Dakota State University

Beadle Scholar

Masters Theses & Doctoral Dissertations

Spring 3-2021

A Consent Framework for the Internet of Things in the GDPR Era

Gerald Chikukwa

Follow this and additional works at: https://scholar.dsu.edu/theses

Part of the Databases and Information Systems Commons, Data Science Commons, Information Security Commons, Other Computer Sciences Commons, and the Other Legal Studies Commons

A CONSENT FRAMEWORK FOR THE INTERNET OF THINGS IN THE GDPR ERA

A doctoral dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Science

In

Cyber Operations

March 2021

By
Gerald Chikukwa

Dissertation Committee:

Dr. Yong Wang, Chair
Dr. Kevin Streff
Dr. David Bishop
Dr. Renae Spohn
Mary Francis

DocuSign Envelope ID: 39400895-CF9C-4619-8FBF-BF9B00C329AE

DAKOTA STATE
UNIVERSITY

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Philosophy degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Gerald Chikukwa

Dissertation Title: A Consent Framework for the Internet of Things in the GDPR Era

Dissertation Chair/Co-Chair: Yong Wang Date: March 31, 2021

Name: Yong Wang

Dissertation Chair/Co-Chair: Date:

Name:

Committee member: Dr. Kevin Streff Date: April 5, 2021

Name: Dr. Kevin Streff

Committee member: Dr. David Bishop Date: March 31, 2021

Name: Dr. David Bishop

Committee member: Dr. Renae Spohn Date: March 31, 2021

Name: Dr. Renae Spohn

Committee member: Mary Francis Date: March 31, 2021

Name: Mary Francis

Original to Office of Graduate Studies and Research
Acid-free copies with written reports to library

ACKNOWLEDGMENT

Education has always been something I value in my life, and would like to acknowledge people that have guided and encouraged me to challenge myself. I want to thank my wife Tonna and the kids for their support throughout the time I worked on my Ph.D. There were times that I was not available for them, but they kept encouraging me during times that I felt I could not keep up with the dissertation work.

I want to thank Dr. Yong Wang, my chair, for the support and encouragement. I would also like to thank Dr. Kevin Streff, Dr. David Bishop, Dr. Renae Spohn, and Mary Francis for the support and being part of the dissertation committee.

Finally, I would like to thank my mother, Debra, and my late father, Jimmy, who taught me the value of education and has supported me throughout my educational journey.

ABSTRACT

The Internet of Things (IoT) is an environment of connected physical devices and objects that communicate amongst themselves over the internet. The IoT is based on the notion of always-connected customers, which allows businesses to collect large volumes of customer data to give them a competitive edge. Most of the data collected by these IoT devices include personal information, preferences, and behaviors. However, constant connectivity and sharing of data create security and privacy concerns. Laws and regulations like the General Data Protection Regulation (GDPR) of 2016 ensure that customers are protected by providing privacy and security guidelines to businesses. Data subjects (users) should be informed on what information is being collected about them and if they consent or not. This dissertation proposes a consent framework that consists of data collection, consent collection, consent management, consent enforcement, and consent auditing. In the framework, there are GDPR requirements embedded in different components of the framework. The consent framework can help organizations to be GDPR consent compliant. In our evaluation of the solution, the results show that our solution has coverage over GDPR consent based on our use case. Our main contributions are the consent framework, consent manager, and the consent auditing tool.

DECLARATION

I hereby certify that this project constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the project describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

GERALD CHIKUKWA

Gerald Chikukwa

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction and Problem Statement

Internet of Things (IoT) enables physical devices and objects to communicate through the Internet. IoT adopts the notion of always-connected customers, allowing businesses to collect large volumes of user data to give them a competitive edge. The data collected by IoT devices from users include personal information, preferences, and behaviors. The collected data can be monitored and used to create user profiles by organizations with or without customer consent (Rantos, Drosatos, Demertzis, Ilioudis, & Papanikolaou, 2018). Furthermore, these organizations can make automated decisions based on the collected data without considering technical and organizational measures which ensure the protection and freedom of user rights (Mendez, Papapanagiotou, & Yang, 2017; Roman, Zhou, & Lopez, 2013). The lack of privacy and user control of their data prompted the European Parliament to introduce the General Data Protection Regulation (European Union, 2016), which gives users control over their data.

1.1.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) outlines the basis of lawful processing of personal data and transfers (European Union, 2016). Lawful processing is based on (a) data subject consent, (b) a contract, (c) compliance with legal obligations, (d) protecting the data subject, (e) considering the public interest, and (f) the controller having a legitimate interest (European Union, 2016). The data controller’s responsibility is to ensure that the lawful processing requirements are adopted within their data processing. However, the GDPR focuses on giving citizens control over their personal data while ensuring that data controllers provide security safeguards to the collected, transmitted, and stored personal data. The GDPR offers guidelines on data protection but does not recommend specific security technologies to be implemented, and it does not provide any security or privacy framework.

Article 7 of the GDPR provides conditions of consent as (1) the controller should be able to demonstrate that the data subject gave them consent to process their personal data, (2) the data subjects consent should be presented in a way that is “clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language” (European Union, 2016) (3) the data subject shall be given the ability to withdraw their consent at any time, (4) consent shall be given freely (European Union, 2016). Consent plays a significant part in privacy protections, and it is a mechanism required by the GDPR. For consent to be meaningful, it must follow the conditions of consent presented above; otherwise, it will not fulfill its role. Providing meaningful consent ensures the data subject understands and agrees to data processing (Wakenshaw, Maple, Gomer, & Ghirardello, 2018).

1.1.2 Internet of Things

The rapid growth of the IoT has introduced many threats that affect user’s privacy. Gartner research states that there are 8.4 billion connected devices, while they forecast 20 billion by 2020 (Gartner, 2017). In 2020 there was an estimated 31 billion IoT devices installed worldwide (Maayan, 2020). The increase in IoT devices is attributed to miniaturization, cheap sensors, and inexpensive network devices. Even though some of the predictions are not accurate, IoT technologies are still being adopted by millions of people each year worldwide. There are enormous IoT applications, including smart homes or buildings, smart cities, environmental monitoring, healthcare, smart business/ inventory, product management, security, and surveillance (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012). Obtaining consent from these IoT applications is challenging (Rosner & Kenneally, 2018). There is a need for new innovative mechanisms for meaningful consent in IoT.

The main challenge in obtaining consent in IoT is due to the design. IoT devices often lack screen-based interfaces, which allow users to have ease of access to privacy settings or information on data sharing (Rosner & Kenneally, 2018). IoT device manufacturers usually do not provide detailed information on data collection and privacy. They also do not provide privacy policies within the IoT devices and refer to an external website which usually does not fully address privacy issues associated with the devices (Rosner & Kenneally, 2018). Users of IoT devices, in most cases, are given no choice but to either consent or not use the product. After the user consented, there is no mechanism to withdraw the consent. Manufacturers who design the IoT systems must reimagine how they incorporate informed consent in IoT devices to make them user-friendly (Rosner & Kenneally, 2018). It will ensure users have a complete understanding of what they consent to, what data they are sharing, and how their data is used.

1.2 IoT Scalability

IoT is being adopted worldwide in billions (Gartner, 2017) each year. The increasing adoption of the IoT brings the issue of scalability. There are several factors to consider for scalability, including business, marketing, software, hardware, and networks (Gupta, Christie, & Manjula, 2017).

Methods of increasing resources fall into two categories: horizontal and vertical scaling. Scalability challenges and issues related to resources include the protocol and network security, identity management, access control, and fault tolerance in IoT. Scaling vertically, also known as scaling up, enables increasing existing hardware or software by increasing resources, for example, adding another CPU to increase the processing power of a server. Furthermore, we can vertically scale a system by “adding more processing power, main memory, storage, and network interfaces to the node to satisfy more requests per system” (Gupta et al., 2017). Horizontal scaling allows the ability to increase capacity by adding multiple hardware or software to work together. Examples of horizontal scaling include adding more machines to a system or network resources, for instance, adding a server to a distributed system or software application (Gupta et al., 2017).

1.3 IoT Interoperability

An IoT ecosystem utilizes different devices, platforms, communication protocols, and so on. Various manufacturers build these technologies, and there are interoperability challenges. To solve the issue of interoperability, IoT manufacturers must be willing to collaborate on interoperability problems.

IoT communication systems should provide seamless connectivity in constrained devices. The application layer enables communication for application services. Some protocols operate on the applications layer to support communication amongst IoT devices. The protocols operate in the application layer include Hypertext Transfer Protocol (HTTP), Constrained Application Protocol (CoAP), Message Queue Telemetry (MQTT), Web Sockets, Extensible Messaging, and Presence Protocol (XMPP), Data Distribution Service (DDS), and so on.

(Collina, Bartolucci, Corolli, & Corazza, 2014). IoT devices utilize various communication protocols depending on the topology and standard protocols.

The interoperability problems are due to the heterogeneous nature of IoT devices, characteristics, and technical requirements. If there is insufficient interoperability amongst IoT devices, there will arise technical and business problems. The IoT market and developed IoT systems are not designed to consider cross-platform applications (Mahalik, Narendra, Badrinath, Jayaraman, & Padala, 2016). IoT interoperability is possible if heterogeneous devices and applications operate together regardless of their technical dependencies (Dave, Patel, Doshi, & Arolkar, 2020).

1.4 IoT Security

Security and privacy are essential elements in IoT, although they are also a challenge for the IoT. IoT adoption from millions to billions increases the risk of connected devices being exploited due to cheap, poorly designed devices, weak passwords, insecure ecosystem interfaces, and insecure network services. Security in IoT has not matured, and it is working progress since it is an emerging technology. The IoT supply chain from manufacturers to users also has security challenges to overcome. These security challenges include manufacturing standards, update management, physical hardening of IoT systems, and user knowledge and awareness.

In IoT ecosystem, there are many resource-constrained devices which include sensor nodes and pervasive computing devices that have limited computing power (Gupta & Shukla, 2016). Therefore, traditional security solutions cannot be applied to IoT due to their high memory and computational power requirements. IoT requires lightweight security solutions that work according to its limited memory and computational power. Securing the IoT ecosystem needs to focus on systems, applications, networks, and the cloud. These are the main pillars of the IoT infrastructure, and their security is important. Manufacturers and service providers of IoT products should not treat security as an afterthought, but they should consider it during the product development phase.

1.5 Research Goal

This research aims to develop an enterprise consent management solution within the IoT ecosystem while ensuring compliance with GDPR principles of consent. The proposed consent framework consists of consent collection and management, consent enforcement, and consent auditing.

1.6 Research Questions

1. **How can we collect and manage consent within an IoT application while ensuring compliance with GDPR?**

IoT consent is one of several data privacy challenges in the connected Internet of Things (IoT) devices. Organizations need to provide a privacy policy and obtain consent, usage, and sharing of the IoT devices' data. There are increasing data privacy concerns amongst consumers because connected devices enable companies to collect large volumes of data from IoT devices. GDPR requires organizations to obtain consent before collecting and processing data. Consent under GDPR article 4(11) must be valid, freely given, specific, informed, and active (European Union, 2016). GDPR article 7(1) states that the data controller must demonstrate data subject consent (European Union, 2016). Addressing these GDPR requirements allows organizations to be GDPR consent compliant in their IoT implementations. Genestier et al. (2017) and Rantos et al. (2018) proposed solutions that lack informed consent and an intelligent component to assist users in making the right decision before providing consent. The consent management components are designed to capture consent, but they do not follow all GDPR consent requirements. Addressing these research limitations in the literature will help us answer this research question. It is essential to ensure any IoT application to comply with the GDPR.

2. How can we enforce the collected consent?

Collecting and managing consent is essential; however, enforcing the collected consent is crucial and beneficial. Consent enforcement allows the data controller to use the collected consent in their IoT implementation to regulate access to what the user agrees or disagrees on when they provide their consent. Heinze et al. (2011) proposed the consent management suite solution that uses eXtensible Access Control Markup Language (XACML) policies to enforce access control. XACML has performance issues. Therefore there is a need to come up with a different way to enforce consent in this research question.

3. How can consent be audited to fulfill GDPR compliance?

Organizations need to be GDPR compliant. Any organization found not to be compliant with GDPR can be fined up to 10 million euros or 2 % of their fiscal year revenue (European Union, 2016). It is crucial to conduct compliance audits reviewing an organization's adherence to GDPR guidelines. Consent can be audited in the organization's loT implementation based on the GDPR requirements. The solutions presented in the literature review lack an auditing process to audit consent, consent management, and consent enforcement. A well-developed process and tools are desired for conducting a GDPR compliance audit.

1.7 Dissertation Outline

This dissertation is organized into eight chapters. This chapter introduces the problem and related background information. Chapter 2 provides a literature review that discusses important research and solutions related to consent, consent management, and consent frameworks in healthcare and the IoT. Chapter 3 describes our research methodology. Chapter 4 presents our proposed consent framework. Chapter 5 discusses solutions that address the research questions. Chapter 6 presents a use case of our framework using a smart meter. Chapter 7 uses our consent auditing tool to evaluate if our use case is GDPR consent compliant. Chapter 8 summarizes our research with a discussion of its limitations, contributions, and future work.

1.8 Summary

This chapter discussed the problems with consent in IoT and provided a general overview of the IoT and GDPR. The research aims to develop an enterprise consent management solution within the IoT ecosystem while ensuring compliance with GDPR principles of consent. The proposed solution will follow our proposed consent framework that consists of data collection, consent collection, consent management, consent enforcement, and consent auditing.

CHAPTER 2

LITERATURE REVIEW

This chapter provides a literature review in consent management, frameworks, and other related topics. From the literature review, the research limitations, including issues with informed consent, access control, consent enforcement, and consent auditing, are identified for GDPR compliance in the IoT.

2.1 Internet of Things

IoT is a network of physical objects that comprise vehicles, buildings, equipment, health monitoring devices, and so on (Brown, 2016). The electronic devices in the network utilize sensors and actuators to communicate and update information. IoT technologies have evolved over the years. It involves the convergence of many technologies that include cloud computing, wireless networking, real-time analytics, machine learning, sensors, and embedded systems (Evans, 2011). Traditional technologies like embedded systems, wireless sensor networks, and control systems have enabled IoT.

Different researchers have proposed many IoT architectures. However, there has not been one agreed standard that can be used universally. There are two basic architectures: the three-layer architecture and the five-layer architecture (Sethi & Sarangi, 2017). The three-layered architecture comprises of perception layer, network layer, and application layer. Simultaneously, the five-layered architecture includes the perception layer, transport layer, processing layer, application layer, and business layer. There are also special-purpose architectures like media-aware traffic security architecture, clock synchronization architecture, humankind neural system architecture, etc. (Said & Masud, 2013).

IoT as an emerging technology has many security and privacy challenges. The IoT security challenges come from open architecture, system limitations, lack of standardization, insufficient trust and integrity, software vulnerabilities, malware targeting IoT devices, insecure web interface, privacy issues, and the weakest security link (Bhattarai & Wang, 2018). The security challenges can lead to the following attacks: denial of service, eavesdropping, node capture, controlling, and physical damage (Roman, Zhou, & Lopez, 2013). These security challenges can be mitigated by having one architecture and security standard that every IoT manufacturer adopts as an industry standard.

2.1.1 Communication in IoT

It is crucial to understand how IoT devices connect and communicate, especially their communication models. The devices in IoT are connected using various technical communication models, including Device-to-Device, Device-to-Gateway, Device-to-Cloud, and Back-End Data Sharing (Terkawi, Innab, Al-Amri, & Al-Amri, 2018). These IoT communication models have different characteristics that determine where they can be implemented. When an IoT system is complex, there are other challenges like security, privacy, interoperability and standards, legal, regulatory, and rights issues (Kulkarni & Kulkarni, 2017) that need to be considered while choosing a communication model.

Device-to-Device Communication: The Device-to-Device communication model connects devices directly to each other and establishes communication between two or more devices. In this communication model, devices use various networks that comprise IP networks or the Internet. Frequently, these communication protocols utilized by these devices include Bluetooth, Z-Wave, and ZigBee (Kulkarni & Kulkarni, 2017). These protocols only allow communication in specific device-to-device networks that use the same communication protocol to communicate and exchange messages (Rose, Eldridge, & Chapin, 2015). Therefore, these communication protocols are not compatible with exchanging messages amongst themselves.

Device-to-Gateway Model: The Device-to-Gateway model allows IoT devices to connect to an intermediary to access a cloud service. However, in this model, application software that operates on a local gateway device is utilized to be an intermediary between the IoT device and cloud service, which "provides security and other functionality such as data or protocol translation" (Terkawi et al., 2018). Devices used in this model usually cannot connect directly to the cloud service. Therefore, the gateway enables interoperability between IoT devices, the cloud service, and communication protocols.

Device-to-Cloud Communication: in the Device-to-Cloud communication model, IoT devices connect and communicate directly with the cloud service. This communication model usually utilizes existing communication mechanisms, for example, Ethernet or Wi-Fi, to connect devices to the IP network, and finally to the cloud service (Rose et al., 2015). The cloud allows remote access to the device through web interfaces. There are also many more challenges in this communication model, including interoperability, integration, and vendor lock-in (Kulkarni & Kulkarni, 2017).

Back-End Data Sharing Model: The Back-End Data Sharing model enables sensor data that has been collected by IoT devices to be accessed by trusted vendors or third parties. This model allows users to export and analyze data collected from the cloud service and enables it to be sent for aggregation and analysis (Rose et al., 2015). Data collected by the sensors is transformed and modeled to discover helpful information that can be used for decision making.

2.2 IoT and GDPR

IoT comprises everyday physical objects that communicate through the internet utilizing IP connectivity without human interaction (Singh & Singh, 2016). The IoT concept is based on the notion of always connected customers. It allows businesses to collect large volumes of customer data to give them a competitive edge. GDPR is concerned with personal data, which is data that can be used to identify a person. Data collection and processing activities that take place in IoT fall under the scope of GDPR. Therefore, data protection must be designed and built into IoT solutions starting from the development life cycle known as privacy by design. The principles of lawfulness, fairness, transparency, purpose limitation, data minimization, data accuracy, storage limitations, integrity and confidentiality, accountability, and data subject rights must be built to design IoT solutions (European Union, 2016).

Security and privacy are challenging issues in IoT. GDPR provisions are currently causing issues for the IoT industry. Consent is one of the provisions that is causing problems. GDPR requires IoT manufacturers or service providers who process data to have legal grounds for processing the data. Consent is the only legal ground, but it has to be informed, given freely, specific, and given in affirmative action (European Union, 2016). The IoT manufacturers or service providers are also required to demonstrate that the data subjects consented to process their personal data and provide the right for data subjects to withdraw their consent at any given time (European Union, 2016). The entity processing data is required to provide information on the nature of the processing, purpose of processing, and the name organization that needs to process the data (European Union, 2016). Providing all the necessary information allows the person to make an informed decision.

IoT manufacturers and service providers have been known for not providing explanations on data processing. In 2016, the Global Privacy Enforcement Network (GPEN) found out that :

- 59 percent of devices failed to adequately explain how personal information is collected, used, and disclosed.
- 68 percent of devices failed to inform users about how personal information collected by the device is stored and safeguarded.
- 69 percent of devices failed to provide device-specific guidance.
- 72 percent of devices failed to explain how users can delete their information (Choi, 2016).

The IoT manufacturers and service providers can address consent by ensuring that consent is the legal grounds for data processing and provides information and choices necessary to be GDPR compliant. Otherwise, they face penalties of up to 4% of the organization’s revenue or 20 million European dollars in fines.

2.3 Consent Management

Obtaining informed consent is not a requirement only brought by GDPR, but it has been in existence in the healthcare industry for many decades.

2.3.1 Consent Management in Healthcare

The medical professions use consent to ensure that the patient understands the risks and benefits of a procedure. Traditionally, the patient would sign paper forms. As the technology evolved, medical facilities utilize technology to implement the consent process. Even though consent in healthcare might have a specific approach, there is a lot to learn and adopt in dealing with GDPR consent implementation. Below we discuss healthcare research on consent and solutions.

Russello, Dong, and Dulay (2008) present a healthcare system framework that gives patients control over their medical data regarding disclosures. In the framework shown in Figure 1, patient's consent is essential in granting permissions to subjects that can have access to the patients' medical data. The workflow execution determines the enforcement of consent policies while empowering patients to fine-tune policies and control subjects based on consent (Russello et al., 2008). The paper also points out that workflows enable the implementation of the need-to-know principle.

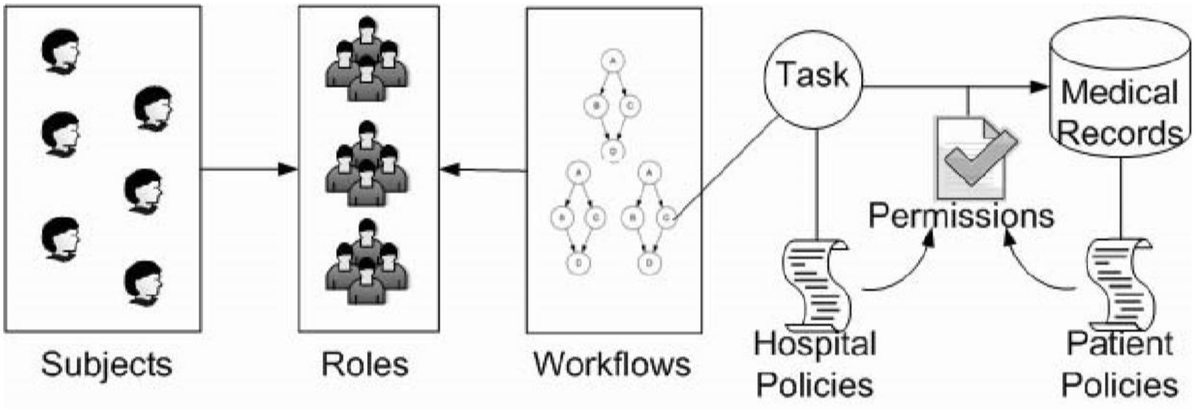


Figure 1. Consent-based Framework

Heinze, Birkle, Köster, and Bergh (2011) propose a standard-based consent management suite that receives and stores consent documents. The consent management suite can be queried about patient consent, processes it, and return an answer. The architecture includes a consent creator service, centralized policy enforcement point, master patient index, and XACML policies. This architecture enables integrating the consent management suite with Personal

Electronic Health Record (PEHR), which allows the recording of consent, publishing documents, and viewing documents.

Can (2013) proposes a semantic model for personal consent management. The model enables consumers to define their consent data and create consent policies on their consent data based on their privacy concerns. This model supports personalized consumer privacy incorporated in consent management, ensuring reasonable information sharing of personal data and its usage. Consumers are involved in protecting their privacy while improving personal data usage.

Ulbricht and Pallas (2016) propose a new approach for a consent management platform that implements multiple federated sources of personal data in the cloud for big data analytics. Their approach allows integrated queries for various data sources considering data subjects consent, purpose, and dynamically changeable consent.

Genestier, Zouarhi, Limeux, Excoffier, Prola, Sandon, and Temerson (2017) illustrate consent management in the health care domain implementing blockchain technology. The solution proposes including a Hyperledger, which integrates with the medical data collection ecosystem. Consent is utilized through smart contracts (operations like create, remove, use, and delete). Users can define consent which interacts with a consent smart contract that generates a new transaction. The transaction is memorized and recorded in a block added to the ledger with information that allows the block's confidentiality and integrity.

2.3.2 Consent Management in IoT

Luger and Rodden (2013) survey results show consent challenges in pervasive computing focusing on smart environments. The paper discusses the current state of consent and how it is relevant to pervasive systems. At the same time, it highlights the principles of consent and challenges brought by pervasive systems. The challenges pointed out by Luger and Rodden include the issues of consent when it comes to the law, the dependence of current methods of 'notice,' the problems associated with informed consent, and consent design. The authors also recommend designers on what they should consider when designing systems in the future. They recommend that electronic consent mechanisms not be designed based on a moment but should be negotiable. Systems should meet user expectations and should be aware of how they interact with third parties. The system designers should focus on user autonomy while understanding the need for user control.

Luger and Rodden (2013) consent reviews in ubiquitous computing systems show that these systems collect sensitive data without fully informing users of data to provide informed consent. Through interviews, Luger and Rodden found out that technology experts supported the idea of rethinking consent in ubiquitous computing and ensuring that there is a balance in system functionality.

Wakenshaw, Maple, Gomer, & Ghirardello (2018) surveyed IoT's meaningful consent mechanisms. Their discussions were based on an "apparency, pragmatic/semantic transparency model" to provide meaningful consent.

Rantos, Drosatos, Demertzis, Ilioudis, and Papanikolaou (2018) propose Advocate, a framework that enables GDPR compliant processing of personal data based on the IoT ecosystem. The framework is intended for data controllers and processors to provide informed consent transparently and unambiguously regarding the data they manage, the processing purpose, and periods. The architecture allows the data subjects (users) to create and edit processing policies and exercise their rights, i.e., access, rectification, erasure, restriction, and objection to data processing. Blockchain infrastructure is implemented as a notary service and consent security and informs data subjects of their consent.

2.4 Prior Research Limitations

2.4.1 Blockchain Consent Management Solution

The blockchain consent management solution proposed by Genestier et al. (2017) provides consent based on patients giving access to his or her data. The patient is not informed of the use by third parties during the time consent is collected. If the patients have more information, they will be able to provide informed consent. The authors did not effectively design their consent process to ensure that the patients are well informed with all the necessary information to provide informed consent.

2.4.2 ADVOCATE Consent Management Solution

Rantos et al. (2018) propose the ADVOCATE consent management platform for personal data processing based on blockchain in the IoT ecosystem. The platform currently lacks an intelligence component. Adding an intelligence component is intended to help users make the right decisions before providing consent to their personal data (Rantos et al., 2018).

2.4.3 Consent Management Suite Solution

The standard-based consent management suite proposed by Heinze et al. (2011) uses a centralized policy enforcement point and eXtensible Access Control Markup Language(XACML) policies. The research does not evaluate the efficiency and performance of the

XACML policies. XACML performance issues arise from real-time policy evaluation, approving each access request, and policy matching and attribute retrieval.

The research studies in the literature deal with consent management and enforcement, but there is no discussion on auditing consent or enforcement. Auditing is treated as a separate process. Auditing helps examine and evaluate the consent management solution and implementation (infrastructure, applications, data usage) against standards and policies.

2.5 Summary

This chapter introduces IoT and GDPR. Our discussions include GDPR, why it is important for IoT, GDPR consent management requirements, etc. We also discussed consent frameworks and solutions implemented by prior researchers to provide consent. There is more work to be done on the Internet of things concerning consent and its regulatory requirements. Our framework and solution for the Internet of Things is an effort to contribute to research.

CHAPTER 3

RESEARCH METHODOLOGY

This research follows the principles of design science. We examined different design science theories. Peffers's research methodology was one that we found suitable for our research. Peffers's research methodology has seven steps: problem identification and motivation, the solution's objectives, design and development, demonstration, evaluation, and communication (Peffers et al., 2007). Section 3.2 demonstrates how our research follows each step of Peffers's research methodology.

3.1 Design Science Research

Design science research seeks to develop solutions for practical problems (Cleven et al., 2009; Kampling et al., 2016; Offermann et al., 2009). To solve practical problems, we need to solve knowledge problems. According to Hevner et al. (2004), design science aims to create useful artifacts that can solve a problem or improve an existing solution. Vaishnavi et al. (2004) point out that design science develops new knowledge relevant to the community. Additionally, Hevner et al. (2004) state that design science research's primary evaluation is the question, "What are the new and interesting contributions?"

Hevner et al. (2004) presented guidelines for design science research in the information systems field. The seven guidelines for design science include design as an artifact, problem relevance, design evaluation, research contributions, research rigor, design as a search process, and communication of research. Design science research involves the development of innovative artifacts to solve a problem. The artifact must be evaluated to ensure the utility of the specified problem. A novel research contribution must solve new problems or introduce effective solutions. Construction and evaluation of artifacts should be rigorous, and results presented to technology communities.

Artifacts in design science research are known to contain knowledge. The knowledge varies from design logic, construction method, and tools that the artifact is intended to function (Gregor, 2002). The artifact construction and evaluation are the crucial parts of the design science research process described by Hevner et al. (2004). Design science artifacts include models, methods, constructs, instantiations, and design theories (March & Smith, 1995; Gregor 2002; March & Storey, 2008, Gregor and Hevner 2013). Other researchers argue that information systems research pertains to how research can be applied to design.

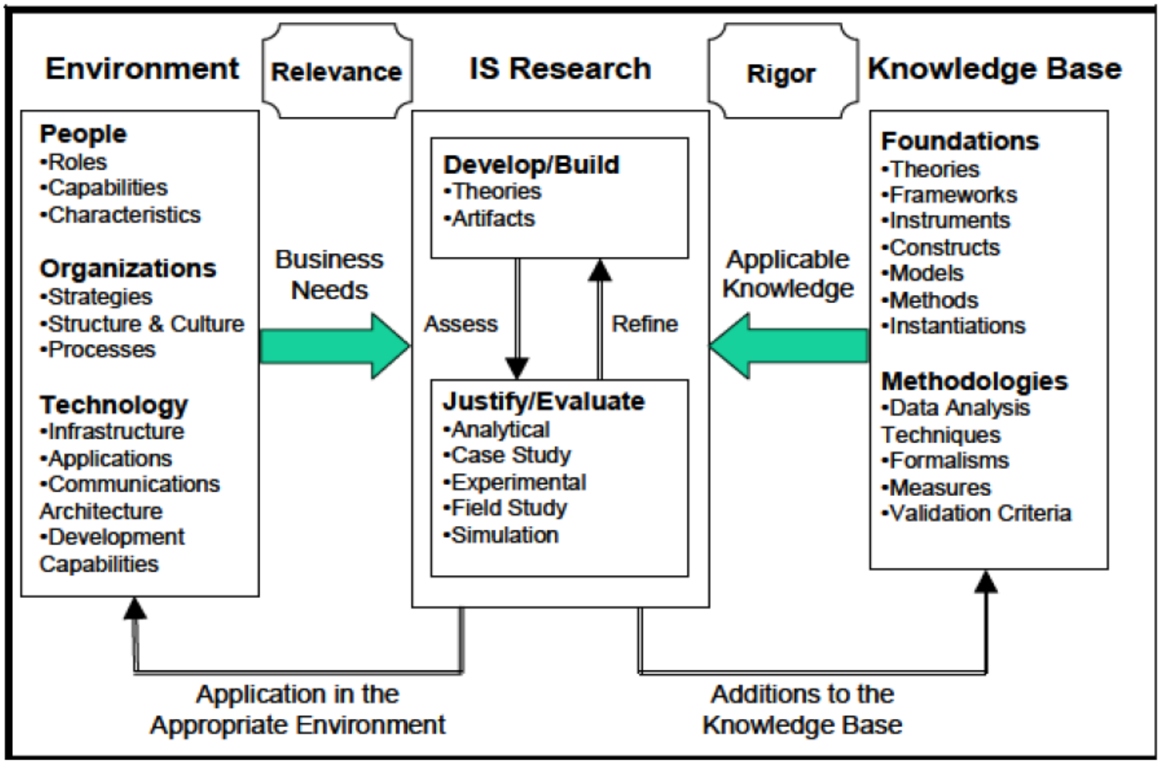


Figure 2. Information Systems Research Framework (Hevner et al., 2004)

Figure 2 shows an information system research framework proposed by Hevner et al.

(2004). The framework presents business and applicable knowledge, which lead to the development of new theories and artifacts.

Peffer's et al. (2007) includes six steps which are: (1) identification of the problem, defining the research problem, and demonstrating the importance of the solution; (2) define objectives of a solution; (3) design and development of artifact; (4) demonstrate how the artifact solves the problem; (5) evaluation of the solution, observe the effectiveness and efficiency of the artifact; (6) communication of the problem, present the artifact, its utility, and effectiveness to the research community.

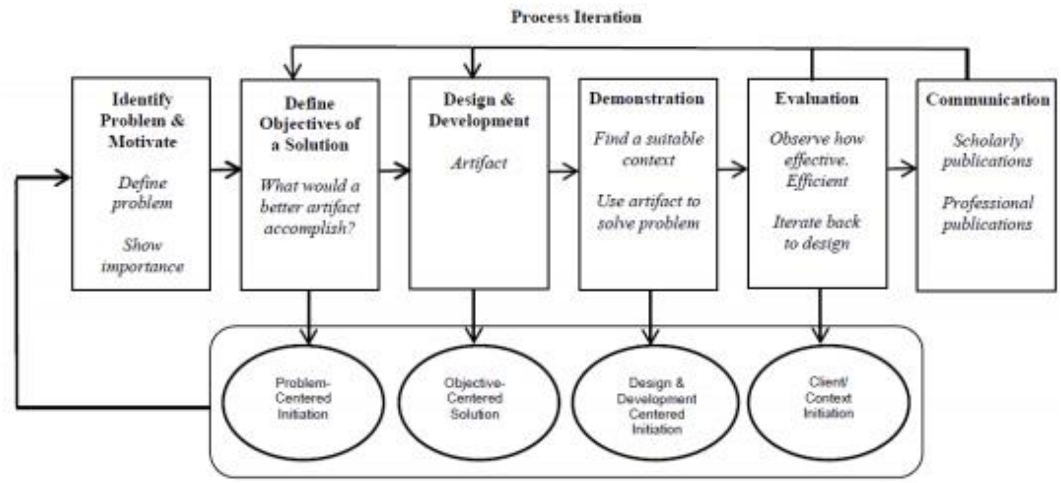

Process Iteration
Identify Problem & Motivate
Define problem
Show importance
Define Objectives of a Solution
What would a better artifact accomplish?
Design & Development
Artifact
Demonstration
Find a suitable context
Use artifact to solve problem
Evaluation
Observe how effective. Efficient
Iterate back to design
Communication
Scholarly publications
Professional publications
Problem-Centered Initiation
Objective-Centered Solution
Design & Development Centered Initiation
Client/ Context Initiation

Figure 3. Design Science Research Process (DSRP) Model (Peffers et al., 2007)

3.2 Our Approach to Design Science Research

Our research follows Peffers's research methodology with six steps, including problem identification and motivation, define objectives of the solution, design and development, demonstration, evaluation, and communication (Peffers et al., 2007). The design science research process model we are following is presented in Figure 3 above.

We begin by identifying problems and gaps by conducting a literature review of consent in the healthcare and IoT domains. During the literature review, we identified research limitations and gaps that presented opportunities for further research. First, we identified that no consent framework was tailored for IoT and addressed GDPR concerns. It is the motivation behind our research. The literature review limitations lead our research to develop a consent framework tailored to IoT and GDPR. Third, the artifact we design and develop addresses our research goals and objectives. Fouth, we demonstrated how our artifacts helps organizations be GDPR compliant. Fifth, we evaluate how our artifacts ensure GDPR compliance by auditing our implementation using the consent auditing tool. Sixth, we present our research to the security community through the publication of our dissertation.

3.3 Summary

This chapter described the design science research methodology and how we applied this methodology in this dissertation. This research follows Peffers’s design science research methodology. This type of methodology is suitable for our research as our goal is to develop an artifact solution.

CHAPTER 4

CONSENT FRAMEWORK FOR THE INTERNET OF THINGS

This chapter introduces the proposed consent framework and each component of the framework and its architecture. The consent framework includes five components: data collection, consent collection, consent management, consent enforcement, and consent auditing. The first three components follow GDPR requirements, while the last two components aid in GDPR compliance. The consent framework addresses consent issues that pertain to the Internet of Things.

4.1 Overview of the Consent Framework

The proposed consent framework is shown in Figure 4. The consent framework has five components: data collection, consent collection, consent management, consent enforcement, and consent auditing. Following the consent framework will help organizations to be GDPR consent compliant in their IoT environments. The framework has GDPR consent requirements embedded in the data collection, consent collection, consent management, and consent auditing components.

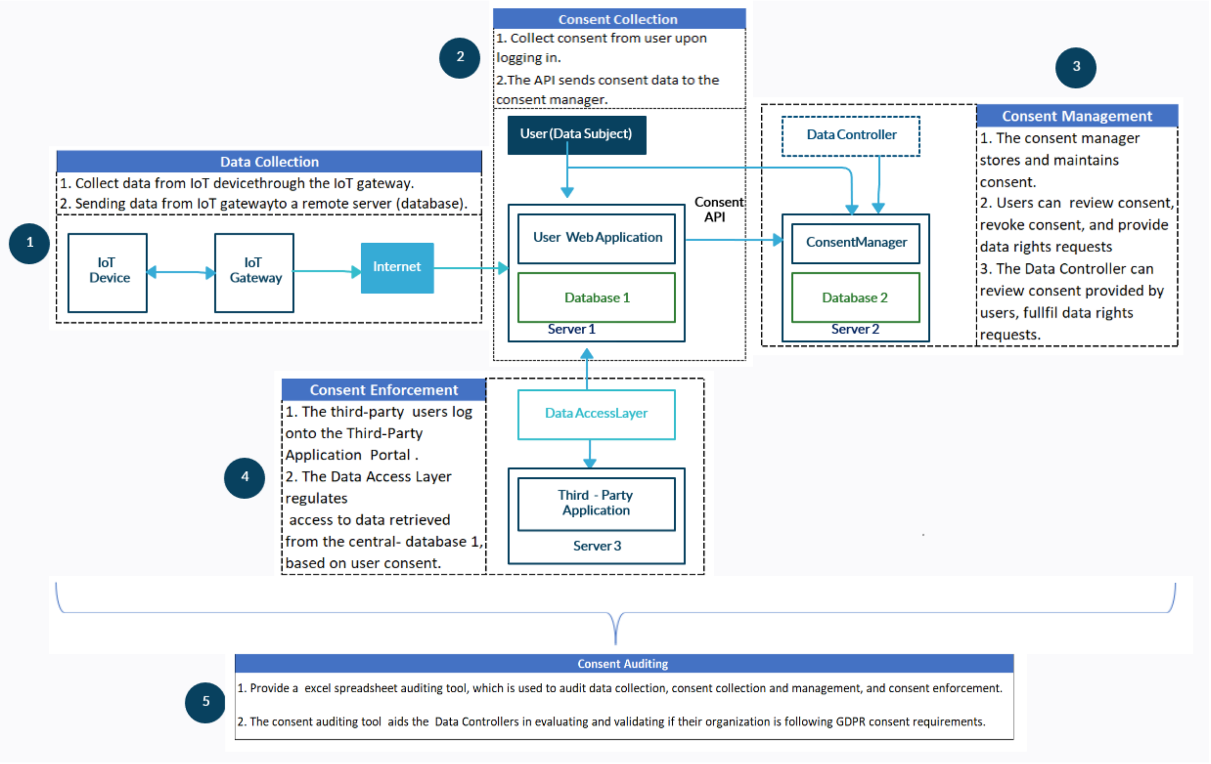

2
Consent Collection
1. Collect consent from user upon logging in.
2.The API sends consent data to the consent manager.
User (Data Subject)
Consent API
User Web Application
Database 1
Server 1
3
Data Controller
Consent Management
1. The consent manager stores and maintains consent.
2. Users can review consent, revoke consent, and provide data rights requests
3. The Data Controller can review consent provided by users, fullfil data rights requests.
ConsentManager
Database 2
Server 2
1
Data Collection
1. Collect data from IoT devicethrough the IoT gateway.
2. Sending data from IoT gatewayto a remote server (database).
IoT Device
IoT Gateway
Internet
4
Consent Enforcement
1. The third-party users log onto the Third-Party Application Portal .
2. The Data Access Layer regulates access to data retrieved from the central- database 1, based on user consent.
Data AccessLayer
Third - Party Application
Server 3
5
Consent Auditing
1. Provide a excel spreadsheet auditing tool, which is used to audit data collection, consent collection and management, and consent enforcement.
2. The consent auditing tool aids the Data Controllers in evaluating and validating if their organization is following GDPR consent requirements.

Figure 4. The Proposed Framework and Architecture

4.2 Data Collection

The IoT device's first interaction with the consent framework begins with the data collection. IoT devices collect data through internal sensors. The data is collected and transmitted through the IoT gateway. The IoT gateways use different protocols to determine connectivity, reliability, real-time data transmission, and data security. The data is collected from the IoT device to the IoT gateway and then to a remote database. The database stores the data, which will be retrieved by the user web application for the user. To ensure that this layer of our framework follows GDPR, we must follow GDPR data protection principles.

4.2.1 GDPR Data Protection Principles

The GDPR's six data protection principles guide how information must be collected and maintained (European Union, 2016). The following are the six principles of data protection:

1. Data must be collected legally and transparently (Lawful, Fairness and Transparency).
2. Data must be collected for specific reasons (Purpose Limitation).
3. Collect data that is necessary to the legal goals of the organization (Data Minimization).
4. Collected data must be accurate (Accuracy).
5. Dara must be kept for a limited time (Storage Limitation).
6. Data must be processed securely (Integrity and Confidentiality) (European Union, 2016).

4.3 Consent Collection

IoT consent is collected through front-end applications that allow users to interact with the data sent from IoT devices to the back-end database. Users are informed about their personal data being processed. A detailed scope of data processing is provided in the privacy policy or a pop-up notice. Users are allowed to make their decision to agree to specific purposes of data processing. To ensure that this layer of our framework is following GDPR, we must consider GDPR consent.

4.3.1 GDPR Consent

Under GDPR, organizations are required to ask for permissions for processing users' data. It is what is called consent per GDPR. Article 4 of the GDPR defines consent as:

> Any freely given, specific, informed, and unambiguous indication of a data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies

agreement to the processing of personal data relating to him or her (European Union, 2016).

Users must take action to provide consent. Information on what they are consenting to must be presented to them in clear and understandable terms. It means that consent must be written in simple language that an average person should understand what they consented to.

4.4 Consent Management

The consent framework deals with the collected consent in the consent management component. GDPR requires that the organization demonstrate that lawful consent was collected from users. Organizations are required to track the following; who gave consent, when the consent was given, what the user consented to, and when consent was withdrawn. This step also offers users an opportunity to make data subject rights and make requests. To ensure that this layer of our framework follows GDPR, we must follow consent requirements and data subject rights under GDPR.

4.4.1 Consent Requirements under GDPR

The following GDPR articles include requirements and explanations on consent. In particular:

a) Controllers must obtain consent, demonstrate the data subject's consent, and keep verifiable consent records (Article 7(1)).

b) Data subjects must be able to withdraw their consent at any time, and withdrawing consent must be as easy as giving consent (Article 7(3)).

4.4.2 Data Subject Rights

There are eight fundamental data subject rights stipulated in the GDPR. These rights are listed in GDPR articles 15 through 22. The eight data subject rights are:

1. The data subject’s right of access (Article 15).
2. The data subject’s right to rectification (Article 16).
3. The data subject's right to erasure or right to be forgotten (Article 17).
4. The data subject’s right to restriction of processing (Article 18).
5. The right to be informed (Article 19).
6. The right to data portability (Article 20).
7. The data subject’s right to object (Article 21).
8. The data subject’s right to not be subject to a decision based solely on automated processing (Article 22(1)).

4.5 Consent Enforcement

The data access layer regulates access to data while enforcing consent. It allows the data controller to control third-party access to data through the data access layer, responsible for communicating with the databases storing consent and user’s personal data. If a user consented to share the data, the data access layer would display the personal data to third parties. When users do not agree to share their data, the data access layer checks for consent and does nothing. The framework utilizes consent data to enforce consent.

4.6 Consent Auditing

The consent auditing component of our framework provides an excel consent auditing tool. The consent auditing comprises data collection, consent collection, consent management, and consent management sections. Each section has requirements that need to be inspected or examined to ensure the solution is GDPR compliance. The second part of each section provides audit worksheets used to validate compliance. Audit worksheets are used to record and track audit evidence obtained during the compliance audit by supporting the audit to assure that the audit was performed according to GDPR requirements.

4.7 Summary

This chapter presents the consent framework and architecture, including data collection, consent collection, consent management, consent enforcement, and consent auditing. The components of the framework were defined and how they relate to each other. We also discussed GDPR requirements for each component in the framework and other requirements that ensure compliance with GDPR.

CHAPTER 5

CONSENT COLLECTION, CONSENT MANAGEMENT, CONSENT ENFORCEMENT, AND CONSENT AUDITING

This chapter discusses solutions that address the research questions that we presented in Chapter 1. The three research questions allow us to demonstrate solutions that solve consent collection, consent management, consent enforcement, and consent auditing problems in IoT while incorporating GDPR consent requirements and consent enforcement requirements.

5.1 Consent Collection and Management

Research question 1 strives to answer the question “How can we collect and manage consent within an IoT solution while ensuring compliance with GDPR?” Figure 5 demonstrates a solution on how to address consent collection and management in IoT. We incorporate consent collection and consent management from our consent framework. For consent collection and consent management, we follow GDPR consent requirements and data subject rights to ensure compliance with GDPR.

GDPR consent requires organizations to get permission from users to process their data. According to GDPR article 4, consent should be “Any freely given, specific, informed and unambiguous indication of a data subject’s wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (European Union, 2016). In the consent collection process, a user must take action to provide consent. In our solution presented in Figure 5, the user must act on the consent form by either consenting (Yes) or rejecting consent (No).

Article 7(1) of the GDPR requires data controllers (organizations) to demonstrate how they collect and manage consent. Article 7(3) further requires that data subject (users) be allowed to withdraw their consent. GDPR articles 15 through 22 provide eight data subject rights. The data subject rights include the right to access, rectify, be forgotten, restrict processing, be informed, data portability, object, and not be subjected to automated processing (European Union, 2016). The solution in Figure 5 demonstrates how consent is collected and managed based on the GDPR requirements discussed above. It will address limitations in the blockchain consent management solution and ADVOCATE consent management solution identified in the literature review, i.e., lack of informed consent and making the right decision before providing consent.

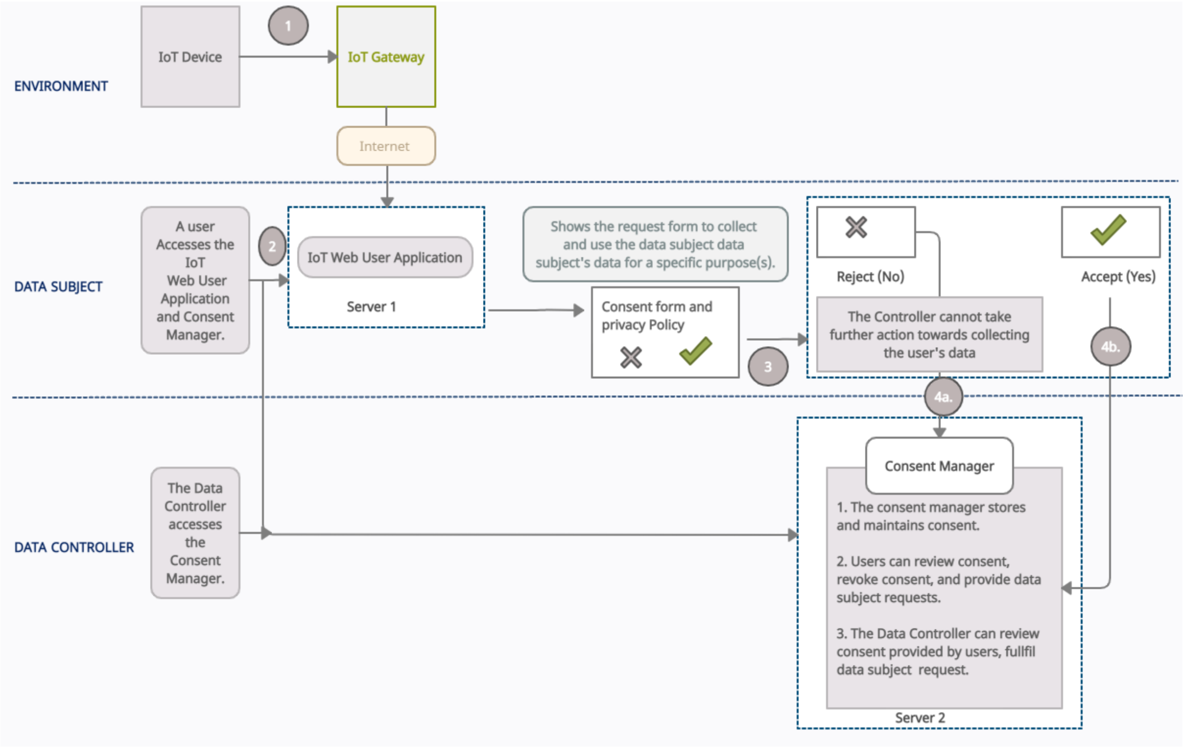

ENVIRONMENT
IoT Device
1
IoT Gateway
Internet
DATA SUBJECT
A user Accesses the IoT Web User Application and Consent Manager.
2
IoT Web User Application
Server 1
Shows the request form to collect and use the data subject data subject's data for a specific purpose(s).
Consent form and privacy Policy
3
Reject (No)
Accept (Yes)
The Controller cannot take further action towards collecting the user's data
4a.
4b.
DATA CONTROLLER
The Data Controller accesses the Consent Manager.
Consent Manager
1. The consent manager stores and maintains consent.
2. Users can review consent, revoke consent, and provide data subject requests.
3. The Data Controller can review consent provided by users, fullfil data subject request.
Server 2

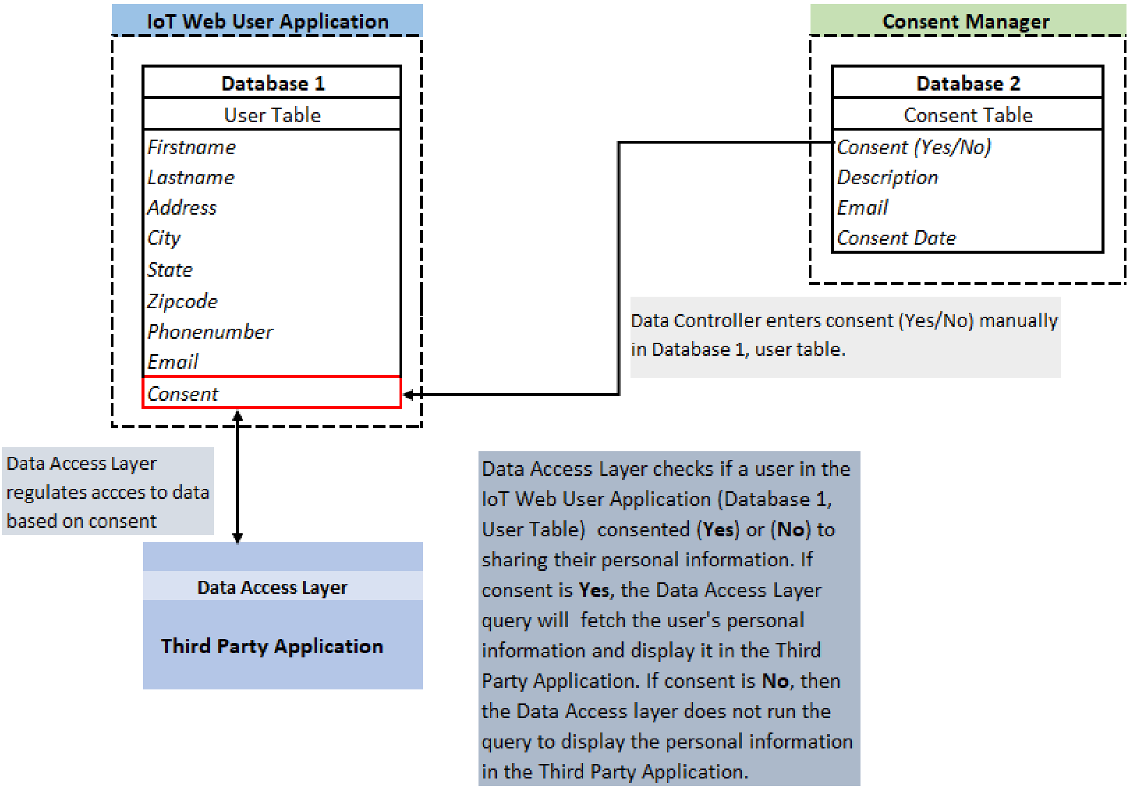
Figure 5. Consent Collection and Management Solution

Obtaining consent can be a challenge in the IoT environment. There are several challenges in consent collection and management in IoT which include:

1. Lack of screen-based interfaces allows users to access privacy settings or information on data sharing.
2. Manufacturers do not provide privacy policies within the IoT device and reference an external website that usually does not fully address the device's privacy issues.
3. In most cases, users of IoT devices are given no choice but to either consent or not use the product. Once the user has consented, there is no mechanism to withdraw consent (Rosner & Kenneally, 2018).

5.2 Consent Enforcement

Research question 2 answers the question "How can we enforce the collected consent?" Figure 6 demonstrates a solution on how to address consent enforcement in an IoT environment. We utilize consent enforcement requirements from our consent framework. For consent enforcement, we follow consent enforcement requirements that we create based on GDPR consent. The consent enforcement requirement is based on if a user has consented to share their personal information or not. If the user consented, the third party is granted access to that data. Figure 6 demonstrates consent enforcement using the collected consent.



Data Controller enters consent (Yes/No) manually in Database 1, user table.

Data Access Layer regulates acces to data based on consent

Data Access Layer checks if a user in the IoT Web User Application (Database 1, User Table) consented (**Yes**) or (**No**) to sharing their personal information. If consent is **Yes**, the Data Access Layer query will fetch the user's personal information and display it in the Third Party Application. If consent is **No**, then the Data Access layer does not run the query to display the personal information in the Third Party Application.

Figure 6. Consent Enforcement Solution

5.3 Consent Auditing

Research question 3 answers the question “How can consent be audited to fulfill GDPR compliance?” We worked with Cody Veselka, an Internal Audit Manager at WEX Inc., to develop an excel consent auditing tool that includes all aspects of GDPR data collection principles, consent requirement, management requirements, and consent enforcement requirements. The consent auditing tool will help conduct an audit on (1) how data is being collected, (2) how consent is being collected, (3) what consent was collected, (4) how consent is managed, (5) how data subject rights are being fulfilled, (6) regulation timelines, and (7) the effectiveness of the consent enforcement mechanism. The enforcement mechanism will be audited based on the data access layer queries and how they execute access control. The consent auditing tool helps with ensuring GDPR compliance. It will address limitation 4 in the literature review by providing an auditing process and auditing tool. The consent auditing tool has the following sections:

1. Data Collection Auditing
2. Consent Collection Auditing
3. Consent Management Auditing
4. Consent Enforcement Auditing

5.3.1 Data Collection Auditing

Table 1 includes GDPR data protection principles. These principles pertain to data collection and processing. We use the GDPR data protection principles to create the audit testing worksheets in Table 2. The testing worksheet allows us to audit data collection in IoT data collection against the data protection principles.

Table 1. GDPR Data Protection Principles (European Union, 2016)

Articles	GDPR Requirements
Article 5(1)	(a) processed lawfully, fairly, and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’).
	(b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be incompatible with the initial purposes (‘purpose limitation’).
	(c) adequate, relevant, and limited to what is necessary for relation to the purposes for which they are processed (‘data minimisation’).
	(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having

	regard to the purposes for which they are processed, are erased, or rectified without delay (‘accuracy’).
	(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’).
	(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

Table 2. GDPR Data Protection Principles Audit Testing Worksheet

Layer One	**GDPR Regulation**	**Question Number**	**Questions**	**IoT Data Collection Evidence**	**Testing Method**	**Is the Requirement Satisfied? (Yes/No)**	**Comments**
	Article 5(1)(a)	1	Is data being collected legally and transparently?				

Data Collection	(b)	2	Is there a purpose or reason for the collection of data?				
	(c)	3	Is data collected necessary for the legal goal of the organization?				
	(d)	4	Is the data being collected accurately?				
	(e)	5	Is there a data retention policy?				
	(f)	6	Is data being processed securely?				
	IoT Scalability	7	Is the IoT solution scalable?				

5.3.2 Consent Collection Auditing

Table 3 shows GDPR consent collection requirements. We utilize these requirements to create the testing worksheet template in Table 4. GDPR consent collection requirements deal with how consent is collected according to regulation. The developed testing worksheet provides us a way to test each component of consent collection for compliance.

Table 3. GDPR Consent Collection Requirements (European Union, 2016)

Articles	GDPR Requirements
Article 4(11)	Any freely given, specific, informed, and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Article 7(2)	If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

Table 4. GDPR Consent Collection Requirements Audit Testing Worksheet

Layer Two	**GDPR Regulation**	**Question Number**	**Questions**	**Consent Collection Evidence**	**Testing Method**	**Is the Requirement Satisfied? (Yes/No)**	**Comments**
Consent Collection	Article 4(11)	1	Is consent freely given, specific, informed, and unambiguous?				
		2	Does consent collection indicate data subject wishes with clear affirmative action and signifying agreement to process their personal data?				
	Article 7(2)	3	Is consent given in a context that does not concern other matters?				
		4	Is the request for consent presented in a manner that is clearly distinguishable from other matters?				

		5	Is the request presented in an intelligible, easily accessible form, in a clear and plain language?				

5.3.3 Consent Management Auditing

Table 5 includes GDPR consent management and data subject rights requirements. Consent management provides conditions of consent and data subject rights. Given these requirements, we create a testing worksheet template in Table 6. These requirements allow us to audit consent management in our consent manager solution in Chapter 6.

Table 5. GDPR Consent Management and Data Subject Rights Requirements (European Union, 2016)

Articles	GDPR Requirements
Conditions of Consent	
Article 7(1)	Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
Article 7(3)	The data subject shall have the right to withdraw his or her consent at any time.
Data Subject Rights	
Article 15	The data subject’s right of access.
Article 16	The data subject’s right to rectification.
Article 17	The data subjects right to erasure or right to be forgotten.
Article 18	The data subject right to restriction of processing.
Article 19	The right to be informed.
Article 20	The right to data portability.
Article 21	The data subject right to object.
Article 22	The data subject right to not be subject to a decision based solely on automated processing.

Table 6. Consent Management and Data Subject Rights Requirements Audit Testing Worksheet

Layer Three		**GDPR Regulation**	**Question Number**	**Questions**	**Consent Management Evidence**	**Testing Method**	**Is the Requirement Satisfied? (Yes/No)**	**Comments**
Consent Management	**Conditions of Consent**	Article 7(1)	1	Can the controller demonstrate that the data subject consented to process their personal data?				
		Article 7(3)	2	Can data subjects withdraw their consent at any given time?				
	Data Subject Rights	Article 15	3	Can data subjects request access to their data?				
		Article 16	4	Can data subjects request rectification of their data?				
		Article 17	5	Can data subjects request data erasure?				
		Article 18	6	Can data subjects request the restriction of data processing?				
		Article 19	7	Can a data subject request be informed?				

		Article 20	8	Can data subjects request data portability?				
		Article 21	9	Can data subjects request to object to data processing?				
		Article 22	10	Can data subjects request not to be subject to automated individual decision making?				
			11	How can you track that the data subject requests are handled in a timely manner? (within 30-45 days)				

5.3.4 Consent Enforcement Auditing

Table 7 includes consent enforcement requirements. These requirements were developed into a testing worksheet template, as shown in Table 8. There are two requirements that are based on user consent that determine access to be granted or denied.

Table 7. Consent Enforcement Requirements

Consent	Consent Statement
Yes	After reading the **Privacy Policy**, I agree to have Company XYZ share my data with third parties.
No	After reading the **Privacy Policy**, I agree to have Company XYZ share my data with third parties.

Table 8. Consent Enforcement Requirement Audit Testing Worksheet

Layer Four	**Consent**	**Question Number**	**Questions**	**Consent Enforcement Evidence**	**Testing Method**	**Is the Requirement Satisfied? (Yes/No)**	**Comments**
Consent Enforcement	Yes	1	Is access granted to user’s data based on consent?				
	No	2	Is access to user’s data restricted based on consent?				

5.4 Summary

In this chapter, we presented solutions to our research questions. We demonstrated solutions for consent collection and management, consent enforcement, and consent auditing. Our solutions are based on our consent framework and GDPR consent requirements. Chapter 6 and 7 provide details of our solutions.

CHAPTER 6

USE CASE: CONSENT FRAMEWORK APPLIED TO THE SMART METER

This chapter provides a use case of the proposed framework and its components. In Figure 7, we implemented a smart meter that collects electricity usage through an IoT gateway. The gateway collects electricity usage in kilowatt per hour (kWh), date and time, and the hourly frequency of data being sent to database 1 on remote server 1. When the user logs onto the web user application, a consent form pops up to allow the user to make consent decisions. After making the decisions and submitting the form, the user is presented with the smart meter data. The consent decisions are sent to Database 2 on Server 2 on the consent manager, tracked, and stored. In the consent manager, the user can review their consent, revoke consent, request data subject requests. Also, the data controller can view user consent and fulfill data subject requests.

6.1 Data Collection

6.1.1 Smart Meter

The smart meter (Elmeasure LG5310) is attached to a house electrical system to record electric energy consumptions. The smart meter is connected to the electrical input of 220V through a 30/5A current transformer, which steps down current levels. Modbus RTU is used as a communication protocol with the meter. It uses the master/slave architecture; in this case, the smart meter is the Modbus slave. The smart meter is connected to the IoT gateway through an

RS232 to RS485 adapter. RS232 to RS485 is a bidirectional adapter that allows RS232 data signal to RS485 and vice-versa. The energy consumption data is sent to the IoT gateway, which is running the Modbus master.

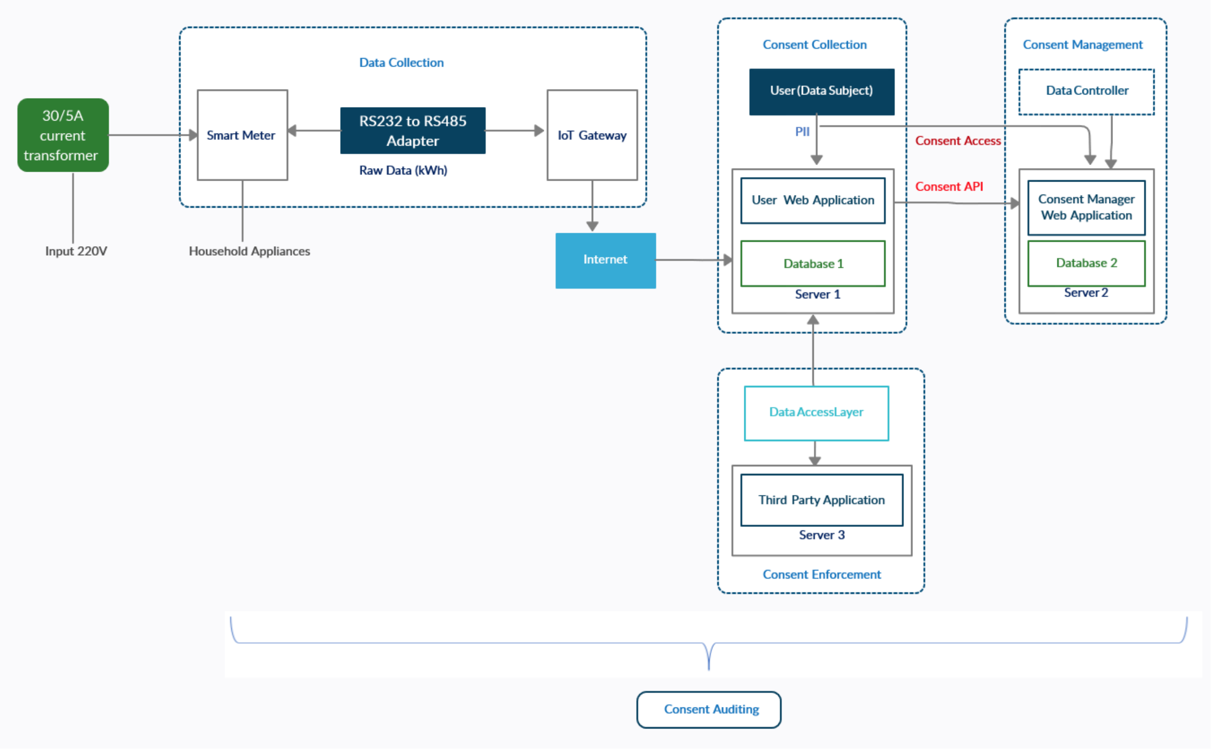
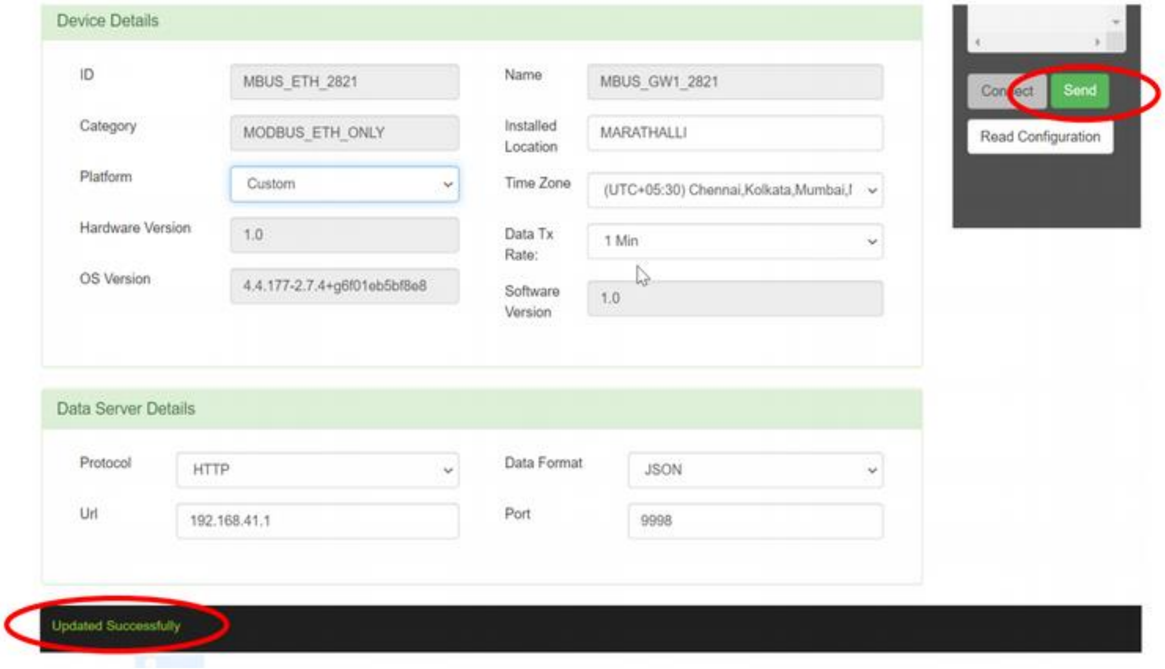


Figure 7. Use Case: Framework and Architecture

6.1.2 IoT Gateway

The IoT gateway (Modbus RTU Ethernet IoT Gateway) is implemented to ensure effective communication between the smart meter and a remote server running a database to store the electric energy consumption data. The IoT gateway configuration settings shown in Figure 8 shows gateway configuration settings for the smart meter (MBUS_GW1_2821) and data server (Server 1, Database 1). The IoT gateway is running the Modbus server. Figures 9 and 10 present the Modbus settings page, which allows us to set communication parameters. Figure 11 shows default command options that will enable the IoT gateway to read or write to the smart meter. The IoT gateway is connected to the household Internet through an ethernet cable to communicate with the remote server. Byte order and data types are configured as shown in Figures 12 through 13. The IoT gateway has a configuration web interface that allows the device administrator to configure the IoT gateway to communicate with the smart meter and from the IoT gateway to the remote server, as shown from Figures 8 through 13.



Device Details

ID	MBUS_ETH_2821	Name	MBUS_GW1_2821
Category	MODBUS_ETH_ONLY	Installed Location	MARATHALLI
Platform	Custom	Time Zone	(UTC+05:30) Chennai,Kolkata,Mumbai,I
Hardware Version	1.0	Data Tx Rate:	1 Min
OS Version	4.4.177-2.7.4+g6f01eb5bf8e8	Software Version	1.0

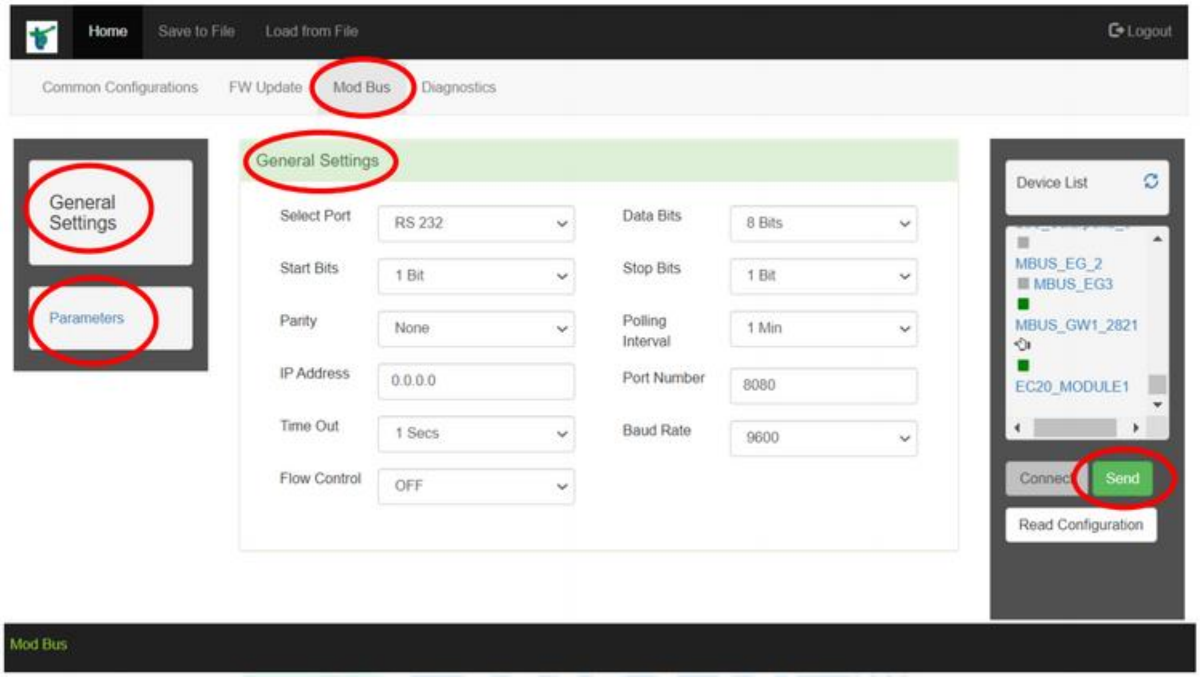
Data Server Details

Protocol	HTTP	Data Format	JSON
Url	192.168.41.1	Port	9998

Updated Successfully

Figure 8. Configuration Settings for the Device and Data Server

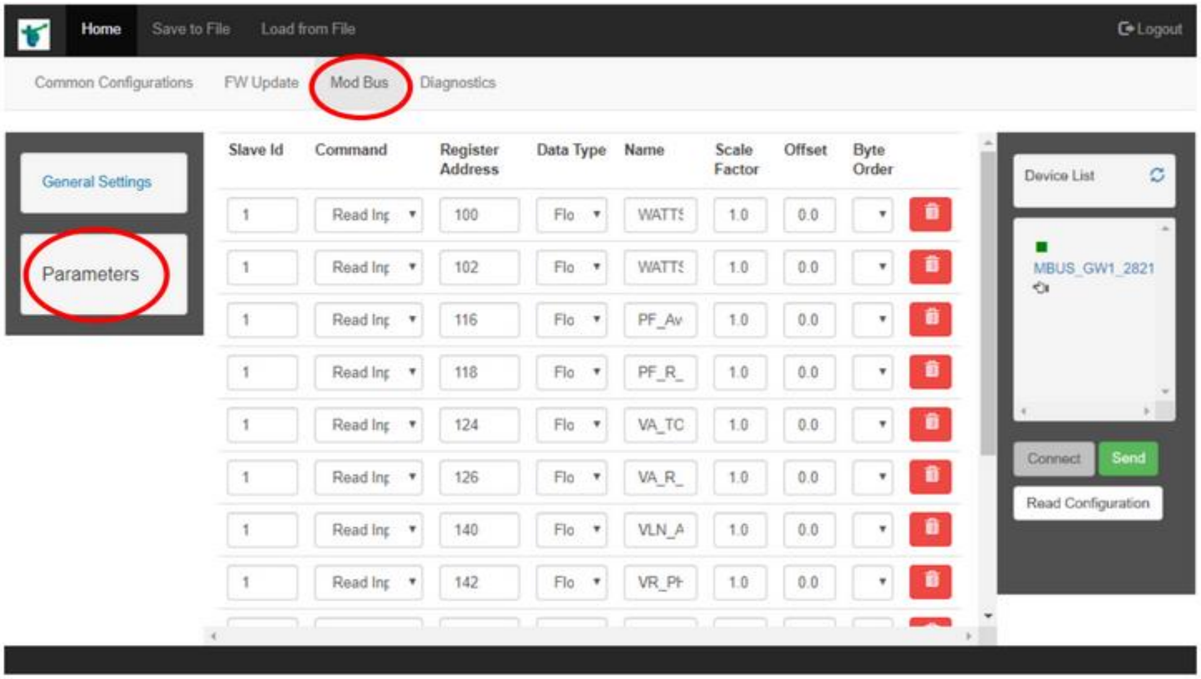
The Modbus settings page on figure 10 through 14 allow us to configure the Modbus protocol. Modbus requires us to configure ports, parameters, commands (read or write), data type, and the byte to facilitate communication.



General Settings

Select Port	RS 232	Data Bits	8 Bits
Start Bits	1 Bit	Stop Bits	1 Bit
Parity	None	Polling Interval	1 Min
IP Address	0.0.0.0	Port Number	8080
Time Out	1 Secs	Baud Rate	9600
Flow Control	OFF		

Figure 9. Modbus Settings Page



Slave Id	Command	Register Address	Data Type	Name	Scale Factor	Offset	Byte Order
1	Read Inp	100	Flo	WATTS	1.0	0.0	
1	Read Inp	102	Flo	WATTS	1.0	0.0	
1	Read Inp	116	Flo	PF_Av	1.0	0.0	
1	Read Inp	118	Flo	PF_R_	1.0	0.0	
1	Read Inp	124	Flo	VA_TC	1.0	0.0	
1	Read Inp	126	Flo	VA_R_	1.0	0.0	
1	Read Inp	140	Flo	VLN_A	1.0	0.0	
1	Read Inp	142	Flo	VR_PH	1.0	0.0	

Figure 10. Parameters Settings Page

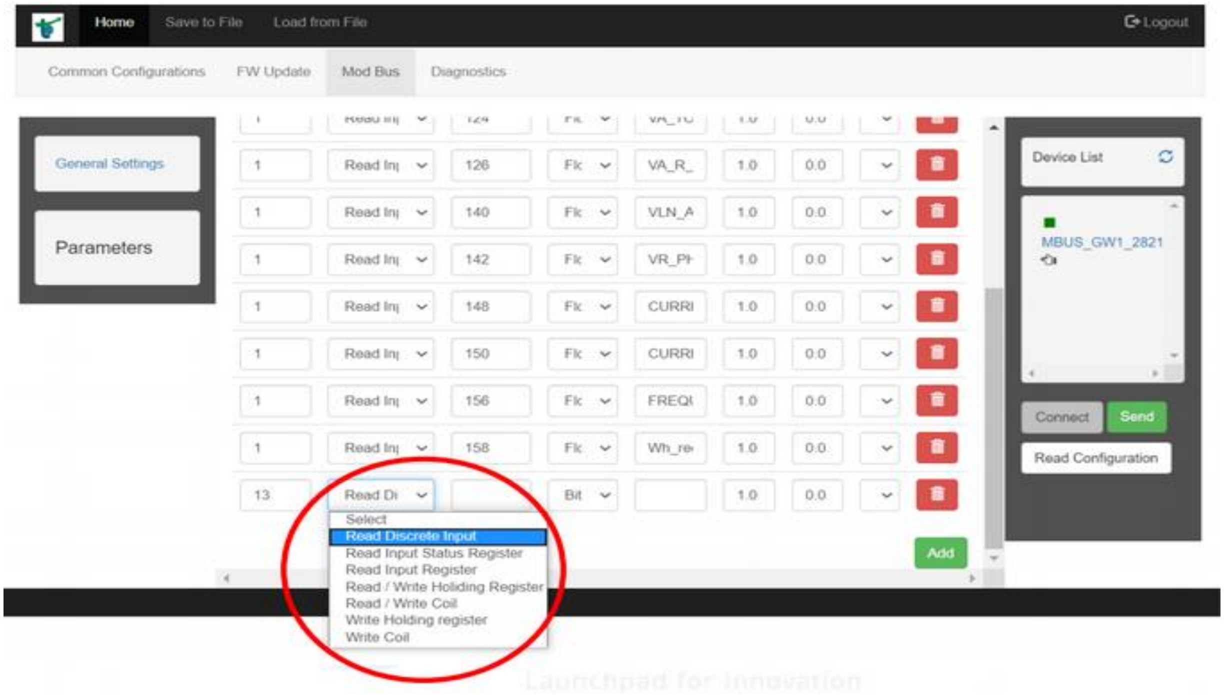


Figure 11. The Default Command Options

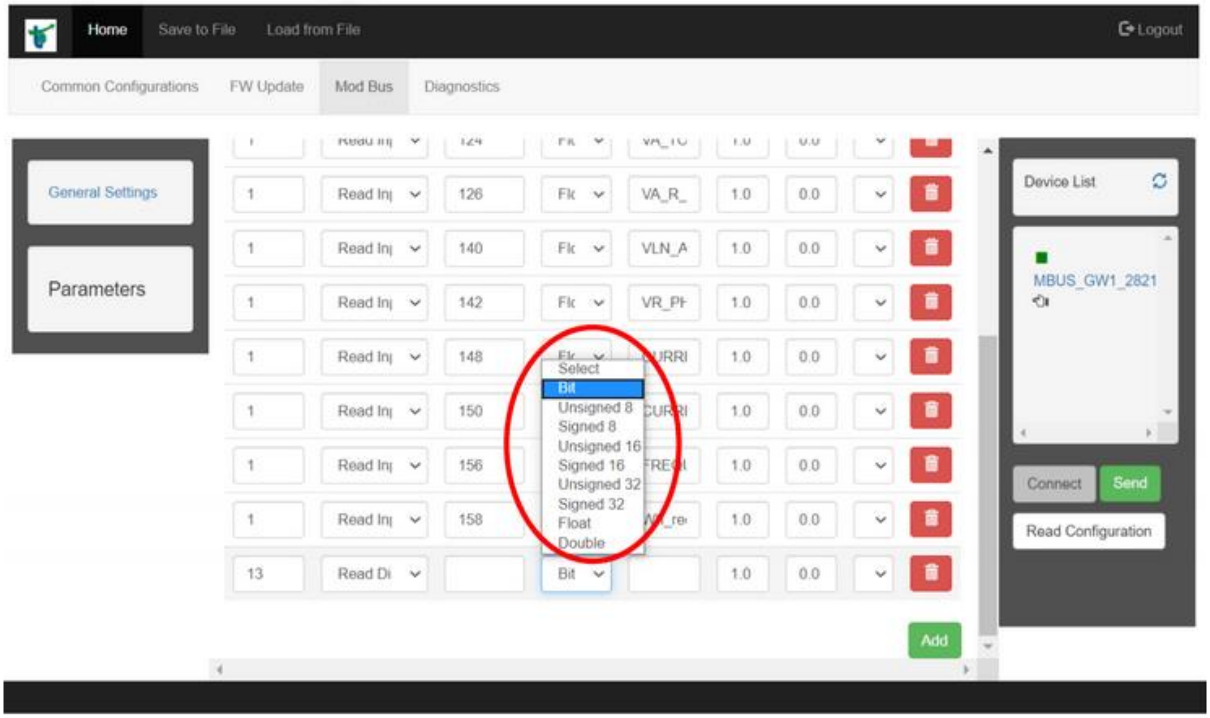
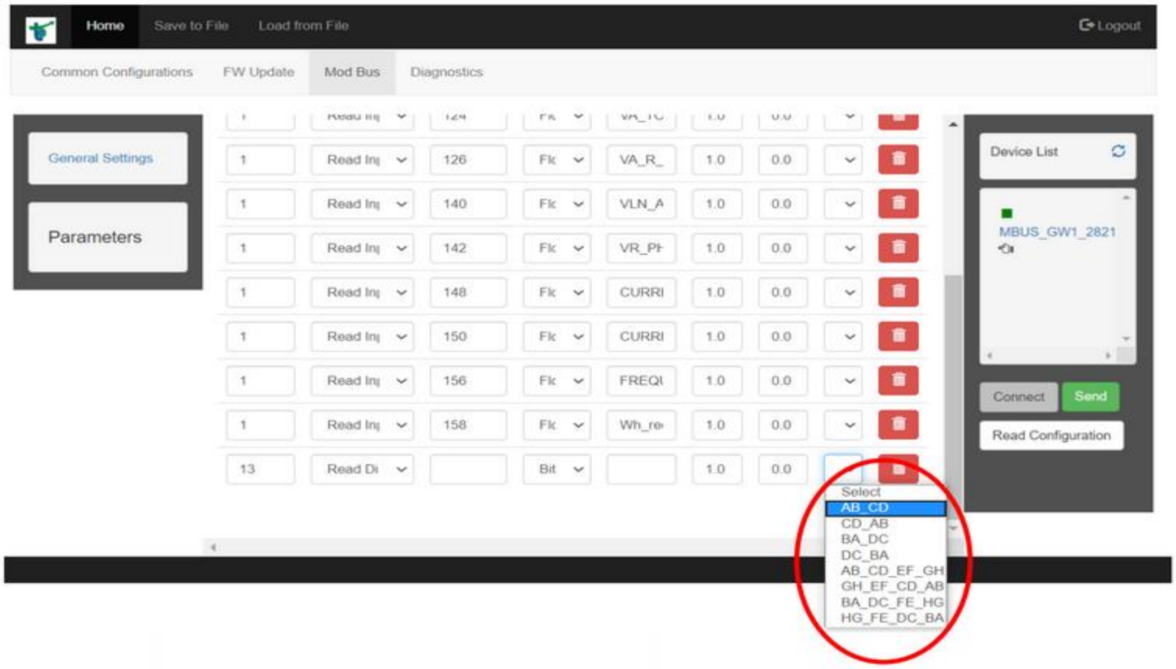


Figure 12. The Default “DATA TYPE” Options



1	Read In	124	Flc	VA_TC	1.0	0.0
1	Read In	126	Flc	VA_R_	1.0	0.0
1	Read In	140	Flc	VLN_A	1.0	0.0
1	Read In	142	Flc	VR_PH	1.0	0.0
1	Read In	148	Flc	CURRI	1.0	0.0
1	Read In	150	Flc	CURRI	1.0	0.0
1	Read In	156	Flc	FREQI	1.0	0.0
1	Read In	158	Flc	Wh_re	1.0	0.0
13	Read Di		Bit		1.0	0.0

Figure 13. The default “BYTE ORDER” Options

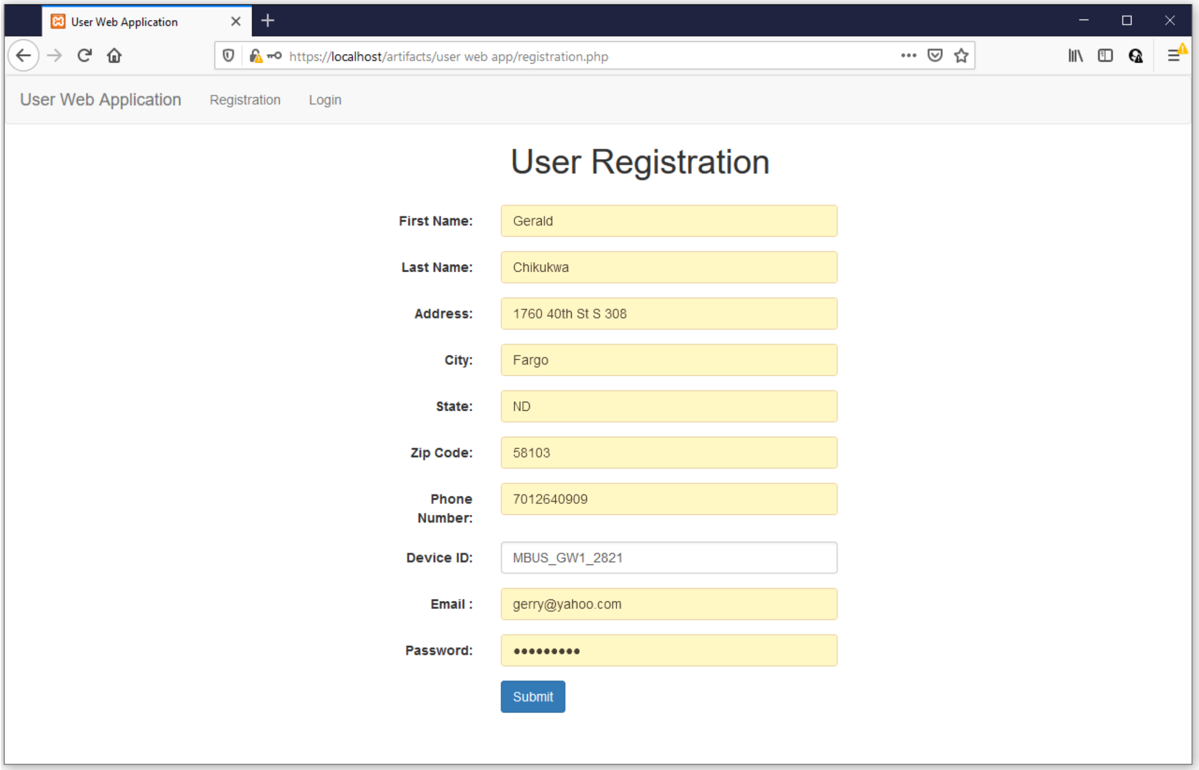
6.2 Consent Collection

6.2.1 User Web Application

The user web application is developed in PHP and MySQL. In the user web application, a user can create their profile, as shown in figure 14. When they complete creating their profile, they can log in, as shown in Figure 15, and access the smart meter readings like in Figure 18. When the user logs onto the user web application, an API developed in PHP between the application and the consent manager presents a pop-up form, as shown in Figure 16. The privacy policy in Figure 17, a section of the form, informs the user on data collection, data processing, data sharing, data retention, and data subject rights. After reading the privacy policy, the user can either agree or disagree with the following statements:

1. After reading the privacy policy, I agree to have my personal data collected and by Company XYZ.

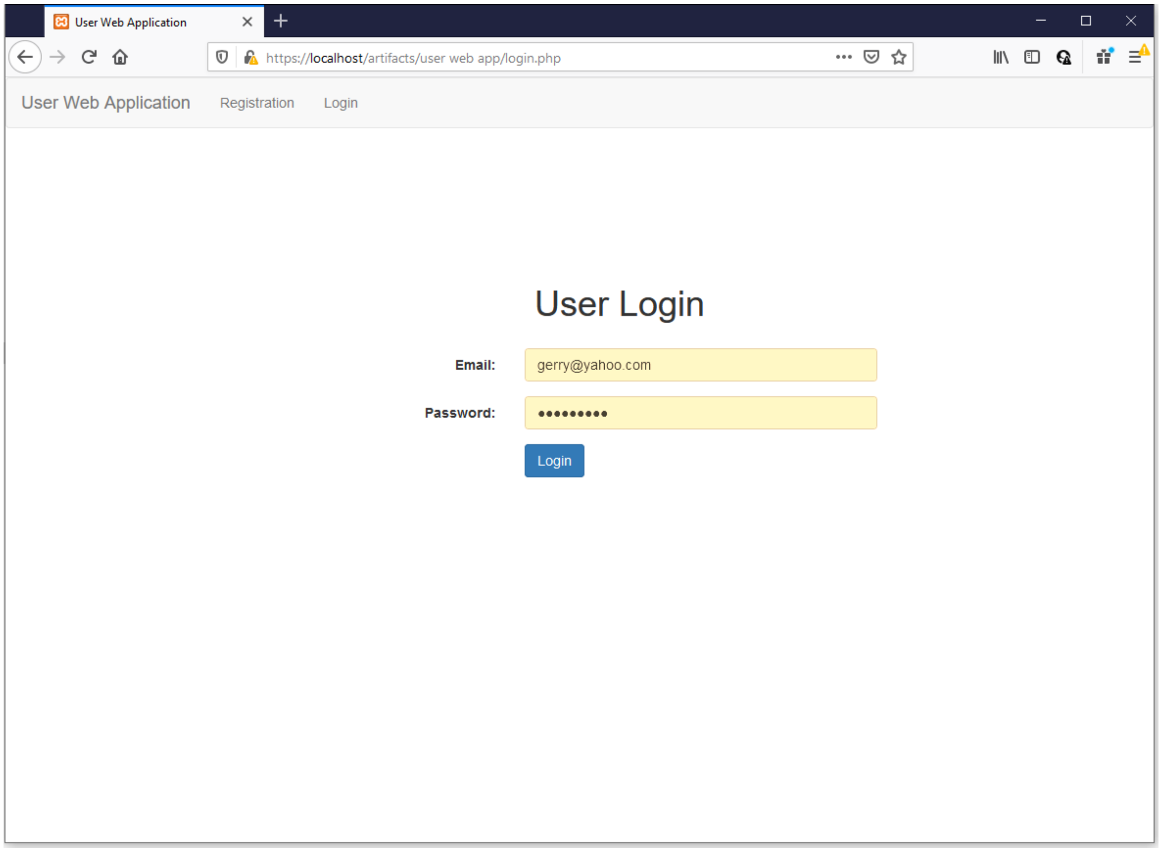
2. After reading the privacy policy, I agree to have my data processed by Company XYZ to record and analyze my preferences (profiling).
3. After reading the privacy policy, I agree to have Company XYZ share my data with third-party companies.



User Registration

First Name:	Gerald
Last Name:	Chikukwa
Address:	1760 40th St S 308
City:	Fargo
State:	ND
Zip Code:	58103
Phone Number:	7012640909
Device ID:	MBUS_GW1_2821
Email :	gerry@yahoo.com
Password:	•••••••••

Figure 14. User Registration

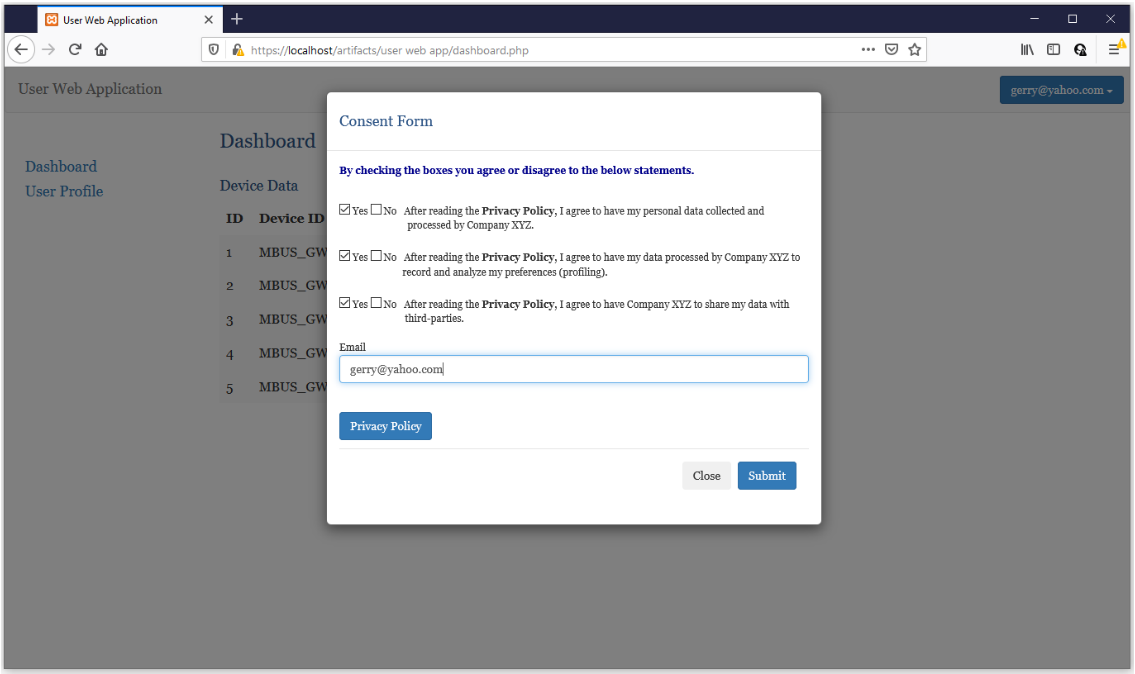


User Login

Email: gerry@yahoo.com

Password: •••••••••

Figure 15. User Login



ID	Device ID
1	MBUS_GW
2	MBUS_GW
3	MBUS_GW
4	MBUS_GW
5	MBUS_GW

Consent Form

By checking the boxes you agree or disagree to the below statements.

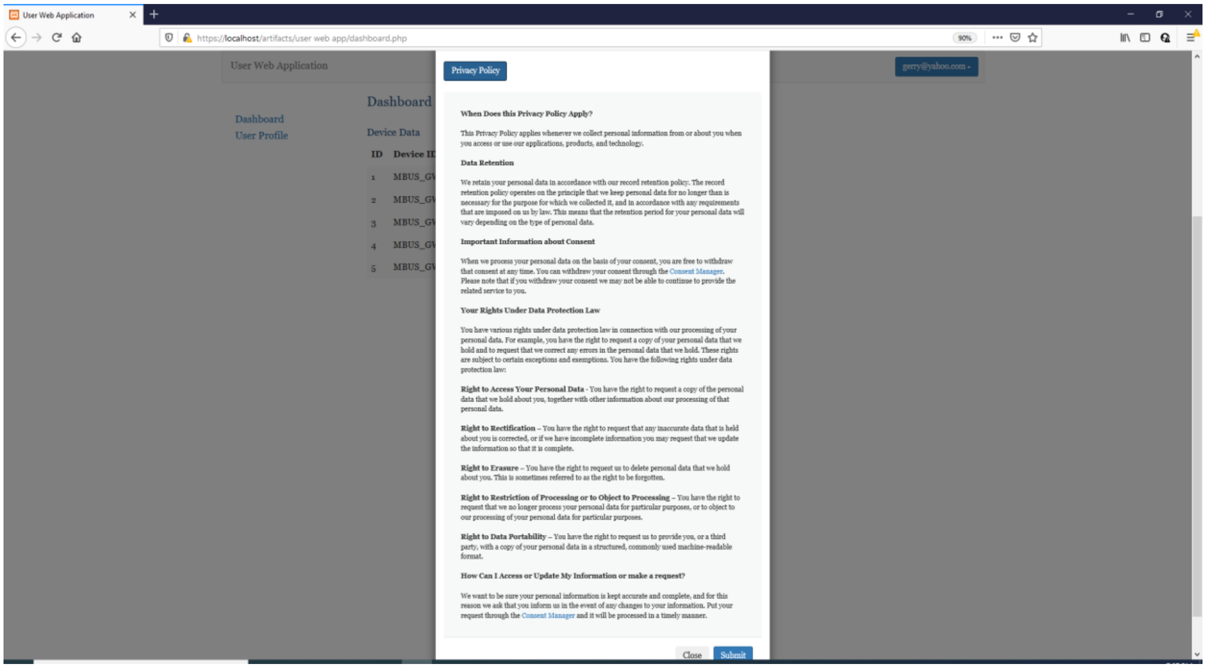
☑Yes ☐No After reading the **Privacy Policy**, I agree to have my personal data collected and processed by Company XYZ.

☑Yes ☐No After reading the **Privacy Policy**, I agree to have my data processed by Company XYZ to record and analyze my preferences (profiling).

☑Yes ☐No After reading the **Privacy Policy**, I agree to have Company XYZ to share my data with third-parties.

Email: gerry@yahoo.com

Figure 16. Consent Form



When Does this Privacy Policy Apply?

This Privacy Policy applies whenever we collect personal information from or about you when you access or use our applications, products, and technology.

Data Retention

We retain your personal data in accordance with our record retention policy. The record retention policy operates on the principle that we keep personal data for no longer than is necessary for the purpose for which we collected it, and in accordance with any requirements that are imposed on us by law. This means that the retention period for your personal data will vary depending on the type of personal data.

Important Information about Consent

When we process your personal data on the basis of your consent, you are free to withdraw that consent at any time. You can withdraw your consent through the Consent Manager. Please note that if you withdraw your consent we may not be able to continue to provide the related service to you.

Your Rights Under Data Protection Law

You have various rights under data protection law in connection with our processing of your personal data. For example, you have the right to request a copy of your personal data that we hold and to request that we correct any errors in the personal data that we hold. These rights are subject to certain exceptions and exemptions. You have the following rights under data protection law:

Right to Access Your Personal Data - You have the right to request a copy of the personal data that we hold about you, together with other information about our processing of that personal data.

Right to Rectification – You have the right to request that any inaccurate data that is held about you is corrected, or if we have incomplete information you may request that we update the information so that it is complete.

Right to Erasure – You have the right to request us to delete personal data that we hold about you. This is sometimes referred to as the right to be forgotten.

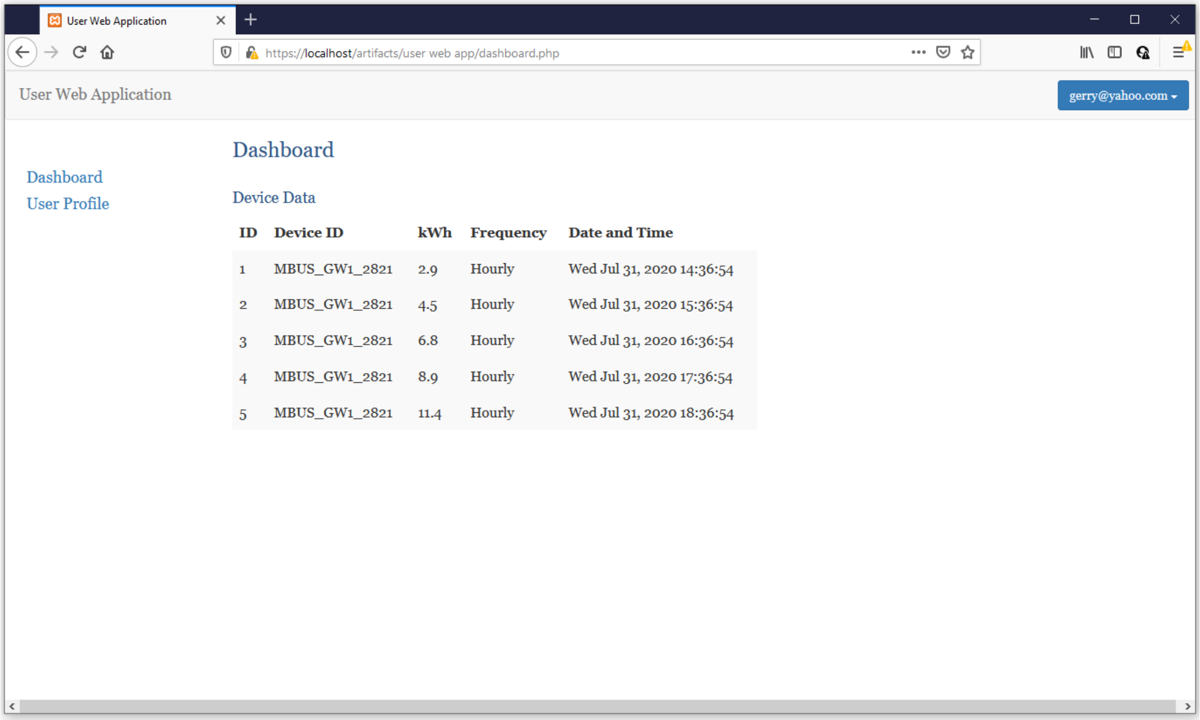
Right to Restriction of Processing or to Object to Processing – You have the right to request that we no longer process your personal data for particular purposes, or to object to our processing of your personal data for particular purposes.

Right to Data Portability – You have the right to request us to provide you, or a third party, with a copy of your personal data in a structured, commonly used machine-readable format.

How Can I Access or Update My Information or make a request?

We want to be sure your personal information is kept accurate and complete, and for this reason we ask that you inform us in the event of any changes to your information. Put your request through the Consent Manager and it will be processed in a timely manner.

Figure 17. Privacy Policy



ID	Device ID	kWh	Frequency	Date and Time
1	MBUS_GW1_2821	2.9	Hourly	Wed Jul 31, 2020 14:36:54
2	MBUS_GW1_2821	4.5	Hourly	Wed Jul 31, 2020 15:36:54
3	MBUS_GW1_2821	6.8	Hourly	Wed Jul 31, 2020 16:36:54
4	MBUS_GW1_2821	8.9	Hourly	Wed Jul 31, 2020 17:36:54
5	MBUS_GW1_2821	11.4	Hourly	Wed Jul 31, 2020 18:36:54

Figure 18. User Web Application Dashboard

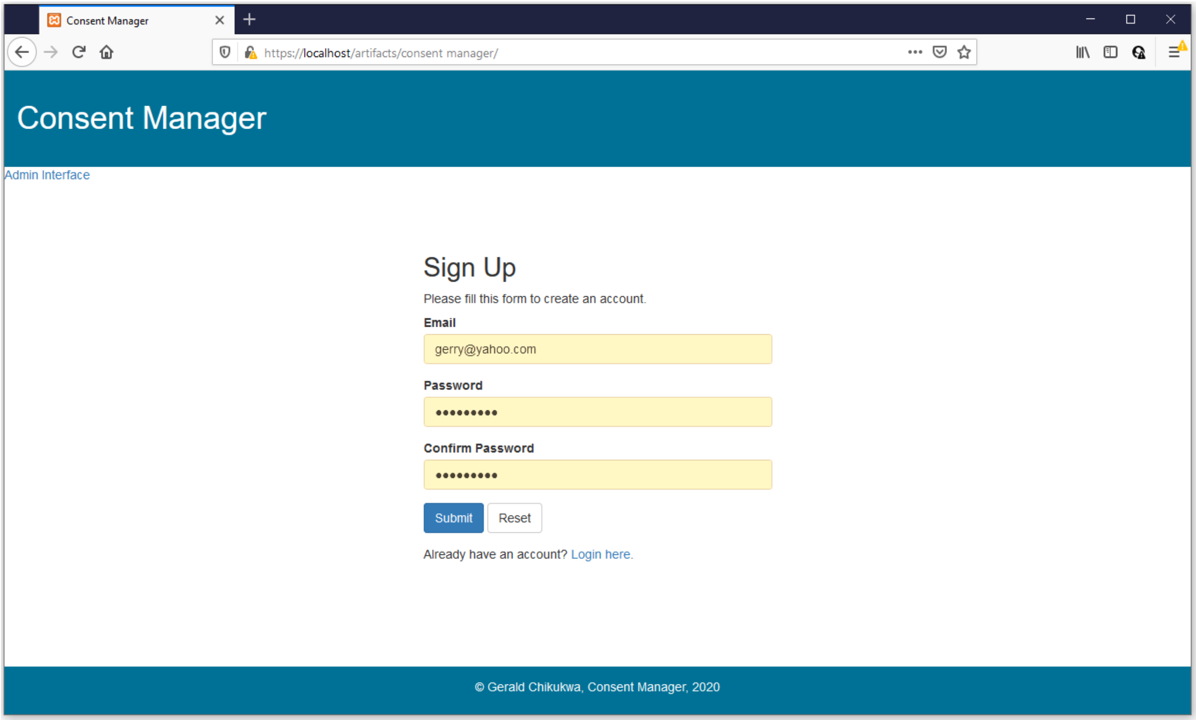
6.3 Consent Management

6.3.1 Consent Manager Web Application

The consent manager developed in PHP and MySQL manages and stores what the user has agreed or disagreed on based on the three statements mentioned above. The consent manager allows the data subject to review and change consent and makes data subject requests through a dashboard. It also tracks data subjects' requests from initial placement of request to completion. The data controller has a dashboard in the consent manager to view all the consent collected and fulfill data subject requests.

6.3.1.1 User Profile

The user can create a profile as shown in Figure 19 in the consent manager using the same email as the one used in the web user application because their consent is associated with that email. Once the user has signed up, they can log in, as shown in Figure 20. When the user has logged in, they have access to the user dashboard, as shown in Figure 21. The user dashboard provides consent information and allows the user to withdraw their consent. The dashboard on the left navigation bar has links to the dashboard and data subject request tabs. On the dashboard, the user can view their consent, and they can also revoke it. There are three sections that present consent on the dashboard, which are consent, did not consent, and revoked consent. The 'consent' section shows all the statements you agreed on. In the 'did not consent' section, the user can view all the user's statements they disagreed on. The user can view all the statements they revoked their consent on the 'revoked consent' section.



Consent Manager

Admin Interface

Sign Up

Please fill this form to create an account.

Email
gerry@yahoo.com

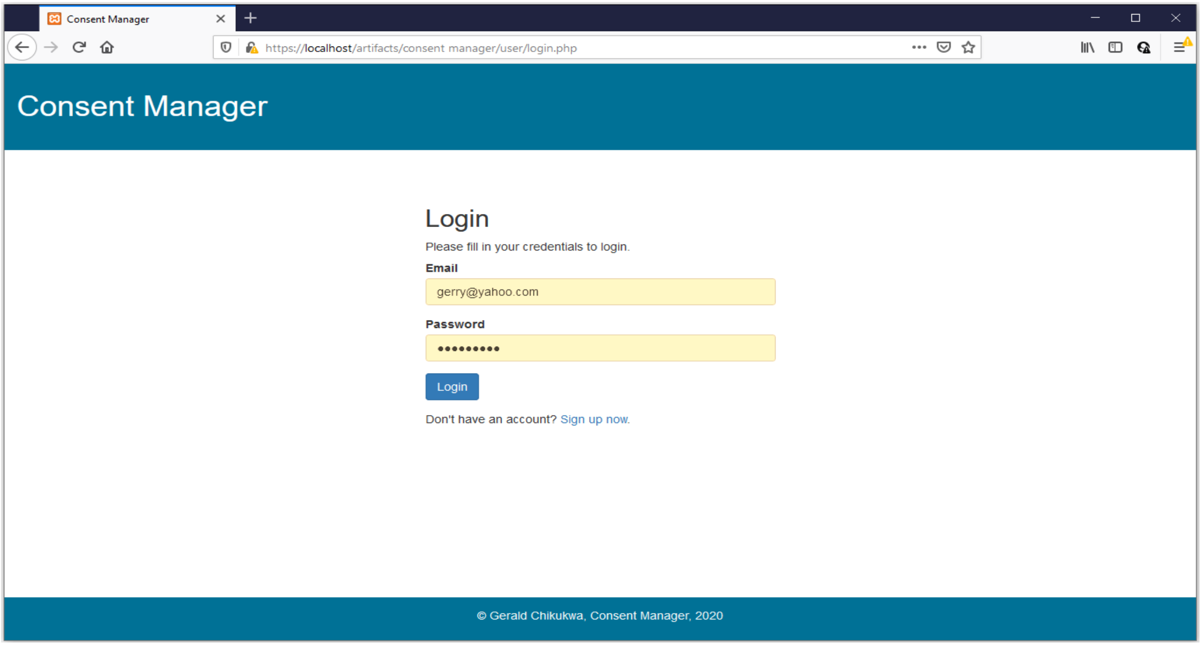
Password
•••••••••

Confirm Password
•••••••••

Already have an account? Login here.

© Gerald Chikukwa, Consent Manager, 2020

Figure 19. Consent Manager User Registration



Consent Manager

Login

Please fill in your credentials to login.

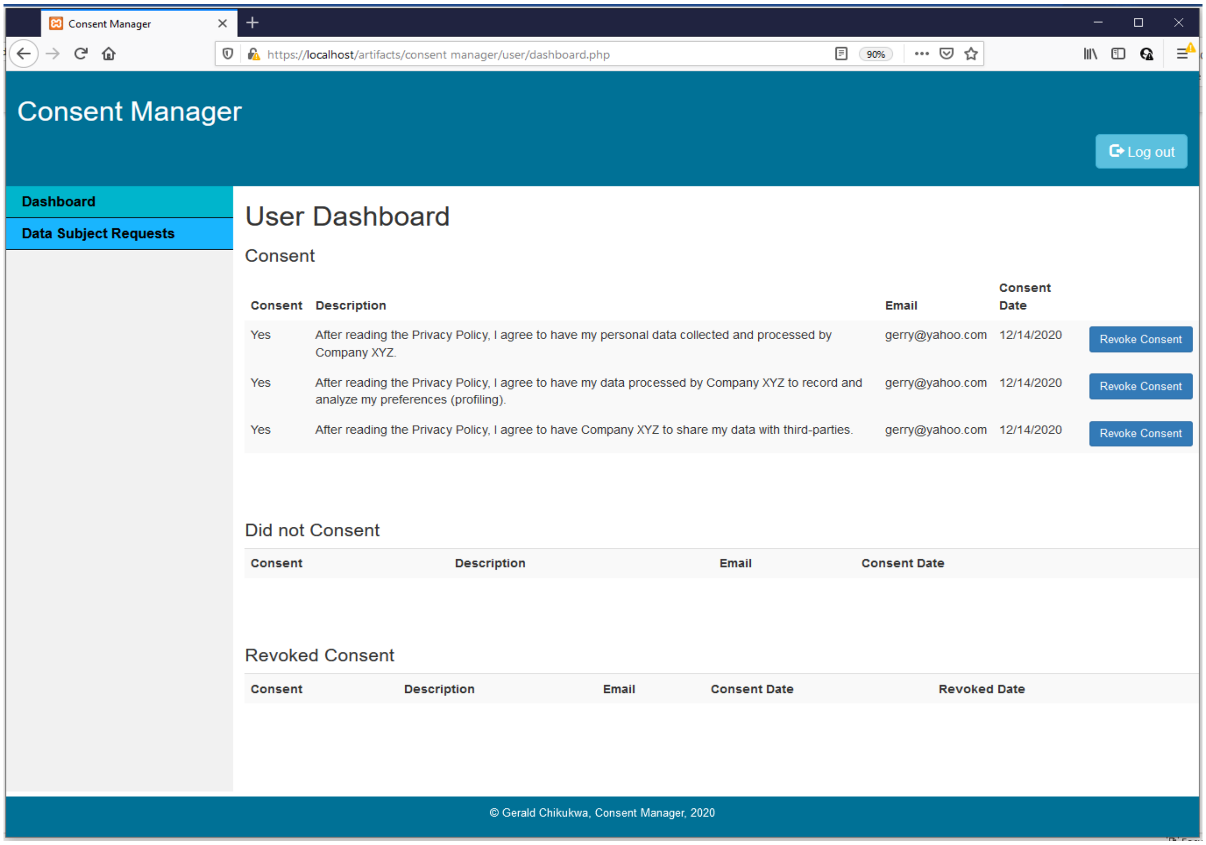
Email
gerry@yahoo.com

Password
•••••••••

Don't have an account? Sign up now.

© Gerald Chikukwa, Consent Manager, 2020

Figure 20. Consent Manager Login



Consent Manager

User Dashboard

Consent

Consent	Description	Email	Consent Date	
Yes	After reading the Privacy Policy, I agree to have my personal data collected and processed by Company XYZ.	gerry@yahoo.com	12/14/2020	Revoke Consent
Yes	After reading the Privacy Policy, I agree to have my data processed by Company XYZ to record and analyze my preferences (profiling).	gerry@yahoo.com	12/14/2020	Revoke Consent
Yes	After reading the Privacy Policy, I agree to have Company XYZ to share my data with third-parties.	gerry@yahoo.com	12/14/2020	Revoke Consent

Did not Consent

Consent	Description	Email	Consent Date

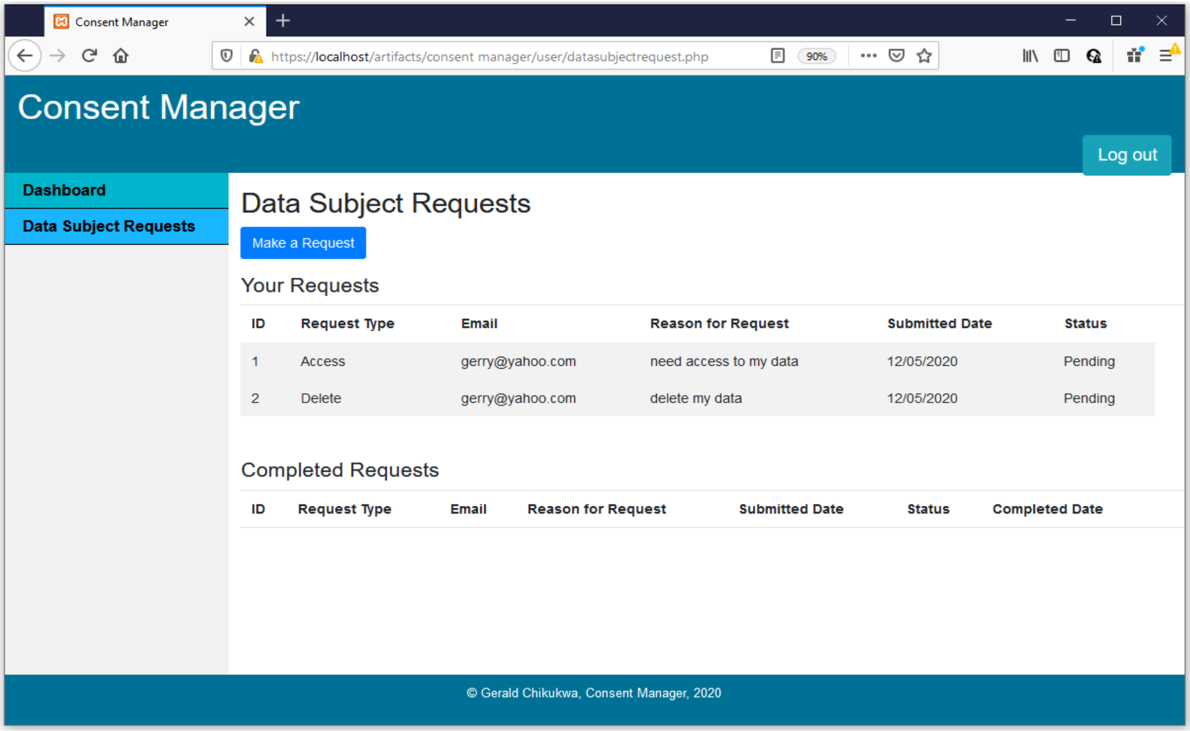
Revoked Consent

Consent	Description	Email	Consent Date	Revoked Date

© Gerald Chikukwa, Consent Manager, 2020

Figure 21. Consent Manager User Dashboard

The data subject requests tab in the user profile allows the user to request, display user requests, pending and completed requests, as shown in Figure 22. When making a request, a user must click on the make a request button, and a pop-up form appears. On the form, the user must select the type of request, provide their email and reason for the request. Eight request types include the right to access, rectify, be forgotten, restrict processing, be informed, data portability, object, and not be subjected to automated processing. Figure 23 shows the processes involved in making the request. After completing all the required fields on the form, the user can submit the form, and the request is pending until the Consent Manager administrator takes the necessary steps to complete the request.



Data Subject Requests

Your Requests

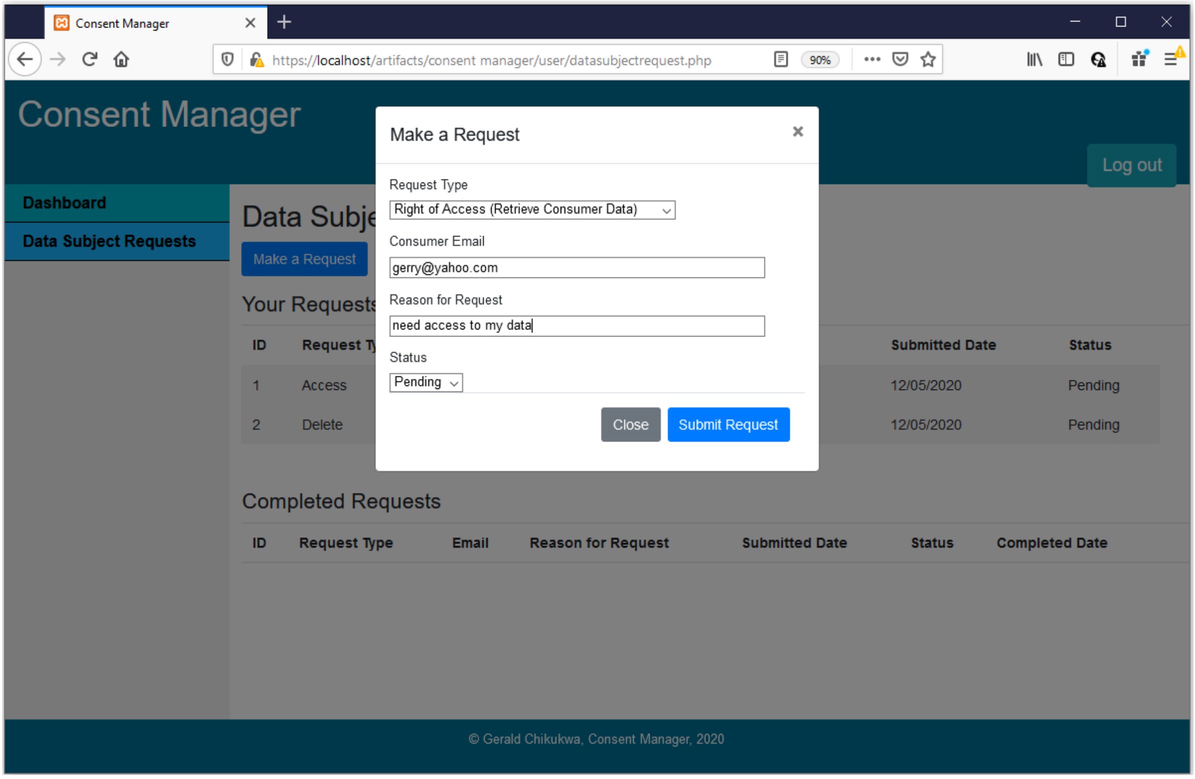
ID	Request Type	Email	Reason for Request	Submitted Date	Status
1	Access	gerry@yahoo.com	need access to my data	12/05/2020	Pending
2	Delete	gerry@yahoo.com	delete my data	12/05/2020	Pending

Completed Requests

ID	Request Type	Email	Reason for Request	Submitted Date	Status	Completed Date

© Gerald Chikukwa, Consent Manager, 2020

Figure 22. Consent Manager Data Subject Requests



Make a Request

Request Type: Right of Access (Retrieve Consumer Data)

Consumer Email: gerry@yahoo.com

Reason for Request: need access to my data

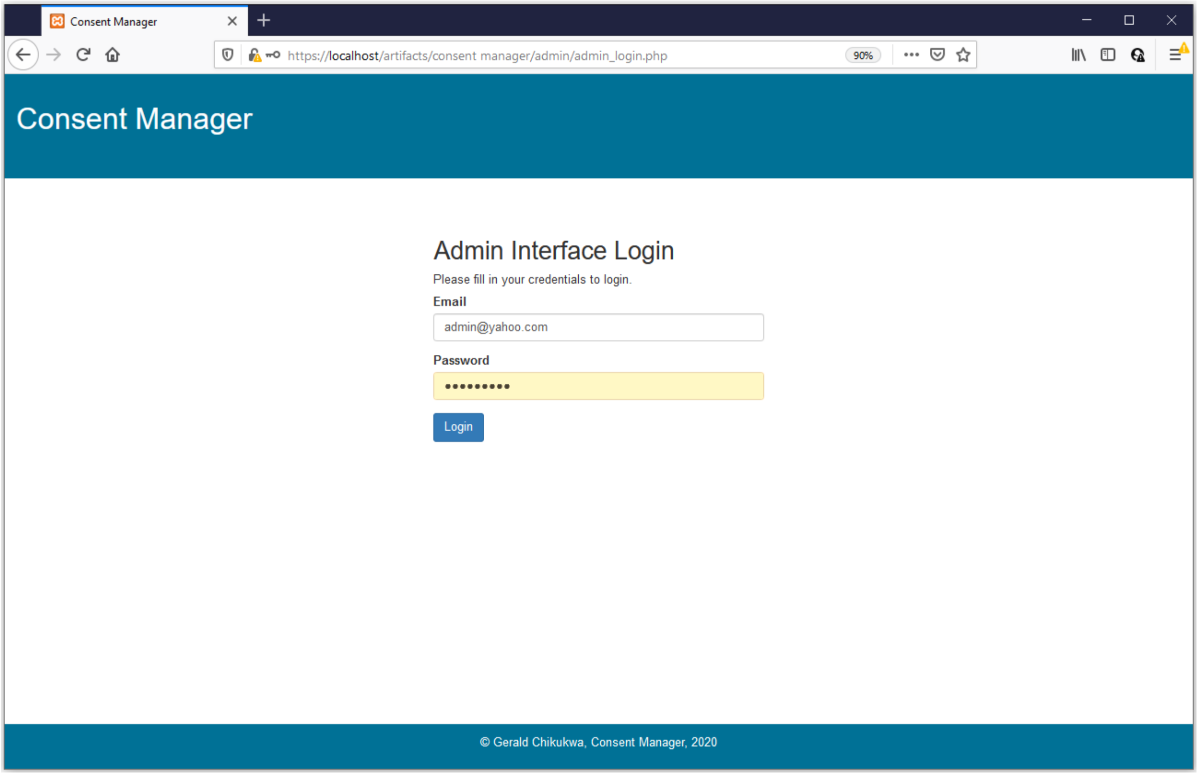
Status: Pending

© Gerald Chikukwa, Consent Manager, 2020

Figure 23. Consent Manager Make a Request Form

6.3.1.2 Administrator Profile

The administrator can log in to the consent manager through the admin interface, as shown in Figure 24. When the administrator has logged in, they can see the admin dashboard, which shows what users have consented to and did not consent to and revoke consent. On the admin dashboard, the administrator can see every consent provided by the users. Figure 25 shows consent information displayed on the admin dashboard. The data subject request tab in the administrator profile, as shown in Figure 26, displays data subject requests submitted by the users. The administrator can review the data subject requests and complete them, as shown in Figure 27. The data controller can either accept or deny a request or request more information from the user depending on the situation.



https://localhost/artifacts/consent manager/admin/admin_login.php

Consent Manager

Admin Interface Login

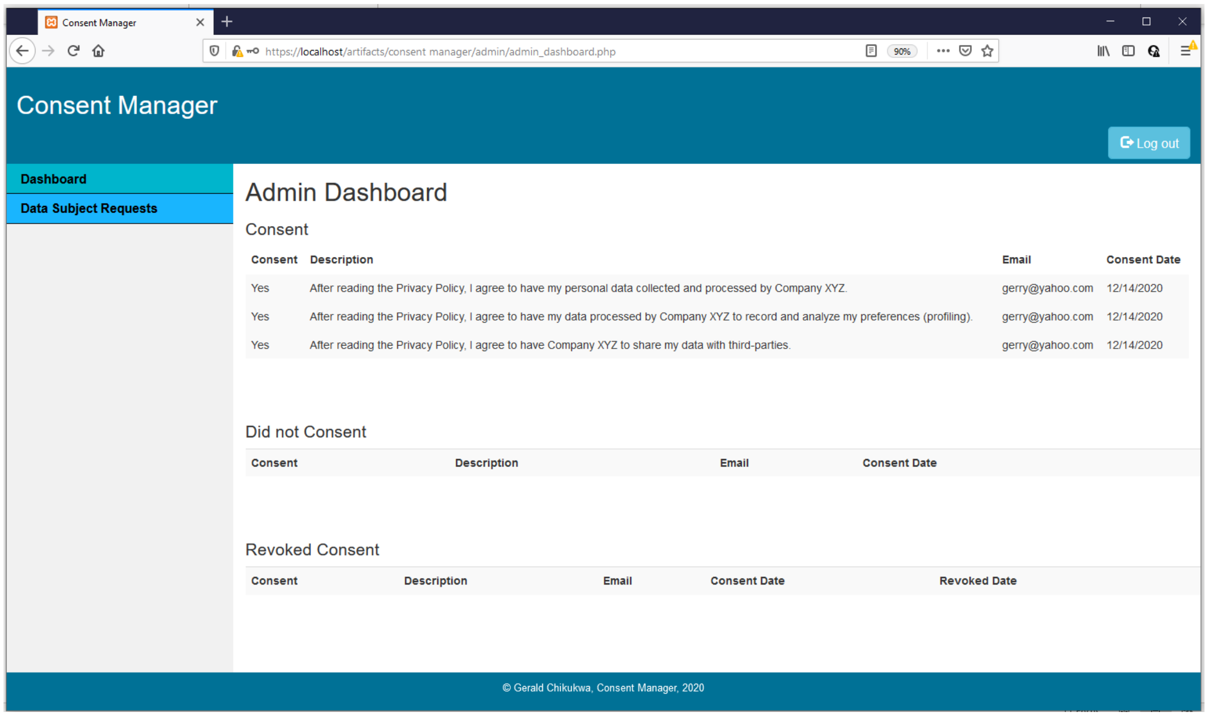
Please fill in your credentials to login.

Email: admin@yahoo.com

Password: •••••••••

© Gerald Chikukwa, Consent Manager, 2020

Figure 24. Consent Manager Admin Login


Consent Manager
https://localhost/artifacts/consent manager/admin/admin_dashboard.php
90%
Log out
Dashboard
Data Subject Requests

Consent Manager

Admin Dashboard

Consent

Consent	Description	Email	Consent Date
Yes	After reading the Privacy Policy, I agree to have my personal data collected and processed by Company XYZ.	gerry@yahoo.com	12/14/2020
Yes	After reading the Privacy Policy, I agree to have my data processed by Company XYZ to record and analyze my preferences (profiling).	gerry@yahoo.com	12/14/2020
Yes	After reading the Privacy Policy, I agree to have Company XYZ to share my data with third-parties.	gerry@yahoo.com	12/14/2020

Did not Consent

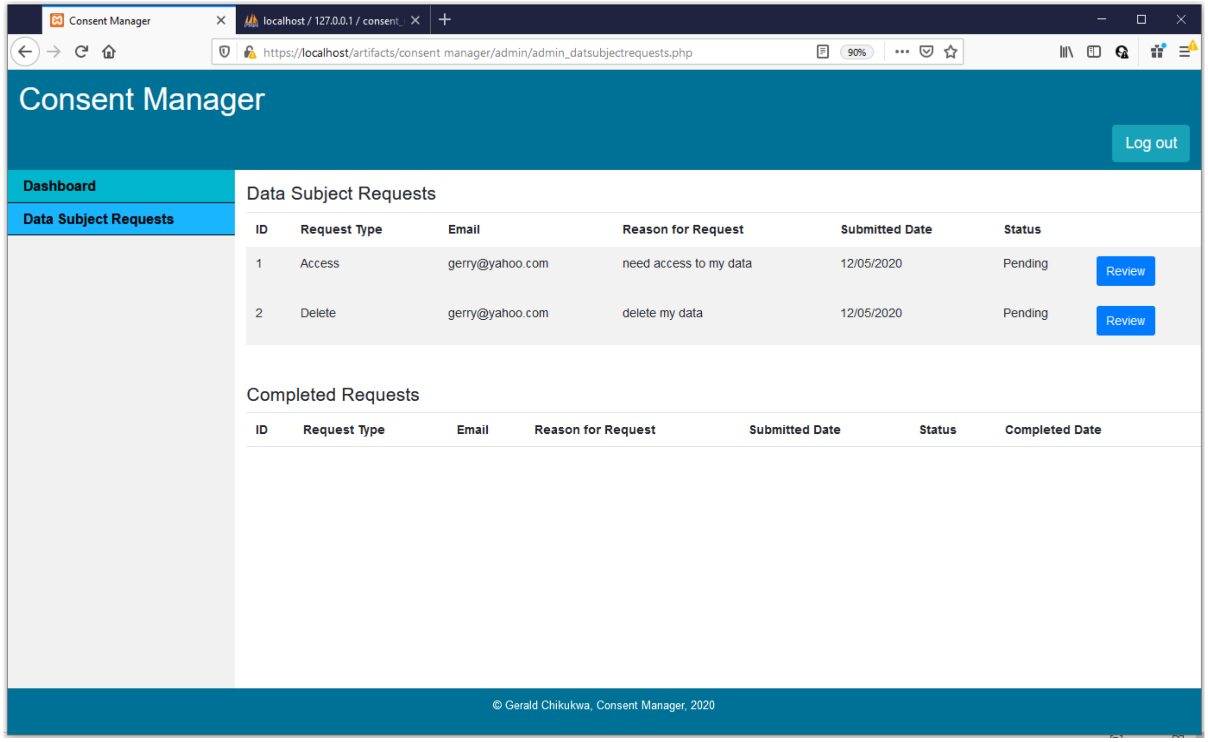
Consent	Description	Email	Consent Date

Revoked Consent

Consent	Description	Email	Consent Date	Revoked Date

© Gerald Chikukwa, Consent Manager, 2020

Figure 25. Consent Manager Admin Dashboard


Consent Manager
localhost / 127.0.0.1 / consent_
https://localhost/artifacts/consent manager/admin/admin_datsubjectrequests.php
90%
Log out
Dashboard
Data Subject Requests

Consent Manager

Data Subject Requests

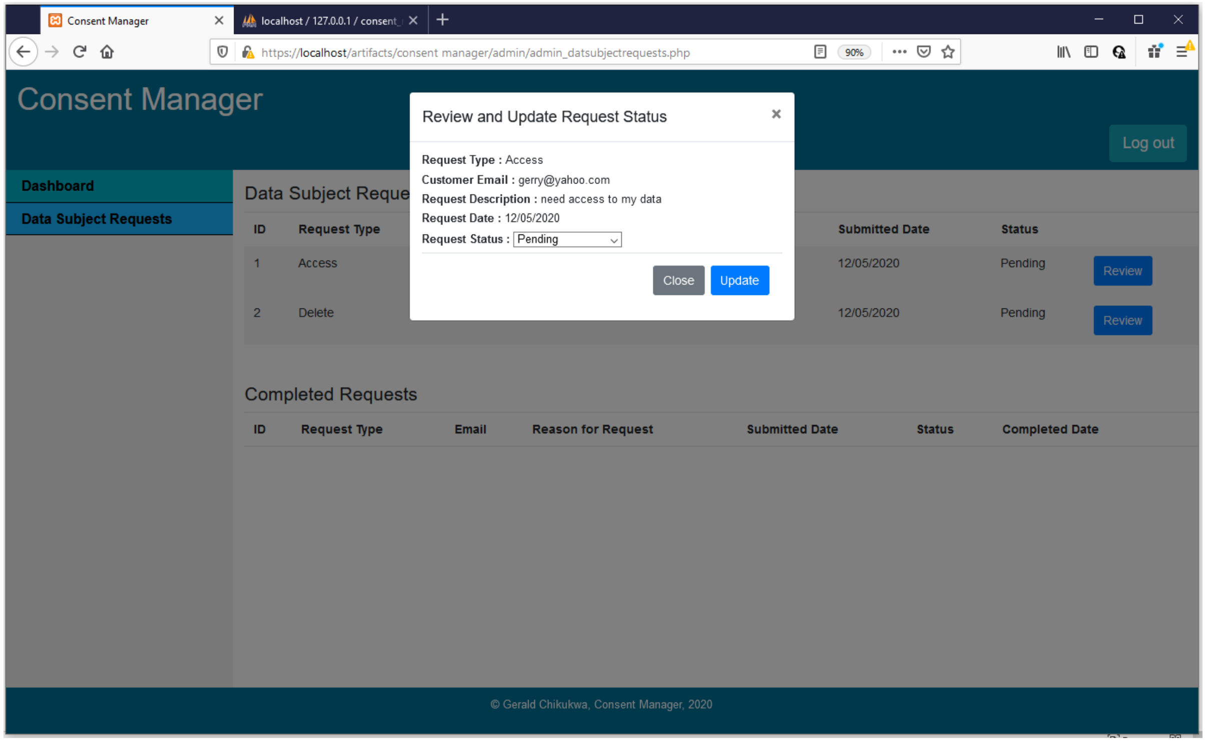
ID	Request Type	Email	Reason for Request	Submitted Date	Status	
1	Access	gerry@yahoo.com	need access to my data	12/05/2020	Pending	Review
2	Delete	gerry@yahoo.com	delete my data	12/05/2020	Pending	Review

Completed Requests

ID	Request Type	Email	Reason for Request	Submitted Date	Status	Completed Date

© Gerald Chikukwa, Consent Manager, 2020

Figure 26. Consent Manager Admin Data Subject Requests


Consent Manager
localhost / 127.0.0.1 / consent_
https://localhost/artifacts/consent manager/admin/admin_datsubjectrequests.php
90%
Consent Manager
Log out
Dashboard
Data Subject Requests
Review and Update Request Status
Close
Update
Review
Review

Request Type : Access
Customer Email : gerry@yahoo.com
Request Description : need access to my data
Request Date : 12/05/2020
Request Status : Pending

Data Subject Reque

ID	Request Type	Submitted Date	Status	
1	Access	12/05/2020	Pending	Review
2	Delete	12/05/2020	Pending	Review

Completed Requests

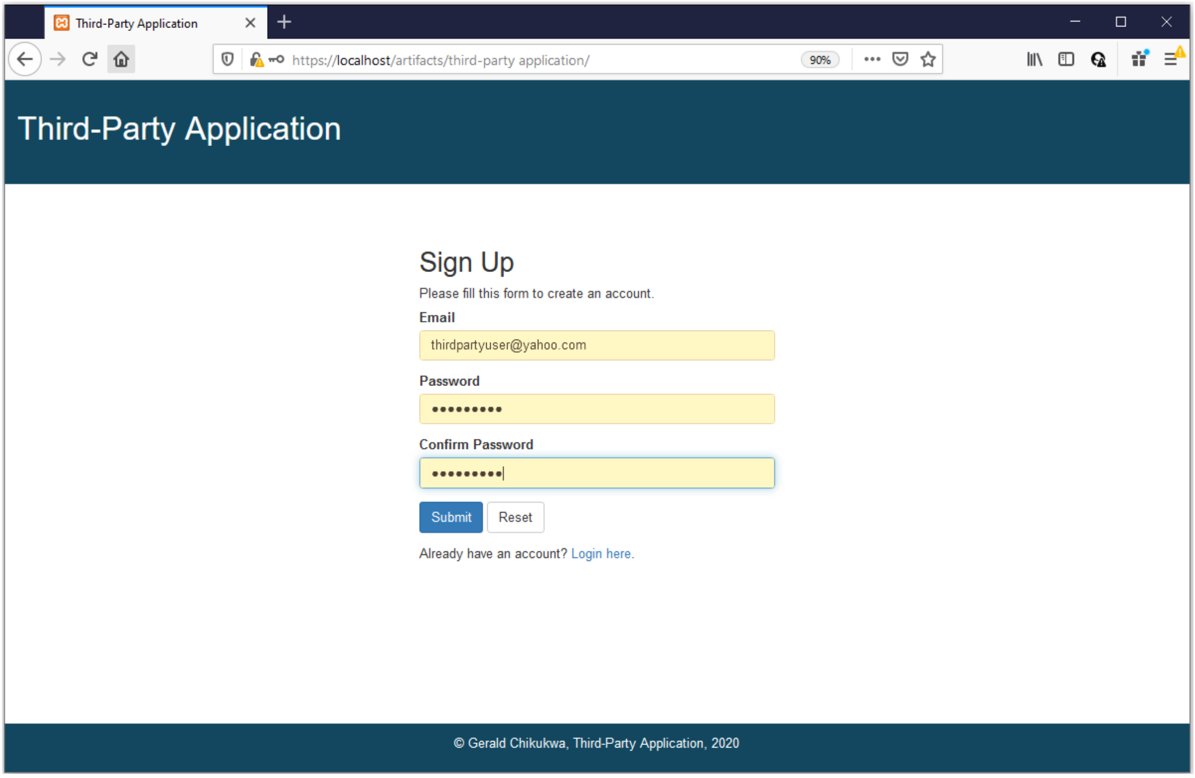
ID	Request Type	Email	Reason for Request	Submitted Date	Status	Completed Date

© Gerald Chikukwa, Consent Manager, 2020

Figure 27. Consent Manager Admin Review and Update Request Status

6.4 Consent Enforcement

The third-party user can create a profile as shown in Figure 28 and log into the third-party application, as shown in Figure 29. In logging in, the data access layer will run necessary queries to fetch the personal information they are granted access to. When the user is logged on, they can access the third-party application dashboard. The dashboard displays all the personal information for all the users who consented to share their data, as presented in Figure 30. Consent enforcement is done through the data access layer, which regulates access based on consent. In Figure 31, there is the code for the data access layer, which shows how it regulates access. The data access layer code has a query that fetches the personal information for all the users that consented to data sharing.



Third-Party Application

Sign Up

Please fill this form to create an account.

Email

thirdpartyuser@yahoo.com

Password

•••••••••

Confirm Password

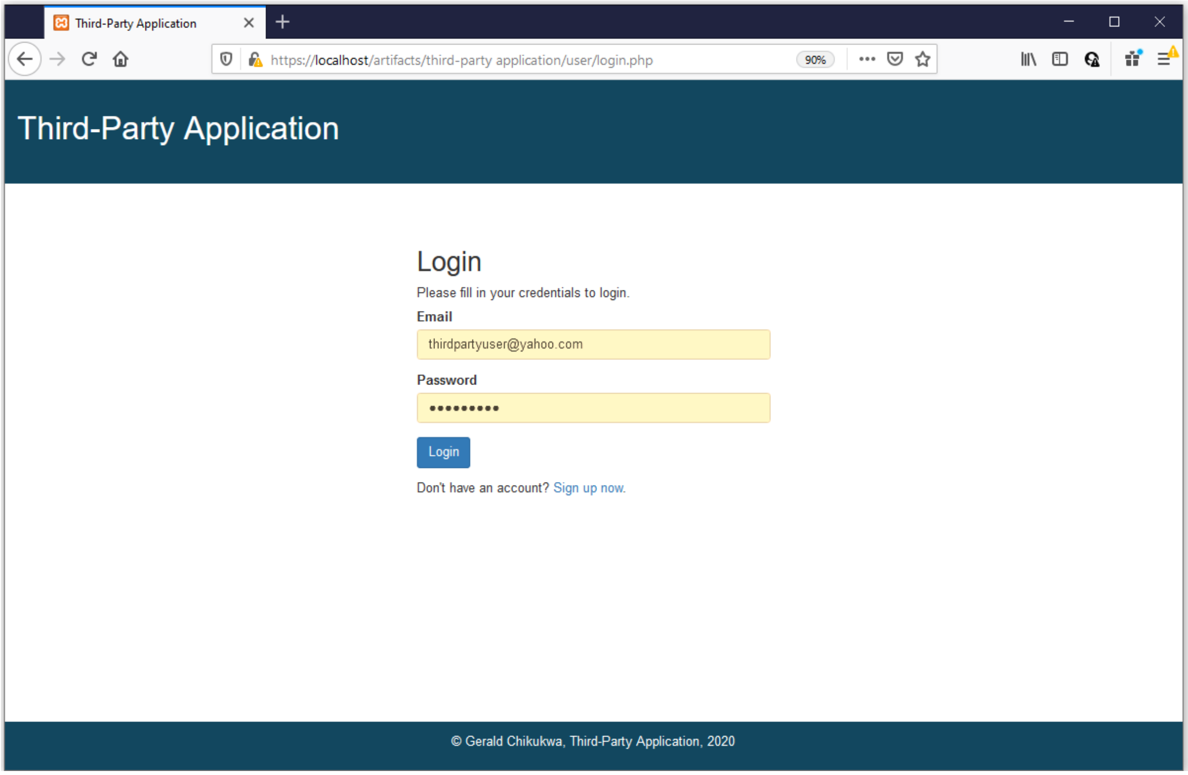
•••••••••

Submit Reset

Already have an account? Login here.

© Gerald Chikukwa, Third-Party Application, 2020

Figure 28. Third-Party Application Registration


Third-Party Application
https://localhost/artifacts/third-party application/user/login.php
90%

Third-Party Application

Login

Please fill in your credentials to login.

Email

thirdpartyuser@yahoo.com

Password

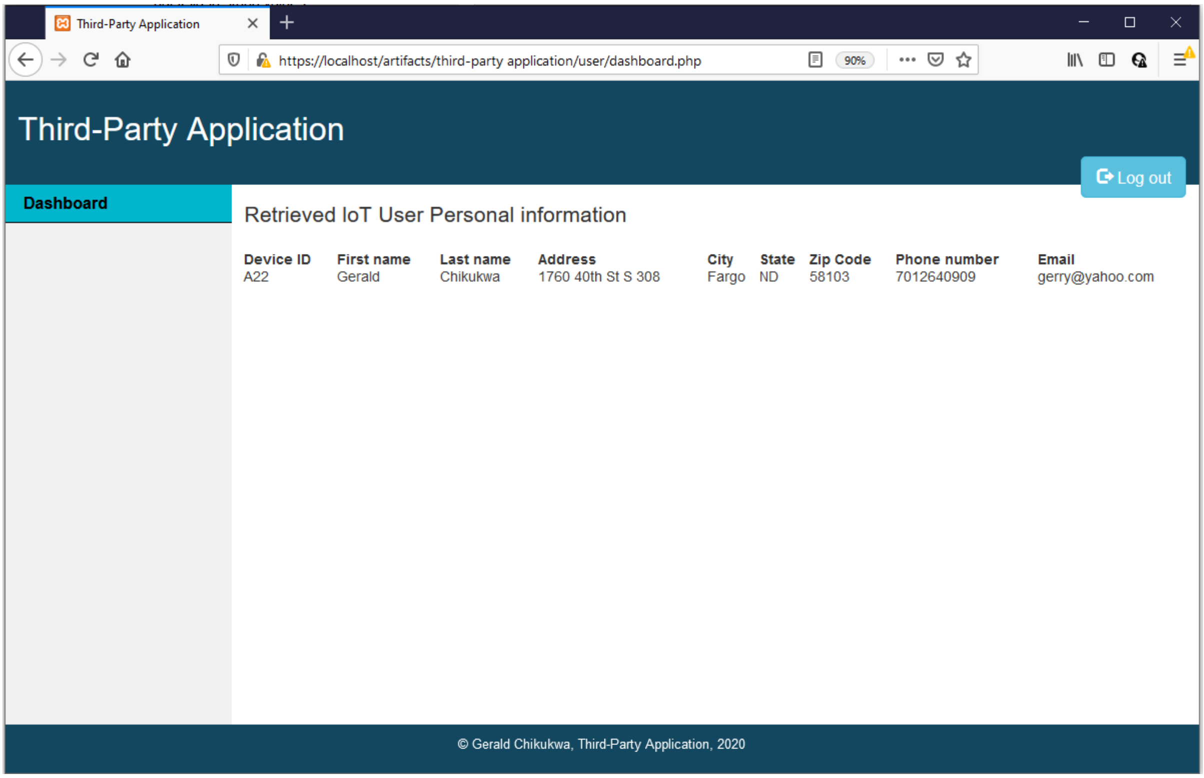
•••••••••

Login

Don't have an account? Sign up now.

© Gerald Chikukwa, Third-Party Application, 2020

Figure 29. Third-Party Application Login


Third-Party Application
https://localhost/artifacts/third-party application/user/dashboard.php
90%
Log out
Dashboard

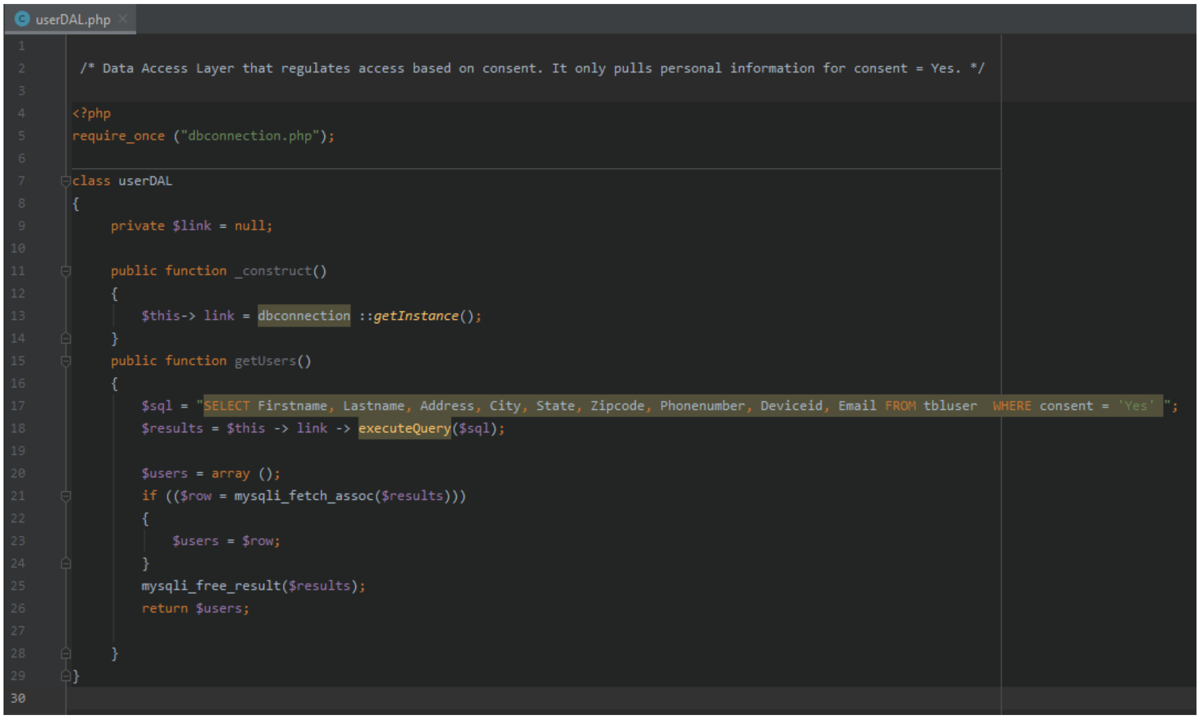
Third-Party Application

Retrieved IoT User Personal information

Device ID	First name	Last name	Address	City	State	Zip Code	Phone number	Email
A22	Gerald	Chikukwa	1760 40th St S 308	Fargo	ND	58103	7012640909	gerry@yahoo.com

© Gerald Chikukwa, Third-Party Application, 2020

Figure 30. Retrieved IoT User Personal Information



```

 /* Data Access Layer that regulates access based on consent. It only pulls personal information for consent = Yes. */

<?php
require_once ("dbconnection.php");

class userDAL
{
     private $link = null;

     public function _construct()
     {
         $this-> link = dbconnection ::getInstance();
     }
     public function getUsers()
     {
         $sql = "SELECT Firstname, Lastname, Address, City, State, Zipcode, Phonenumber, Deviceid, Email FROM tbluser  WHERE consent = 'Yes' ";
         $results = $this -> link -> executeQuery($sql);

         $users = array ();
         if (($row = mysqli_fetch_assoc($results)))
         {
             $users = $row;
         }
         mysqli_free_result($results);
         return $users;

     }
}

```

Figure 31. Data Access Layer

6.5 Summary

This chapter introduces different components that we developed in our solutions. We discussed data collection, consent collection, consent management, and consent enforcement. In this chapter, we also demonstrated how our IoT implementation works, the use of the user web application and how consent is collected, the consent manager's use and how it manages consent, the use of the third-party application, and how it enforces consent. The components we demonstrated follow GDPR data protection principles, GDPR consent requirements, and GDPR data subject rights.

CHAPTER 7

TESTING, EVALUATION, AND RESULTS

This chapter focuses on evaluating our artifacts to ensure that they follow GDPR consent requirements within our framework. To evaluate our solutions, we (1) compared our solution against similar solutions, (2) utilized our excel consent auditing tool in auditing the use case above. To validate our work, we worked with Cody Veselka, an Internal Audit Manager at WEX Inc., to conduct the audit. We also went through GDPR data protection requirements, consent collection requirements, consent management requirements, and consent enforcement requirements. Table 9 summarizes the location of each piece of evidence used in our testing.

Table 9. Evidence Location

Layer	Evidence
Data Collection	Evidence 1 - Chapter 6, Figure 17. Privacy Policy
	Evidence 2 - Chapter 6, Figure 9. Modbus Setting Page
Consent Collection	Evidence 3 - Chapter 6, Figure 16. Consent Form
Consent Management	Evidence 4 - Chapter 6, Figure 25. Consent Manager Admin Dashboard
	Evidence 5 - Chapter 6, Figure 21. Consent Manager User Dashboard
	Evidence 6 - Chapter 6, Figure 23. Consent Manager Make a Request Form
	Evidence 7 - Chapter 6, Figure 22. Consent Manager- Data Subject Requests
Consent Enforcement	Evidence 8 - Chapter 6, Figure 31. Data Access Layer

7.1 Evaluation by Comparison to Similar Solutions

Evaluating our solution against similar solutions enables us to assess the strength and weakness of our solution. In this research, we selected three similar solutions to compare with our solution. The three solutions are the ones that we selected from the literature review. These three solutions include:

1. Blockchain Consent Management (Genestier et al., 2017)
2. ADVOCATE Consent Management (Rantos et al., 2018)
3. Consent Management Suite (Heinze et al., 2011)

Table 10. Consent Framework vs. Existing Solutions

Solutions	**Informed Consent**	**Consent Collection**	**Consent Management**	**Consent Enforcement**	**Auditing Process**
Our Solution - Consent Framework	Yes	Yes	Yes	Yes	Yes
Blockchain Consent Management (Genestier et al., 2017)	No	Yes, but it lacks the informed consent	Yes	Yes	No
ADVOCATE Consent Management (Rantos et al., 2018)	Yes	Yes, but it lacks an intelligent component to assist users in making the right decision	Yes, users manage consent policies.	Yes, consent policies regulate access to user’s data.	No

		before providing consent.			
Consent Management Suite (Heinze et al., 2011)	Yes	Yes, but consent is collected as a CDA document with embedded XACML through the Consent Creator Service.	Yes, the Consent Management Service receives and stores consent documents.	Yes, it uses the XACML policies to regulate access to data. XACML has performance issues.	No

Compared to the three other solutions above, our solution provides all the coverage on informed consent, consent collection, consent management, consent enforcement, and providing a consent auditing process. It also follows GDPR consent requirements which are important in being GDPR compliant.

7.2 Data Collection Testing

We use the data collection testing worksheet in Table 11 to test the GDPR data protection principles against our IoT implementation. The implementation is tested based on the legality, transparency, purpose, accuracy, data retention, and secure processing of data. The GDPR data protection principles are requirements for organizations that collect, process, and store personal data (European Union, 2016).

Table 11. Data Collection Testing Worksheet

Layer One	**GDPR Regulation**	**Question Number**	**Questions**	**IoT Data Collection Evidence**	**Testing Method**	**Is the Requirement Satisfied? (Yes/No)**	**Comments**
Data Collection	Article 5(1)(a)	1	Is data being collected legally and transparently?	Evidence 1	Inspection / Examination	Yes	Reviewed the Privacy Policy.
	(b)	2	Is there a purpose or reason for the collection of data?		Inspection / Examination	Yes	
	(c)	3	Is data collected necessary for the legal goal of the organization?		Inspection / Examination	Yes	
	(d)	4	Is the data being collected accurately?		Inspection / Examination	Yes	
	(e)	5	Is there a data retention policy?		Inspection / Examination	Yes	
	(f)	6	Is data being processed securely?	Evidence 2	Inspection / Examination	Yes	Reviewed IoT Gateway

							Configuration
	IoT Scalability	7	Is the IoT solution scalable?	In our use case, we used one smart meter and gateway. We can scale the use case by: 1. Adding a smart meter and gateway in multiple locations. 2. Move the user web application to the cloud to handle multiple connections from many locations and handle large volumes of data. Also, move the consent manager and third-part application to the cloud as well.			

7.3 Consent Collection Testing

In the consent collection testing worksheet in Table 12, we focus our testing on consent collection. We look at the consent form's functionality in our solution and how it follows GDPR consent requirements.

Table 12. Consent Collection Testing Worksheet

Layer Two	GDPR Regulation	Question Number	Questions	Consent Collection Evidence	Testing Method	Is the Requirement Satisfied? (Yes/No)	Comments
	Article 4(11)	1	Is consent freely given, specific, informed, and unambiguous?		Inspection / Examination	Yes	

Consent Collection		2	Does consent collection indicate data subject wishes with clear affirmative action and signifying agreement to process their personal data?	Evidence 3	Inspection / Examination	Yes	Reviewed the consent form
	Article 7(2)	3	Is consent given in a context that does not concern other matters?		Inspection / Examination	Yes	
		4	Is the request for consent presented in a manner that is clearly distinguishable from other matters?		Inspection / Examination	Yes	
		5	Is the request presented in an intelligible, easily accessible form, in a clear and plain language?		Inspection / Examination	Yes	

7.4 Consent Management Testing

We utilize the consent management testing worksheet in Table 13 to test how consent is stored and managed in the consent manager. The testing looks at the consent manager and how it fulfills GDPR consent management requirements and data subject rights.

Table 13. Consent Management Testing Worksheet

Layer Three		**GDPR Regulation**	**Question Number**	**Questions**	**Consent Management Evidence**	**Testing Method**	**Is the Requirement Satisfied? (Yes/No)**	**Comments**
Consent Management	**Conditions of Consent**	Article 7(1)	1	Can the controller demonstrate that the data subject consented to process their personal data?	Evidence 4	Inspection / Examination	Yes	Reviewed the Consent Manager for collected consent
		Article 7(3)	2	Can data subjects withdraw their consent at any given time?	Evidence 5	Inspection / Examination	Yes	Reviewed the Consent Manager for consent revocation. functionality
	Data Subject Rights	Article 15	3	Can data subjects request access to their data?		Inspection / Examination	Yes	
		Article 16	4	Can data subjects request rectification of their data?		Inspection / Examination	Yes	

		Article 17	5	Can data subjects request data erasure?	Evidence 6	Inspection / Examination	Yes	Reviewed the Consent Manager for the data subject request functionality
		Article 18	6	Can data subjects request the restriction of data processing?		Inspection / Examination	Yes	
		Article 19	7	Can a data subject request be informed?		Inspection / Examination	Yes	
		Article 20	8	Can data subjects request data portability?		Inspection / Examination	Yes	
		Article 21	9	Can data subjects request to object to data processing?		Inspection / Examination	Yes	
		Article 22	10	Can data subjects request not to be subject to automated individual decision making?		Inspection / Examination	Yes	
			11	How can you track that the data subject requests are handled in a timely manner? (within 30-45 days)	Evidence 7	Inspection / Examination	Yes	Review the requested date and completion date of the request in the Consent Manager.

7.5 Consent Enforcement Testing

The consent enforcement testing worksheet in Table 14 is used to test consent enforcement requirements to ensure that access is granted based on user consent (Yes or No).

Our testing involved looking at how the consent mechanism works by review the data access layer code to understanding how it works.

Table 14. Consent Enforcement Testing Worksheet

Layer Four	**Consent**	**Question Number**	**Questions**	**Consent Enforcement Evidence**	**Testing Method**	**Is the Requirement Satisfied? (Yes/No)**	**Comments**
Consent Enforcement	Yes	1	Is access granted to user’s data based on consent?	Evidence 8	Inspection / Examination	Yes	Reviewed the Data Access Layer code
	No	2	Is access to user’s data restricted based on consent?		Inspection / Examination	Yes	

7.6 Results

Our evaluation aims to ensure that our implementation and the artifacts we developed follow GDPR data protection principles, consent collection, management requirements, and consent enforcement requirements. We tested data collection from the smart meter to the web user application against the GDPR data protection principles. In the web user application, we tested consent collection through the pop-up consent form. Tested consent management from the user web application to the consent manager compared to GDPR consent management and data subject rights requirements. We also tested consent enforcement against consent enforcement requirements.

After our testing, we are comfortable that our implementation and artifacts developed meet GDPR data protection principles, GDPR consent requirements, GDPR consent management, data subject rights requirements, and enforcement requirements. It also indicates that our proposed consent framework can ensure GDPR consent compliance in our use case in Chapter 6.

7.7 Summary

This chapter audited our use case in Chapter 6 using the auditing tool testing worksheets for data collection, consent collection, consent management, and consent enforcement on our implementation and artifacts. The other evaluation was on our solution compared to a similar solution. The comparison showed that our solution provided coverage on informed consent, consent collection, consent management, consent enforcement, and providing a consent auditing process. The evaluation results show that the implementation and artifacts meet GDPR consent compliance, and our consent framework can help organizations be compliant.

CHAPTER 8

SUMMARY AND CONCLUSION

The proposed consent framework allows organizations to fulfill GDP consent requirements by following the steps: data collection, consent collection, consent management, consent enforcement, and consent auditing. This dissertation introduces a solution that collects consent from a user, manages consent, enforces consent, and audit consent. The user interacts with the framework during data collection, consent collection, consent management. On the other hand, the data controller interacts with the framework during consent management and consent auditing. Third-party organizations interact with the framework during consent enforcement.

8.1 Summary

In this research, we developed a consent framework that follows GDPR consent requirements. The framework has five steps: data collection, consent collection, consent management, consent enforcement, and consent auditing. The data collection of the framework deals with collecting data from IoT devices and applications. In this step, we include GDPR principles which are lawfulness, fairness, transparency, the purpose of limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality (European Union, 2016). Step two of the framework involves consent collection. Consent is collected according to GDPR consent requirements. Consent is informed, given freely, specific, and given in affirmative action (European Union, 2016). The third step of the framework is consent management, which manages consent collected from the consent collection. Consent management embeds GDPR conditions of consent and data subject rights. The fourth step is consent enforcement, which regulates access to personal data based on consent. The last step of the framework is consent auditing, enabling data controllers to test their implementation or environment to ensure data collection, consent collection, consent management, and consent enforcement are GDPR consent compliant.

We implemented a smart electricity meter that sent data to a remote server database in the use case. The web user application accesses meter data to display for the user. When the data subject (user) logs on the web user application, a pop-up consent form appears, and the user is informed on how their information is collected, used, and disclosed. The user makes their decision by selecting options on the form and submitting the form. Consent information is sent through an API to the consent manager.

The consent manager manages and stores what the user has agreed or disagreed on based on the three statements discussed above. The consent manager allows the data subject to review and change consent and makes data subject requests through a dashboard. It also tracks data subjects' requests from initial placement of request to completion. The data controller has a dashboard in the consent manager to view all the consent collected and fulfill data subject requests.

Third-party organizations are given access to the web user application's personal data. It is done through the data access layer, which regulates access based on consent. The data access layer code has a query that fetches the personal information for all the users that consented to data sharing.

8.2 Contributions

8.2.1 Consent Framework

The framework includes data collection, consent collection, consent management, consent enforcement, and consent auditing. The first three components follow GDPR requirements, while the last two components aid in GDPR compliance. The consent framework addresses consent issues that pertain to the Internet of Things. Rantos et al. (2018) also proposed a similar but different framework called the Advocate that enables GDPR compliant processing of personal data based on the IoT ecosystem. The framework has the consent management component, consent notary component, and intelligence component. Our consent framework captures all aspects of GDPR consent requirements to ensure coverage over IoT.

8.2.2 Consent Manager

The consent management component of our framework provides a consent manager. The consent manager we developed collects consent through an API in an informed and unambiguous way. The consent manager has a dashboard that manages consent and allows the user to revoke their consent and make data subject requests. It also enables the data controller (admin) to view all the consent through a dashboard and fulfill data subject requests. The consent manager is developed to ensure GDPR consent management and data subject rights requirements are embedded to ensure compliance. Our consent manager is developed based on the conditions of consent article 7(1) (3) and data subject rights articles 15-22 requirements.

8.2.3 Consent Auditing Tool

The consent auditing component of our framework provides an excel consent auditing tool. The consent auditing tool comprises data collection, consent collection, consent management, and consent management sections. Each section has requirements that need to be inspected or examined to ensure that our solution is GDPR compliant. The second part of each section provides audit worksheets used to validate compliance. Audit worksheets are there to record and track audit evidence obtained during the compliance audit by supporting the audit to assure that the audit was performed according to GDPR requirements.

Our literature review indicated that the existing solutions and frameworks lack the auditing component. There are no discussions on auditing consent or proposed solutions. Auditing is treated as a separate process. The advantages of our framework are that we include auditing and provide an auditing tool. The auditing tool allows an auditor to manually document their findings as they inspect/examine processes, technologies, applications, and GDPR compliance. Therefore, auditors do not use paper checklists, which are ineffective and prone to errors, rather than using an audit tool.

8.3 Limitations

There are some limitations to this research. The first limitation is that we developed and tested our use case in a virtual environment. We also used one smart meter, one user, and an administrator for demonstrating purposes in our implementation. The second limitation is that the administrator must look up each user’s consent on data sharing in the consent manager, go to the user web application database, and update whether they consent or not to data sharing. The third limitation is that our use case was based on a smart meter. However, this is not fully representative of PII variables. There are many different IoT devices with different implementations. Therefore, each IoT device may collect various PII from other devices.

The issue with the limitations above is that IoT devices are being adopted in their millions each year. Therefore, it is important to address the limitations before implementing the solution in an enterprise environment. Another issue is that we need to continuously monitor GDPR amendments and changes to ensure new requirements coverage. It requires corresponding updates in the framework and the artifacts.

Enforcing GDPR in large enterprises can be challenging due to scalability and interoperability. The increasing adoption of IoT brings the issue of scalability. IoT ecosystem utilizes different devices, platforms, communication protocols, and so on. The diversity in IoT devices brings us to the problem of interoperability. IoT communication systems should provide seamless connectivity in constrained devices. However, if there is insufficient interoperability amongst IoT devices, there will arise technical and business problems. The interoperability problems are from the heterogeneous nature of IoT devices, characteristics, and technical requirements. In our use case, we implemented one electricity smart meter and one gateway. Our implementation does not address the scalability and interoperability issues in the IoT.

8.4 Future Work

Future research will focus on implementing our framework and solutions in an enterprise environment. The enterprise environment allows us to test our solutions and implementation on a large scale. The idea is to add a variety of IoT devices in the implementation to simulate real-world scenarios. It will ensure that our framework and solutions can be implemented in various IoT devices, applications, and environments.

As stated in the limitations section, another opportunity for future work is the manual nature of copying consent from one database to the other. Future research will design the data access layer to automatically check if the user consented to data sharing in the consent manager and then run a query to display personal data based on the consent. The solution does not require the data controller to manually copy consent from the consent manager to the IoT web user application. The manual nature of the solution is not ideal on a large scale.

Finally, we plan to work on scalability and interoperability in enforcing GDPR in the enterprise environment. The enterprise environment has interesting use cases for IoT. Use cases range from supply chain optimization, surveillance and security, fleet management, vehicle telematics and infotainment, facilities management, remote health monitoring, and so on. Since we have a generic consent framework that can be applied to any IoT environment to deal with GDPR consent compliance, organizations can have multiple different IoT environments, which can be challenging to collect and manage consent. To solve interoperability problems, we can create API's that collect consent from different IoT environments to the consent manager. The consent manager server can be scaled to handle large volumes of data from multiple IoT environments.

REFERENCES

Bhattarai, S., & Wang, Y. (2018). End-to-End Trust and Security for Internet of Things Applications. *Computer*, *51*(4), 20–27. https://doi.org/10.1109/MC.2018.2141038

Brown, E. (2016). 21 Open Source Projects for IoT. https://www.linux.com/news/21-open-source-projects-iot/

Can, O. (2013). A Semantic Model for Personal Consent. *Metadata and Semantics Research Conference*, *390*, 146–151. https://doi.org/10.1007/978-3-319-03437-9_15

Choi, S.(2016). Global Sweep Finds Shortfalls in Privacy Protections of IoT Devices. Data Protection & Privacy. https://www.hlmediacomms.com/2016/10/10/global-sweep-finds-shortfalls-in-privacy-protections-of-iot-devices/

Colina, M., Bartolucci, M., Coralli, A.V., & Corazza, G.E.(2014). Internet of Things application layer protocol analysis over error and delay prone links. Advanced Satellite Multimedia Systems Conference and the 13th Signal Processing for Space Communication Workshop (ASMS/SPSC), pp. 398-404.

Cleven, A., Gubler, P., & Huner, K. M. (2009). Design alternatives for the evaluation of design science research artifacts. Paper presented at the Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, Philadelphia, Pennsylvania

Dave, M., Patel, M., Doshi, J., & Arolkar.(2020). *Chapter 15. Ponte message broker bridge configuration using MQTT and CoAP protocol for interoperability of IoT*. Springer Science and Business Media LLC.

European Union. (2016). Regulation 2016/679. *Official Journal of the European Communities*, *2014*(March 2014), 1–88. https://doi.org/http://eurlex.europa.eu/pri/en/oj/dat/2003/l_285/l_28520031101en00330037.pdf

Evans, D.(2011). The Internet of Things: How the Next Evolution of the Internet is Changing Everything. http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Gartner, “Gartner Says 8.4 Billion Connected ‘Things’ Will Be in Use in 2017, Up 31 Percent From 2016” (press release, Gartner, February 7, 2017). https://www.gartner.com/newsroom/id/3598917

Genestier, P., Zouarhi, S., Limeux, P., Excoffier, D., Prola, A., Sandon, S., & Temerson, J.-M. (2017). Blockchain for Consent Management in the eHealth Environment: A Nugget for Privacy and Security Challenges. *Journal of the International Society for Telemedicine and EHealth*, *5*(e24), 1–4. Retrieved from https://journals.ukzn.ac.za/index.php/JISfTeH/article/view/269

Maayan, G. David. (2020). The IoT Rundown For 2020: Stats, Risks, and Solutions. *Weak passwords, Insecure Network Services, and a Lack of Secure Update mechanisms top the Risks list for Companies utilizing IoT Technology*. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=1

Gupta, A., Christie, R., & Manjula, R.(2017). Scalability in the Internet of Things: Features, Techniques and Research Challenge. International Journal of Computational Intelligence Research, Volume 13(7), 1617-1627. Retrieved from http://www.ripublication.com/ijcir17/ijcirv13n7_06.pdf

Gupta, K., & Shukla, S. (2016). Internet of Things: Security challenges for next-generation networks. *2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016*, (Iciccs), 315–318. https://doi.org/10.1109/ICICCS.2016.7542301

Heinze, O., Birkle, M., Köster, L., & Bergh, B. (2011). The architecture of a consent management suite and integration into IHE-based regional health information networks. *BMC Medical Informatics and Decision Making*, *11*(1). https://doi.org/10.1186/1472-6947-11-58

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75-105.

Kampling, H., Klesel, M., & Niehaves, B. (2016, 5-8 Jan. 2016). On Experiments in Design Science Research and Theory Development: A Literature Review. Paper presented at the 2016 49th Hawaii International Conference on System Sciences (HICSS).

Kulkarni Sanjeev Kulkarni Lecturer Professor, S. (2017). Communication Models in Internet of Things: A Survey. *IJSTE-International Journal of Science Technology & Engineering* |, *3*(11), 87–91. Retrieved from www.ijste.org

Luger, E., & Rodden, T. (2013). Terms of agreement: Rethinking consent for pervasive computing. *Interacting with Computers*, *25*(3), 229–241. https://doi.org/10.1093/iwc/iws017

Luger, Ewa, & Rodden, T. (2013). An informed view on consent for UbiComp, 529. https://doi.org/10.1145/2493432.2493446

Magrassi, P.,& Berg, T.(2002). A World of Smart Objects. Gartner research report

Mohalik, S.K., Narendra, N.C., Badrinath, R., Jayaraman, M.B., & Padala, C.(2016). Dynamic Semantic Interoperability of Control in IoT-based Systems: Need for Adaptive Middleware. 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics, and Cloud)(I-SMAC). https://doi.org/10.1109/I-SMAC49090.2020.9243377

Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of Things: Survey on Security and Privacy, 1–16. https://doi.org/10.1080/19393555.2018.1458258

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

Offermann, P., Levina, O., Sch, M., #246, nherr, & Bub, U. (2009). Outline of a design science research process. Paper presented at the Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, Philadelphia, Pennsylvania.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems. https://doi.org/10.2753/mis0742-1222240302

Rantos, K., Drosatos, G., Demertzis, K., Ilioudis, C., & Papanikolaou, A. (2018). Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem. *Proceedings of the 15th International Joint Conference on E-Business and Telecommunications*, (July), 572–577. https://doi.org/10.5220/0006911005720577

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Rose, K., Eldridge, S., & Chapin, L. (2015). The Internet of Things: An Overview - Understanding the Issues and Challenges of a More Connected World. *The Internet Society (ISOC)*, (October), 80. https://doi.org/10.5480/1536-5026-34.1.63

Rosner, G., & Kenneally, E. (2018). *Privacy and the Internet of Things. Emerging Framework for Policy and Design*. UC Berkeley Center for Long-Term Cybersecurity/Internet of

Things Privacy Forum. https://cltc.berkeley.edu/wp-content/uploads/2018/06/CLTC_Privacy_of_the_IoT-1.pdf

Russello, G., Dong, C., & Dulay, N. (2008). Consent-based workflows for healthcare management. *Proceedings - 2008 IEEE Workshop on Policies for Distributed Systems and Networks, POLICY 2008*, 153–161. https://doi.org/10.1109/POLICY.2008.22

Said, O., & Masud, M. (2013). Towards the Internet of Things: Survey and Future Vision. *Omar Said & Mehedi Masud International Journal of Computer Networks*, *5*(1), 2013–1. https://doi.org/5859 [pii]

Sethi, P., & Sarangi, S. R. (2017). Internet of Things : Architectures, Protocols, and Applications, *2017*. https://doi.org/10.1155/2017/9324035

Singh, S., & Singh, N. (2016). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015*, 1577–1581. https://doi.org/10.1109/ICGCIoT.2015.7380718

Terkawi, A., Innab, N., Al-Amri, S., & Al-Amri, A. (2018). Internet of Things (IoT) Increasing the Necessity to Adopt Specific Type of Access Control Technique. *21st Saudi Computer Society National Computer Conference, NCC 2018*, 1–5. https://doi.org/10.1109/NCG.2018.8593084

Ulbricht, M. R., & Pallas, F. (2016). CoMaFeDS: Consent management for federated data sources. *Proceedings - 2016 IEEE International Conference on Cloud Engineering Workshops, IC2EW 2016*, 106–111. https://doi.org/10.1109/IC2EW.2016.30

Vaishnavi, V. and Kuechler, W. (2004). Design science research in information systems. Retrieved from http://www.desrist.org/design-research-in-information-systems/

Wakenshaw, S. Y. L., Maple, C., Gomer, R., & Ghirardello, K. (2018). Mechanisms for Meaningful Consent in the Internet of Things. *Living in the Internet of Things: Cybersecurity of the IoT*, 1–10. https://doi.org/10.1049/cp.2018.0014

APPENDICES

APPENDIX A

USER WEB APPLICATION README FILE

Program Description

This application is used as a user portal for IoT users accessing smart meter data. The smart meter sends meter data through the IoT gateway to the remote database associated with the user web application. When users access the user web application, they can see their electricity consumption data. The data is sent on an hourly basis to the remote database for the user. The user can only access all the data that is linked to their smart meter.

Technical Specification

- Windows Environment
- PHP 8.0.0
- MySQL 5.5.0

System Features

- **Dashboard** – The dashboard displays all the electricity consumption data that is collected from the smart meter on an hourly basis.
- **User Profile Tab** – The user profile displays the user’s personal information (first name, last name, address, phone number, email, and device id).

Note: The User Web Application complete code is available at

https://github.com/gchikukwa/artifacts/tree/main/user%20web%20app

APPENDIX B: CONSENT MANAGER README FILE

Program Description

The consent manager application manages collected consent from the user web application. Users can access and manage their consent in the consent manager. The users can view their consent, revoke consent, and request their data subject rights. Administrators can view all the consent provided by all users and fulfill data subject requests. The consent manager tracks all actions by the user and administrator by keeping an audit trail for compliance.

Technical Specification

- Windows Environment
- PHP 8.0.0
- MySQL 5.5.0

System Features

- **Dashboard –** The user/admin dashboard displays three sections consent, did not consent, and revoked consent. In the ‘consent’ section, consented information is displayed. The ‘did not consent’ section displays consent that the user disagrees with. On the other hand, the ‘revoked consent’ section shows all the user's consent revoked.
- **Data Subject Requests Tab –** The user can make a data subject request according to data subject rights. Users can make a request, and the data subject can fulfill that request.

Note: Consent Manager complete code is available at

https://github.com/gchikukwa/artifacts/tree/main/consent%20manager

APPENDIX C: THIRD-PARTY APPLICATION README FILE

Program Description

The third-party application allows third-party organizations to access user's personal information. Access to the user's personal data is based on the consent provided by the user. If the user consented to data sharing, access is granted; otherwise, access is not granted. When access is granted, the third-party organization can access the user's personal data in the third-party application dashboard.

Technical Specification

- Windows Environment
- PHP 8.0.0
- MySQL 5.5.0

System Features

- **Dashboard** – The dashboard only displays personal information that the user has agreed to share.

Note: The Third-Party Application complete code is available at https://github.com/gchikukwa/artifacts/tree/main/third-party%20application

APPENDIX D: CONSENT AUDITING TOOL FILE

Tool Description

The excel consent auditing tool can be used to audit consent. The auditing tool audits data collection, consent collection, consent management, and consent enforcement. Auditing is done against GDPR requirements and other requirements in the consent auditing tool. The consent auditing tool can ensure GDPR compliance if followed step by step.

Note: The Consent Auditing Tool excel spreadsheet is available at https://github.com/gchikukwa/artifacts/blob/main/Auditing%20Tool.xlsx