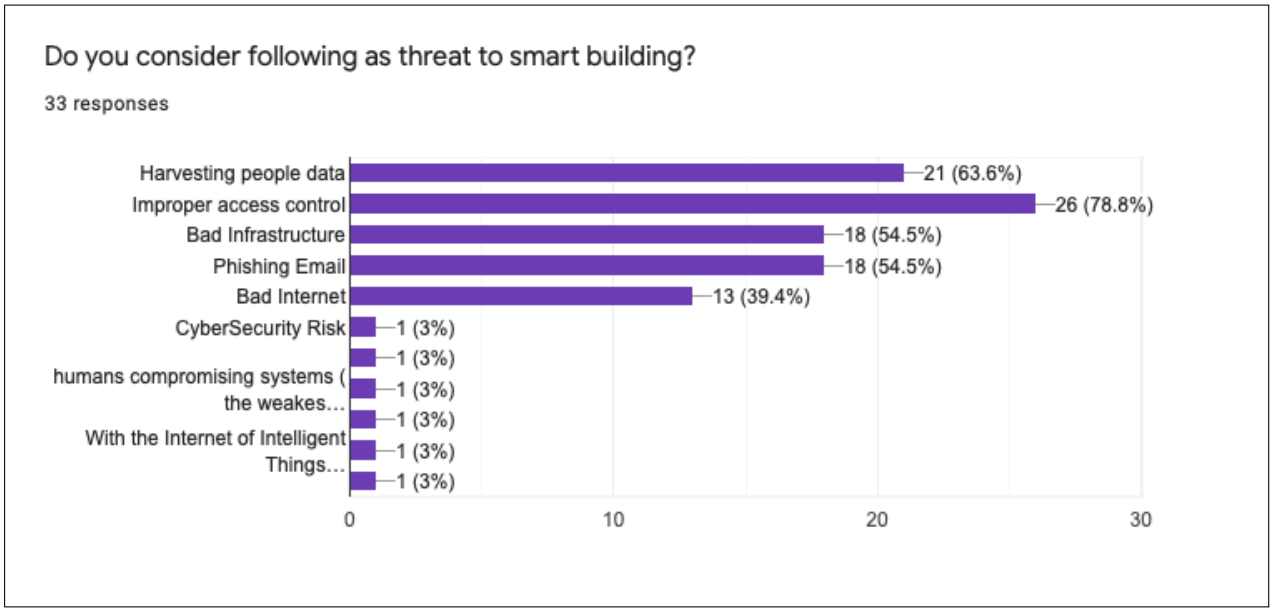

Figure 7: smart buildings threats survey

6.3 Case Study 3: smart buildings mitigation

The third survey question (Figure 8) is on the mitigation of smart buildings threats. In which intrusion detection and prevention is on the first with 81.8 percent then we have security awareness training on second with 75.8 percent. Whereas audit and accountability on third with 63.6 percent and cryptography-based defense and role-based access are

42.4 and 24.2 percent respectively.

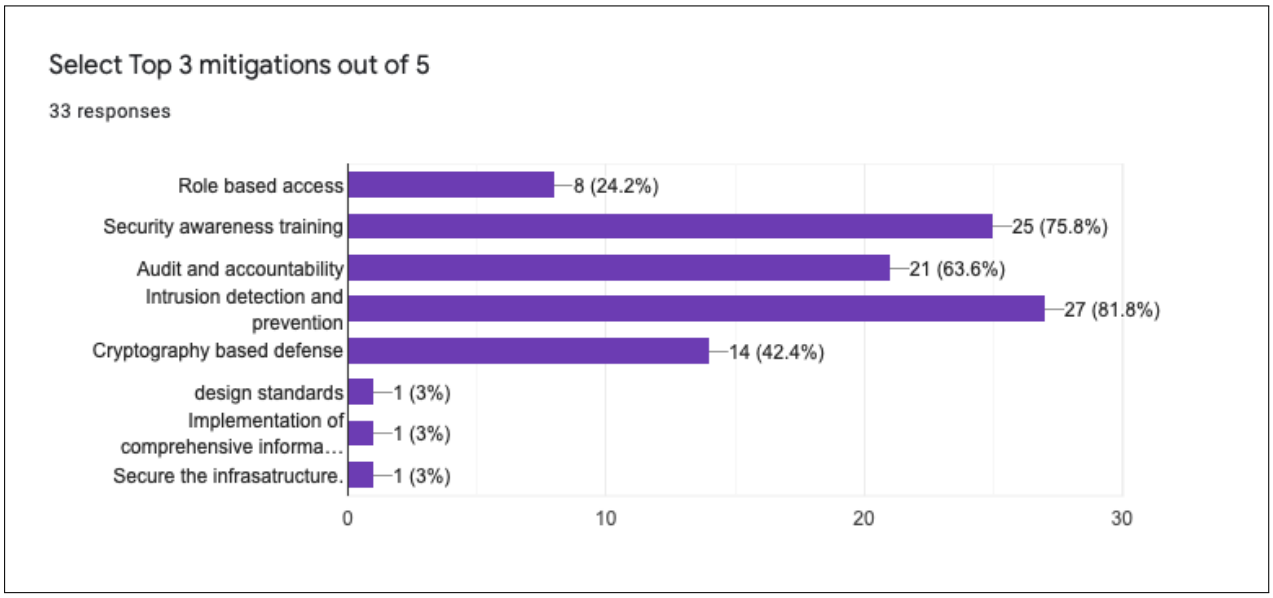

Figure 8: smart buildings mitigation's survey

6.4 Case Study 4: Potential features of smart buildings

The fourth survey question (Figure 9) is for potential features of future smart buildings. In which sensor, network security, and alerts are the top three with 69.7, 66.7, and 60.6 percent respectively. Whereas robotic automation is on fourth with 42.4 percent and log analysis is on fifth with 36.4 percent.

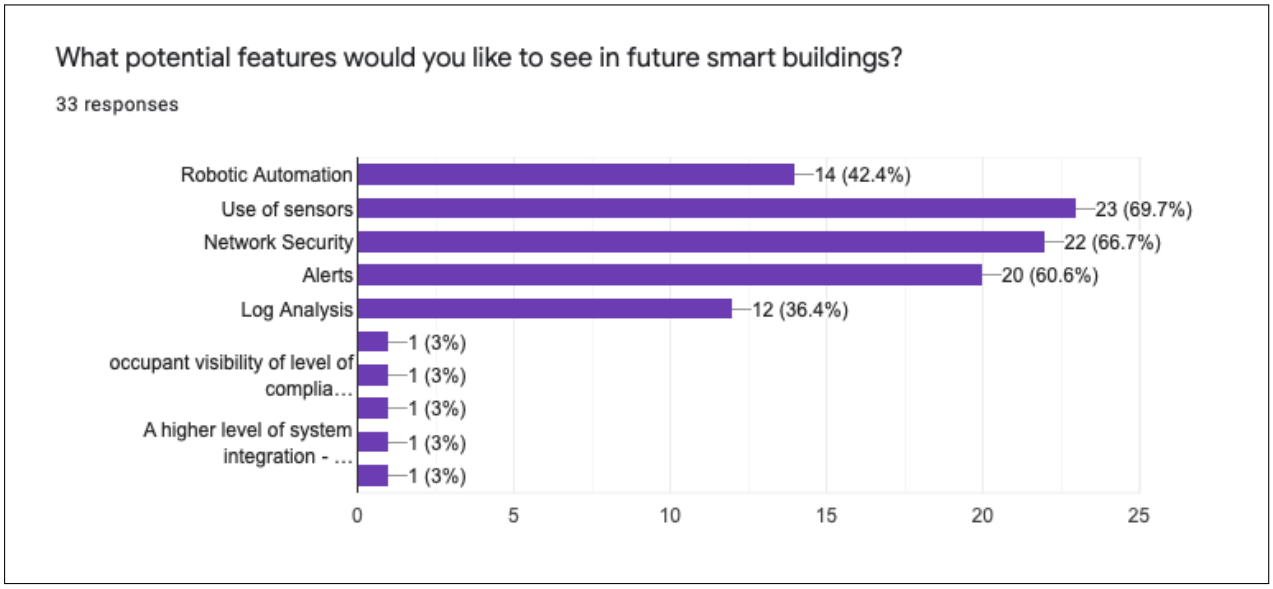

Figure 9: smart buildings potential surveys

6.5 Discussion

Results obtained from different questions of the survey states that parameters taken for the thesis model are correct according to the industry point of view by the survey statistics filled by industry experts. It also gives a brief summary about, what do you consider as smart buildings, threats of smart buildings, top three mitigation's and most important are potential features of smart buildings which enhance the output of smart buildings in an efficient way. In addition to all the given choices survey also accepts the manual input from each person which enlarges the quality of inputs. So in the survey, we got a lot of suggestions which provide benefits to the thesis by giving a lot more valuable suggestions.

Therefore this paper is compatible with practical world implementation. Moreover, the report also contains all the threats mitigation procedures listed by working experts in the survey. Perhaps the best opportunity is around developing Cybersecurity guidance and standards for this space - and a methodology to ensuring that smart buildings infrastructure meets this requirement which this report provides.

7 Conclusion and Future Work

To conclude, sooner or later all the buildings will convert into smart buildings to save energy and the environment. So this paper will give a better understanding of the security of smart buildings and what are the measures that should be considered while making smart buildings cyber secure. Wherever in prior researches, there were no criteria to measure the cyber maturity of your smart building, but after reading this paper everyone can check the maturity of their building in the cyber aspect and can also patch all the possible vulnerabilities by reading given suggestions for each vulnerability.

Moreover, in the future, I will carry forward this research with my job company by implementing all these security measures in the real-world in the existing smart buildings. As they have a lot of projects on smart buildings cybersecurity. So all the given suggestions like, impact areas, potential incidents, cyber defense components, and preventative aspects given in this paper will be used in the real smart buildings after assessing all the loopholes and components used in that building.

For assessing the building Table 2 and Figure 5 will be in use as mentioned in the design specification which will tell us about the smart components present in the building and are they safe or not and if not, the proper analysis will be done that what are the possible attacks can be done on the particular vulnerability, what will be the impact of those attacks and as seen in implementation part patching of particular vulnerability will be done and best practice guidelines will come in use. After patching all the existing vulnerabilities in the building, the analysis will be done on potential vulnerabilities and a list will be made to mitigate them.

References

[1] F. M. Bhutta, "Application of smart energy technologies in building sector — future prospects," in *2017 International Conference on Energy Conservation and Efficiency (ICECE)*, 2017, pp. 7–10.

[2] M. Botticelli, L. Ciabattoni, F. Ferracuti, A. Monteriù, S. Pizzuti, and S. Romano, "A smart home services demonstration: Monitoring, control and security services offered to the user," in *2018 IEEE 8th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*, 2018, pp. 1–4.

[3] S. Ghosh, "Smart homes: Architectural and engineering design imperatives for smart city building codes," in *2018 Technologies for Smart-City Energy Security and Power (ICSESP)*, 2018, pp. 1–4.

[4] "Figure," GAURAV. H .TANDON. Cyber Security in Smart Buildings https://www.slideshare.net/gauravhtandon1/cyber-security-in-smart-buildings./, 2020, [Online].

[5] A. M. Q. Abdulmunem and V. S. Kharchenko, "Availability and security assessment of smart building automation systems: Combining of attack tree analysis and markov models," in *2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, 2016, pp. 302–307.

[6] J. Farquharson, A. Wang, and J. Howard, "Smart grid cyber security and substation network security," in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 2012, pp. 1–5.

[7] R. Srinivasan, A. Mohan, and P. Srinivasan, "Privacy conscious architecture for improving emergency response in smart cities," in *2016 Smart City Security and Privacy Workshop (SCSP-W)*, 2016, pp. 1–5.

[8] H. Ju and J. Kim, "Security architecture for smart devices," in *2012 International Conference on ICT Convergence (ICTC)*, 2012, pp. 94–95.

[9] H. A. Boyes, R. Isbell, P. Norris, and T. Watson, "Enabling intelligent cities through cyber security of building information and building systems," in *IET Conference on Future Intelligent Cities*, 2014, pp. 1–6.

[10] V. Novák and M. Prokýšek, "Large smart metering system security," in *2014 International Conference on Intelligent Green Building and Smart Grid (IGBSG)*, 2014, pp. 1–5.

[11] P. Hanumanthappa and S. Singh, "Privacy preserving and ownership authentication in ubiquitous computing devices using secure three way authentication," in *2012 International Conference on Innovations in Information Technology (IIT)*, 2012, pp. 107–112.

[12] Y. Li, "Design of a key establishment protocol for smart home energy management system," in *2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks*, 2013, pp. 88–93.

[13] F. K. Santoso and N. C. H. Vun, "Securing iot for smart home system," in *2015 International Symposium on Consumer Electronics (ISCE)*, 2015, pp. 1–2.

[14] G. Dinc and O. K. Sahingoz, "Smart home security with the use of wsns on future intelligent cities," in *2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*, 2019, pp. 164–168.

[15] W. Bo, Y. Zhang, X. Hong, H. Sun, and X. Huang, "Usable security mechanisms in smart building," in *2014 IEEE 17th International Conference on Computational Science and Engineering*, 2014, pp. 748–753.

[16] A. Wall, H. Raddatz, M. Rethfeldt, P. Danielis, and D. Timmermann, "Ants: Application-driven network trust zones on mac layer in smart buildings," in *2018 15th IEEE Annual Consumer Communications Networking Conference (CCNC)*, 2018, pp. 1–2.

[17] H. Li and H. Zhang, "A survey on smart collaborative identifier networks," *China Communications*, vol. 15, no. 3, pp. 168–185, 2018.

[18] T. Adiono, S. Harimurti, B. A. Manangkalangi, and W. Adijarto, "Design of smart home mobile application with high security and automatic features," in *2018 3rd International Conference on Intelligent Green Building and Smart Grid (IGBSG)*, 2018, pp. 1–4.

[19] E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic readiness of smart buildings: Preconditions for subsequent cybersecurity tests," in *2016 IEEE International Smart Cities Conference (ISC2)*, 2016, pp. 1–6.

[20] Q. L. Sun, "Information under the network environment using computer information security technology," in *2015 International Conference on Intelligent Transportation, Big Data and Smart City*, 2015, pp. 474–477.

[21] M. Mrinal, L. Priyanka, M. Saniya, K. Poonam, and A. B. Gavali, "Smart home — automation and security system based on sensing mechanism," in *2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2017, pp. 1–3.

[22] S. E. Bondarev and A. S. Prokhorov, "Analysis of internal threats of the system "smart home" and assessment of ways to prevent them," in *2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2017, pp. 788–790.

[23] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[24] D. Meyer, J. Haase, M. Eckert, and B. Klauer, "A threat-model for building and home automation," in *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, 2016, pp. 860–866.

[25] G. H. Merabet, M. Essaaidi, M. E. Brak, and D. Benhaddou, "Agent based for comfort control in smart building," in *2017 International Renewable and Sustainable Energy Conference (IRSEC)*, 2017, pp. 1–4.

[26] D. Snider, G. Mayo, and S. Natarajan, "Similarity measures in smart building electrical demand data," in *SoutheastCon 2015*, 2015, pp. 1–4.

[27] N. I. Bazenkov, B. A. Boldyshev, S. V. Dushin, S. A. Frolov, M. V. Goubko, V. O. Korepanov, and L. A. Sereda, "Intensive data collection system for smart grid and smart building research," in *2019 1st International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA)*, 2019, pp. 411–415.

[28] S. Krishnan, M. S. Anjana, and S. N. Rao, "Security considerations for iot in smart buildings," in *2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 2017, pp. 1–4.

[29] M. Bajer, "Iot for smart buildings - long awaited revolution or lean evolution," in *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2018, pp. 149–154.