jamk.fi

Cyber Security in Modern Agriculture

Case Study: IoT-based Insect Pest Trap System

Ganeas Dorairaju

Master's thesis
April 2021
Technology
Master's Degree Programme in Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Dorairaju, Ganeas	Master's thesis	April, 2021
		Language of publication: English
	Number of pages 76	Permission for web publication: Yes

Title of publication

Cyber Security in Modern Agriculture

Case Study: IoT-based Insect Pest Trap System

Degree programme

Cyber Security

Supervisor(s)

Kokkonen, Tero; Hautamäki, Jari

Assigned by

Marja Aaltonen, Natural Resources Institute Finland

Abstract

A simple traditional insect pest trap system is transformed by Internet of Things (IoT for short) into an advanced connected device. The benefits are immense but cyber security imposes a great threat. The goal is to develop a checklist of requirements for developers of IoT-augmented traps that are alert to the challenges. The initial joy of creating prototypes using IoT in an end-to-end system is an achievement that needs to be reinforced with good knowledge of cyber security. Theory about the use of IoT in agriculture is comprehensive; technical details, architectural descriptions and general uptake of modern ICT is vast. Still, there are gaps and some neglect from a practical perspective on the requirements to develop IoT prototypes to ensure system continuity; a shortcoming that is addressed here.

There is a need to study the cyber security requirements for a development project of an IoT-based insect pest trap monitoring system. Guidance is needed to assist developers with limited cyber security knowledge to understand and be aware of the threat scenarios and mitigation efforts to minimize the potential cyber-attacks. Using a case study involving a combination of investigations of IoT modules used in the field experiment prototypes' and related literature review, concrete guidance is developed.

The fundamental principles of developing a proper business case and requirements apply equally to the insect pest project as any other project implementation. Basic cyber security knowledge is essential for developers including familiarity to regular IoT news. The contemporary cyber security and IoT environment within the agriculture sector is dynamic and evolving rapidly with modern technology. The significance of this study is that it informs about theoretical understanding of IoT and cyber security and gives practical guidance to developers on how to be diligent about the fundamentals.

Keywords/tags (subjects)

IoT, insect pest trap, remote monitoring system, smart farming

Miscellaneous (Confidential information)

Contents

Figures

Tables

List of Abbreviations

AI	Artificial Intelligence
BCP	Business Continuity Planning
CVE	Common Vulnerabilities and Exposures, Mitre
DSS	Decision Support System
EDB	Exploit Database (a CVE compliant archive of public exploits)
FAO UN	Food and Agriculture Organization of the United Nations
GIS	Geographical Information System
GPS	Global Positioning System
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPM	Integrated Pest Management
ISMS	Information Security Management System
ISO	International Organization for Standardization
ML	Machine Language
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database, NIST
OWASP	Open Web Application Security Project
PDCA	Plan-Do-Check-Act cycle
SIEM	Security Information and Event Management
SOC	Security Operations Center

1 Cyber Security Risks Widen as IoT Becomes Pervasive

1.1 About the research

The research aims to study cyber security implications in the use of new ICT technologies in agriculture. The Natural Resources Institute Finland (Luke) is involved in research in food and renewable natural resources to promote bioeconomy. There is a strong emphasis on the use of new technologies and digitalization in its research activities. Insect pest infestations research involves studying pests affecting various crops in agriculture. The traps play a key role in studying them as part of Integrated Pest Management (IPM) process. These studies have been undertaken before in Luke but now attempts are made to use modern technology to convert simple traditional traps to more sophisticated ones. The new remote automatic sensing traps are expected to bring benefits such as saving resources by remote monitoring, being faster with appropriate corrective actions and building large knowledge base for decision support actions. Simultaneously, there are growing and uncharted cyber security risks that lurk within the new trap systems.

The thesis deals with security vulnerabilities in a remote insect-pest IoT monitoring system which is a key component in Smart Farming. As stated by Malavade 2016, ICT has far-reaching impact as IoT progressively takes a significant position in agriculture as seen in Figure 1 below. Use of modern IoT technology in a network of processing devices, transforms the system from a mundane world of agriculture into the advanced digital world. Cyber security risks are a reality as the agricultural sector establishes a renewed growth by embracing a variety of developing ICT solutions (Demestichas, Peppes, Alexakis, 2020). It is noted that cyber security risks are critical factors that may slow the broad embracement of modern technologies in the sector. As researched by Sulkamo (2018), the need to secure IoT devices, with its phenomenal growth and acceptance of use, rests on applying the primary rules for defending the IoT environment against vulnerabilities and potential attacks.

The objective of the research is to further investigate such basic rules to study cyber security impact of digital data in a future agriculture platform where the insect pest data will be linked. The study will enable better understanding of IoT to develop

better requirements for trap systems. The insect pest infestation data will eventually be a part of a common agricultural platform for end users as farmers, researchers, and policy makers (AgriHub, 2020).

Figure 1: Role of IoT in agriculture (Malavade, 2016)

Cyber security is becoming increasingly important as computers enter every sphere of our lives in this era of the Internet and ICT systems. It has far-reaching implications for the people and systems that use technology and are dependent on its security. The technologies and computing devices that are interconnected digital devices are a part of IoT system. These IoT systems are becoming more and more prevalent in major areas of economic activities such as in agriculture. With the growing demand to advance and improve agriculture, farming practices are witnessing a surge in the use of modern technologies. Finland is a modern society where technology is emphasized, with a strong inclination towards engineering approaches and mechanization (MMM, 2014) in farming.

1.2 How the study was conducted?

Luke is involved in developing new data-driven innovations in many sectors of the economy including the agriculture sector. The original field experiments were

conducted to test new IoT-based prototypes to replace the old traditional traps. Cyber security requirements were not part of the original development requirements of the traps. They form the focus of this study so that the next prototype development will have specific cyber security requirements. The goal of this study is practice-based research to generate concrete information that can be applied directly to a real-world problem in the form of the new IoT-based prototypes. The research was conducted in several phases as follows:

1. Development and testing of IoT insect pest trap system prototypes
2. Testing and analysis of IoT devices used in terms of cyber security
3. Literature review of IoT cyber security and modern agriculture
4. Analysis and framing of the findings to the research questions
5. Discussion and conclusion of the results

The cyber security requirements for new prototype of the insect pest trap will be based on results of this study. With growing evolution of technological solutions and need to learn new opportunities, we decided to enhance existing insect pest traps with new IoT functionalities. Together with students of HAMK, new prototypes of insect pest traps using the traditional sticky-pad trap were developed. Luke has a long tradition of research in IPM together with expert researchers who have built an extensive body of knowledge in IPM and agriculture. This specific research was carried out with Marja Aaltonen, Senior Scientist at Luke, as the project manager.

The priority of the study is in remote sensing and monitoring of insect pests by IoT. The traditional sticky-pad traps were now enhanced with IoT sensors and other components to develop a fully automatic trap system. The study makes use of IoT functionalities, using sensors and cameras for data capture and GPS network for sending data through 3G/4G communication links to cloud database. The captured data is sent to remote computers for data processing and analysis of insect pests using image recognition and automatic counting techniques of machine learning algorithms. The important application areas of IoT is shown in Figure 2 below. There are a plethora of areas and applications where IoT has made inroads into and ploughed on as identified in the figure. Smart farming and precision farming spearhead the uptake of modern ICT in agriculture and the growing spread of IoT.

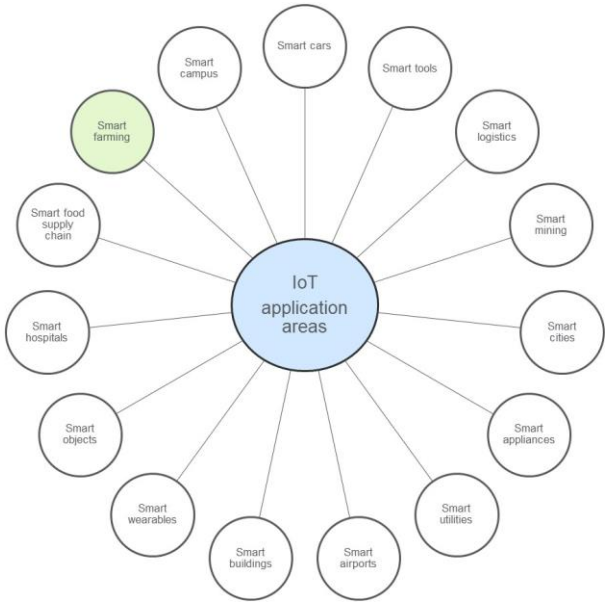

Figure 2: Important application areas of Internet of Things, IoT

1.3 Examples of IoT and cyber security issues in the news

1.3.1 Cyber-attacks and disruptive events on the increase

The UK's Department of Culture, Media and Sport's recent publication (Cyber Security Breaches Survey, 2020), highlights key findings from business and organizations on cyber security breaches and attacks and the resulting damages and consequences. UK businesses report of having had 46% cyber attacks or breaches in the last 12 months. Of these businesses 32% say they experience cyber attacks or breaches at least once a week. The report shows that the number of cyber-attacks and breaches are rising while identification of these attacks may also be improving.

Similarly, according to the findings of the Global Data Protection Index, "cyber attacks and troublesome activities are increasing; impacting 82% of institutions reviewed" (Dell Technologies Research, 2020). As high as 98% of businesses are investing in technologies such as IoT, but 52% report a lack of data protection solutions for these technologies.

These statistic show that cyber security is a growing problem world-wide and threats are constantly evolving in the environment within which they operate. Attacks such as phishing and ransomware have become more common and vindictive.

1.3.2 Malware targets IoT devices with outdated operating systems

IoT networks with connected devices are targeted by cyber-attacks due to old and outdated operating systems. “Older versions of Microsoft operating systems such as Windows Vista, Windows XP and Win7 fall victim to malware due to unpatched vulnerabilities” reports Zdnet (2020). As Microsoft declares “it will discontinue the release of new security fixes for Windows 7”, a new malware campaign targets roughly 200 million devices worldwide embedded with this now outdated operating system as reported by TrapX Research Labs (2020).

The manufacturing sector faces large challenges due to its reliance on embedded devices running legacy operating systems. These devices cannot be updated easily, and frequently must be supplanted and enhanced to latest, more safe operating systems. “Devices operating older operating systems leave the networks exposed to assault campaigns causing risks to staff wellbeing, disturbances in manufacturing and sometimes loss of important and vulnerable data” (TrapX Research Labs, 2020). Even medical equipment’s running outdated and old operating systems with sensitive patient data can be hacked. In one case unpatched ultrasound equipment running Windows 2000 OS without security patches was vulnerable to attacks (Bleeping, 2019). Simple mitigation procedures usually involving updating passwords, installing antivirus, and segmenting the network will fix these problems

1.3.3 Crops ravaged by insect infestations

Insect infestations in field crops and forests have increased in Finland and the world, “with explicit instances of burgeoning forest insect bugs threats due to climate becoming warmer” (Viiri & Neuvonen, 2017). Some of the worst outbreaks of insect pest infestations have occurred this year in East Africa as reported by the Guardian (2020). Even small-scale infestations can mean that pests can devour enough food for what could have been meant for 35,000 people in a day according to the UN humanitarian office in Geneva. From pine bark weevils to pea moths, insect bugs are estimated to cause destruction of twenty percent of the earth’s total crop production yearly, according to the Food and Agriculture Organization of the United Nations,

FAO (2020). A comparable percentage exists for the destruction of millions of hectares of forest globally Bloomberg (2020).

The infestations are a global problem and one that occurs rapidly bringing about enormous destruction in its path. Technology has in many cases finally caught up over the last decade with this situation and has the means and know-how to implement solutions that may provide early warnings and relief. As reported by Niemi & Väre (2018) in the Policy Brief to the Prime Minister's Office, "we need brave people who can think outside the box" and that digitalization will improve the food chain. And herein lies the new predicament – the emerging cyber security related vulnerabilities, exploits and threats!

These news and development stories show that cyber security has become a major challenge in the world over the past few years as the Information and Communication Technologies (ICT) sector matures. It starts to impact and affect every industry as the world becomes more connected and the Internet more pervasive, Smith (2017). The agriculture sector is no exception. New technologies and advances in modern agricultural practices are bringing about tremendous benefits and potentials to deal with food crisis in many parts of the world amid booming consumption as world's populations increase. The study scrutinizes this dichotomy of using technology and dealing with the perils of cyber security threats.

1.4 What are the next chapters about?

The thesis is structured in a way that: Chapter 2 presents an outline of **Qualitative Field Test Design and Experimentation** (research questions and methodology); Chapter 3 concentrates on **Cyber Security Knowledge and ICT in Agriculture** (theoretical framework and literature review); Chapter 4 describes the practical IoT insect pest trap system **Case Study** actions, design and investigations for the research question; Chapter 5 centers on **Results and Analysis** based on field test findings and analysis of vulnerabilities in cyber security framework and literature review; Chapter 6 concentrates on **Discussions** linking the overall theory and case study results and finally, Chapter 7 concludes the thesis in a summary of **Conclusion**.

2 Qualitative Field-Test Design and Experiments

2.1 Objective of the study

The objective is to resolve the research question through several ways; field experiment, testing of IoT modules and literature review. A qualitative applied approach was adopted as the research methodology directed to resolve the concrete practical question. As stated by Guest (2012), applied research “attempts to enrich our comprehension of a predicament, with the focus of providing a resolution to that issue”. The concrete real-world problem of insect pest infestations was studied with a physical modern IoT trap system where routine and methodology enhanced both process and experience of research (Andrew, 2018). The case study research was a step by step process involving many stages of planning, designing, collecting, analyzing and reporting of results. The routine involved several iterations and cross-routine activities to resolve the challenges.

The case study investigates cyber security issues and challenges of using IoT sensors and devices. “Qualitative research endeavours to seize typically occurring events ensuing a convention of social constructivism” (Portney, 2019). There is a strong drive towards digitalization in every sector of the economy; while digitalization brings many benefits, it also brings us closer to many risks and threats related to cyber security. Sulkamo (2018) states that an IoT environment or appliance needs to be considered like as any ICT or computer device, as IoT appliances have similar modules as traditional computers and in turn are as vulnerable to different kinds of external threats.

The theoretical framework provides the orientation for the study in an IoT-based insect pest monitoring trap system and the implications to cyber security. The literature review shows that extensive work has been done in the farming domain, IoT and cyber security. The theoretical framework will be the basis of the interpretation for the results. Together with the wealth of information available on the subject and the case study, the research will attempt to contribute concrete actions to developers of IoT traps systems in Luke.

The sections that follow develop and discuss theoretical findings of cyber security challenges in relevant and recent literature of Smart Farming and IoT. IoT systems including architecture, IoT modules used in field experiments and overall technical infrastructure are investigated. This is followed by cyber security theoretical framework and interactions and how they influence one another. Lastly, a comprehensive overview of the IoT-based elements and the interconnections via the network elements to a future common agricultural platform will be explored.

2.2 Qualitative research methodology

The research is predominantly qualitative in nature and research method used is a qualitative research based on data gathered during field experiments, further investigations and tests of the trap system IoT modules and a careful literature review of the pertinent areas linked to the research questions. According to Portney (2019), qualitative research has its emphasis on points of view, findings and discussions by experts of cyber security environment; fundamentals, goals and implications with a broad analytical focus.

This study aims to increase the overall understanding of the characteristics, quality and significance of cyber security issues related to IoT. “Doing case study active research is a step by step and vastly iterative process” (Yin, 2018). There are a variety of paths to achieve the goal and every case is in a way is unique and has its own investigative approach. The combination of activities that were a part of the study is illustrated in a flow chart as shown below in Figure 3.

The IoT modules were seperately investigated with literature and current information from Internet websites, search engines and databases with the latest and up-to-date vulnerability cases. The physical modules were also tested with simple tests involving scanning. The qualitative method however, did not present any data in the form of numbers.

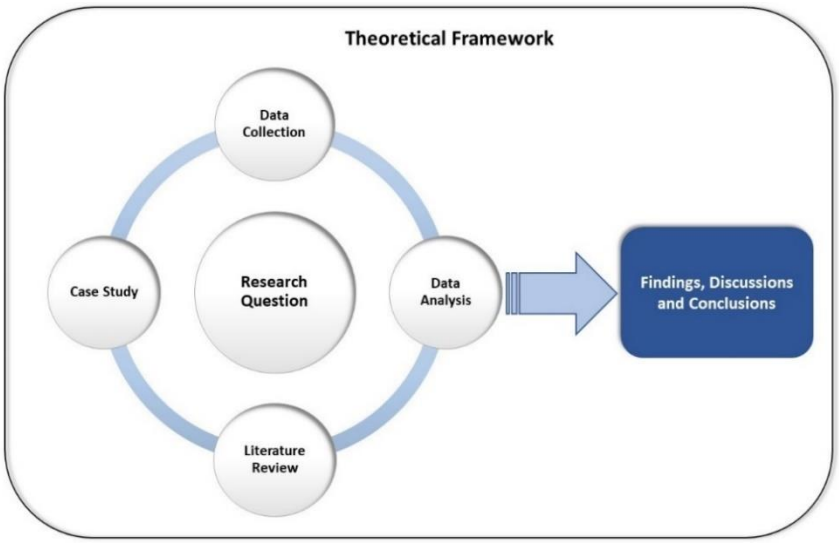

Figure 3: The research process

The case study facilitates the understanding of the research question through the interconnections of other elements that crisscross the integral parts of the study. This process was the basis of harmonizing the overall approach to carrying out the research and sequencing the steps in the process.

In summary the process shown in Figure 3 above, included all the standard steps put together as a collection of activities as follows:

1. starting with the overall view and broad picture to identify the problem
2. reviewing the literature and exposing the study to a larger body of knowledge
3. setting the research question and the sub questions and objectives
4. designing studies to analyze IoT prototypes to answer the research question
5. performing data collection, processing, testing, and analyzing
6. drafting and writing the thesis based on the research methodology

The thesis has been an interesting journey and personal learning experience to plan for its utilization in the research world and working environment at Luke. The findings will add to the growing knowledge base regarding cyber security and in an eventual implementation for developers of IoT-based traps.

The sections that follow will give more detailed information about the motivation and background to the research to get a broader view of the nature of the research and the ongoing research work in the institute. A descriptive overview of the qualitative research and the case study will then be provided. This will be followed by an overview of the case study design itself and the nature of the field work and design process. Following this, the research questions will be stated.

The research investigates the existing IoT deployments and represents these in the experimental and design procedures through the case studies. The experimental and constructive attributes of the case studies give a lot of scope for improvisation and examination through trial and error to penetrate the inner workings of those who attempt to misuse the good fortune of finding vulnerabilities in the system. As stated by Jahn (2019) in her study, which demonstrate the alarming nature of modern cyber security threats in causing “unknown unknown” risks to appear in systems that are perceived to be stable by virtue of their historically “analogue” structure. The agriculture sector which is undergoing the current transformation may unwittingly fall prey to wrongdoers who lurch and pounce on the vulnerabilities of IoT systems with their fraudulent activities.

2.3 Motivation of the research

The project develops prototype insect pest trap systems that are augmented with new IoT sensors, like what was already available in the market. The motivation for the research comes from a need to proactively address the cyber security related threats and risks posed by new technology such as IoT. There is growing pressure for the farming sector in Finland to be economically viable and sustainable. The Finnish farming sector is taking the new possibilities offered by technological advances to improve and grow (MMM, 2014).

The research has the objective of exploring how the IoT sensors and the associated devices and accessories that enhance an existing farming technology may inevitably introduce security vulnerabilities and risks into the system. A lot is already understood in terms of ICT technologies and devices used in other industries, but

what they mean to the farming sector in terms of the associated risks is something that needs further investigation.

During the 2019-20 growing seasons, the usability of the new, remote-monitoring insects trap devices was examined and compared with the operations of more traditional manual glue-based traps in Finnish field conditions. The aim of the first year was to find and develop independently working remote-reading insect trap prototype models (Aaltonen, 2019). The purpose of the automatic commercial traps was to send information either to the farmer's mobile devices and/or email and to deliver notifications when the insect control thresholds are exceeded.

IoT devices are opening opportunities for the development of plant pest control monitoring devices on 4G or 5G networks. The usage of artificial intelligence and machine learning with image recognition capabilities has evolved into an area of significant activity for research and development in recent years. Pest recognition and accurate timing of necessary sprayings is very crucial for crop health and this in turn affects crop yields and quality. The spraying of pesticides is unfortunately a necessary evil in modern farming practices, but the impact can be mitigated by targeted spraying if infestation can be proactively identified. The need to spray pesticide at regular intervals for the entire crop field will become redundant. The new IoT devices have this advantage when they can accurately and reliably identify and notify potential insect pest outbreaks so that more targeted spraying in only affected areas can be performed, avoiding the need for "blanket" spraying.

There is a strong need to understand cyber security vulnerabilities and the potential risks posed not just in the farming sector but also in a wider sense when taking new technologies and devices for use in remote monitoring work. The study conducted by Sulakamo (2018) is explored to reveal vulnerabilities encountered in cloud based IoT appliances. Together with the basic guidance and requirements checklist, serious consideration is given to the future AgriHub (2020) platform in the face of potential cyber-attacks. The system needs to withstand such attacks based on solid business continuity plans and management framework. Information and experience gained will be a source of knowledge to create improved requirements list for future work that involves use of modern IoT technology.

2.4 Research questions

There is a strong need to develop modern trap systems that can be more suitable for performing the more demanding and resource intensive tasks in the agriculture sector. The extension of the initial field studies in the IoT based insect pest trap development proceeded to investigate and study the cyber security aspects of IoT against a requirements list.

The primary research question is **"What are the cyber security requirements of an IoT-based insect pest trap monitoring system"?** This guidance will consist of a comprehensive requirements checklist for developers of IoT traps. When diligently followed prior to prototype development, it helps to anticipate and ensure system resilience and continuity by also considering the following sub-questions:

- What cyber-attacks may affect IoT based devices in Smart Farming?
- What are the hypothetical threat scenarios?
- What are the possible mitigation efforts to minimize potential cyber-attacks?

2.5 Related prior research

The research by Sulkamo (2018) in the investigations of IoT environment and cloud-based appliances is comparable to this study. It serves a strong basis for furthering some of the specific requirements and guidance for developers of the IoT insect pest trap system involved in this study. The IoT environment needs to be treated similarly to that of any ICT system in terms of protecting the system against possible security threats. The basic guidelines for management, storing and conveying confidential data between the various elements of the system needs to be secured. The life-cycle management of IoT environment includes the Information Security Management System (ISMS), disaster recovery procedures and risk analysis and calculations of the assets. In addition to this the creation of a SIEM system for IoT will help mitigate IoT ecosystems exposed to security threats from different angles. Like an ICT system, the IoT environment is investigated through the three key CIA attributes and concepts of confidentiality, integrity, and availability which constitute an indication of security levels

of the fundamental system. SIEM-based detection and mitigation efforts can be configured to block malicious traffic.

The study firstly investigated the level of cyber security within the IoT ecosystem by considering the architectural perspectives and the devices. The findings showed that the base cyber security level of an IoT ecosystem is insufficient to protect it. The minimum acceptable level of cyber security in an IoT ecosystem is ensured when management teams have a critical role. It is to confirm that security policies and practices are enforced by making sure that security controls are implemented. Sulkamo (2018) continues to emphasize the minimum implementations and importance of management treating cyber security as a business investment to protect the business assets. This needs to be done by management by taking the monetary and market values into account when defining security controls.

2.6 Research ethics

The thesis work follows the Ethical Principles for Jyväskylä University of Applied Sciences (JAMK, 2018). Every effort has been made to ensure that credit is given to the original sources and their efforts. There are no intentional violations regarding citations, listing of references and use of software licenses and applications.

The study and the writing of the thesis is based on my own work. All the initial prototype development and field studies have been done in a collaborative environment based on agreed principles and confidentiality agreements. The results of the study are being presented in openness for the benefit of readers who may find it useful. It is the wish that no attempt is made to misuse the information presented for any illegal or nefarious activities.

The conclusions of this work are intended to contribute to the common pool of knowledge and at the same time to enable new requirements to future prototype improvement and guidance activities. They are not intended to benefit any specific interested party but to address security needs of every party working with IoT systems where knowledge was also gained from the sharing process.

3 IoT in Modern Agriculture and Cyber Security Framework

3.1 The changing world of agriculture

Agriculture is an age-old human activity of cultivating plants and livestock for the main purpose of food production. Modern agriculture is today a major economic activity that employs millions of people in the entire provision and distribution of food commerce. The activities range from production, processing, storage, delivery and consumption. As world population multiplies and is expected to be about 9,7 billion in 2050 from the current 7,8 billion in 2020, there is a tremendous amount of pressure on global food reserves to nourish the planet. The United Nations (UN) Food and Agriculture Organization (FAO) assess that “world food output needs will grow dramatically in order to satisfy the demands of the years to come”. The agriculture sector is undergoing a massive transformation with the biodiversity for modern food production methodologies, advanced machinery, new technologies and state-of-the-art digital systems taking a drivers seat in its delivery.

According to the “FAO State of Biodiversity for Food and Agriculture” in Finland report by the Ministry of Agriculture and Forestry (MMM, 2014), due to the location of Finland in the north, the variety of crops and farm animal stocks used for food is rather low and production is centered on grain producing crops and straw. They make up about 80–90% of the field crop area and are an important contributor to the agriculture sector. The report emphasizes the implementation of IPM as a rule in pest management aimed at decreasing the use of pesticide while expanding the dependence on organic and other chemical-free actions. Significant risks and dangers from insect infestations are also stemming from climate change as more insect pests which generally did not survive the harsh Finnish winter are starting to thrive with the milder climate that is currently prevailing.

3.1.1 Modern ICT in agriculture

Agriculture is undergoing a tremendous change with the new possibilities offered by modern ICT technologies. As stated by the Food and Agriculture Organization of the

United Nations (FAO, 2020) report; “despite five years of entrusting to end starvation, food uncertainties and all forms of famine, the world is even now far behind in achieving this objective by 2030”. The need for a more sustainable development in the agriculture sector about achieving this goal is on the rise and is becoming critical. However, “the task to meet the challenges in production and sustenance in the years to come will be complicated without an incorporation of achievements from many sectors” (Zhang, 2015). These will involve better technologies in areas such as plant genetics, farming procedures, weather forecasting, tools management, and improved farm operations such as smart and precision farming practices. Elijah (2018) reports that these new practices be adequately and “accurately combined into the crop production systems to provide to strengthened production and maintenance capabilities”.

Contemporary agriculture has made great strides over the past 100 years through better crop cultivation and livestock production practices, crop alteration and biotechnology. New developments and advancements to traditional farming practices in agriculture, such as Smart Farming and Precision Farming are remodeling farming activities. Smart Farming is concerned with making use of new technologies and ICT infrastructure such as IoT devices for capturing, monitoring, automating and analyzing activities. Precision Farming and site-focused crop operations is a farming “operational abstraction relying on sensing, calibrating and reacting to spatial and temporal variabilities in crops”, Zhang (2015). Both these contemporary farming activities depend heavily on new technologies and advancements in computing capabilities in the form AI, ML, robotics, GPS and IoT. As reported by Ferrag et al. (2020), the research and enhancement of IoT and ICT applications security in the farming sector is growing rapidly with these new technologies.

Farm data and information is becoming progressively valuable, thanks to the proliferation of novel software applications for data analysis and leading platforms for data aggregation (Zhang, 2015). These new digital tools and platform provide the foundation on which farm data can leverage on the enormous potentials available to the entire agriculture sector. This contributes to a growing need to change and use new systems and processes that bring many new possibilities and benefits to the farming community.

3.1.2 Smart Farming

The modern agricultural transformation involves Smart Farming as a key component that employs the benefits afforded by the new opportunities provided by ICT. Zhang (2015) further states that it involves the application of precise and correct amount of inputs like water, fertilizer and pesticides among other things at the appropriate time for increasing productivity and maximizing quality and yields. ICT is a critical enabler of Smart Farming by providing and integrating geospatial technology such as GIS. The IoT integration means that remote sensing provides many opportunities in mapping for pest infestations or disease incidences. Together with early warnings and forecasting based methods, they are efficient components of Smart Farming to lower crop loss, improve pest control and cut cost of farming (Elijah, 2018)

Smart Farming is the clever utilization of ICT and IoT in the farming area “to advance decisions on operations and strategy that impact far-reaching outcomes on the farm” (Castrignanò, 2020). Smart Farming spreads across several key topics such as farm management information systems (FMIS), automation and robotics. According to Zhang (2015), “the transformation in farming are being driven by data and applications-oriented Smart Farming. It is composed of ICT solutions for smart farming equipment, IoT, sensors and actuators, network and wireless systems, Big Data, drones, robotics and other components”. There is a new surge of events that are bringing upheavals and transforming modern agriculture; starting with new and superior farm equipment to nowadays innovations in green technologies and genetic modification of food crops.

The key design feature of Smart Farming is the development of digital and electronic monitoring of crops, including factors related to the environment, soil, pest management, fertilization, and irrigation (Farooq et al., 2019). Smart Farming adopts intelligent networking architecture, mobility, flexible agricultural operations and interoperability, integration with the supply chain and the embracing of innovative business models (Elijah et al., 2018). The farming industry benefits from Smart Farming actions to advance the operations and long-term strategic decisions on the farm. As stated by Elijah (2018), these better decisions deliver benefits ranging from

higher crop yields and profits, to reducing negative environmental impacts and well-being of farm livestock and better farm management.

As stated by Zhang (2015), intelligent networks play a crucial role in Smart Farming as its operations are monitored, coordinated, controlled and integrated by a computer and communication system that allows it to interact with the physical world using a set of networked agents. According to Zhang (2015), these network agents are identified as sensors, actuators, control processing units, and communication devices.

3.1.3 Integrated pest management and traps

"The elevated recurrence of severe climate bouts, shifting weather patterns, and the related proliferations of insect pests and maladies in the last 15 years are elements that provide to dangerous rounds of food scarcity and famine, particularly when aggravated by weak establishments, strife, war and pervasive uprooting of populations" (FAO, 2020). The new possibilities that the new systems offer are remarkable advantages and benefits to managing farming quality achieved with the use of technology. On the downside, "there are critical security threats in the vigorous and scattered cybersecurity environment" (Gupta et.al, 2020)

Heightened episodes of bug and microorganism invasions acknowledged in modern studies could possibly show waning of pest and disease supervision procedures and could be compelled by climate change. The IPM system is a mixture of efficient and environmentally sensitive series of pest management approaches for evaluation, decision and control actions. The use of modern insect trap systems in the monitoring of pest infestations is an efficient, timely and accurate method because it can provide the data required for site specific crop management (Castrignanò, 2020).

Acquired raw data captured by sensing devices is transformable to usable format by uploading them to cloud services and remote servers as shown in Figure 4 below. The data is then stored into databases or data-lakes which can then be further analyzed before displaying appropriate information through digital dashboards

employing advanced visualization techniques and user interfaces (Farooq et al., 2019). The figure shows IoT sensors and cloud computing connected via the Internet.

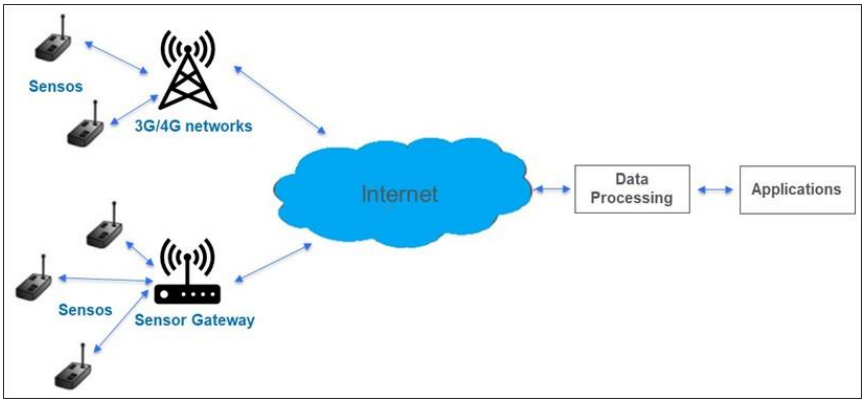

Figure 4: Cloud based IoT applications

A key prototype requirement has been recognized to be also a key benefit in IPM for developing a system capable of monitoring insect pest recognition and automatic counting. In traditional field studies and experiments, insect pests are monitored by using mostly yellow glue traps and pheromone delta traps for the pheromone sensitive pest butterflies (Huusela-Veistola et.al, 2006). The traps are checked manually several times per week in late spring and during the growing seasons. This is labor-intensive work with the risk that the traps are checked too late when unexpected infestations occur thus endangering the entire yield.

The problem can be solved by automated insect identification and counting with pheromone-based visual traps enhanced with IoT sensors and cloud services. As reported by Farooq et al. (2019), the agriculture sector is facing pressure to increase crop yields with less manpower and time to harvest. New IoT-based technologies can achieve this prerequisite by finding comparable data from the material surroundings with more efficiency and accuracy in a consistent manner and so reduce this issue.

3.2 IoT and modern farming

IoT has become a mainstay in the digital world and gaining more importance as its use burgeons in almost every sector of the economy. The farming sector has

welcomed and wholeheartedly embraced IoT-based technologies in its practices and processes. Things were not like this until just over 20 years ago (Gubbi, 2013) when IoT came into the limelight and quickly gained acceptance and expanded throughout the entire food supply chain management. The concept of remote sensing with computers where manual involvement of humans is reduced was widely adapted to other fields such as healthcare, home, environment, and transportation.

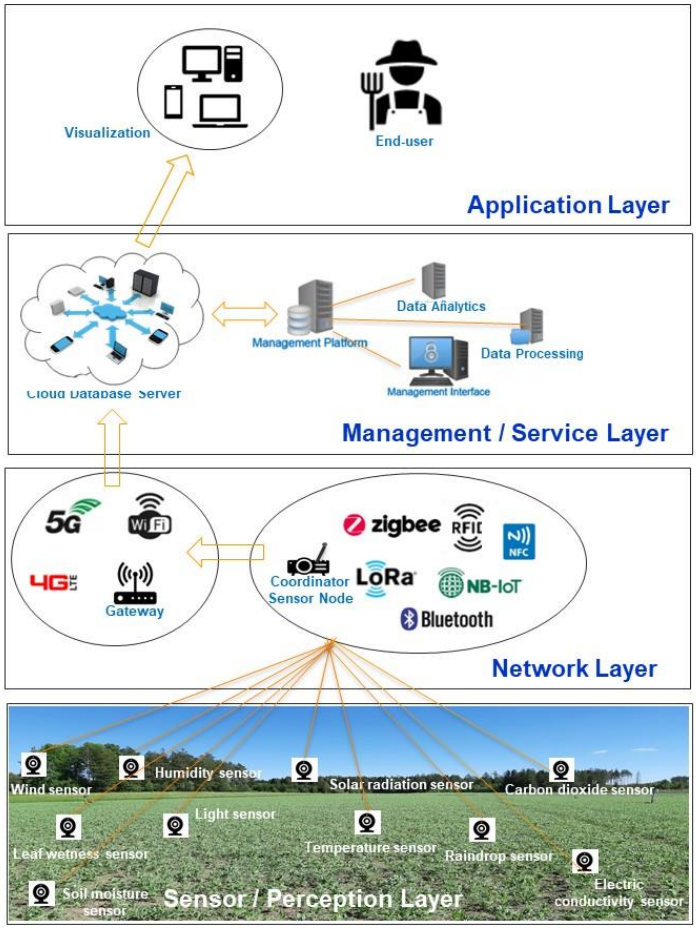

Figure 5: Smart Farming IoT architectural model (Adapted: Farooq et al., 2019)

Today IoT systems are very advanced and ubiquitous, thanks to their cheap prices, ease of use and implementation. In such circumstances, securing them is not a priority as Smith (2017) argues that there is a difference in securing IoT devices and other computers. According to him, device security, be it computers, phones or servers, is based on a human-machine symbiosis because people care when they are broken or not updated. In the case of IoT devices, this symbiosis is missing because

there may be just too many of them for us to care about, they are cheap, or people do not even know that they must care. The IoT architectural model is displayed in Figure 5 above with the four-layers of perception, network, management and application, together with all the key elements of each of these layers.

IoT systems provide unique and novel ways to convert any device to become an “intelligent” one, therefore making the devices more accessible and essentially available remotely. The devices become independent or partly dependent as they can be supervised and managed by following specific programming. With the overwhelming evolution in Internet capabilities and connectivity, IoT devices have found themselves a niche position in the new digital world when 24/7 availability and remote accessibility are highly pursued. According to Barreto et al. (2018), the growing rise of security challenges due to the daily use of IoT technology, demand ample attention, security planning and counter measures.

When IoT sensors are augmented onto any device, the IoT sensors act as a nerve center or a minicomputer with enough capabilities to receive and send data from the environment to another computer which is likely in a different remote location as shown in Figure 5. These IoT sensors can be made to have audio, video, text and sensory functions to detect changes of different environmental parameters such as temperature and pressure. The perception layer poses a critical part of IoT security terrain, Sicaria et al. (2015), “as an assortment of preceptors are placed in the land” .

In farming, IoT sensors are used in farm equipment and machinery, and it is now being tested in our research facilities with insect pest traps. The shift of conventional traps to more sophisticated IoT enhanced trap systems is a recent phenomenon but an ever-growing one. Farmers faced with the threat of insect infestations that occur rapidly over large areas of field crops, can recognize the warning signals based on the current IoT systems in a remote field. These signals are critical for the farmer to take rapid action, usually the spraying of insecticides, as infestation can occur very quickly, sometimes within 24 hours. The scope for future development in this area is enormous as the use-cases as seen by farmers in practice makes their development compelling. IoT-based Smart Farming continues to intensify the use of new ICT methods like AI and ML to make farming more efficient and effective(Ferrag et al., 2020).

3.2.1 IoT architecture

IoT is attributed to the rigorous associations between virtual and material spheres (Atzori et al., 2010, Sterling, 2005, Internet Reports, 2005) by “interlocking things supported by present, developing and interchangeable ICT”. According to Ray (2017), “IoT architecture is an arrangement which can be material, digital, or an amalgamation of both”. It consists of a set of several live items as perceptors, actuators, cloud computing services, IoT protocols, communication layers, end users, developers, and organization layer. “An IoT system is made up of a number of utility parts to simplify system services as, perception, recognition, control, interchange, and operations” (Kuppusamy, 2019).

Smart Farming technologies that are based on IoT involve the incorporation of technology and data powered by farm services to better crop produce and the quality of food products. There are various Smart Farming user scenarios that show the affect of the new model in farming. Smart Farming, though, surpasses mere essential production, and has a knock-on effect on the entire food supply chain. A high-level model to depict comprehensive and complete operations among the numerous parties in Smart Farming, identifies cloud services and applications bridging between conventional farming communities and practices with the IoT devices and sensors. A multi-layerd architecture focused on Smart Farming by featuring the multiple entry points and communication across the layers. The four layers of the overall architecture consist of the physical, edge, cloud and network communication layers creating an IoT ecosystem for agriculture (Gupta et al., 2020).

In the literature review on Smart Farming issues and possibilities (Gupta, 2020), “there seems to be general agreement based on the multiple surveys and concrete Smart Farming utilities, that the Smart Farming design satisfy most of the use cases”. However, not all end-user cases automatically incorporate all four layers as suggested in the architecture. Continous advances in technology surges forward at a rapid rate by introducing revolutionay and novell approaches towards Smart Farming crop monitoring systems. This according to Farooq et al. (2019), has recently been demonstrated by drones or unmanned aerial vehicles (UAV) via assimilation wih GIS mapping and imaging.

IoT has multiple definitions with various notions. It is described as an arrangement of interrelated devices providing services by connecting, sharing data and carrying out and assortment of work in many applications. The highly distributed and dynamic constitution of IoT empowers it to receive and store data continuously in large amounts. The Internet is the basis for IoT and provides the underlying backbone and connectivity. This means that the vulnerabilities and risks in the networks are inherently part of the same security threats as found in the Internet. Together with the fact that IoT has limited capabilities and is a lot simpler in architecture, IoT systems are much easier to compromise (Gupta B, 2020).

At the simplest form, an IoT system is made up of several functional blocks to ease different system services as perception, recognition, control, communication, transport, security and management (Bhaga, 2015). Figure 6 below shows these different functional blocks of IOT in a simplified manner.

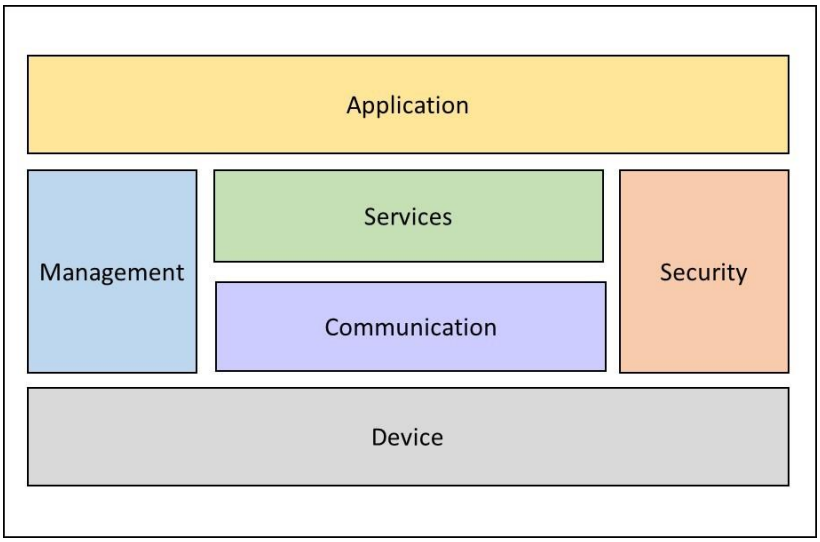

Figure 6: Functional blocks of IoT (Source: Ray P, 2017)

The functional block components show how the key element of Smart Farming systems are supported by the automation of data acquisition, processing, visualization, system management and managing the external services. The reference architecture block model helps to understand the overall structure without the details. The concrete IoT architecture design with the functional details, according to Bhaga (2015) is critical in helping to further optimize the targeted Smart

Farming goals. A brief description clarifies the functions of the different functional blocks as stated by Ray P (2017) is given in the Table 1 below:

Table 1: Description of IoT functional blocks

Functional block	Function
Device	Sensing and connectivity with embedded systems to provide perception, actuation, control and monitoring activities
Communication	Performing the link between devices and remote servers using specific communication protocols
Services	Serving the device modeling, control, publishing and data analytics
Management	Administrating the different functions to command the IoT system
Security	Defending the system through authentication, approval, privacy, integrity and data security functions
Application	Controlling and monitoring many aspects of the IoT system, such as visualization and predictive analysis

The IoT device itself being an important element of this study required further diagnosis. Figure 7 below shows the next level structure and elements of the device in respect to its component blocks:

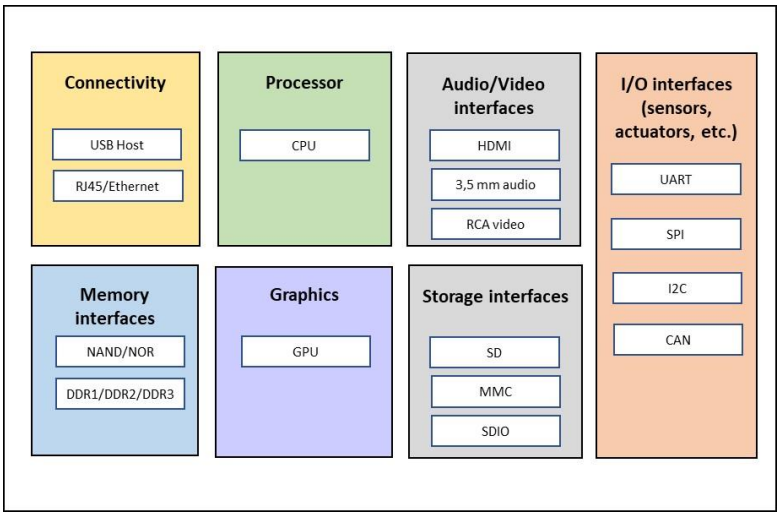

Figure 7: Block diagram of an IoT device (Source: Ray P, 2017)

3.2.2 IoT cyber security

The burgeoning of IoT devices in data gathering, processing and analysis is now being accomplished at a rapid pace. According to Gartner's report (2019), by 2025, 95% of consumer electronics will be enabled by IoT having 50 billion internet-connected things by 2020. This phenomenal growth is mostly due to IoT devices that are consumer based and has provided a multitude of business benefits and enormous opportunities, such as smart homes, robotics, control systems and automobiles.

This phenomenal growth since the first European IoT conference was held in 2006, has been driven by many factors such as advances in technology, manufacturing process improvements for mass production and breakneck price erosion of IoT components that contribute to devices being constantly sold cheaply. The focus has drifted more to quantity and speed rather than quality where product maintenance and software updates begin to suffer as shown in the surge of reported vulnerabilities and breaches by the UK survey (2019).

This is further coupled with a lack of global IoT risk standards as described by the Garner report (2019) despite the complexity of the IoT ecosystem and the presence of a plethora of devices from a slew of vendors globally. As reported by Enisa (2019), this rapid increase in IoT use, contributes to an assortment of security issues. These devices face increased security threats and risks that exploit the many weaknesses, however according to Barreto et al. (2018), the security issues are complex and require end-to-end security solutions where encryption and authentication play a major role to ensure strong security. The lack of in-built security features such as secure communication medium, appropriate authentication and authorization configurations lead further to security threats.

A further underlying reason for the vulnerabilities and threats directed at IoT devices is the Internet itself. As the key provider of connectivity, it adds further to the vulnerabilities in the IoT networks which have limited capabilities and having simpler architectures, thus making them vulnerable and easier to compromise as sated by Barreto et al., (2018).

3.2.3 IoT agriculture framework

Investigations by Farooq et al. (2019), demonstrate the key components of IoT based Smart Farming: the physical configuration, data acquiring, data handling, and data diagnostics. The physical structure or the hardware is the visible and most important element made up of the sensors, actuators and devices. They perform and supervise the required sensing through microcontrollers embedded within them. All the other three activities of data acquisition, processing and analytics are hidden from view of the user and accomplished as software activities.

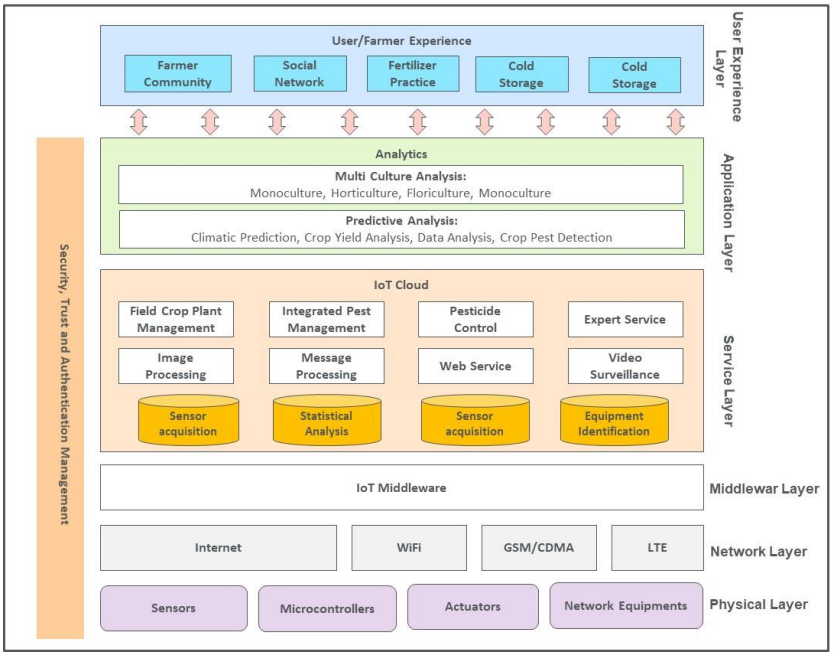

Figure 8: IoT-based crop Smart Farming framework (adapted from Zhang, 2015)

Accompanying the Smart Farming growth and use of IoT systems, the probability for cyber-crime is on the increase as the farming sector is now increasingly exposed and vulnerable to cyber-attacks (Gupta et al., 2020). Studies conducted by Gupta et al. have also shown that the agriculture sector is becoming progressively vulnerable to intrusive and wrongful activities against its infrastructure and production facilities.

The integration of Smart Farming and IoT has many advantages and benefits created by streamlining and optimizing traditional agricultural operations (Elijah, 2018). It is now generally accepted that along with these improvements, the sector is also facing many challenges and potentially risky cyber security problems (Gupta et al., 2020). The evidence points to several policies and standardizations of IoT-based Smart Farming (Gupta et al., 2020) that attempt to address this growing challenge. The challenges faced by the sector is a key reason for this study that strives to further develop strategies and guidelines. The classification of the IoT based agricultural framework based on the 7-layers according to Ray P (2017) are shown in Table 2 below.

Table 2: Classification of IoT agricultural framework based on 7-layers

Layer	Description
Physical layer	Data-collecting layer oversees conversion of analog to digital signals. Classifies objects within IoT network by using sensors deploying WSN or RFID to collect data from neighboring objects
Network layer	Processing layer processes data from the sensor layer and data is sent to a transport layer providing the access to communication technologies such as Bluetooth, Wi-Fi and LTE to send/receive data
Middleware layer	This layer serves a set of communication protocols and network support methodologies to IoT devices
Service layer	This layer receives processed data from its ensuing layers and uses the data corresponding to its requirements
Application layer	Deals with interoperability and distinguishes among various applications which comprise the custom applications using IoT data
User Experience layer	People and process layer involving stakeholders of organizations, partners and decision-making of information from IoT computing

Standardization organizations such as IEEE and IETF work towards developing standards and protocols for IoT architecture. The current lack of standards is partly because IoT does not have a fixed architecture yet. Various groups are working on developing protocols and standard modular or layered IoT architectures. The existing

idea of an IoT architecture has three layers (which in some cases are further subdivided): perception, network and application. Every level contains its own security defense to be resolved to facilitate its improvement. We need security components at every tier of IoT to prevent security and privacy threats, Gupta and Tewari (2020). The IoT-based crop smart farming framework with the interactions and interfaces to the principal elements are shown in the Figure 8 above.

Most IoT devices use integrated Radio-frequency identification (RFID) technology with wireless sensor networks (WSN) at the physical layer for their monitoring functions. According to Gupta and Tewari (2020), ensuring the basic security at the physical RFID layer can secure the data from any threat to security and privacy.

The IoT framework is the basis for understanding the cybersecurity implications that determine the nature of the vulnerabilities and security threats which are discussed in the next section.

3.3 IoT modules

IoT modules are embedded electronic devices that interact with sensors and actuators that connect to a wireless network. The modules contain circuitry and technology to have “always-on” connectivity features (Pattnaik, 2020).

3.3.1 Raspberry Pi

The Raspberry Pi is an almost complete and inexpensive computer. However, the default security level may be insufficient for our use since we access the Internet. This implies that some hardware design and manufacturing compromises have led to some limitations and weaknesses when working with it (Sainz Raso, 2019).

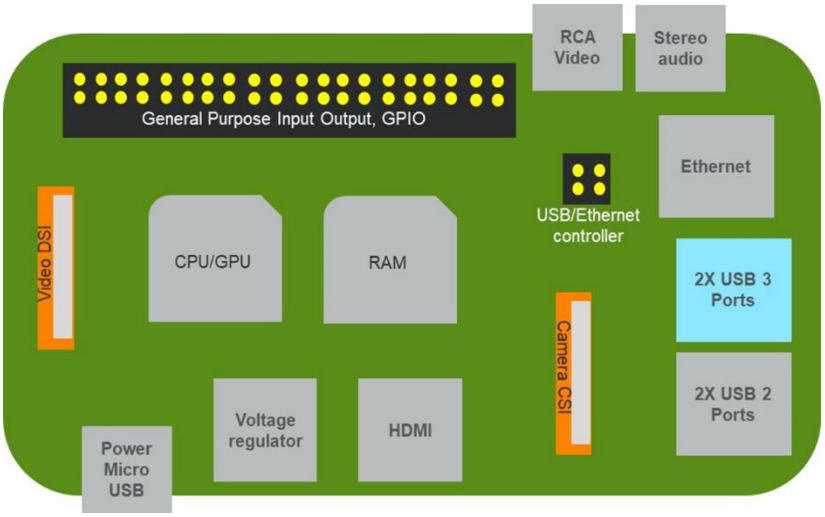

Figure 9: Raspberry Pi Model 3+ block diagram (Source: Raspberry Pi)

As a self-contained single board computer shown in Figure 9 above, the Raspberry Pi performs the input, output and processing tasks in small scale and slower than a regular laptop or a desktop. Despite its small size, this low-priced System on a Chip (SoC) has enough features to support our needs in the construction of the IoT trap system. The core of the Raspberry Pi is mostly proprietary and as such not fully open source and requires some amount of programming for boosting performance and security.

3.3.2 ESP32 microcontroller

The ESP32 is an alternative IoT module for the trap system that we developed. There are equally many advantages and disadvantages as compared to the Raspberry pi. TCP/IP protocol layers are combined with the ESP32 microcontroller so that it allows passage to the Wi-Fi network. The ESP32 chip function block diagram is shown in Figure 10 below.

Based on studies of the datasheet, ESP32 clearly has improved and increased cybersecurity since the hardware and software are open source. The block diagram as shown in Figure 10 helps explain some of the security features and shows the location of these items.

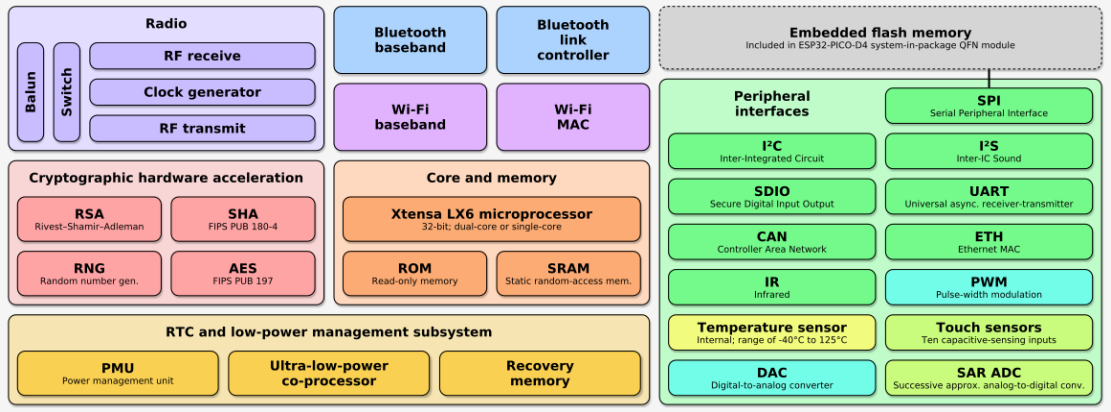

Figure 10: ESP32 Chip Function Block Diagram (Source: Espressif)

Secure Boot is a feature to ensure that the microcontroller achieves every software as assured and signed from flash. This feature provides an even more secure environment when used together with flash encryption. Flash encryption backing secures that “any application firmware, that is stored in the flash of the ESP32, stays encrypted” (v3 user guide, 2020). Together, both flash encryption and secure boot features protect from the side-effects of unwanted accesses to the flash.

As stated in the ESP32 datasheet (v3 user guide, 2020), several advanced security features are supported by the device. To secure an optimal cryptographic system security protocols and adequate key management are required. The cryptographic hardware acceleration supports Advanced Encryption Standard (AES), SHA-2 (Secure Hash Algorithm 2), RSA (Rivest–Shamir–Adleman) algorithm to encrypt and decrypt messages, Elliptic-Curve Cryptography (ECC) approach to public-key cryptography and RNG (Random Number Generator) for ensuring strong and unique encryption keys (v3 user guide, 2020).

3.4 Cyber security implications in modern farming

Cyber security has been important ever since the advent of computing, but its significance and criticality are of utmost importance today. The importance of data is extremely crucial and has far-reaching implications to those who own or are the users of the data. The CIA triad of confidentiality, integrity and availability of data forms the foundation for treating and handling data in a secure and safe

environment. This is necessary as data is valuable and as such always under threat of theft and other harms. It needs to be protected and safeguarded from people who sought to cause such damage for financial gains, destruction for fun or revenge or other more sinister activities in terms of ICT security (Barreto et al., 2018).

As more and more IoT devices are being taken into use in the farming sector, there leads to a question of a new entry point to access data in a specific platform or as a route to another location within the system. This requires that cyber security elements that have been developed and exercised over the years must be reviewed and implemented in the context of IoT and the faming environment (Kuppusamy, 2019). Albeit continuous development in cyber security, much has been learned and studied, that the entire agriculture sector will benefit from the enormous amount of knowledge and practical capabilities that cyber security is able to provide.

This study is precisely looking into these capabilities, in the hope of contributing guidance to practitioners of modern farming to secure and protect the set-up, networks and arrangements from attacks. Cyber security knowledge is at the core of providing the required guidance and safeguards to protect the valuable data from harm. With the growing embracement of IoT sensors and devices together with cloud-based applications in farming, new threats and risks have been mobilized by cyber attackers. As attested by Gupta (2020), the three major security issues surveyed in Smart Farming are data security and privacy, authorization and trust, and authentication and secure connections.

A reliable operation in a Smart Farming ecosystem depends upon highly stable data security and privacy where complex and dynamic data is triggered by various heterogenous tools and appliances. Cyber attackers use an assortment of techniques such as phishing and injecting malicious software to access and steal data without detection (Cheruvu, 2020). The issuance of commands and control through automated systems are extremely valuable and provide efficient experiences. Malicious adversaries can however take advantage of IoT communication protocols and as such all authorization must follow standardized and accepted protocols and procedures during the tranfer and exchange of data (Peng, 2020). Cheruvu (2020) claims, authentication mechanisms like the traditional public key infrastructure (PKI) are insufficient to provide verification of connected devices in a Smart Farming

system. Other methods such as dynamic authentication and cryptography have proven to be more effective.

In keeping with the Smart Farming ecosystem survey by Gupta et al. (2020), four different classes of attacks are discussed: attacks on data, networks and devices, supply chain and others. The data attacks can be classified into insider data leakage, cloud data leakage, false data injection attack and misinformation attack. The networking and equipment attacks can be classified into Radio Frequency (RF) jamming attack, malware injection attack, Denial of Service (DoS) and Botnet attack and side channel attack. The supply chain attacks are classified into third-party attacks, supply chain software update attack, data fabrication attacks and supply chain interdiction attack. The other relevants attacks are compliance and regulation violation, cyber terrorism and cloud computing attacks (Gupta et al. 2020). As attested by Gupta et al. (2020), all these four classes of attacks are likely cyber attack situations that culminate in open questions and research questions of tomorrow.

The spread of IoT devices in agriculture have released a vast and myriad of Smart Farming user services which bring with them many benefits. But all this is at a potential risk of increased cyber security vulnarabilites as shown by real attack experiences and anticipated scenarios. The literature review of the theoretical constructs and configurations help outline a Smart Farming architecture so as to systematically analyze and investigate the different entities and their impact.

The theoretical framework is central to understanding and exploring the cyber security in agriculture to study the vulnerabilities in a remote insect-pest IoT monitoring system. The previous sections broadly described a comprehensive and extensive literature review of the current status of Smart Farming, IoT and cyber security, it gives a strong foundation on which to develop a methododology to direct the research questions of the thesis. While the study does not consider other measures, such as decision support and early-warning systems, the case study is focused upon the ongoing research questions and further questions that are raised for future studies. This thesis furthers the scope of extension and improvement of the system by adding to that body of intergrated knowledge.

3.4.1 CIA triad

The CIA triad represents the three Information security goals of confidentiality, integrity, and availability as shown in Figure 11 below. It is a model for the advancement of critical security policies and attributes in information security. Whenever there is a security breach, it means that one or more of the CIA goals have been violated by a threat factor. The critical information characteristics enable the incident to be isolated and analyzed for further actions (ISO/IEC, 2018). The purpose of information security is to ensure the Confidentiality, Integrity and Availability attributes of assets are adhere to and defended against threats.

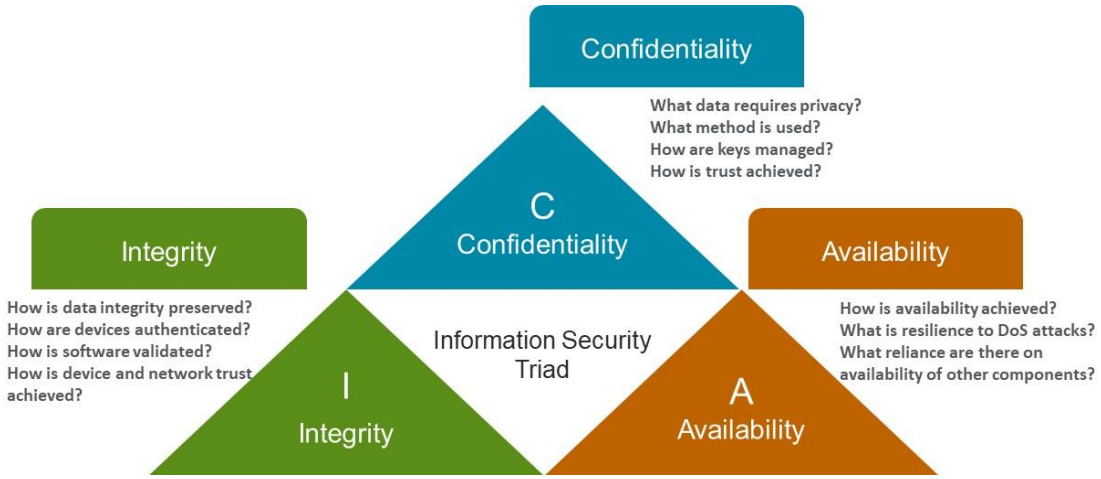

Figure 11: Confidentiality, Integrity and Availability triad (Source: NIST adapted)

The CIA triad shown above in Figure 11 is at the heart of examining the IoT cyber security environment based on the CIA principles. As published by the IoT Security Foundation (2018) the levels of integrity, availability and confidentiality set security requirements for a comprehensive compliance framework.

According to Kohnke (2017), threats and vulnerabilities are assessed based on the probable impact they have on the confidentiality, integrity, and availability of the assets—namely, its data, applications, and critical systems. This evaluation is the basis for security actions to implement a set of security controls that help to reduce

risk within the environment. The IoT Security Foundation issued the IoT Security Compliance Framework in 2016 to champion current best practices in IoT security.

3.4.2 IoT cyber security vulnerabilities and threats

According to the U.S. government repository of standards-based vulnerability management database NVD (NIST, 2012), cyber security vulnerability identifies an exploitable weakness that threatens the cyber security of an organization. The weak spot or attack surface can be exploited by an attacker using a tool or technique that can take advantage of the vulnerability and infringe on the system's security policy.

ISO 27005 (2018) defines a vulnerability as a deficiency of an asset that can be abused by a threat. An asset can be data, device, or some other component of the environment that backs information-related activities. The organization and its business operations derive value from these assets.

The information security CIA triad is used as a basis for understanding the possible equipment and data vulnerabilities and cyberattacks in agriculture (Gupta, 2020). As reported by Gupta (2020), IoT Smart Farming security stipulations are analogous to the common information security scheme originating from farm data and networks. The main thing is to have a coherent understanding of the type of attacks and how it impacts the various IoT layers and their overall impact of the agriculture sector.

The incomplete CVE list of publicly disclosed vulnerabilities is shared with the NIST, in which vulnerabilities are given risk scores through disclosure mechanisms. The OWASP keeps a list of vulnerability classes to educate software designers to decrease the unintentional writing of codes that introduce vulnerabilities into the software.

As noted by Enisa (2019), IoT solutions require CIA triad mediation and appropriate safety measures in their design, to prevent attackers from leveraging on vulnerabilities to take charge of automated processes and in turn cause process malfunctions and have serious impact on human safety.

The Table 3 shows the various types of attacks and the list keeps evolving and growing. these are attacks that have been known in the data and ICT world. As there

is significant financial value in the new agricultural platforms and businesses, the survey by Demestichas et. al (2020) shows how cybersecurity in the agricultural business environment can grow. This added with the dependencies with the various networks, there could be severe consequences in the future.

Table 3: Outline of potential attacks, security attributes and impact in agriculture

Security Attribute	Attack Type	Impact in Agriculture
Privacy	Physical Attack, Replay Attack and Masquerade Attack	Theft and vandalism of information, equipment, infrastructure, privacy of system and production standards
Confidentiality	Tracing Attack, Brute force Attack and Known-key Attack	Theft and serious threats to confidential data and user information due to many interconnected devices and protocols
Integrity	Forgery Attack, Man-In-The-Middle Attack, Biometric Template Attack and Trojan horse Attack	Financial or authentication fraud due to unauthorized and lack of trustworthiness of data or resources
Availability	Denial of Service (DoS) attacks (SYN Flood, Ping of Death, Botnets)	Business disruption, loss of confidence and revenue due to unavailable real-time operations
Authenticity	Attacks against Authentication (Dictionary attack, Session hijacking, Spoofing)	Data breach or losses, loss of devices connectivity and system corruption leading to forged identity theft and mimicry
Non-Repudiaton	Malicious Code Attack and Repudiation Attack	Refusing services, authentication information or data transmissions

Investigations by Manninen (2018), show that farm-based telecommunication network solutions implemented with consumer-level devices are vulnerable to cyber-attacks as farming becomes more reliant on ICT. Weak points and threats within the internal networks of farms or external threats give entry to cyber thieves to trigger criminal activities. Hassija et al. (2019) have stated a five layer-based classification of an IoT application and their security concerns: (1) physical layer, (2) network layer,

(3) internet layer, (4) middleware layer, and (5) application layer. There is ample space for security breaches and attack surfaces for any illegal activity within the realm of smart farming as earlier seen in the IoT architecture of Figure 5. The IoT system comprises a combination of different technologies and protocols that communicate with each other, and so the potential risk of attack and security vulnerabilities is high (Ferrag et al., 2020; Hassija et al., 2020) as can be seen in Table 4 below.

Table 4: IoT layers and security threats in smart farming

Layer	Security Threat / Attack	Smart Farming Impact
Application	Data Theft, Access Control, Service Interruption, Malicious Code Injection, Sniffing and Reprogram	Problems in delivery of services, accessibility difficulties and lack of security and privacy
Middleware	Man-In-The-Middle, SQL Injection, Signature Wrapping, Cloud Malware Injection and Cloud Flooding	Data, disclosure, vulnerabilities in device information, user access control and management
Internet	Phishing Site, Access, DDoS/DoS, Data Transit and Routing	ICT system out of service or communications disruptions
Network	Secure on-Boarding, Extra Interfaces, End-to-End Encryption and Firmware Updates	Intercepting sensitive data easily for lack of transport encryption or integrity verification
Physical	Node Capture, Malicious Code Injection, False Data Injection, Side-Channel, Eavesdropping, Booting, Interference and Sleep Deprivation	Interference in entire monitoring and sensing system, theft and tampering of data

3.4.3 Hypothetical IoT threat scenarios

The European Union Agency for Network and Information Security or Enisa gathered and published information for critical attack scenarios (Enisa, 2020). According to Enisa (2020) it is important to understand and analyze cyber threat scenarios to be better prepared to identify and deal with the mechanisms to withstand an exploit. The criticality percentages are based on information gathered from IoT expert interviews with relevant stakeholders. Their ranking of the attack scenarios; based on their acuteness and troublesome nature, are shown the Table 5 below:

Table 5: Average criticality of attack scenarios (Source: Enisa)

#	Attack against	Criticality % (approx.)
1	Control and administration systems	90
2	Sensors	85
3	Devices	80
4	Network links	75
5	Information transfer	75
6	Actuators	70
7	Protocol exploits	65
8	Power source	60

The order of criticality of the assets are sensors, devices and network management controls, communication protocols, gateways, services, and applications. This means that these critical assets need to be prioritized when dealing with IoT security.

The IoT agriculture ecosystem is growing rapidly but is not yet established enough to highlight and discover all possible threats and vulnerabilities (Farooq et al., 2019). There are various types of exploits to which an attacker follows a method on existing or future IoT farming devices and network. As stated by Gupta et al. (2020), the entire farm ecosystem works in a coordinated manner to supply food to the consumer in a synchronized chain. IoT technology being used in many parts of the chain introduce cyber security threats. Farm equipment and connected sensors to provide data can also be manipulated (Jahn, 2019) by infected malware.

The interconnected devices and IoT system introduce new possibilities for cyber criminals to exploit the farming sector. Some known attacks including global botnet and large scale DDos attacks (Gutpa et al. 2020, Farooq et al. 2019) have been launched in 2018. Three attack scenarios (Enisa, 2020) that are common in this respect, as shown in Figure 12 below, are:

1. IoT administration system concede attack shields a disruption planned to take charge of IoT devices enclosed in an ecosystem
2. Value manipulation in IoT devices manipulates tuning factors in the sensors and leads to severe threats to critical systems.
3. Botnet Commands inject directives through internal vulnerabilities to attain administrator privileges

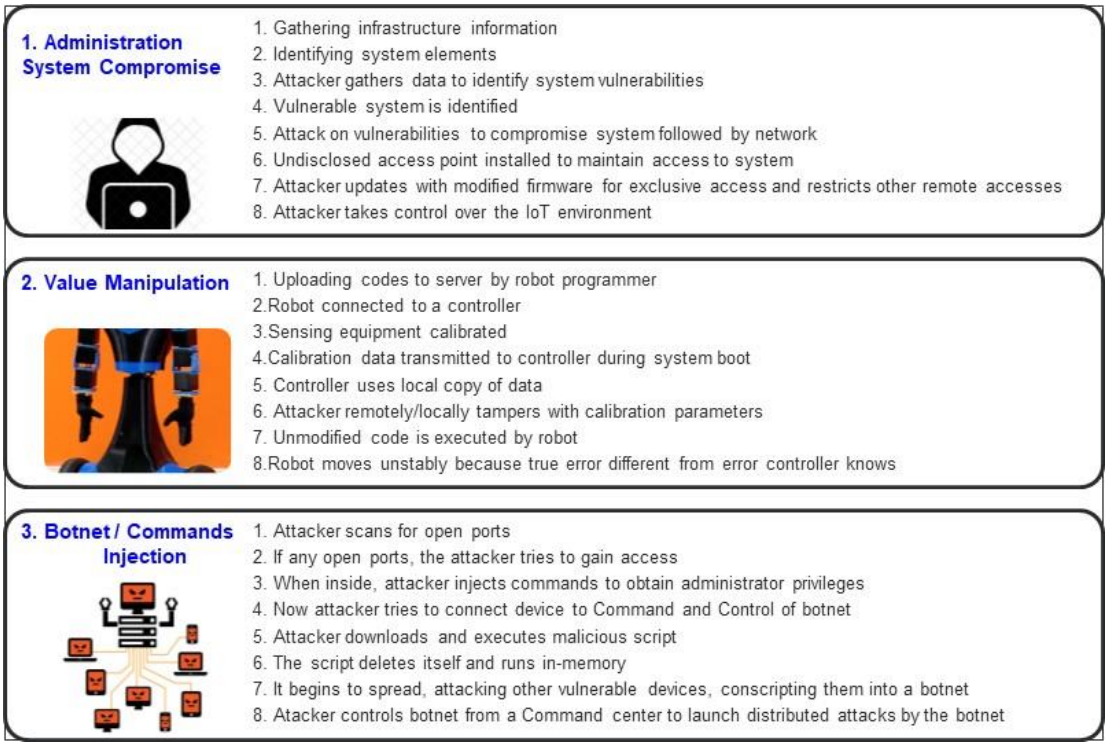

Figure 12: Three key attack scenarios (Source: Enisa)

The threat surface of IoT devices grows ever larger (Barreto et al., 2018) and lifecycle protection features of these devices are necessary “to allow users to gain from the value of linked devices and equipment while maintaining the risks”.

3.4.4 Mitigating IoT security vulnerabilities

The implementation of actions to protect against a threat is a countermeasure aimed at preventing, eliminating or minimizing the damage that it can cause. According to studies by Ferrag et al. (2020) it is an extensive, unsecured and fast changing field as new risks relentlessly emerge. Thus, new countermeasures are developed to take corrective actions to discover and report these threats as shown in Table 6 below.

Table 6: Mitigation measures description and security attributes of IoT layers

Mitigation measure	Description	Security attribute	IoT Layer
Firmware update	Ensuring latest software updates are installed	Privacy, Confidentiality, and Availability	Application
Blocking unnecessary ports	Unused ports easily become forgotten backdoors to attack	Privacy, Authenticity and Non-repudiation	Internet, Network
Strong passwords	User action to keep security level of device at high level	Privacy, Confidentiality, and Authenticity	Middleware
Encryption	Secure protocols to keep data impassable in case of theft	Integrity, Authenticity, and Confidentiality	Middleware Physical
Password recovery	Retrieving credentials in a secure manner	Privacy, Confidentiality, Authenticity	Middleware
2-factor authentication	Data protection through encryption	Privacy, Confidentiality, Authenticity	Middleware

Cyber security exploit is launched when an attacker identifies a security weakness on an attack surface to enter a system to steal data. A vulnerability scanner is a program that can scan computer systems, networks, servers and applications among others to identify weaknesses and report a severity rating. Common scanners are such as

OpenVAS, Nikto, Nmap and *Nessus*, to name a few in the industry are commonly used.

In addition to vulnerability scanners, there are other measures to assist with identification and mitigation of the vulnerabilities such as the "National Vulnerability Database (NVD) which is the U.S. government storehouse of standards and guidelines-based vulnerability management data". The data facilitates systematization of vulnerability governance, security appraisal, and conformity. The NVD performs analysis on the Common Vulnerabilities and Exposures (CVEs) that have been published to the CVE Dictionary.

In summary, the CIA triad is a conceptual model that provides an efficient and systematic way how different threat scenarios can be studied to understand them better. Cyber security mitigation efforts and strategies are a fast expanding and growing area (Demesticahs, 2020) that are responded by new and developing technologies such as ML, AI, fog and edge computing, and blockchain to improve the degree of IoT security. Cybersecurity vulnerabilities, threats and risks can so be handled and analyzed in a structured way.

3.5 Continuity planning and management framework

Actions necessary to protect the CIA triad of the information critical to the business may sometimes be missed. The continuity planning is a part of business continuity planning (BCP) that converses with planning and creating procedures to manage an organizations operation during a disruption (ISO/BSI, 2019). The capabilities of the organization to continue to deliver and maintain operations is critical with any cyber-attack situation. The risk management system in cyber security is synonymous to an organizations' business capabilities through business continuity management system (BCMS). The focus is on the continuity, recovery, and resumption of the critical operations in the event of a disruption. As stated in ISO/BSI (2019) "the Plan-Do-Check-Act (PDCA) cycle is used to realize, sustain, and constantly advance" the effectiveness of an organization's BCMS.

As stated in NIST (2012), the cyber resilience of an organization can be seen in the risk tolerance thresholds. The continuity planning plays a key role in mitigating an attack to safeguard the business assets and regain normal operations. The resilience is shown in the organization's readiness assessments, regular testing and recovery planning from realistic attack scenarios and incidences. Based on ISO/BSI (2019), organizations need to reinforce their capabilities in cyber continuity planning as well as risk management system with components that more specifically address the supply chain and external factors perspective.

The best procedures and action in continuity planning (ISO/BSI, 2019; NIST, 2012) consist of procedures that are taken during an interruption:

a) are specific to immediate steps taken
b) are flexible to respond to changing conditions
c) that focus on impact of incidents
d) are effective in minimizing impacts, and
e) are assigned roles and responsibilities for the internal tasks

Cyber security threats are a major danger of the present and the future. Businesses and organizations are continously targeted and reputations have been harmed by cyber-attacks presently (Yle, 2020; UK Department for Digital, Culture, Media and Sport, 2020; Enisa, 2019) that have intensified obstructive procedures globally.

Organizations must be alert regarding cyber risks as the dependency on technology increases for data management, product creation and maintenance, and communications. The same attentiveness must be required in confronting ongoing threats from potent attackers and cyber terrorists. The degree of threats should be followed by organizational experts when released by governments. Continuous cybersecurity vigilance, reinforcing training and increasing the alert levels of employees (UK Department for Digital, Culture, Media and Sport, 2020; Enisa, 2019) is a major line of defense for any organization.

4 Case Study: IoT Insect Pest Trap System

4.1 Field experiment design

The prototypes were developed and tested with a twofold goal:

a) firstly, to study the ability of the new traps to attract insect pests, and
b) secondly to monitor the functions of the IoT modules and end to end data flows

The first goal is not in the scope of this study as it belongs to a study performed by Aaltonen (2019) to understand how the new IoT-based trap system compares with the traditional traps. The prototypes were developed without any requirements for cyber security but only to ensure a working IoT-based system. The second goal, which is an integral part of the new IoT-based trap system, is the focus of this study. The IoT modules used in the field experiments, Raspberry Pi and ESP32, were studied in combination with cyber security literature, to develop a comprehensive requirements checklist for the next prototype development.

The electronics and hardware, including the IoT modules were investigated according to a list of requirements. The prototype development was based on a business plan (Appendix 1). The entire end to end chain of data flows from the data capture by the sensors to data transfer through the cloud services, data storage and analysis in the system and data retrieval in the platform were studied. The literature review provided the needed support to substantiate the design in terms of cyber security.

The research methodology described in Chapter 2 is the basis to design and investigate security vulnerabilities and related risks posed by an IoT based remote insect pest monitoring device in a crop field. The device uses IoT sensors and cloud-based analytics in an end-to-end digital chain system of a Smart Farming experiment in agriculture. The investigation was conducted on two successful prototypes that used a Raspberry Pi IoT sensor and another using ESP32 microcontroller.

The objective of the system was to be able to “plug-in” to farm data of a potential future “agri-business” platform that will contain farm and food related data originating from farmers and other key stakeholders of the agriculture sector. Farm

data will contain private and valuable commercial and financial information in the platform. This data may be increasingly vulnerable to current and potentially unknown risks of the future as the sector becomes increasingly dependent on availability, integrity and confidentiality of data.

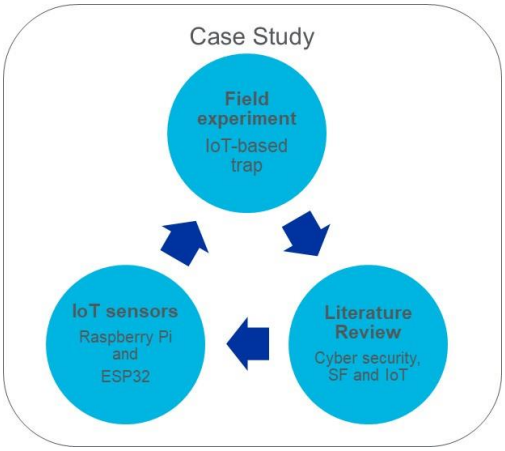

Figure 13: A conceptual schema of the case study focus areas

The following overview with description and figures is provided as part of the first goal as illustrated in Figure 13 above, to enable the reader to better visualize the experiments in the field with the IoT-based traps. The cyber security nature of the study was done outside the field experiments by investigating and analyzing the IoT modules and the subsequent cyber security literature reviews. The traps were placed in specific spots in the field as shown in Figure 14 below to attract the insect pests.

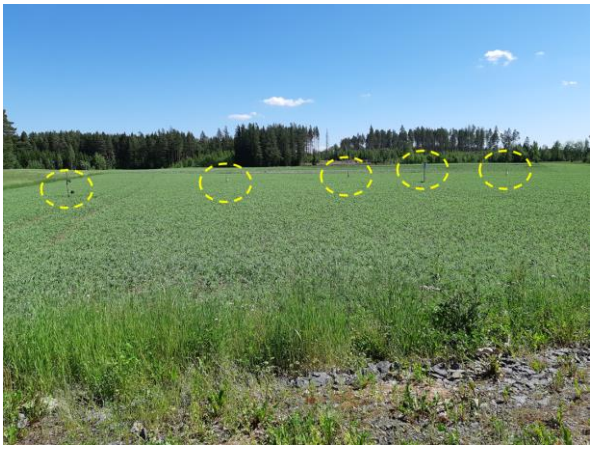

Figure 14: IoT insect pest traps installed in a pea field

The IoT electronic systems was set-up to operate automatically in remote crop-fields to capture and send data over the cloud for analysis and processing. When the prototypes were ready, the hardware components were further investigated for cybersecurity related vulnerabilities.

4.1.1 From traditional traps to IoT-based insect pest traps

Current manual trapping methods are based on traditional traps. They were introduced in open crop fields and orchards in the 1990's in Finland. The current recognition techniques for field and vegetable pests mainly rely on manual counting of the insects caught in the traps and statistical interpretation. Furthermore, there are many other shortcomings such as being heavily labor intensive, with low efficiency, feedback delays and no real-time decision support for farmers to take remedial action such as pesticide sprayings. There is however a growing trend where commercial remote monitoring devices are becoming available to the farmers.

The field experiments tested the presence of pea moth by automated monitoring and compared with the traditional manual delta traps as the control. Specific pheromone ampoules, i.e. chemicals, are used to monitor target pests in agriculture.

Current manual trapping methods are based on yellow or blue glue traps and pheromone traps, as shown in Figure 15. They were introduced in open crop-fields and orchards in the 1990's In Finland. The current recognition technology for field and vegetable pests mainly relies on artificial statistics, and there are many other shortcomings such as being heavily labor intensive, inefficient, having feedback delays and no real-time decision support for farmers to spray pesticides at the right moment in the right amounts. The Figure 15 also shows the overall set-up and the scheme how a traditional trap was converted to an advanced IoT inset pest trap. It shows the diverse constituents and outcomes obtained from pea-field monitoring system like (a) traditional trap, (b) model of an IoT trap (c) a prototype based on the model, and (d) the trap system in a pea-field.

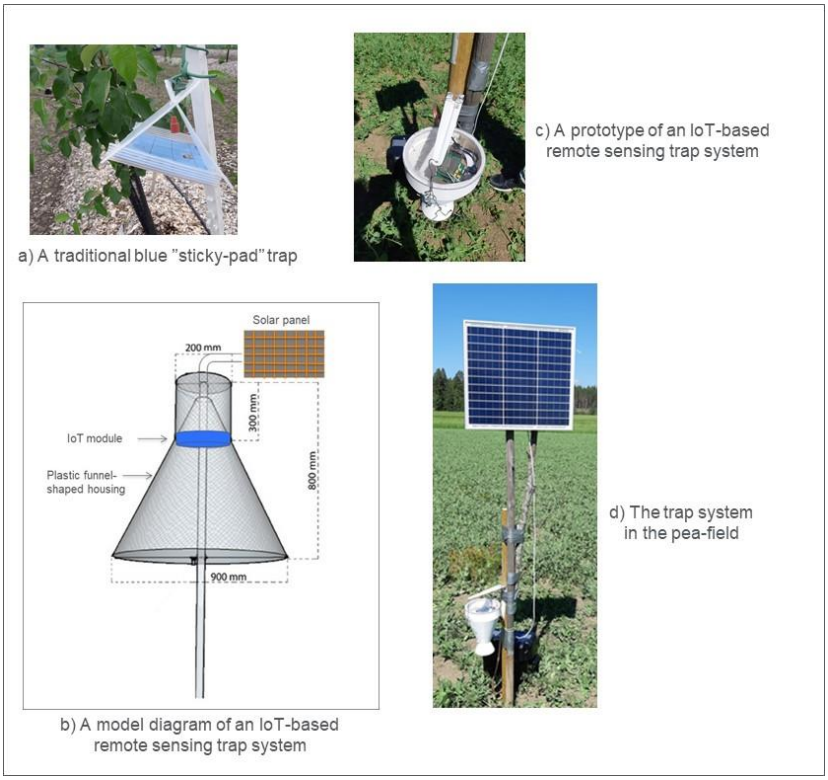

Figure 15: IoT-based pea-field monitoring system

The same prototype was also used in an apple orchard as shown in Figure 16 to attract another species; the codling moth. In this case the specific pheromone ampoule to attract the codling moth was used in the trap. Some variations were employed in the fitting mechanism of the trap itself as it must be placed appropriately in the apple trees. Otherwise, the IoT based trap system is similar except that the image recognition software now recognizes the new species. The original study also attempted to experiment with different housing structures as the behaviors of the moths are different from an entomological sense. But from a cybersecurity perspective, what was important was to study the IoT systems and the implications on security vulnerabilities.

The ease of use of the IoT modules and testing of the other parameters and configurations such as the interfaces to the network and cloud service settings were investigated. Connectivity to the Internet and the remote computers and the subsequent data analysis and processing were studied with both the prototypes.

Figure 16: IoT-based trap system in an apple orchard

When the traps functioned successfully, the testing moved indoors where the IoT electronics were investigated separately. A simple set of requirements (Appendix 2) were used as a checklist to study the IoT modules proactively to understand the landscape and be aware of possible risks introduced by the devices. This checklist help give important considerations for securing IoT devices in the organization.

4.1.2 Raspberry Pi based IoT trap

The Raspberry Pi is an easy and convenient step to building the prototype as modules are easily integrated work together as an integrated device. The operating system is the Raspberry Pi OS (previously known as Raspbian). The cost of the entire construction with the camera modules is inexpensive and that coupled with its efficient, lightweight, and user-friendly use, it was a suitable choice for our trap system.

The ease of use comes with the fact that it uses an external keyboard, mouse, screen and power supply. In this case the main requirement is to have the device take

pictures and regular instances. As soon as a picture is taken, connection is established, and the image is sent across the network to a distant computer.

The Figure 17 below shows the components of the Raspberry Pi IoT trap system. The main components in addition to the Raspberry Pi computer, is a 4G/LTE module for connectivity, a camera module and lens and the SIM card for accessing the network. The trap system required a power bank which was supplied with an external solar panel.

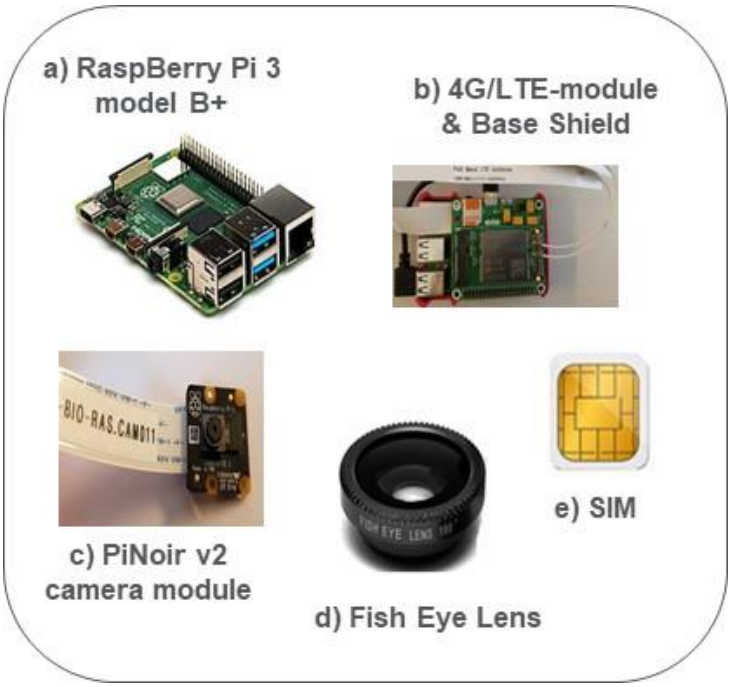

Figure 17: Components of the Raspberry Pi IoT-trap system

The field experiment succeeded and the IoT device performed as it should. When this is established all the investigations regarding cyber security were based on further studies with the datasheets of the Raspberry Pi and the literature.

4.1.3 ESP32 microcontroller based IoT trap

The ESP32 microcontroller is a key component of the second IoT trap system that is developed. ESP32 is commonly used in IoT projects since it is an inexpensive, low-

power consumption system and is integrated with Wi-Fi and dual-mode Bluetooth. The microcontroller is generally used in IoT applications ranging from home and industrial automation, Smart Farming and health care applications. The trap performed very well in its function as a remote sensing and monitoring device and proved to be an alternative system to the Raspberry Pi.

The ESP32 is a commonly used open source microcontroller in IOT applications in Smart Agriculture including Smart Farming, Smart Greenhouses, Smart Irrigation and Agriculture robotics. Compared to the Raspberry Pi, the ESP32 is a microcontroller that is more of an integrated circuit like a personal computer. It receives input, processes the input, and generates an output. As a microcontroller, the ESP32 which is open source, gives much more access to its hardware compared to the Raspberry Pi which required extra effort; through the software application programming interfaces (APIs). ESP32 also uses a system a SoC architecture with integrated CPU, RAM, Wi-Fi, Bluetooth and controllers on a single chip. As an efficient single purpose device, it had good timing though the user interface was with external systems. The Figure 18 below indicates the components that made up the ESP32 IoT trap system.

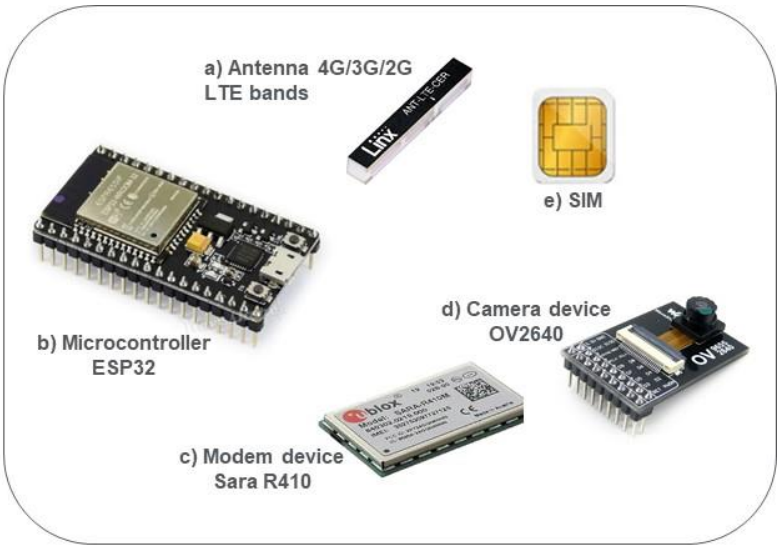

Figure 18: Components of the ESP32 IoT trap system

The ESP32 microcontroller gives the user full and direct access to hardware compared to the Raspberry Pi. The datasheet, websites and literature are used to make further analysis regarding cybersecurity vulnerabilities.

4.1.4 Designing for a future ecosystem with IoT-based systems

An important goal in this project is also to study the prospects of having a series IoT based nodes of insect pest traps feeding information which will be aggregated in a platform as illustrated in Figure 19 below.

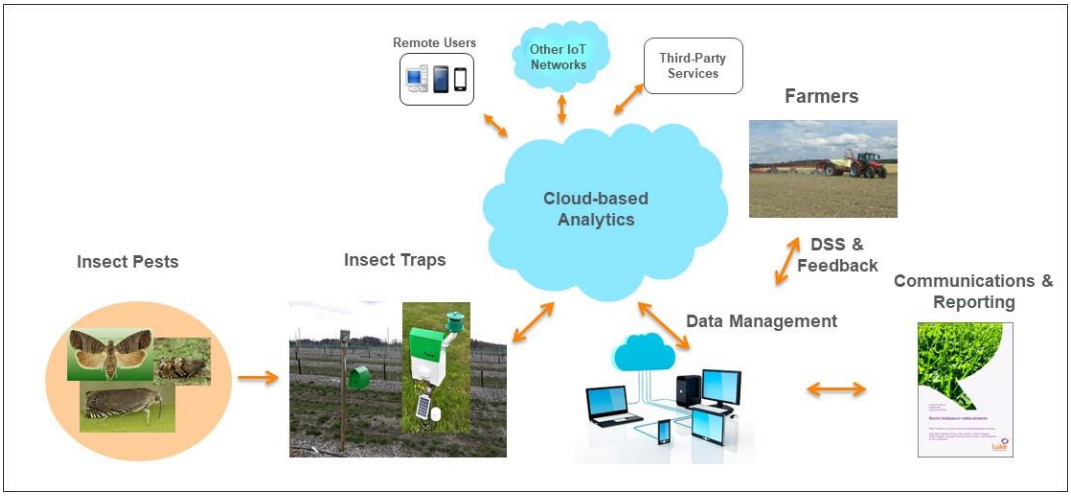

Figure 19: Insect pest IoT ecosystem

The field experiments were made up of a combination of elements to address the research questions. The other elements such as Decision Support System (DSS) are for a future environment when we have an integrated platform with agricultural data (AgriHub, 2020).

4.2 IoT Security Testing and Scanning

The IoT modules were investigated to detect the vulnerabilities by taking a holistic approach from the module and hardware level to the overall system level which is linked to the Internet. The IoT trap system is not connected to the Luke network but is an isolated system connected to the Internet through 4G/LTE GPS SIM card. The IoT modules were separately scanned using a Kali Linux in VirtuaBox using some simple scanning techniques with *Nmap* and *OpenVas*.

Publicly known cyber security vulnerabilities related to IoT were investigated with Mitre Corporation's CVE and NIST's NVDE databases. The OWASP (2017) was studied to better understand components and modules created by software developers to impede known vulnerabilities and apply application defenses. Shodan, the specialized search engine to explore the Internet for connected devices, was used to detect potential IoT-device vulnerabilities. It is a free and easy to use search engine that checks devices ports, hauls resulting banners and indexes the IP addresses.

4.2.1 Raspberry Pi

The Raspberry Pi 3 Model B+, being a compact computer, was used to create an IoT device but also to learn aspects of penetration testing and sharpen scanning skills. It is small computer containing the basic elements of a computer such as a processor, memory, graphics processors, Wi-Fi Bluetooth and Ethernet. According to the Raspberry Pi (2021) datasheets, it does not have very strong cybersecurity protection by default and is often used for building simple home appliances or used in small networks. This was an important part of this study to investigate and ensure how to improve its security features to protect the IoT system based on the Raspberry Pi.

The Kali Linux OS within VirtualBox was installed on Raspberry Pi to perform some simple single host scanning, cracking WPA/WPA2 and creating Wordlists. First the scanning tool *OpenVas* was installed, the configurations were constructed and finally the vulnerability scanning was executed. The *OpenVAS* (Open Vulnerability Assessment System) scanner v20.8.1 is created and supported by Greenbone Networks was executed within VirtualBox virtualization system.

4.2.2 ESP32 microcontroller

No experiments were designed to test the vulnerabilities on the ESP32 microcontroller. However, an extensive web-search was done to investigate the current situation with the ESP32 IoT device. It is noted that Espressif IoT devices are prone to WiFi vulnerabilities where devices connected to networks can be crashed.

There were, according to a CVE search 4 reported vulnerabilities. Three were WiFi vulnerabilities Zero PMK Installation (CVE-2019-12587), Beacon Frame Crash (CVE-2019-12588) and Extensible Authentication Protocol (EAP) client crash (CVE-2019-12586), while one was an ability to read the contents of read-protected eFuses in the bootloader (CVE-2019-17391). The last attack requires an attacker to have physical access to the device.).

The SOC of the manufacturer Espressif, issued revisions after monitoring the microcontroller's security situation. Espressif (2020) had this to say “Security experts have lately explained a fault injection attack on ESP32, that possibly follows as security concession and unplanned leakage of information. ESP32’s security design though continues to stay protected for most of the products.” The manufacture has issued firmware changes and update for these known vulnerabilities.

4.3 Literature review conclusion

The comprehensive literature review was accomplished in conjunction with the case study to have an in-depth grasp of the cyber security implications of the new IoT trap system. It is stated here to merely emphasize all the aspects of this literature review during the research that are relevant to IoT and farming.

This included books, journals and articles in paper and web sites, discussion forums and on-line shared videos in electronic form. A list of relevant research papers concerning IoT in Smart Farming and their vulnerabilities were collected. The publicly available Google Scholar and IEEExplore database were queried to identify relevant publications. The review was part of the close reading of relevant scholarly sources to create a schema of current information to investigate and pinpoint relevant theories, methods and gaps in the existing research.

A thorough library search of the latest and relevant publications in the field of cyber security, agriculture and IoT was performed. Several months were spent in critically analyzing and evaluating the sources. Suitable themes were identified for analysis, synthesis and critical evaluation of the subject.

This Internet media being extensive and real-time was remarkably robust and fast in delivering the latest knowledge. The information was gathered from cyber security and IoT standardizing organizations, databases, chatrooms, wiki pages, blogs, forums and communities. The relevant information from the sources visited were critically analyzed for reliability and integrated into this work wherever applicable. Shodan is a useful search engine to find IoT and other devices connected to the Internet. Shodan information is crossed with known exploits databases such as NIST's NVDE, Mitre Corporation's CVE, and OWASP overview of cyber security vulnerabilities.

5 Results

5.1 Findings of IoT trap system case study

The findings of the research are focused on the:

- general operations of the IoT-based trap system,
- investigations in cyber security of IoT modules in remote sensing system, and
- IoT cyber security related literature reviews

The Figure 20 below depicts and summarizes these actions.

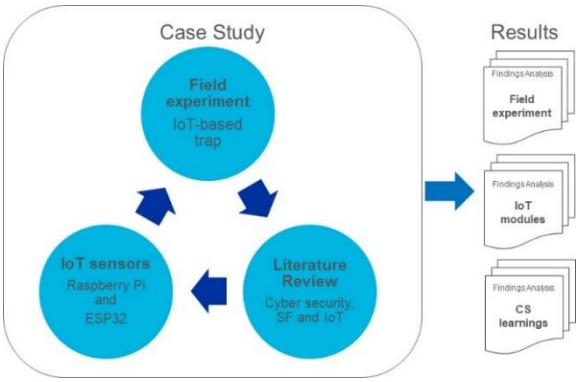

Figure 20: Synthesis of research results

5.1.1 Field experiment discoveries

The field experiment succeeded in several aspects with good results while it had some challenges in certain other respects as shown in the Table 7 below.

Table 7: Findings from the field experiments

#	Issue	Finding
1	Data sensing	IoT module able to sense data at specified time
2	Data capture	Camera module captures images at specified time
3	Data connectivity	IoT sensor establishes connection to the cloud
4	Data transport	TCP data transmission is secured
5	Data acquisition	Remote computer receives and stores the image

The IoT modules both Raspberry Pi and ESP32 were able to sense and capture data as per the requirements. There were some connectivity issues with the ESP32, but it was sorted out with some adjustments to the settings and pin configurations. The Raspberry Pi had no issues and worked well to deliver the data till the end point. The biggest challenge was with the power as its power consumption was high. An additional power bank and a solar panel was used to ensure enough power supply. The ESP32 was very efficient with power and did not need extra power sources.

5.1.2 IoT module and system investigations

Raspberry Pi results

The Pi is used to efficiently build trap systems showed in Figures 15 and 16. A key study here is related to the security features of the Pi trap system to test and ensure security built on the Raspberry Pi Model 3+ block diagram as shown in Figure 17.

The trap system is connected through the router SSH firewall and not directly connected to the Internet through some basic security changes. Some of the subsequent fundamental steps that were tested and studied were:

- Changing of default password by using the command line *passwd* application.
- Changing username to make the Raspberry Pi even more secure.
- Making *sudo* requiring a password since our trap system is exposed to the Internet and to test extra protection though further credential requirements.
- Ensuring latest security fixes by ensuring our version of Raspberry Pi OS has all the latest security fixes and checking for known CVE's from time to time.
- Improving SSH security as it is used to remotely connect to the trap system and enforcing username/password pair for extra security.
- Installing a Firewall by using the default firewall tool in Ubuntu, *ufw* command line.

In addition to the above steps, there are some very important best practices that will be important to do on a continuous basis such as system backup, checking logs

frequently and staying informed about cybersecurity vulnerabilities. This information is tabulated in Table 8 below:

Table 8: Lessons learned with the Raspberry Pi (https:/www.raspberrypi.org)

#	Action	Command line	Notes
1.	Changing default password	sudo raspi-config passwd xxxxxxxxxx sudo adduser Ganeas	Raspberry Pi comes with default username *pi.* The pi user is a common brute force login with root.
2.	Ensuring latest security fixes and keeping system updated regularly	apt install openssh-server sudo apt update sudo apt upgrade	A daily *cron* job, to ensure the latest SSH security fixes and frequent CVE check: https://cve.mitre.org/index.html
3.	Improving SSH security (changing SSH default port 22 to something else, e.g. xxxx)	sudo nano /etc/ssh/sshd_config #Port 22 -> Port xxxx	sshd_configuration is altered to allow or deny specific users.
4.	Installing a firewall	sudo apt install ufw	'Uncomplicated Fire Wall' (ufw) is installed on our Raspberry Pi.
5.	Unnecessary services were removed	sudo service <service-name> stop	To avoid breaches by an attacker.
6.	Backup of system	Correct and regular system backup	A major consequence of any attack, so this is very good practice.
7.	Checking logs regularly	/var/log/syslog	This is very good practice to detect suspicious activity.
8.	Staying Informed about cybersecurity	CVE Details, Exploit DB, NVD Feeds, etc.	This is very good practice.

The prototype that was developed for the case study was a trial, and the learnings will be used to improve the IoT modules for the next field experiments which will have higher security requirements than what was provided by the Raspberry Pi.

ESP32 microcontroller results

The goal was to test and learn the many different issues when working with these new IoT devices and the implications they may have for security. There was frequent use and check made in the CVE list of publicly known cybersecurity vulnerabilities records including using the NVD and the Exploit DB. There are several latest CVEs as listed in the NVD database and frequent checks will be important when developing prototypes.

- CVE Details (https://www.cvedetails.com/)
- Exploit DB (https://www.exploit-db.com/)
- NVD Feeds (https://nvd.nist.gov/vuln/data-feeds)

The CVE and NVD are both good sources of standardized information locators in a rapid and correct manner that comes from diverse information sources, while the Exploit DB is a resource and store of exploits and vulnerable software.

5.1.3 Cyber security and IoT learnings

The research is a study that started with the age-old human endeavor of agriculture and its transportation into the inner world of new technologies. IoT is this transport mode that however is vulnerable to the dark threats of cybersecurity and the lurching risks. It involved all the three major phases of the study; agriculture, IoT and cybersecurity. The new concept of Smart Farming encompasses all these three different aspects. Through that, it carries with it the burden of enjoying all the benefits and opportunities offered by modern ICT while at the same time having to inevitably deal with the challenges of cybersecurity threats. The major challenges for IoT based Smart Farming will be in the implementation, connectivity and maintenance of the IoT systems (Gupta, 2020) that are based on micro-electronics.

5.2 Analysis of IoT trap system and cyber security

The IoT based end-to-end trap system that was developed worked as planned with a few challenges that were overcome with some effort. The original development plan did not include a requirement for cyber security. It is in fact the focus of this research to develop such a requirement checklist for future prototype developments. This was accomplished with the investigation of the IoT modules and the end-to-end system, and the comprehensive literature review of IoT and cyber security.

5.2.1 Challenges of using IoT in a trap system

There is continuous change and development in ICT, and this is not new to the agriculture sector. On the contrary, the sector embraces the new opportunities that ICT offers and will continue to enjoy the benefits that it brings. The case study with the insect pest trap system, albeit being a small area within IPM and the overall agriculture sector, is a highly important one as the discussions by Farooq et al. (2019) in chapter 3 illustrate.

The IoT based trap system protypes were further analyzed in terms of cybersecurity and what it means for farming platforms. IoT security is concerned with safeguarding connected devices on the internet and preventing unauthorized use or access. The analysis based on the two different IoT sensors, raspberry Pi and ESP32 microcontroller, reveal the following findings shown below in Table 9:

Table 9: Basic best practices of IoT in connected devices

#	Issue	Finding
1	Firmware	Patching the IoT devices
2	Good practice	Changing default password of devices
3	Data	Exercising caution with putting data on the internet
4	Mitigation	Attack defenses, e.g. with DDoS protection services
5	Network access	Restricted to Internet exposed IoT devices

The field experiments were to test and learn the many different issues when working with these new IoT devices and the implications they may have for cybersecurity.

In the agriculture sector there are multiple applications, protocols and prototypes. The new ICT assimilation of technology and farming applications are motivated and steered by data that is earning more appeal from the benefits they bring and a potential to meet the growing demand for the global food supply (FAO, 2020). There is constantly new research, as in Luke, to make full use of the potentials offered by ICT and its smart technologies in the food system supply chain (Luke, 2020)

5.2.2 Vulnerabilities posed by IoT in the system architecture

Agriculture is becoming vulnerable to cybersecurity threats with the use of IoT devices. The survey by Farooq et al. (2019), clearly shows the strong security challenges originating at the physical layer down to the application layer. Each layer introduces attack surfaces that can be exploited through the potential vulnerabilities. The analysis of the case study clearly shows that challenges exist from hardware to networks and eventually to the platforms. The ambition is to take advantage of the new possibilities of these IoT devices whilst still being vigilant.

The growth in IoT technologies within the agriculture sector has been a strong impetus for Smart Farming, influencing IoT network architecture, platform, topology and protocols as outlined by Farooq et al. (2019). There is strong demand from farmers and agricultural companies for data analysis and larger production efficiency that IoT sensors can influence positively. Insect pest infestations is a growing problem and the IoT based trap system development is important as in Luke (2019).

5.2.3 A holistic view of IoT challenges in the digital platform

The technological growth in the agriculture sector, particularly in Smart Farming, is gaining more acceptance and IoT-based solutions are being developed so that they enable an aggregation of agriculture services to the farmers and other interested stakeholders. Currently there are some online platforms that aggregate and provide

useful services to farmers. IoT-based platforms are growing by providing farming solutions to users (particularly the farming community) to help increase productivity as in the case of AgriHub (2021). Many forms of monitoring devices, such as insect pest traps, will eventually become a collection of nodes providing the data required to analyze and alert the user of the system by providing useful infestation information. As stated by Farooq et al.(2019), several agricultural servers, gateways and databases will play a critical function to accumulate farm registers and dispense requested utilities to approved users.

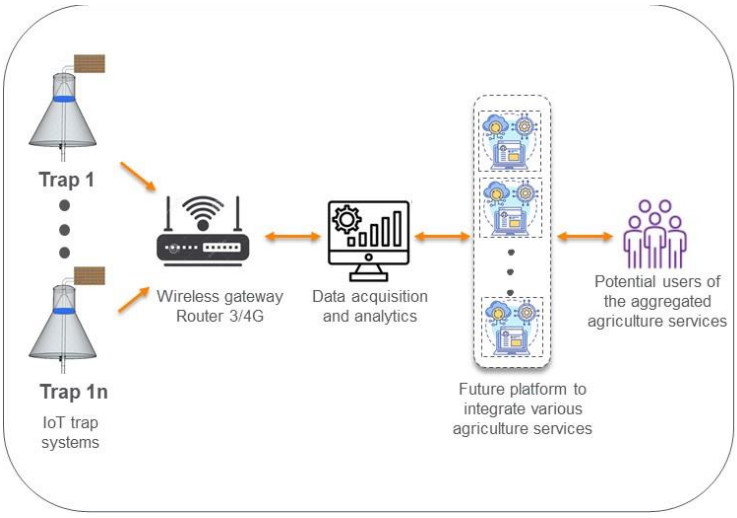

Figure 21: IoT-based trap system as a part of the future agriculture platform

This is a future scenario of Smart Farming and IoT-based technologies as illustrated above in Figure 21. A simple trap system, when enhanced with IoT-based sensors immediately becomes a powerful entry point and a potential source of concern in terms of cyber security. This concern has been recognized by many researchers (Ray 2016, Farooq et al. 2019 and Gupta, 2020).

6 Discussions

6.1 Main findings of research

The findings of the research are centered on the twofold goals of the case study:

- investigation of the cyber security of IoT modules in remote sensing system, and
- literature review of IoT cyber security challenges in the agriculture sector

The results help to rationalize the main research question of the study, “what are the cyber security requirements for an IoT based insect pest monitoring system”. In addition, the results also help to give guidance on possible cyber-attacks in Smart Farming, hypothetical threat scenarios and mitigation efforts to minimize these attacks. The overall scheme of the process is displayed below in Figure 22.

Cyber security issues are a major part of ICT that is not going to disappear and will happen simultaneously with technological developments. IoT will bring forth these vulnerabilities despite the phenomenal technology, partly due to its own shortcomings. As reported by Smith (2017), IoT modules are cheap and in abundance but enhancing their security capabilities may hamper this advantage for a mass-produced product and put pressure on its pricing. The lack of global IoT standards, as noted by many authors (Bagha (2015); Gartner (2017); Kohnke (2017)) means that the industry contributes to the complexity for users in their selection process.

The case study and analysis has made the following findings:

- That developers of IoT systems like the traps system, need to exercise caution when introducing IoT into the system
- The people involved in such IoT deployment projects need to have enough knowledge and training in cyber security principles
- The project needs to have an in-depth implementation plan and a business case
- A requirements checklist as developed in this study to review the requirements
- An understanding of security threat and attack scenarios and their mitigations
- All new technologies, including IoT come with risks, but having an overall understanding of security risks in both device and network side is important.

The findings and analysis of the case study demonstrate the need for a systematic and good understanding of cyber security and IoT. A list of high-level guidance and requirements checklist is generated for developers to help improve the security level of IoT trap systems. It helps to first focus on the easily attainable goals to start with.

The research helped to investigate and generate many important findings in:

- IoT module and end-to-end data collection, processing and analysis technologies
- Cyber security and its threats within and IoT environment
- Learning the importance of modern technologies and cyber security risks
- New IoT requirements to create trap systems with better cyber security defense
- General guidance to deal with cyber security awareness and training

The research question was to create the guidance and a set of requirements for developing IoT-based trap systems. The case study enabled a journey into the intricacies of cyber security through the concrete case of the IoT modules. These efficient IoT modules are lacking in strict quality controls and safety regulations as noted by Sicaria (2015) and continue to pose many security challenges in open fields.

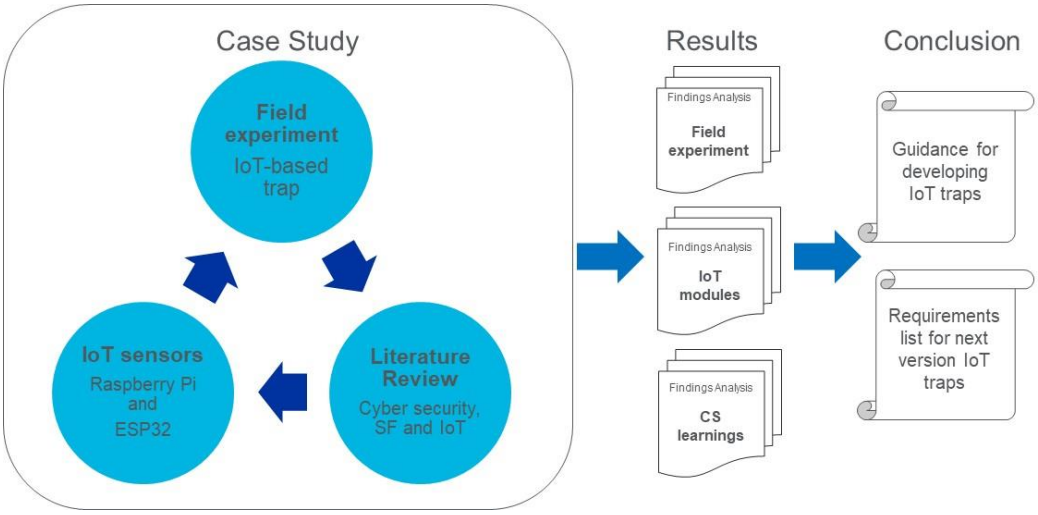

Figure 22: Overall conclusion of the research

As pointed out by the research in Chapter 3 of the literature review, there is a general shortcoming of security of IoT devices caused by widespread shortage of

standards, compulsory guidance and legislative acts to regulate IoT security. IoT devices are essentially insecure as they were built to capitalize on its enormous benefits and opportunities that it provided. The farming sector outside the huge commercial farms is still traditional and operates on tight budgets. IoT devices are appealing, even for research purposes of this study, because they are typically focused on being inexpensive, usability and handiness as preferences above security.

However, the study also reveals that prudence will be key over taking rash decision. The IoT system with its simple processing capabilities and functionalities may not be more secure than the Internet in general as it encompasses it. There is acute need to secure first the internal IoT ecosystem including the surrounding networks. In addition to basic care in setting up the environment, there is growing need to use the new and emerging technologies together with ML, AI, fog and edge computing, and blockchain. This is a continuing area of study for developers of IoT systems to be well informed and knowledgeable.

The study shows that developing the insect pest trap system takes advantage of remote access as a crucial reason for adopting IoT. So, the devices using modems and cellular data connectivity to the Internet must be secured. Due diligence needs to be given to identify and check the equipment and update default credentials.

Finally, the use of ICT and IoT also mean that the agriculture sector continues to indulge and reap the benefits of these new tools and methodologies. The end-result as envisaged today is that all new data made readily available have a potential to end up being used in new services bundled together in future agricultural platforms like the AgriHub (2020), that will benefit the farming community.

These agriculture platforms will also be an attraction for cyber criminals internationally for thieving data, cash, intellectual property, trade secrets and other assets. According to Barreto et al. (2018), “companies and other stakeholders need to empower and endorse initiatives and policies that will be crucial in protecting IoT and ICT systems”. It will be an ideal playground and attack surface for would be cyber criminals who will attempt to exploit the security related vulnerabilities that emerge.

6.2 A requirements checklist for IoT project developers

The requirements and guidance checklist are the outcome to the main research question as summarized by the Figure 22 above. The objectives of developing a guidance for future IoT-based trap systems for developers of IoT solutions can be stated in general terms as follows:

- To elevate the cyber security familiarity and knowledge of IoT technology,
- To assist creators to integrate common IoT security best practices,
- To provide checklists for developers to verify their IoT solutions,
- To build unanimity for feasible operations across the IoT ecosystem, and
- To install secure IoT product and service lifecycle management.

When developing an IoT-based trap system in the farm environment, a measured and prudent effort is required. The requirements checklist highlights the need to invest the time and effort to implement adequate measure that can alleviate risks and shun unwanted outcomes. The guidance is grouped, as in Figure 23 below, according to organization, operation, processes, people, technical, statutory and standardization. This classification helps to focus the requirements on all the main operational areas in an organizational setting, thus making it a living and active document that can be improved.

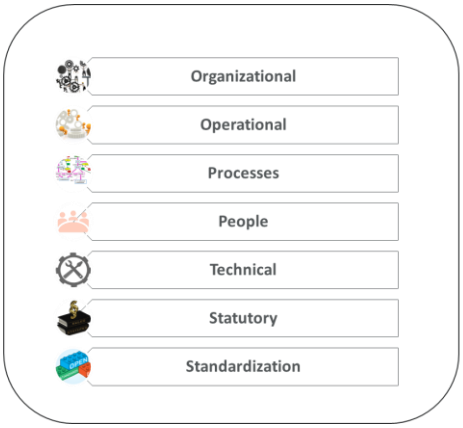

Figure 23: Categories for IoT developers' guidance

The key areas for each of the categories are elaborated based on the findings. The focus, as can be seen, is on technical aspects. The developers shall apply the requirements that are described in a concise manner in the Table 10 below.

Table 10: Requirements checklist for new IoT project

Category	Key Area
Organizational	☐ Set cyber security goals, and ☐ Create a business case
Operational	☐ Perform a gaps analysis: “As-Is” to “To-Be” ☐ Develop the transition plans (roadmap) ☐ Continuity planning and management
Processes	☐ Define policies, guidelines, and procedures for cyber security ☐ Define the device management processes for hardware (HW), and ☐ Define the device management processes for software (SW)
People	☐ Develop cyber security awareness, education, and training plan ☐ Develop skills competence development, as scanning techniques
Technical	☐ Develop a cyber security architectural model ☐ Explore IoT technologies and security implications ☐ Develop overall strategy – purpose and functions ☐ Perform the vulnerabilities and threats impact analysis ☐ Create LCA map for software, hardware, and system ☐ Perform interoperability analysis between devices ☐ Define use-cases and user scenarios ☐ Create attack scenarios - implications and assets affected ☐ Perform risk assessment - map likelihood and impact on assets ☐ Plan mitigations and countermeasures (as recovery times) ☐ Identify physical constraints – weight and dimensions ☐ Design the operational technical environment ☐ Identify power requirements and constraints ☐ Plan for connectivity and wireless requirements ☐ Plan for the different IoT sensor requirements ☐ Identify the processing capacity and limitations ☐ Establish the visualization and display needs
Statutory	☐ Harmonize compliance requirements, liabilities and mitigations
Standardization	☐ Review global standards regularly ☐ Review training and continuous upkeep

The agriculture sector is a large but sensitive sector to cyber security threats where the mitigation and countermeasures need to be ongoing research. As stated by Demestichas (2020), cyber security mitigation measures against security threats and attacks is an evolving field. New technologies emerge in AI, ML and other improved security measures.

The broad literature review and a comprehensive guidance and requirements checklist was developed to avoid the dangers and potential mitigations when developing the IoT-based insect-pest system in general. The organizations' continued operations are anticipated and shielded with proper continuity planning.

6.3 Hypothetical cyber-attack scenario's and their usefulness

An IoT attack surface is the total sum of potential security vulnerabilities that can be exploited for a security attack in devices related to software framework in a network, either local or the remote Internet (OWASP, 2017). The availability of attack surfaces pose a significant threat where an attacker can leverage to execute malicious activities (Enisa, 2019). The findings from literature review show a variety of different types of attacks where different attack surfaces are targeted to exploit the vulnerabilities present in the IoT.

The scenarios describe the interaction with the IoT system to help focus the developer of the design efforts based on the requirements checklist. This is a key part of the study to assist in strengthening the IoT insect pest trap development project work to define critical attack stages and develop plausible scenarios to discuss the impacts and responses. In so doing, it also acts as an important analysis and learning tool to develop mitigation activities and contingency plans for possible cyber-attacks.

The threats in cyber-security environment can also change rapidly with changes in new developments in the farming sector. The study of these hypothetical scenarios, though not fool-proof, enable developers to be more adaptive and make informed decisions in the face of security threats and uncertainties. They offer a glimpse into the emerging attack scenarios and trends of the future. Continuous training and

learning possibilities to be familiar with the current threat scenarios and real cases in IoT exploits will be very useful for the developers of the new trap system.

6.4 Mitigation efforts to minimize potential cyber-attacks

The mitigation efforts in IoT trap system development project is to be based on a set of actions taken to reduce or help to eliminate threats and the impacts. Executing mitigation activities will help achieve the project goals. Understanding and reducing the vulnerabilities to threats, based on the threat scenarios, will form the basis of the project plan. As the literature review has shown, any connected IoT device can be hacked, causing disruption to the functionalities of the device and inflict possible ill-effects and loss of data. Mitigation efforts refer to policies and processes to help protect against such disruptions and limit the extent of the attack to recover.

IoT trap development will require the requirements checklist to be reviewed systematically. Luke networks are managed by government ICT center, but when introducing IoT modules the staff have the responsibility to be extra attentive with appropriate user behavior. Mitigation will help reduce and stamp out the need for future fire-fighting actions. It is based on awareness raising, and education for better understanding of vulnerabilities and threats, and basic cybersecurity defenses. The organization needs to have a general cyber security readiness culture supported by effective best practices and policies. Basic cyber security training needs to be a part of competence development of every employee for direct improvement measures.

Iot-based systems must follow basic housekeeping; strong passwords and default password updates, firmware updates and blocking open ports. The knowledge of malware, social engineering and phishing attacks need to be essential for developers of IoT systems. The requirements checklist embeds good knowledge of the risk factors and perform risk assessment, and quick and light audits on a regular basis. This is to check the system and help detect and reduce the number of security incidences. Firmware updates and patching needs to be a part of the security practice. Periodic assessment of the devices in the open crop fields need to be arranged, although this is a challenging exercise that needs further research.

The development of new technologies in ML, AI, fog and edge computing, and blockchain are open future research topics that are watched by the sector as it takes more interest in IoT-based systems. The evolution of these new technologies and techniques will be important in the mitigation of cyber security attacks of the future.

6.5 Operational readiness in IoT development project

An essential component of the requirements checklist and guidance is to ensure endurance through continuity planning to preserve organizational operations in the face of system vulnerabilities . As stated in section 3.5, the BCP framework commonly invokes mitigation, preparedness, response, and recovery. IoT developers need an outline about these events when dealing with possible attacks.

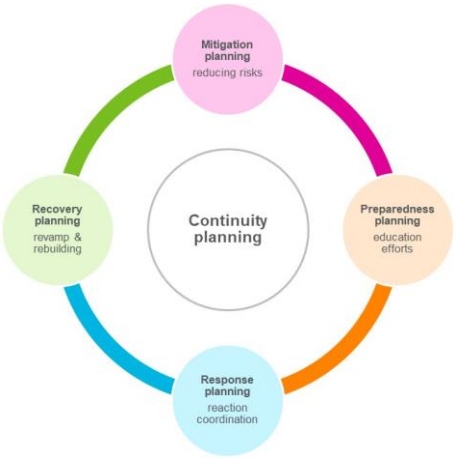

Figure 24: Types of cyber-attack planning

Mitigation efforts as discussed in Table 6, are directed to reduce the potential impact caused by various attacks by identification and risk assessment. Planning preparedness embodies a wide range of activities around training, cyber exercises, scenario planning and information sharing (Enisa, 2019) to encourage overall resilience to cyber risks. Response planning incorporates incident response, crisis communications and directions by SOC rapidly and efficiently. The planning covers taking essential steps to deal with the consequences, to rebuild and strengthen the capabilities and to manage cyber risk by adopting NIST critical security controls.

7 Conclusion

The goal of this study was to create a new set of cyber security requirements to better enable IoT-based insect pest trap system development of the future. Research began with a general overview of the new ICT technologies in the farming sector and the need to advance Smart Farming and reap the benefits it brings. The emerging security threats that come together with ICT and IoT-based technologies raise many questions about the preparedness in the sector for dealing with these challenges. As the discussions have shown, cyber security knowledge is extremely crucial for all developers of IoT-based systems. Organizations need to be prepared to provide more cyber security training and take a professional approach to ensure that developers have the needed information and skills. Investigating hypothetical threat scenarios and the mitigations raises the general awareness and education of developers of the new IoT-based systems. Contemporary cyber security skills will improve the IoT readiness.

The new requirements checklist was developed by a comprehensive study of theory and the practical case study by considering the looming threats of cyber security. The Raspberry Pi and ESP32 IoT modules of the case study were a valuable source of learning about IoT security that provided a focal point to investigate the challenges of security vulnerabilities and threats. There are various Smart Farming developments where IoT will play a key role. The new guidance and requirements are a benchmark of the current situation and is hoped that it will help improve the new Luke projects which will be better prepared to deal with cyber security matters. As new technologies emerge, efficient and better AI and ML techniques will have an impact in the future. But unfortunately, criminal activities will lurk in the shadows as more agricultural data is digitalized for better access and made accessible in future platforms. The readiness to meet the cyber security challenges will be crucial.

The discussions in Chapter 6 show how it helped contribute to the creation of the set of requirements for future prototype development. In that aspect, the goal has been accomplished. The next interesting question is how we meet the security challenge of the rapid pace of IoT development in terms of technology and uptake by the

agriculture sector. These IoT devices will continues to pose many challenges as they potentially stay insecure for a very long time to come, if not forever.

The case study of the IoT trap system gave an extensive opportunity to gaze into the inner workings and intricacies of cyber security and the myriads of possibilities for a thief to do harm by exploiting the vulnerabilities of a system.

Despite the unavoidable need and allurement to transform the agriculture sector with the immense possibilities that were once unthinkable, a certain degree of old-fashioned, calculated and knowledgeable vigilance is vital when designing and adopting new technologies and tools for the years to come. The farming sector will remain susceptible in comparison to other sectors that enlist electronic tools, simply because of the vastness of the area and that ICT is just a means to an end. Cyber security guidance and mitigation of threats will be an open research theme for a long time to come.

The key learnings are that the sector exercise caution as it adopts IoT in its improvement plans and operational continuity planning activities. IoT-based development projects need to plan and develop in a stepwise and systematic manner from the operational perspective. But they also need to invest in time and effort for traditional due diligence to develop a good business case and a set of requirements. Transforming the agriculture sector to modernity is going to take much more than new equipment and technologies; it will also mean being cyber security savvy.

Acknowledgement

I wish to thank JAMK for opening this whole new world of cyber security. I want to thank my supervisor Tero Kokkonen for his support and valuable comments. Finally, I want to thank my dear wife for her support and letting me off the hook with family duties while working on the thesis. And now that this is done, it will be payback time!

References

Aaltonen, M. 2019. *IoT-tekniikalla tuholaisseurantaan*. Puutarha-Sanomat 4/2019.

AgriHub, 2021. https://www.luke.fi/en/projektit/agrihubi/

Andrew, C. and Hildebrand, P. 2018. *Applied agricultural research - foundations and methodology*. Routledge.

Bagha, A. and Madesetti, V., 2015. *Internet of Things: A Hands-on Approach*, Universities Press.

Barreto L. and Amaral A., 2018. "*Smart Farming: Cyber Security Challenges*," 2018 International Conference on Intelligent Systems (IS), Funchal - Madeira, Portugal, pp. 870-876, doi: 10.1109/IS.2018.8710531.

Bleeping, 2019. https://www.bleepingcomputer.com/news/security/medical-iot-devices-with-outdated-operating-systems-exposed-to-hacking/

Bloomberg, 2020 https://www.bloombergquint.com/global-economics/mountain-pine-beetle-infestations-are-killing-forests-could-worsen-emissions

Castrignanò, A. (ed.), 2020. *Agricultural Internet of Things and Decision Support for Precision Smart Farming*, Academic Press.

Cheruvu, S. 2020. *Demystifying Internet of Things Security: SuccesSmart Farmingul IoT Device and Platform Security Deployment*, 1st ed., Apress.

CVE, Mitre. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=esp32

Dawei, W. et al., 2019. *Recognition Pest by Image-based Transfer Learning*. J Sci Food Agric; 99: 4524–4531.

Dell Technologies Research, 2020. https://corporate.delltechnologies.com/en-us/newsroom/announcements/detailpage.press-releases~usa~2020~03~20200309-dell-technologies-survey-cyber-attacks.htm#/filter-on/Country:en-us

Demestichas, K., Peppes, N., Alexakis T. 2020. *Survey on Security Threats in Agricultural IoT and Smart Farming*. Sensors. 2020; 20(22):6458.

Elijah, O et. al., 2018. *An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges*. IEEE IoT, Vol.5(5), pp.58-73.

ENISA (European union Agency for Cybersecurity), 2019. *Good Practices for Security of IoT* https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

ESP32 Eco v3 *User Guide*, 2020. Espressif Inc. https://www.espressif.com/sites/default/files/documentation/ESP32_ECO_V3_User_Guide__EN.pdf

FAO, IFAD, UNICEF, WFP and WHO. 2020. *The State of Food Security and Nutrition in the World 2020. Transforming food systems for affordable healthy diets.* Rome, FAO. *https://doi.org/10.4060/ca9692en*

Farooq, M et al., 2019. *A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming*. Article in IEEE Access, Vol.7, pp.237-271.

Ferrag, M.A., Shu, L.; Yang, X., Derhab, A., Maglaras, L. 2020. *Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges*. IEEE Access 8, 32031–32053.

Gartner Report, 2019. *Leading the IoT*, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Guardian, 2020. https://www.theguardian.com/world/2020/jan/26/kenya-suffers-worst-locust-infestation-in-70-years-as-millions-of-insects-swarm-farmland

Gubbi, J et al. 2013. *Internet of things (Iot): A vision, architectural elements, and future directions*, Future Generation Computer System, vol. 29, no.7, pp. 1645–1660.

Guest, G. 2012. *Research Methodology: Collecting qualitative data - a field manual for applied research*. SAGE Publications.

Gupta, B and Tewari, A. 2020. *A Beginner's Guide to Internet of Things: Security*. CRC Press, Taylor & Francis Group.

Gupta, M et al., 2020. *Security and Privacy in Smart Farming: Challenges and Opportunities*. Article in IEEE Access, Vol.8, pp.64-84.

Hassija, V., Chamola, V., Saxena, V.,Jain, D., Goyal, P., Sikdar, B. 2019. *A Survey on IoT security: Application areas, security threats, and solution architectures*. IEEE Access.

Huusela-Veistola, E., Jauhiainen, L., 2006. *Expansion of pea cropping increases the risk of pea moth infestation*. J. Appl. Entomol. 130, 142–149.

IoT Security Compliance Framework, 2018. Release 2. IoTSF. https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf

ISO/IEC, 2018. "*Information technology - Security Techniques-Information security risk management*" ISO/IEC 27005:2018, https://www.iso.org/standard/75281.html

ISO/BSI, 2019. *Business continuity management systems requirements*, BS EN ISO 22301:2019, https://www.iso.org/standard/75106.html

Jahn, M. 2019. *Cyber Risk and Security Implications in Smart Agriculture and Food Systems*. White paper. https://jahnresearchgroup.webhosting.cals.wisc.edu/wpcontent/uploads/sites/223/2019/01/Agricultural-Cyber-Risk-and-Security.pdf

Kohnke, A., Sigler, K., and Shoemaker, D. 2017. *Implementing Cybersecurity, A Guide to the National Institute of Standards and Technology (NIST) Risk Management Framework*. CRC Press, Taylor & Francis Group.

Kuppusamy, P. 2019. *Smart education using Internet of Things technology, emerging technologies and applications in data processing and management*, pp 385-412.

Luke, 2019. *Insect pest monitoring by IoT*, https://www.luke.fi/projektit/insectpest-iot/

Luke, 2020. *Emerging digitalization: integrating IoT technologies in food production*, https://www.luke.fi/en/news/greetings-from-projects-session-at-ae2019-sustainable-european-aquaculture-4-0-nutrition-and-breeding-innovations/

Malavade, V.N. and Akulwar, P.K. 2016. *Role of IoT in Agriculture.* IOSR J. Computer Engineering, 56–57.

Manninen, O. 2018. *Cybersecurity in Agricultural Communication Networks: Case Dairy Farms*. Master's Thesis, JAMK University of Applied Sciences, Jyväskylä, Finland.

Ministry of Agriculture and Forestry (MMM), 2014. *FAO State of Biodiversity for Food and Agriculture in Finland.* Report by Ministry of Agriculture and Forestry, Finland.

Niemi, J., Väre, M. 2018. *Agriculture and food sector in Finland*. https://portal.savonia.fi/amk/sites/default/files/agriculture_and_food_sector_in_finland_2018.pdf

National Vulnerability Database, NVD. https://nvd.nist.gov/general

NIST, 2012. *Guide for Conducting Risk Assessments*, SP 800-30 Rev. 1, EPUB.

OWASP, 2017. *Using Components with Known Vulnerabilities* https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities

Pattnaik, P. 2020. *Internet of Things and Analyticyber security for Agriculture*, Volume 2, Springer.

Peng, S-L. 2020. *Principles of Internet of Things (IoT) Ecosystem.* Springer.

Portney, L. 2019. *Foundations of Clinical Research: Applications to Evidence-Based Practice*. 4th edition, F.A. Davis Company.

Raspberry Pi, 2021. https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/

Ray, P.P. 2017. *Internet of things for smart agriculture: Technologies, practices and future direction*. Journal of Ambient Intelligence and Smart Environments 9(2017) 395–420 395, IOS Press.

Sainz, J.R., Martín, S., Diaz, G., & Castro, M. (2019). *Security Vulnerabilities in Raspberry Pi–Analysis of the System Weaknesses*. IEEE Consumer Electronics Magazine. 8. 47-52. 10.1109/MCE.2019.2941347.

Shodan, Search engine. https://www.shodan.io/

Sicaria, S. Rizzardia, A. Griecob, L. Coen-Porisinia, A. 2015. *Security, Privacy & Trust in Internet of Things: the road ahead*. Comput. Netw. vol 76, pp 146-164.

Smith, S. 2017. *The Internet of Risky Things: Trusting the devices that surround us.* O'Reilly Media Inc.

Sulkamo, V. 2018. *IoT from cyber security perspective: Case study JYSECTEC*, JAMK. https://www.theseus.fi/bitstream/handle/10024/151498/IoT%20from%20cyber%20security%20perspective.pdf?sequence=1&isAllowed=y

TrapX Research Labs, 2020. https://finance.yahoo.com/news/trapx-security-identifies-malware-campaign-130000671.html?guccounter=2&guce_referrer=aHR0cHM6Ly9maXJlZG9tZS5pby8&guce_referrer_sig=AQAAACbnQqRP5PIp-_90IvEaLUGsXoYHtLYGR57cHnUMAPKJ3Axv1SvK-ahjeRksi9-DIvjGfe_ixLO-SkfYnmsL-8shVDnZ4sFhqp8MVDIec8_z7le6Xc0-DpmecywFFfJlFTeS-q3U00-qJ0JkTwXZhZBrE2uhbGTxPVj6KJMS6f_t

UK Department for Digital, Culture, Media and Sport, 2020. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020

Viiri Heli, Neuvonen Seppo, 2017. *Changing climate and outbreaks of forest pest insects in a cold northern country, Finland*. https://link.springer.com/chapter/10.1007%2F978-3-319-57532-2_5

Yin, R. 2018. *Research Methodology: Case study research and applications*, 6th ed. SAGE Publications.

Yle. 2020. *Hacked therapy center emailed clients' ID numbers on invoices.* https://yle.fi/uutiset/osasto/news/hacked_therapy_centre_emailed_clients_id_numbers_on_invoices/11618590

Zdnet. 2020. https://www.zdnet.com/article/how-poor-iot-security-is-allowing-this-ten-year-old-malware-to-make-a-comeback/

Zhang, Q, 2015. *Precision Agriculture Technology for Crop Farming*, 1st ed. CRC Press.

Appendices

Appendix 1. Project Business case

Project Business Case			
Project Name	IoT-based Insect Pest Trap System		
Project Sponsor		Project Manager	
Contribution to Luke Strategy	What recommendation or optimization based on the use of the data you will have would be useful for the client? What data needs to be gathered? How responsive will the "adjustments" or optimizations be (specify the time frame)? Will notifications be consistent and fixed, or will it be necessary to configure, update and manage them? What are the consequences of the data not being gathered? What are the consequences of the data being gathered but not transmitted?		
Key issues	Have the cyber security plans been reviewed with the relevant experts? Has the cyber security communicated to the organization? Has a prototype been developed for feasibility testing? Do configuration and API enable integration with other IoT components? Has the project considered Open Source/Proprietary platform solutions? Has the project considered mobile applications for the IoT platform?		
Benefits	What problem are you solving for the end user? What insights would be useful for the end user?		
Timescales	dd.mm.yy - dd.mm.yy		
Costs	What is the operational cost for the operational infrastructure? Have all cyber security software and application costs been considered?		
Expected Return on Investments, ROI	xx € / year		
Risks	Connectivity risks with tele operators for reliable coverage? Complexity of the algorithms? Have the cyber security vulnerabilities and threats been analyzed? Does the project have the required technical skills? Does the project have the right partners? Is it protected against fraud and misuse? *Reference: Adapted from Lukenet.fi*		

Appendix 2. Checklist to review IoT-based solution development

Before choosing an IoT device	▪ Is the device from a reputable or known manufacturer? ▪ Is the hardware tamper proof? ▪ Does the device have multiple access ports (USB, Serial, LPT, Optical)? Are those necessary? ▪ Does a device operate in multiple range? Are those needed? ▪ Is the device built around secure hardware? ▪ Is the firmware and software upgradable? ▪ What level of open source usage is in the product? ▪ Does the device have default usernames and passwords? Can they be changed? ▪ Are the default usernames and passwords common across the entire set?
Before choosing an IoT device Security Management Solution	▪ Is the communication encrypted? ▪ Is every access authenticated and logged? ▪ Does the communication involve internet access? ▪ If cloud components exist, is the Cloud and Cloud operations certified? ▪ Is the data stored securely? Are third parties involved? ▪ Have privacy and audit requirements been met for data and access to data? ▪ Is support available?
During deployment of IoT device/solution	▪ Is the device deployed at secure locations? ▪ Are all the unneeded access ports closed so tampering can be detected? ▪ Is the network planning done and the access rights to the internal network determined? ▪ Is access to the internet determined and understood? ▪ Are vulnerability assessment and penetration testing complete?
During operation of IoT device/solution	▪ Identify in real time all connected devices ▪ Audit and track location, assignment, and other details in an asset management system ▪ Develop deep context on every device ▪ Turn off any functionality that is not needed ▪ Regularly check for default usernames, passwords, change passwords regularly ▪ Understand functionality and control internet access ▪ Control access to network and implement strict segmentation ▪ Monitor that only permitted, authorized devices exist in each segment ▪ Perform regular risk & vulnerability assessment, pen testing and patch updates ▪ Implement strong real time policies to alert on issues ▪ Monitor behavior and Implement tools for real time anomaly detection ▪ Monitor device movement and implement micro-location-based alerting ▪ Monitor operational time of the devices ▪ Ensure proper disposal of devices, remove credentials and access rights for employee, contractor devices once they are no longer in organization. *Reference: Adapted from WootCloud.com*