RESEARCH ARTICLE OPEN ACCESS

# Internet of Things Based Data Integration Ontology in Cybersecurity

Ahmed Abdullah Kudini
*A research project submitted for the requirements of the degree ofExecutive Master of Cybersecurity*

## Abstract

Smart houses depend on the implementation of the Internet of Things (IoT) to produce efficient housing and ensure smart consumption in our current scarce economic state. Machines have proven their ability to control a home system in different aspects like security, electricity, water consumption, air conditioning, and lighting. Results show a significant change in the statistics comparing consumption under human control vs. under machine control. This research will explore the new field of IoT and address the current global crises that we face and will try to show the roles that IoT installation will play in trying to lower the human domestic impact on increasing the global ECO crisis and overconsumption. Finally, this dissertation will conclude by showing the security factor that this smart system excels in and proving that it can reduce consumption and be as ecofriendly as possible.

**Key Word**: IoT, Security, ECO, Machine, Attacks

Date of Submission: 20-10-2024 Date of acceptance: 04-11-2024

## I. Introduction

With the diffusion of the Internet of things technologies, most smart home devices are connected through a unified network that receives its commands from specific applications on phones. Still, this convenient technology may instantly turn into a weapon in the hands of "hackers." And in this context, serious security holes have emerged that allow hackers to take control of the control unit of the lights connected to the network and the entire network.

At the same time, networks are usually attacked by malicious software that allows them to be remotely controlled by a threat agent. It is developed and prepared by hackers whose goal is to provide a dark and robust cloud computing network to launch cyberattacks of a criminal nature.

Considering that the growth in the number of mobile and networked devices has brought us social and productive benefits, as we can now access computers, security systems, cameras, and home appliances remotely, along with a long list of devices connected to the cloud, all of which is referred to Together with the term Internet of Things.

A worrying aspect of the increasing of Internet-connected devices is the lack of basic security precautions, as most end users rarely change factory defaults - a vulnerability that hackers exploit to gain control of these devices. Another vulnerability that enables cybercriminals to gain control of networked devices is backdoor access, which is the manufacturer's access to the device through an unauthorized connection, used to test and update devices remotely. This extensive and vast network of computers in the hands of the threat represents a tremendous collective force that can be used to create a devastating effect, which requires protection measures of a high degree of flexibility and efficiency.

Based on the Open Security Foundation research, there had been half a million breaches at the beginning of 2014 only. Since then, this number has grown significantly because of humans' increasing dependability on the Internet and its services. Therefore, IoT devices are also prone to such cyber-attacks. For this reason, the introduction of cyber security to all operating systems connected to the cloud has become crucial. Providing encrypted data transfer methods and advanced firewall software is now just as essential as having a good lock on your door, if not more important. Because when it comes to smart homes that are almost entirely operated by intelligent systems and microcontrollers that have control over all the household items, entrances, and appliances and are connected using wireless technologies, cyber security should be the primary protection against personal or cyber-attacks on them.

However, the term "Cyber Security" and its operation are complex and follow more compound rules and axioms. The ontology of cyber security is usually mainly composed of three interconnected levels that get more advanced the higher you go with them. Each of these levels contains sub-ontologies rather than a single monolithic ontology . The upper-level ontology is the biggest because it involves domain-specific ontologies that have ontologies of their own. Moving down, we explore mid-level ontologies that work as realizations and assertions of the domains of the upper levels in a more configured manner based on our security system. Finally, we transition to the domain ontologies, which specify concepts that are particular to the domain of interest and represent those concepts and their relationship from a domain-specific point of view .

## II. Literature Review

Cybersecurity is essential for protecting computers, networks, and electronic systems from unauthorized access and malicious attacks. With a broad application scope across military, healthcare, education, and residential sectors, it addresses threats like malware (ransomware, botnets, Trojans), backdoors, form-jacking, and cryptojacking. More severe attacks include distributed denial-of-service (DDoS) and domain name system (DNS) attacks, which disrupt network function by overloading servers or misdirecting traffic to malicious sites.

**To counter these threats, several cybersecurity types have emerged:**

Network Security: Protects systems from vulnerabilities at the network level, securing operating systems, servers, and network protocols.
Cloud Security: Focuses on safeguarding cloud-stored data, applications, and infrastructure.
Application Security: Ensures security through rigorous software design and coding practices.
IoT Security: Particularly critical for this study, IoT security protects smart, internet-connected devices like fire alarms, thermostats, and appliances that operate autonomously without human input.
These diverse security practices collectively strengthen defenses against the ever-evolving landscape of cyber threats.

### Problem Statement

IoT has integrated seamlessly into daily life, with smart devices connected to the internet to perform tasks that simplify and enhance convenience. From adjusting home lighting, temperature, and music based on personal preferences to notifying users when groceries are needed or even preparing coffee in sync with a car’s arrival, IoT devices cater to numerous aspects of home and personal management. Many people are unaware that by using these devices, they become part of the IoT network, which also collects and processes data for tailored advertisements, especially in health and wellness.

However, this connectivity comes with significant security risks. IoT devices, often left with default settings or lacking robust security measures, are vulnerable to hacking, making personal privacy a critical concern. This research highlights the urgent need for tools and security measures that protect user privacy and secure IoT networks against unauthorized access and data exploitation.

### Motivations

Many people use the Internet of Things (IoT) in their daily lives without realizing it. For example, when someone connects smart bathroom scales to an app on their phone to track their weight, heart rate, and other health metrics, they are utilizing IoT technology. This connectivity enables targeted advertising, often leading to an influx of health and fitness product promotions based on the data collected. This example illustrates the widespread, often unnoticed presence of IoT in modern life and its implications for user data privacy.

## III. Research Methodology

The research methodology relies on constructing a comparative review of existing literature on IoT ontologies, leading to the development of a new, domain-specific ontology for IoT. The methodology follows these steps:

1. **Study Existing Ontologies**: Review and analyze current ontologies relevant to IoT to understand their scope, structure, and limitations.
2. **Comparative Analysis**: Identify and compare functional ontologies, selecting the most suitable aspects for the new ontology.
3. **Ontology Construction**: Develop a proposed ontology that effectively represents the IoT domain, incorporating necessary entities and relationships.
4. **Example Integration**: Use practical examples to enrich and validate the ontology.
5. **SPARQL Query Development**: Create SPARQL queries to demonstrate the ontology’s usefulness in generating semantic insights from IoT data.

The **Protégé** tool supports this process by enabling ontology construction and query testing. The final output is a comprehensive IoT ontology, representing various devices, data flows, and interactions within the domain, and offering a framework for semantic queries to extract deeper insights from IoT networks.

### Expected Deliverables

This research aims to provide insights into the security risks associated with the Internet of Things (IoT) and its potential threat to electronic systems as IoT applications proliferate. Key deliverables include:

Risk Assessment: Establish an understanding of the risks posed by IoT in compromising electronic systems, with indicators that reveal the level of threat from various IoT applications.

Weakness Identification: Use the developed ontology to pinpoint vulnerabilities within IoT systems that could be exploited by cyberattacks.

Solution Development: Offer solutions to mitigate identified vulnerabilities, enhancing security frameworks within IoT systems and improving defenses against unauthorized penetration.

These deliverables aim to strengthen IoT security by targeting and addressing specific weaknesses within interconnected systems.

## Related Work

Several studies have examined cybersecurity ontologies in the IoT domain, emphasizing their critical role in securing IoT devices from cyber threats. Six key studies have influenced this research:

IoT Data Collection and Reasoning: One study developed concepts around data collection, reasoning, and inference in IoT devices, specifically for sensor capabilities and context-awareness. This research identified limitations in existing ontologies and proposed improvements, aiming to unify IoT ontology concepts for more comprehensive application (FCIT_Research_Project_T…).

Malware Ontologies: Another study investigated foundational malware ontology standards, focusing on core concepts such as time, location, and network operations. This work aimed to enhance cyber ontology methods and offered steps toward evolving cybersecurity ontologies in IoT (FCIT_Research_Project_T…).

Cloud-Based Communication for IoT: This study improved semantic management within IoT-enabled smart homes, particularly in cloud-based data management. Researchers designed an intelligent home ontology model, creating a more efficient, personalized home service structure based on existing data(FCIT_Research_Project_T…).

Smart Home Device Integration: Researchers explored home automation methods using IoT devices, including actuators and microcontrollers, to improve interoperability and functionality. They proposed a solution to centralize control, enhancing home automation efficiency through a unified interface (FCIT_Research_Project_T…).

Simulation of Smart Home Activity: Another study examined smart home environments by designing a simulator for human activity within IoT-enabled homes. This tool integrated virtual sensors and AI-driven agents to simulate interactions, providing a low-cost method for testing smart home configurations(FCIT_Research_Project_T…).

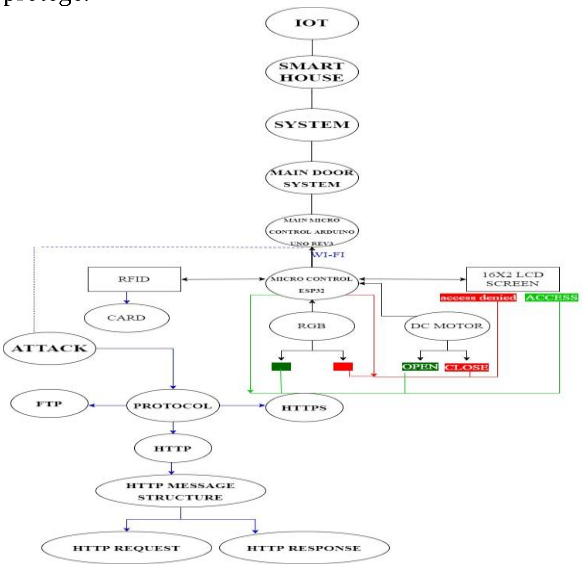
IoT in Healthcare: Focusing on healthcare, researchers proposed an ontology for intelligent healthcare systems to support patient-provider communication. This study used a Belief-Desire-Intention (BDI) model and illustrated its application in healthcare monitoring, demonstrating the potential of IoT in improving healthcare services(FCIT_Research_Project_T…).

These studies collectively support the development of a cybersecurity ontology tailored to smart homes, providing insights and methodologies crucial to addressing IoT security challenges in this project.

## Implementation

We implement a smart system in our home called the "Main Door System" This system is mainly responsible for opening the main door, but before opening the door, there is a security measurement it needs to be correct, and the following figure below explains how the system.

We implement this system in an application called protégé.



## References

[1]. Symantec, “Internet Security Threat Report,” Symantec Corporation, Mountain View, 2018.

[2]. D. Eidenskog and F. Kamrani, “Internet of Things En IT-säkerhetsmässig mardröm,” FOI Totalförsvarets forskningsinstitut, 13 12 2018

[3]. C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, “DDoS in the IoT: Mirai and Other Botnets,” Computer, vol. 50, no. 7, pp. 80-84, 7 July 2017.

[4]. NA, “Data Breach Trends during the First Half of 2014,” Risk-Based Security Open Security Foundation, July 2018.

[5]. R. J. Walls and P. McDaniel, “Building an Ontology of Cyber Security,” Pennsylvania State University, Jan 2014

[6]. L. Obrst, P. Chase, and R. Markeloff, “Developing an Ontology of the Cyber Security Domain,” The MITRE Corporation, 2012

[7]. i. governance, "What is Cyber Security? Definition and Best Practices," [Online]. Available: https://www.itgovernance.co.uk/what-is-cybersecurity.

[8]. "Cyberspace," techopedia, 2020 Septamber 2020. [Online]. Available: https://www.techopedia.com/definition/2493/cyberspace#:~:text=Cyberspace%20refers%20to%20the%20virtual,used%20to%20facilitate%20online%20communication.

[9]. N. University, "Keeping cyber space safe," Nature, 2018. [Online]. Available: https://www.nature.com/articles/d42473-019-00220-6.

[10]. A. S. Gillis, "What is the internet of things (IoT)?," TechTarget, [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[11]. S. Shea, "IoT security (internet of things security)," TechTarget, [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security.

[12]. J. M. D. SANTOS, "Best IoT Software," project-management.com, 17 December 2020. [Online]. Available: https://project-management.com/iot-software/#:~:text=IoT%20software%20is%20the%20enabling,transform%20and%20present%20as%20information.

[13]. D. Flair, "IoT Hardware | IoT Software – A Complete Tour," Data Flair, [Online]. Available: https://data-flair.training/blogs/iot-hardware/#:~:text=IoT%20Hardware%20includes%20a%20wide,support%2Dspecific%20goals%20and%20actions.

[14]. "A Guide for selecting the right microcontroller for your IoT project," IIoT World, 15 February 2018. [Online]. Available: https://www.iiot-world.com/industrial-iot/connected-industry/a-guide-for-selecting-the-right-microcontroller-for-your-iot-project/#:~:text=What%20is%20a%20microcontroller%20in,be%20connected%20to%20the%20internet..

[15]. "Internet of Things (IoT)," TREND MICRO, [Online]. Available: https://www.trendmicro.com/vinfo/us/security/definition/internet-of-things.

[16]. "Actuators in IoT," Geeks for Geeks, 24 February 2021. [Online]. Available: https://www.geeksforgeeks.org/actuators-in-ot/#:~:text=An%20IoT%20device%20is%20made,the%20mechanism%20or%20the%20system..

[17]. R. A. P. S. N. G. Garvita Bajaj, "A study of existing Ontologies in the IoT-domain," HAL open science, New Delhi, India, 2017.

[18]. P. C. R. M. Leo Obrst, "Developing an Ontology of the," The MITRE Corporation, 2012.

[19]. K. O. M. D. Ming Tao, "Ontology-based Data Semantic Management and Application in IoT- and Cloud-Enabled Smart Homes," College of Computer and Network Security, Dongguan University of Technology, Dongguan, China, 2016.

[20]. M. C. M. B. a. L. G. Irina-Ioana Pătru, "Smart Home IoT System," University POLITEHNICA of Bucharest, Bucharest, Romania.

[21]. S. C. P. C. H. V. S. H. W. S. Y.-S. J. K. C. Wonsik Lee, "Automatic Agent Generation for IoT-based Smart House Simulator," Elsevier, Republic of Korea, U.S.A., China, 2015.

[22]. M. N. K. S. Salwa Muhammad Akhtar, "An Ontology-Driven IoT based Healthcare Formalism," International Journal of Advanced Computer Science and Applications, Lahore, Pakistan, 2020.