Evaluation of Home Energy Management System (HEMS) Using State of the Art Info Security Frameworks

by

NS Muhammad Atif Iqbal

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

May 2023

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Mr. Muhammad Atif Iqbal**, Registration No. **00000321024**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: ____________________________

Name of Supervisor Engr Dr. Imran Rashid

Date: ________________________________

Signature (HOD): _____________________

Date: ______________________________

Signature (Dean/Principal) _____________

Date: ________________________________

Declaration

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

____
MS Student

Dedication

"In The name of ALLAH the most Beneficent and the most Merciful"

Dedicated to my family who has always been a source of motivation for me and also to my supervisor Engr Dr Imran Rashid for being forthcoming and helping in fulfillment of this research work.

Abstract

In the modern world, cybersecurity poses an enduring challenge for the IT sector, with organizations investing heavily in securing their assets, especially consumer personal data. Unfortunately, the past decade has seen a significant increase in cyber-attacks against IT setups. Main target of such attacks is to get access to the data owned by organizations. Such incidents have necessitated the establishment of cyber security controls and their assessments in an organization. This has made it essential for organizations to establish and assess cybersecurity controls. Numerous renowned institutes have developed frameworks to address cybersecurity issues. While some frameworks address overall security issues, others target significant threats to an organization's security, helping organizations achieve confidentiality, integrity, and availability of their assets. Risk management, as a subset of cybersecurity, is the most crucial stage in implementing cybersecurity in any organization, encompassing security controls' employment, selection, implementation, and defining mitigations.

This project report presents the design and evaluation of various cyber security frameworks on an IT environment developed for Home Energy Management System (HEMS) that utilizes a local network to monitor and control energy usage. In addition to providing energy efficiency, the system also addresses cybersecurity concerns by assessing the applicability of different cybersecurity compliance standards, including NIST, CIS-20 and ISO. The report outlines the architecture of the system, including the hardware and software components, and provides an analysis of the system's performance.

Acknowledgements

With profound humility, I pay my gratitude to ALLAH Almighty for enabling me to achieve another astounding milestone in my literary career. This arduous work would have not possible without the support of my supervisor Engr Dr. Imran Rashid who not only provided timely guidance, profound encouragement and positive criticism but also ensured that I complete the assigned tasks in stipulated time despite of prolonged illness including multiple hospitalisations of my son and my twice illness due to covid-19 varients. His affectionate and kind consideration towards my research helped me to carry on with my project in odd circumstances. I am also very obliged to my committee members, Engr Dr. Imran Makhdoom and Engr Muhammad Sohaib Khan for their intimate help in fulfillment of this research work.

I am deeply indebted to my great parents, siblings and colleagues (especially Engr Usman Dilawar) for their encouragement and affectionate selfless prayers. Most importantly I would like to thank my beloved wife for understanding the significance of this assignment and sharing the burden of domestic liabilities. She always infused motivation to my efforts and encouraged me whenever I was fatigued and tended to relax. Last but not the least, her invariable appreciation was a constant source of motivation for me.

LIST OF ACRONYMS

1.	Home Energy Management System	**HEMS**
2.	Energy Management System	**EMS**
3.	Internet of Things	**IoTs**
4.	Home Area Networks	**HANs**
5.	Neighborhood Area Networks	**NANs**
6.	Power Line Communication	**PLC**
7.	Energy Storage Systems	**ESS**
8.	Renewable Energy Sources	**RESs**
9.	Photovoltaic	**PV**
10.	Demand Response	**DR**
11.	Time-Of-Use	**TOU**
12.	Human Machine Interfaces (HMIs)	**HMIs**
13.	Industrial Automation & Control Systems	**IACS**
14.	Enterprise Resource Planning	**ERP**

TABLE OF CONTENT

DEDICATION i

ABSTRACT.. ii

ACKNOWLWDGEMENTS iii

LIST OF ACRONYMS iv

TABLE OF CONTENTS v

LIST OF FIGURES vi

LIST OF TABLES vii

Chapter 1 Introduction …………………………………………………………….. 1

Chapter-2 Literature Review.. 5

Chapter-3 Cyber Security Frameworks Selection and Experiment Setting………...1**0**

3.1 Objectives.. 10

3.2 Selection of Cyber Security Frameworks 11

3.3 NIST 800-30 11

3.4 Centre of Internet Security (CIS) 13

3.5 ISO 27001 15

3.6 Experiment Setting... 15

Chapter-4 Selected Cyber Security Framework Implementation…………………....18

4.1 NIST.. 18

4.2 CIS (Top 20 Controls).. 25

4.3 ISO 27001 27

4.4 Inventory Management 30

4.5 RASCI Matrix………………………………..……….……..………….......30

4.6 Implementation Results…………...31

Chapter-5 Conclusions and Future Work **…**...33

References…………………………………….. 35

LIST OF FIGURES

Figure 3.1 **CIS Controls** …………………………… **14**

Figure 3.2 **Home Energy Management System** …………………………… **16**

Figure 4.1 **Risk Matrix** …………………………… **22**

Figure 4.2 **Impact/ Livelihood Matrix** ……………………….......... **22**

LIST OF TABLES

Table 3.1 NIST 800-30 Model ……………………..…………..…. 12

Table 4.1 List of Inventory ………………………………………. **30**

Table 4.2 List of Responsibilities …..…………………………….... **30**

Table 4.3 Comparison of Frameworks ………………………………………. **31**

CHAPTER - 1

INTRODUCTION

A Home Energy Management System (HEMS) or Energy Management System (EMS) is a technological solution consisting of software and hardware components that allow households to supervise and regulate a variety of appliances and fixtures present within the household. As HEMS gain prominence, they are becoming increasingly crucial for both residential and commercial settings. These systems provide users with the ability to track their energy usage and make informed decisions about optimizing energy consumption. HEMS also offer features to enhance energy efficiency, including automated scheduling and remote control of energy-related activities. To ensure that HEMS are effective and secure, they need to be designed and implemented with the latest security measures. Smart homes have emerged as a fundamental component of the smart grid in numerous countries because of their substantial environmental and socioeconomic benefits. They help to optimize energy consumption, cut costs, and enhance the dependability and efficiency of the power grid by allowing users to synchronize home appliances with demand response programs proposed by energy providers. Moreover, smart homes are critical in reducing the investments required for electricity generation, transmission, and distribution to satisfy future demands by promoting distributed energy generation. The advent of smart sensors, advanced metering systems, intelligent appliances, and Internet of Things (IoT) devices has fostered the development of smart homes, facilitating the adoption of Household Energy Management Systems (HEMSs) that lay the groundwork for future smart grids. HEMSs have grown in popularity around the world and are now necessary for the efficient management of electricity consumption in the smart grid. Globally, there is a growing field of HEMS research that attempts to lower electricity costs in residential and commercial power networks while enhancing energy security and efficiency. These studies do suggest, however, that control and communication technologies, which are essential to HEMSs, still present a number of difficulties.

To ensure efficient operation of Household Energy Management Systems (HEMSs), it is essential to integrate sensing, communication, and control technologies that enable the retrieval of energy demand data and the timely dissemination of control techniques across the network. In smart grid applications, communication networks are classified into three categories, namely Home Area Networks (HANs), Neighborhood Area Networks (NANs), and Wide Area Networks (WANs) [2]. A typical HAN comprises a smart meter for electricity that connects various household devices, sensors, displays, gas and water meters, electric vehicles, and renewable energy sources. The HEMS regulates and monitors power generation, storage, and consumption for all these components [3], [4]. The central controller of the HAN is linked to the utility grid via a smart meter, and the data collected from different HANs is consolidated and stored in a database, which can form either a NAN or WAN based on the area covered. The utility administrator utilizes information from various NANs/WANs to make informed decisions regarding system parameters, such as pricing and projected load.

A HAN typically consists of a smart electricity meter that connects different household appliances, sensors, displays, water and gas meters, electric vehicles, and renewable energy sources. A HEMS is responsible for overseeing the various components involved in generating, storing, and consuming power, [5] including traditional media such as Ethernet and Power Line Communication (PLC) as well as wireless media like Wi-Fi, wireless cellular networks, and low-rate wireless personal area networks conforming to the IEEE 802.15.4 standard. PLC has become popular due to its low cost and ease of implementation, and the Home Plug Alliance has set standards to encourage its use in smart grid applications. [6],[7],[8] While PLC is a secure option for connecting users with utility companies, it suffers from lower transmission rates and poorer transmission quality compared to Ethernet. Wireless solutions offer better connectivity, but their deployment may compromise security. While Ethernet is the most effective solution in terms of security, robustness, and connectivity, it is costly and difficult to install new cables.

To ensure the successful implementation of HEMSs, it's crucial to integrate a multitude of cutting-edge technologies. Among these technologies, communication technologies, energy storage systems (ESSs), power electronic devices, and hybrid renewables are the key players. With the integration of ESSs, the management of renewable energy sources becomes more efficient, especially when combined with power electronics. The integration of these technologies can stabilize the intermittent power generation and optimize energy utilization through demand response. Presently, a wide range of ESS technologies are available, such as low and lead-acid batteries, chemical energy storage, and ultra-capacitors. Given the variability of renewable energy sources due to weather conditions, implementing intelligent battery charging and discharging methods can greatly aid in balancing energy supply and demand, ensuring power stability and dependability. During peak-load periods, smart homes can operate on renewable energy sources, and ESSs can be activated to address supply-demand imbalances at any time, thereby increasing the power grid's resilience.

To guarantee a stable and dependable power supply, hybrid renewable energy systems that blend diverse renewable energy sources (RESs) with complementing weather patterns are often utilized [13]. These systems can decrease the unfavorable consequences of RES variability and maintain a constant power supply [11]. In today's world, the concept of smart homes has gained tremendous popularity due to the numerous benefits they offer. One of the most significant advantages of smart homes is their ability to combine various renewable energy sources (RESs) such as photovoltaic (PV), wind, and biomass. This combination is achieved through the use of energy conversion systems that rely on advanced power electronic devices to control energy production and distribution. For instance, power converters are commonly used in home energy generation systems to efficiently extract power from solar panels and small wind turbines while ensuring that it is regulated to match the desired use context, RES and ESS integration. The integration of different power supply systems and voltage levels is crucial in creating hybrid RES systems that function optimally. However, this can be quite challenging since PV systems typically produce DC voltage, which must be transformed to single- or three-phase AC voltage, whereas wind turbines generate AC voltage with varying magnitude and frequency. Furthermore, battery ESSs require an initial DC/DC conversion step to generate the necessary voltage level from several cells in series to the DC-link, from which the ultimate AC output voltage is produced through a DC/AC conversion step.

Over the past few years, we have witnessed significant advancements in the way we generate and distribute electricity. One of the most remarkable developments is the rise of "smart" grids, which have transformed traditional power grids into highly sophisticated and intelligent systems. Through the integration of advanced metering infrastructures, utilities and consumers can now engage in bidirectional communication in both neighborhood and wide area networks, leading to improved reliability and efficiency. Moreover, the adoption of power monitoring and control technologies such as HEMSs has further enhanced the productivity of smart grids by allowing for automated optimization of home appliance usage. This, in turn, has resulted in substantial energy savings while maintaining end-user comfort. HEMSs leverage advanced communication protocols to facilitate the exchange of critical information on energy availability and needs between devices and the grid, thereby enabling intelligent scheduling of appliances using sophisticated optimization techniques that consider both user comfort and the expected energy supply and demand.

HEMSs, or home energy management systems, have become increasingly popular due to their ability to offer a wide range of services that cater to different needs. These systems not only offer management, control, logging, monitoring, and problem detection services, but also incorporate a plethora of components that allow them to perform these tasks efficiently. Some of the key components that HEMSs must incorporate include advanced sensors, measuring devices, intelligent controllers and actuators, a communication infrastructure and a user interface system. These sensors play a crucial role in providing valuable feedback to the HEMSs by detecting occupancy, smoke, light and temperature, which are then used to modify actuators for maximum comfort and energy efficiency. Additionally, the measuring devices incorporated in HEMSs inform the system about the present condition of the building or residence being monitored, including resource utilization, allowing the system to make more informed decisions. The smart controllers, on the other hand, use voltage and current sensing to make decisions locally, ensuring optimal energy usage. The communication infrastructure of HEMSs is also critical, as it includes the networking medium and communication protocols used by HEMS devices, which have varying requirements for physical media, transmission rates, and physical security. Finally, the HEMS management controller, which is typically an embedded computer or workstation with energy management software, allows for easy viewing of the present condition of the building or residence being monitored, offers control features, and integrates different protocols seamlessly. With all these components working together, HEMSs have revolutionized the way we manage and monitor energy consumption, making them an indispensable tool for modern homes and buildings.

Smart meters are a pivotal component in Home Energy Management Systems (HEMSs) as they serve as a conduit for two-way communication between customers and utility providers, thereby facilitating the exchange of feedback. These meters are designed to collect data on various utilities, including but not limited to electricity, gas, and water, and serve multiple purposes. For instance, they are capable of monitoring energy consumption during different time periods and modes, enabling user preferences to affect smart load shedding, and interfacing with other power infrastructures like HEMSs to provide backup power during instances of primary grid failures. Thus, it is safe to say that smart meters are a cornerstone of modern energy management systems, enabling consumers to take greater control over their energy consumption while providing utilities with vital information necessary to make informed decisions.

Despite the various services that HEMSs offer, most research has focused on theoretical design rather than implementation and operational issues. To validate the design of HEMSs and address deployment challenges, it is crucial to address this imbalance and focus on real-world applications. Despite ongoing efforts, the incorporation of power electronic converters, renewable energy sources, and energy storage systems into HEMSs continues to pose a significant challenge. As a result, addressing operational and implementation issues is necessary to ensure the successful deployment of HEMSs in practical settings.

CHAPTER – 2

LITERATURE REVIEW

The use of HEMS has prompted utilities to increase their focus on demand-side management, which has become more attractive to consumers due to its ability to lower electricity bills by reducing usage. Customers faced with incentive or price-based DR schemes have three options. One is to limit consumption during busy times, which may be uncomfortable. One other possibility is to alter utilization patterns from high-demand to low-demand times, such as by operating appliances during low-demand periods. Additionally, a third approach entails implementing renewable energy sources on-site to diminish dependence on conventional power grids and alleviate the burden on distribution and transmission systems. Programs utilizing price-based demand response tactics furnish diverse tariff options at varying times, incentivizing patrons to decrease their power usage during high-demand periods via time-of-use pricing mechanisms.

HEMSs help manage power demand for distributed renewable energy generation and energy consumption while ensuring customer comfort. These frameworks take into account factors such as energy expenses, weather conditions, usage patterns, and user choices to enhance energy efficacy. Up-to-date HEMSs are equipped with resilient constituents that can maintain their operation in the event of a breakdown. Cloud computing offers a trustworthy medium for data computation and preservation, while IoT gadgets simplify the acquisition of data on each HEMS element. A regular HEMS comprises of detectors, measuring equipment, smart regulators, effectors, communication infrastructure, and a control management unit. These systems are expected to become increasingly prevalent in the home technology market, enabling users to seamlessly operate appliances and devices. HEMSs can also aid in the development of federated micro grids as a solution for future power systems. [13]

Real-time automated solutions have the potential to bring economic benefits to all stakeholders by engaging on both sides of the meter. Smart houses and network management significantly increase the possibilities for demand management and network support. With the growing popularity of smart home devices due to the increasing cost of energy, it is becoming imperative to automate the monitoring and coordination of these hypothetical homes in real-time while also participating in wholesale markets. Nevertheless, the presence of numerous device ecosystems can create possible vulnerabilities in network security and privacy concerns, making it vital to establish protocols and standards for standardized communication and interoperability.

In order to make the energy transition a top priority for the country, it is essential to invest a significant amount of resources into stabilizing the network and promoting the adoption of distributed renewable generation. [9]

In response to the ever-evolving cyber threat landscape, companies are implementing cyber security strategies to reduce risks to their critical infrastructure. The corporate cyber security standards must be adhered to as the Power Management System (PMS) currently depends on IT solutions such as human machine interfaces that are open system-based and networks that utilize Internet Protocol. One of the primary security controls is to physically separate Industrial Automation & Control Systems (IACS) from IT business systems, but this approach limits the IT team's ability to efficiently manage IACS technologies. To operate these systems and cyber security measures efficiently, the IACS maintenance staff needs to receive training in network and computer competencies. Integrating the PMS network and systems into the IACS Operational Technology (OT) architecture allows for the efficient implementation and maintenance of cyber security measures for the PMS infrastructure, such as controlling access to the PMS using centrally maintained user access credentials and appropriately managing additions, transfers, and modifications to user credentials.

Cybersecurity expertise is typically lacking among smart home residents, even for common technologies like email and social media. In addition to the resident's time and skill requirements to implement security measures, smart homes require adequate cybersecurity safeguards to address the risks. The prevention of attacks and their potential consequences is a security concern for smart home residents. A more extensive optimization framework that includes a meticulous quantification of crucial elements can offer additional perspectives into investments in cybersecurity. Subsequent investigations may aid in establishing secure smart home environment protocols and formalizing security measures centered on atypical actions. Such measures are imperative to guarantee a more robust and secure home. [12]

The CIS Controls were developed with the aim of furnishing companies with an all-inclusive inventory of security-related deployments. This collection consists of 20 controls and 171 sub-controls. These controls have been well-received and endorsed by powerful groups, which is why there are few negative reviews about them. However, alternative options have also been introduced by the likes of the PCI consortium, NIST, and ISO. Despite this, there is a need for greater engagement from the scientific community to ensure that businesses have access to the best possible security strategies. To promote the use of CIS Controls, SANS and CIS must engage with this issue and promote their benefits over other strategies. [1]

Home automation is one of the most substantial applications of the Internet of Things (IoT), and it has become increasingly popular in recent years. This sector is growing rapidly, and IoT system security is becoming increasingly challenging due to the heterogeneity of devices and their low processing and storage power. Unfortunately, end users and system designers are often not motivated to create secure IoT solutions. Therefore, it is essential that both end users and developers consider the security of IoT devices. Regulatory agencies can use security categorization techniques to determine what constitutes appropriate security. SHEMS, for example, offers a security classification technique. The use of security classes is an excellent way to evaluate security and provide guidance for enhancing the security of IoT devices. [3]

The utilization of technology has become a ubiquitous presence in the operations of Polari. Nevertheless, there seems to be a deficiency in the organization's level of information security management competency. To tackle this problem, it is crucial to formulate suggestions and a roadmap for information governance that is based on the standards of COBIT 2019 and ISO/IEC 27001:2013. The timeline for this roadmap should span from 2021 to 2025, encompassing an outline for the organizational structure, human resources, policies, and procedures that Ditreskrimsus Polda XYZ should implement to ensure efficient information security management. A comprehensive assessment of the 29 core model domains of COBIT 2019 reveals that Ditreskrimsus Polda XYZ's level of competency has yet to achieve level three, and thus, the implementation of the recommended roadmap is crucial to reach the desired level. [4]

To mitigate the risks of information security threats and cyberattacks, companies can utilize Information Security Management Systems (ISMSs). However, creating an effective ISMS entails a crucial and time-consuming step, which is conducting a risk assessment. Although there are various techniques in deploying an ISMS, the main objective is to identify, assess, and categorize all possible hazards. Failure to identify these threats can lead to significant consequences that could negatively impact the organization. A unified information security strategy would also improve the practicality of certain commercial elements, especially with the rapid growth of a company, which could make it an attractive target for cyberattacks. The optimization of tasks related to the implementation and maintenance of best practices is crucial in information technology businesses as they are completely devoted to delivering outcomes and resolving ongoing survival concerns. Effectively executing these tasks can enhance efficiency, and adopting ISO 27001 can also produce mid-term benefits for the company's daily operations, reducing the amount of workload and duplication of effort. [5]

PT. IndoDev Niaga Internet is a widely recognized company that offers business solution applications and implementation services, encompassing a range of software such as enterprise resource planning (ERP) and human resource information systems (HRIS). The company is committed to maintaining the confidentiality and security of sensitive information by utilizing ISO 27001: 2013. They believe that implementing this standard will positively impact their company's continuity. In line with this, PT. IndoDev Niaga acknowledges that internet usage affects security operations and access management.

PT. IndoDev Niaga found 11 access control check items categorized as Non-Conformance (NC) out of 33 check items during the ISO 27001:2013 audit period. Nine of these items were categorized as major, while the remaining two were categorized as minor. As for operations security aspects, they found five out of 12 check items to be Non-Conformance (NC), and all were classified as minor. By complying with the ISO 27001: 2013 standard, PT. IndoDev Niaga Internet ensures that their data security is at par with global best practices. [6]

The EU General Data Protection Regulation (GDPR) stands out as a pivotal milestone in data privacy legislation within the past two decades. The regulation impacts every sector that handles data, and it took two years to put it into action. While the rule has been challenging to apply for businesses, several authors note that it is a tool for creating a competitive advantage based on trust among partners, clients, and workers. Furthermore, the General Data Protection Regulation (GDPR) promotes the adoption of accreditations like ISO 27001 to prove that an enterprise proactively handles its information protection. This is where the use of ISO 27001 can be beneficial for enterprises, as it aids them in meeting these demands.

A business must ensure that necessary risk-containment measures related to confidentiality, integrity, and availability are in place and operational. This ensures that the company's data security is at its highest level, giving their clients, partners, and workers the assurance that their sensitive information is safe and secure. By complying with GDPR and using certifications such as ISO 27001, businesses can create a competitive advantage based on trust, which is vital for success in today's digital age. [8]

The Information Security Management System (ISMS) is an indispensable management element for corporations to guarantee the security of their data, which plays a vital role in monitoring, evaluating, and improving the organization's overall security. Security policies and protocols to address security risks are created continuously, as it is an ongoing process. The primary purpose of conducting a gap analysis is to identify where an organization's security processes are lacking, and it should be continuously reviewed to keep the organization's security defenses up to date against potential security breaches. Technical methods can only achieve the minimum level of security, and proper policies and procedures must be implemented to complement it. Careful preparation and attention to detail are necessary to determine which controls should be implemented to ensure information security. Furthermore, all stakeholders, including employees, suppliers, third parties, and other external parties, must be involved in information security management, as it is a fundamental requirement [10].

The evaluation of cyber security risk is a challenging but necessary process for all organizations, regardless of their size or structure. A Western Australian local government agency's cyber security concerns were assessed using NIST CSF to quantify the risks associated with specific NIST CSF core functions and their corresponding categories. By identifying any gaps and implementing recommendations to achieve the necessary level of compliance, the organization has been able to target its people, processes, and technology deliberately, reducing both current and potential hazards [2].

CHAPTER-3

CYBER SECURITY FRAMEWORKS SELECTION AND EXPERIMENT SETTING

Introduction

Cybersecurity is an ongoing challenge that continues to confront the IT industry in the modern world. Companies are investing significantly in this field to protect their assets, especially those related to their customers' personal data. However, in the last decade, there has been a significant increase in the number of cyber-attacks against IT systems in various forms. To mitigate this problem, an examination of a compact IT ecosystem established in a domestic dwelling is conducted, relying on multiple cybersecurity frameworks, such as the NIST Model 800-30, CIS Top 20 Security Controls, and the ISO 27001, for assessment. Various renowned institutes world-over have developed frameworks to tackle the issues related to cyber security. Few of them addresses the overall security issues linked to the organization, while other address only significant threats to an organization's security. Generally, all of them help organizations to achieve confidentiality, integrity and availability of their assets in desired manners. Risk Management, being a subset, is the most significant stage of implementing Cyber Security in any organization. The employment of security controls, their selection, implementation and defining mitigations all are linked with Risk Management.

This study is aimed to carry out research to identify the best cyber security standards for evaluation of a home energy management network. First of all, three security standards namely NIST, CIS Top 20 and ISO 27001 are shortlisted that are applicable to our home energy management network.

3.1 Objectives

The main objectives of thesis are: -

- Identifying the strengths and weaknesses of each cybersecurity standard, and comparing them against each other providing an overview of the cybersecurity landscape.
- Evaluating the suitability of each standard for the specific requirements of the home energy management network, based on factors such as compatibility, cost, and practicality.

- To perform asset identification and vulnerabilities to find out threat linkages on a self-designed network.
- To carry out risk management and suggest mitigation strategies by applying techniques defined in selected frameworks.

3.2 Selection of Cyber Security Frameworks

The realm of information technology (IT) is constantly grappling with a persistent challenge in the form of cyber security. Organizations, in their quest to safeguard their assets, particularly customer data, are investing heavily in this field. Unfortunately, these efforts seem to have fallen short as cyber-attacks against IT setups have increased significantly over the past decade. These cyber-attacks are usually geared towards accessing sensitive data of organizations. In response to this issue, reputable institutions globally have developed frameworks aimed at helping organizations achieve confidentiality, integrity, and availability of their assets. These frameworks are not only designed to assist organizations in implementing cyber security controls but also aid in conducting assessments. One crucial subset of cyber security implementation is Risk Management. Risk management involves selecting, implementing, and defining mitigations for security controls.

This research endeavors to evaluate various cyber security frameworks on a residential home IT environment that interconnects home appliances over the network. The primary focus is on identifying assets, threats, and linkages, performing risk management and suggesting mitigation strategies using techniques defined in the selected frameworks. The frameworks under consideration include NIST Model 800-30, CIS Top 20 Security Controls, and ISO 27001. By conducting a thorough analysis of these frameworks, we can determine the most effective approach to manage the risks associated with cyber-attacks. Despite the challenges that the IT sector faces in ensuring the security of their assets, it is our hope that this study will contribute to addressing this pressing issue.

3.3 NIST 800-30

The NIST 800-30 is a comprehensive set of recommendations for handling information security threats, which was formulated by the National Institute of Standards and Technology (NIST) in the United States. It is a holistic approach that encompasses risk evaluation, risk management, and risk surveillance. The goal of the framework is to help organizations of all sizes and industries identify, assess, and manage the risks that they face effectively. The framework places a strong emphasis on using a risk-based approach to security, which involves prioritizing risks based on their potential impact on an organization's goals and objectives. Because of its comprehensiveness and flexibility, the NIST 800 – 30 framework is widely utilized for risk management in both public and private sectors. It is also regularly updated to keep pace with new and evolving cyber threats and emerging technologies. In addition, the model includes the integration of Threat modeling into the System Development Life Cycle (SDLC) through various phases, which are described in detail below:-

Table 3.1: NIST 800-30 Model

Phases	Title	Requirement and Risk Management
1	Initiation	Need for system development and its usage strategy is written. Risks are identified on the wholesome system security requirements.
2	Development & Acquisition	In this phase system is designed and developed. The hazards pinpointed in the initiation stage are leveraged to incorporate security measures while implementing the system.
3	Implementation	During the implementation phase, the risks management process is integrated so as to meet the requirements of the system.
4	Operation & Maintenance	Risk mitigation activities identified and worked during previous phases are performed to avoid any security breach during operation.
5	Disposal	During this phase, the actions documented for risk mitigation are performed. Desired disposal of the system is made as per its risk categorization.

1. **Risk Assessment**

NIST 800-30 model comprises of 9 x steps for risk assessment as described below: -

a. System Characterization

b. Threat Identification

c. Vulnerability Identification

d. Control Analysis

e. Likelihood Determination

f. Impact Analysis

g. Risk Determination

h. Control Recommendations

i. Results Documentation

3.4 Centre for Internet Security (CIS)

The Centre for Internet Security (CIS) has created a series of measures intended to offer IT organizations a fundamental Defense in Depth approach by condensing global best practices. As a non-profit organization, CIS's goal is to identify, formulate, verify, promote, and sustain best cybersecurity practices while developing world-class cybersecurity solutions to assist IT organizations in responding to security incidents. The CIS Top-20 highlights several significant components of cyber defense, including Offense informs Defense, Prioritization, Measurement and Metrics, Continuous Diagnosis and Mitigation, and Automation. By answering the question "What should an enterprise do?" to "What all should we be doing?" CIS Top-20 helps IT organizations identify the necessary steps to strengthen their defense. CIS Top-20 help IT Organizations in identifying as to “What should an enterprise do?” to “What all should we be doing?”

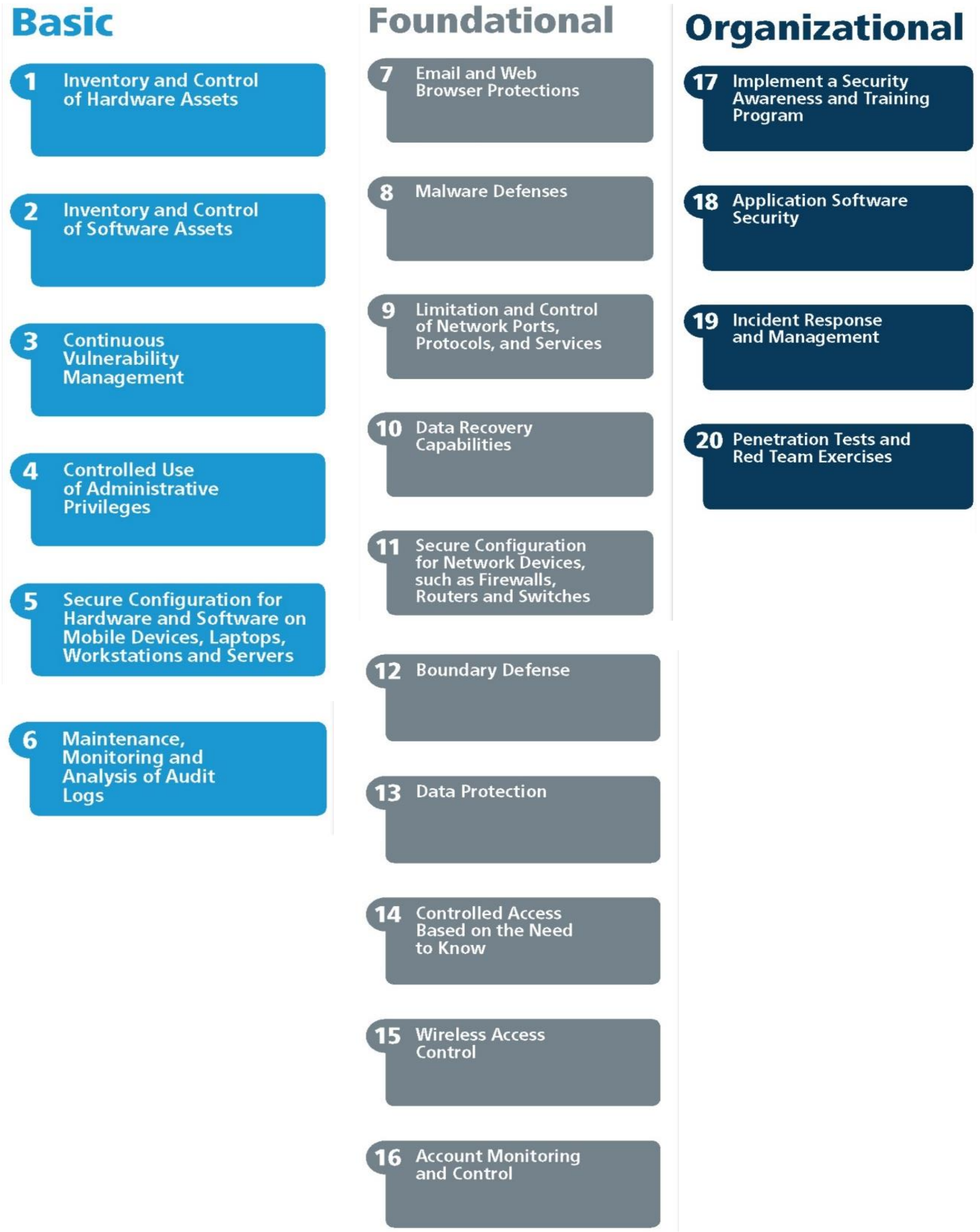
The CIS has developed a framework of measures to oversee the information security aspects of a company, with the goal of reducing the risks of cyber threats. Various subsets of controls are relevant in different areas of cybersecurity. The first six controls pertain to the basic cyber hygiene of any organization, but some of these controls may not be feasible for certain organizations with limited resources. Therefore, international best practices are needed to help organizations achieve balanced cybersecurity. To address this need, CIS has developed a tiered control system known as Implementation Groups (IGs), which are divided into three levels as documented by the CIS. CIS has thus come up with tiered control mechanism namely Implementation Groups (IG). There are three IGs that are usually mentioned in the documentation of the CIS.

- IG-1, which is a family-owned business with about 10 workers;
- IG-2, a service provider that operates in a specific region;
- IG-3, a large corporation that employs thousands of people.

The CIS has classified these groups based on the available resources and cyber security attributes, with each IG representing a list of controls that are equivalent to an organization with a similar risk profile. The controls are marked horizontally according to the IG's class, with each higher class including the controls of the lower class. IG-3 contains additional controls as well as those applicable to IG-1 and IG-2. Implementing IG-1 is crucial for the success of a cybersecurity program. IG-1 comprises sub-controls that the CIS refers to as "Cyber Hygiene." These measures are vital in defending against common attacks. When determining their organizational category, organizations base their criteria on three factors:

- The sensitivity of their data and criticality of their services,
- The expected technical expertise of their staff,
- The resources allocated to cybersecurity activities.

In total there are 20 Top CIS controls. Hence, CIS classifies the controls into three categories: fundamental, organizational, and basic, independent of the kind of industry. The CIS CSC guidelines prioritize standards, which sets them distinct from other security controls and lists that may acknowledge the necessity for prioritizing but refrain from making particular recommendations. Controls 7 through 16 are categorized as Foundational, controls 17 through 20 as Organizational, and the first six as Basic. Basic structure is as depicted below: -



Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Figure 3.1 – CIS Controls

3.5 ISO-27001

ISO 27001 is an internationally recognized guideline that outlines the most effective methods for creating an Information Security Management System (ISMS) within an organization, ensuring that the system meets the highest standards of security and protection. This standard presents a methodical approach to safeguarding confidential business data to maintain its security. It is meant for all organizations of various sizes and sectors. ISO 27001 requires companies to create, implement, maintain, and continually improve their ISMS based on a risk management approach. The standard suggests that organizations should identify their data assets, evaluate their risks, and deploy appropriate security measures to manage those risks.

ISO 27001 does not prescribe specific security measures for an organization to follow. Instead, it provides a framework that allows organizations to customize their security protocols to their specific requirements. This standard includes guidelines for information security policies, risk assessment, security controls, incident management, and business continuity planning. Companies can achieve ISO 27001 certification by undergoing an independent ISMS audit to ensure compliance with the standard. Certification assures customers, partners, and stakeholders that the company values information security and has implemented adequate measures to protect confidential information.

3.6 Experiment setting

A small home energy management system (HEMS) has been created as shown in Fig.-1 to test a network of connected appliances. The appliances, including an air conditioner, fridge, Huawei Smart Phone and smart TV, have been connected together to form the HEMS. The purpose of the system is to manage and monitor the energy usage of these appliances in a home setting. The PRTG software has been installed as a monitoring tool to track and analyze the performance of the network. A separate laptop has been used to launch DDoS attacks on the network and check the security policies.

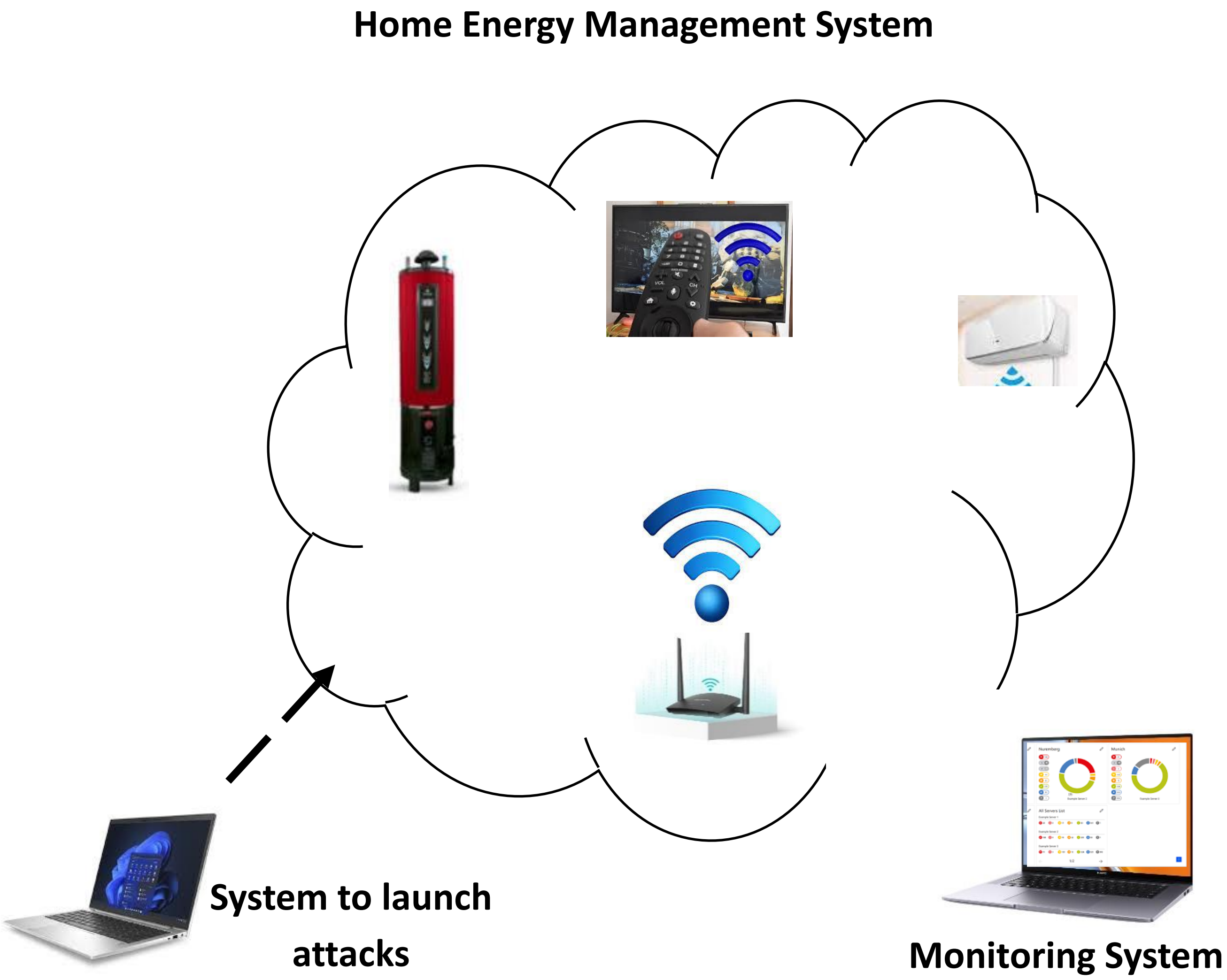


Figure 3.2: Home Energy Management System

Conclusion

This chapter is aimed to carry out research to identify the best cyber security standards for evaluation of a home energy management network. First of all, three security standards namely NIST, CIS Top 20 and ISO 27001 are shortlisted that are applicable to our home energy management network. Each standard is then evaluated based on the specific requirements of the home energy management network considering their strengths and weaknesses, as well as its practicality, compatibility. Subsequently, findings of the evaluation are analyzed and different standards are compared against each other based on the evaluation criteria and the network's specific requirements. Three chosen standards are implemented for the evaluation of the home energy management network, and to monitor the network's performance to ensure that it meets the required cybersecurity standards.

CHAPTER-4

Selected Cyber Security Framework Implementation

Introduction

Previous chapter was aimed to carry out research to identify the best cyber security standards for evaluation of a home energy management network. All three selected security standards namely NIST, CIS Top 20 and ISO 27001 are discussed that are applicable to our home energy management network. Each standard evaluated based on the specific requirements of the home energy management network considering their strengths and weaknesses, as well as its practicality, compatibility. Subsequently, findings of the evaluation were analyzed and different standards were compared against each other based on the evaluation criteria and the network's specific requirements. Three chosen standards were implemented for the evaluation of the home energy management network, and to monitor the network's performance to ensure that it meets the required cybersecurity standards

The results achieved by applying different controls and standards are discussed in this chapter. All three selected standards are implemented on our own created HEMS, results are elaborated in as follows.

4.1 NIST

Implementation of NIST Now we will elaborate these nine steps into our own HEMS.

a. **Step-1** In this step we characterize the system as per our security requirements: -

Category	Asset
Hardware	• Home Appliances • Network Devices
Software	• Policies • Network Architecture • Application Used • Security Architecture

Data & Information	• Data/ Information • Storage • Encryption
People	• Users • Administrators

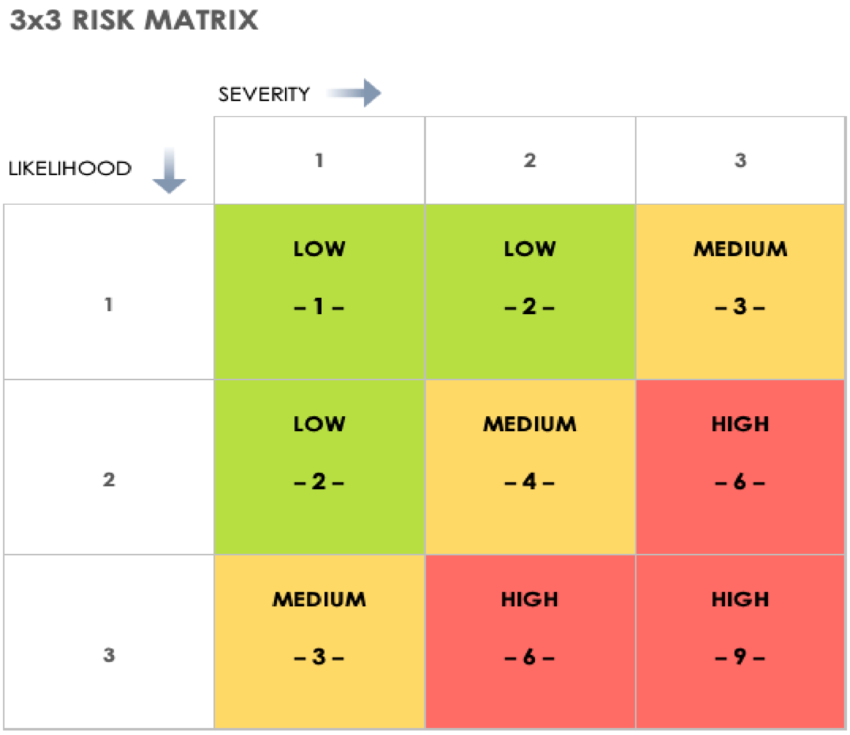
b. **Step-2** In this step threats related to the system characterized in previous stage are identified as following: -

Category	**Asset**	**Threat Linkage**
Hardware	• Home Appliances • Network Devices	• Home Use Electronic Devices • Terminal devices • End devices • Network devices • Communication devices
Software	• Policies • Network Architecture • Application Used • Security Architecture	• Misconfiguration • Non-implementation of Policies • Malicious Software/ Application • System Interface • Database • Operating System • Leakage of information
Data & Information	• Data/ Information • Storage • Encryption	• Communication between plugins /sensors and compilers • Communication between compilers and servers • Storage access • Encryption keys
People	• Users • Administrators	• Home users • Administrators • Engineers// Operators

c. **<u>Step-3,4,5 & 6</u>** In these steps' vulnerabilities related to threats identified in previous stage are identified as following: -

Asset	Threat Linkage	Vulnerability	Risk Level		Risk Categorization
			Impact	Likelihood	
• Devices • Network Devices	• Home Use Electronic Devices • Terminal devices • End devices • Network devices • Communication devices	• Physical security	3	1	Medium
		• Phishing	2	1	Low
		• Hacking	3	1	Medium
		• Eavesdropping	2	1	Low
		• Spam	2	1	Low
• Policies	• Misconfiguration • Non-implementation of policies • Malicious Software/ Application	• System access through loopholes	3	1	Medium
• Network Architecture		• Access to administrative rights	2	1	Low
		• Man in the Middle attack	2	2	Medium
• Application Used	• System Interface • Database • Operating System	• Denial of services Attacks DoS/ Distributed DoS	1	1	Low
• Security Architecture	• Leakage of information	• XSS (Cross Site Scripting)	2	2	Medium
		• Poor network monitoring	2	2	Medium
		• OS command injection			
		• SQL injection	3	3	High
		• Buffer overflow	2	2	Medium

		• Missing authorization • Unrestricted upload of dangerous file types • Use of broken algorithms • Bugs • Weak passwords • Software that is already infected with virus • Hacking the Session • Misconfiguration	2 3 1 2 2 3 1 1 1	2 3 1 2 2 3 1 1 1	Medium High Low Medium Medium High Low Low Low
• Data/ Information	• Communication between servers	• Eavesdropping packets	3	1	Medium
• Storage	• Storage access	• Missing data	2	1	Low
• Encryption	• Encryption keys	• Encryption	3	1	Medium
		• Access to public/ private encryption keys	2	1	Low

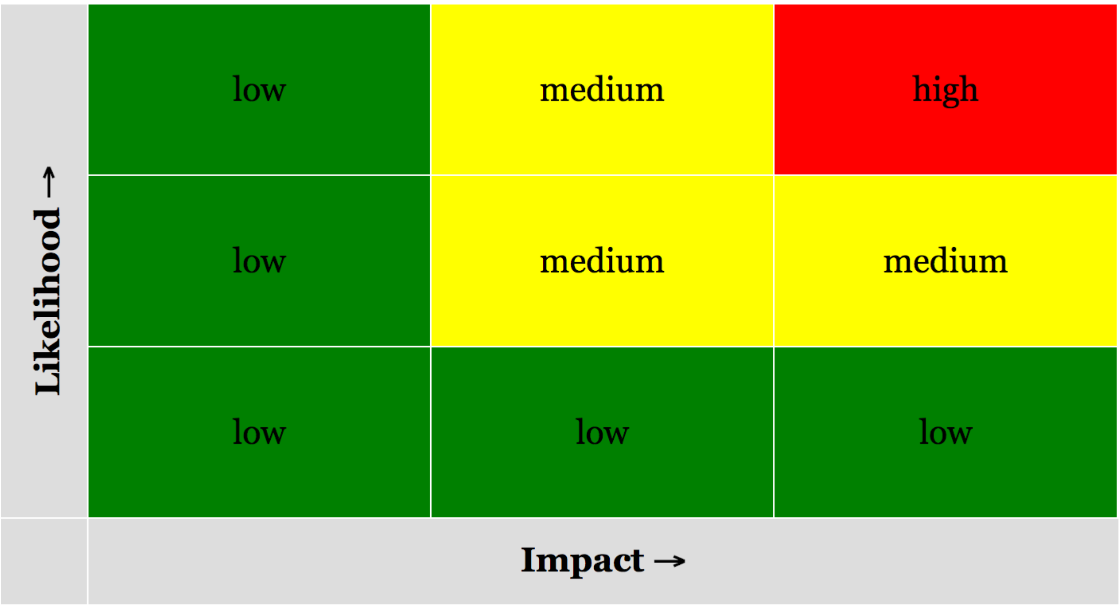


3x3 RISK MATRIX

LIKELIHOOD ↓ \ SEVERITY →	1	2	3
1	LOW – 1 –	LOW – 2 –	MEDIUM – 3 –
2	LOW – 2 –	MEDIUM – 4 –	HIGH – 6 –
3	MEDIUM – 3 –	HIGH – 6 –	HIGH – 9 –

Figure 4.1 – Risk Matrix

d. **Strep 7** In this step, the level of impact and likelihood factors are taken into consideration to determine the risk.



Likelihood ↑			
	low	medium	high
	low	medium	medium
	low	low	low
	Impact →		

Figure 4.2 – Impact/ Livelihood Matrix

e. **Step 8 & 9** Control and results are recommended in this step.

Assets/ Information	**Threat**	**Vulnerability**	**Controls/ Mitigation Strategies for Desired Results**
Devices Network Devices	• Terminal devices • End devices • Plugins/ Sensors • Network devices	• Security • Phishing • Hacking • Eavesdropping • Spam	• Physical Security • Users training • Authentication • Encryption
Policies Network Architecture Application Used Security Architecture	• Misconfiguration • Non-implementation • Malicious Software/ Application • System Interface • Database • Operating System • Leakage of information	• System access through loophole • Man in the Middle attack • Denial of services Attacks DoS/ Distributed DoS • XSS (Cross Site Scripting) • Poor network monitoring • OS command injection • SQL injection • Buffer overflow • Missing authorization • Unrestricted upload of	• Access control • Strict implementation of policies • Frequent checks on any mis-configuration • Encryption • Defining Traffic patterns • Assigning static IPs • Blacklisting/ Whitelisting of applications and IPS • Properly configured Firewall • Roll based authentication • Writing Secure codes • Use of strong passwords • Using Licensed OS.

		dangerous file types • Use of broken algorithms • Bugs • Weak passwords • Software that is already infected with virus • Hacking the Session • Misconfiguration	• Checking logs and keeping tracks of Common errors/ viruses. • Performing checksum of software being used in the system. • Using software/ application after proper software development protocols • Using up to date antivirus
Type of Data/ Information Storage	• Communication between plugins /sensors and compilers • Communication between compilers and servers • Storage access • Encryption keys	• Eavesdropping packets • Missing data	• Data Encryption while accessed and when stored • Ensuring safe custody of encryption keys • Role based Authentication • Checks on user logins and system logs • Frequent checks on storage for un authorized logins/ access
Users Administrators	• Home users • Remote users • Engineers/ Techs/operators	• Privileged account access • Weak authentication Management	• Role based Authentication • Checks on user logins and system logs

4.2 CIS (TOP-20 CONTROLS)

Ser	Control	Asset – Function	Action
1.	**Record and Control of Hardware Resources**	Devices – Identity	**A record is kept of all assets capable of storing or processing information, comprising an inventory list.** Laptop – Corei5, Air Conditioner - Wireless
2.		Devices – Respond	No unauthorized asset is connected to the network **by implementing MAC binding.**
3.	**Inventory and Control of Software Assets**	Applications – Identity	**List**: PRTG 22.2.77 Windows 10
4.		Applications – Identity	Licensed software are being used in the network.
5.		Applications – Respond	No unauthorized software is being used in the network.
6.	**Continuous Vulnerability Management**	Applications – Protect	Recent security patches of windows operating system are installed.
7.		Applications – Protect	Third party software are configured with installation of automatic updates.
8.	**Controlled Use of Administrative Privileges**	Users - Protect	Default passwords are changed and new complex passwords are configured on all devices in the network.
9.		Users – Protect	Administrator account is being used to carry out elevated actions as well as administrative tasks,
10.	**Secure Configuration for Mobile Devices, Laptops, Workstations, and Servers**	Applications – Protect	Documentation is being maintained to ensure all security configurations.
11.	**Maintenance, Monitoring, and Analysis of Audit Logs**	Network – Detect	Logging has been enabled on all devices to maintain the activity log.

12.	**Email and Web Browser Protections**	Applications – Protect	Latest version of the Google chrome is being used as it is supported by all the software being used in the network.
13.	**Malware Defenses**	Devices – **Protect**	Licensed Antivirus is used in the network to detect malwares.
14.			Scanning of removable media is configured for malware protection.
15.			Necessary configuration has been done to block auto run.
16.	**Restraint and Control of Network Ports, Protocols, and Services**	Devices – **Protect**	Windows Firewall is configured with necessary role-based traffic control.
17.	**Data Recovery Capabilities**	Data – Protect	Not applicable, however backup of network configuration has been carried out and saved on separate storage.
18.	**Protected Configuration for Devices, such as Switches, Routers, and Firewalls**	Network Protect	Licensed Antivirus is used in the network to detect malwares.
19.	**Boundary Defense**	Network Identity	Inventory of network IPs and boundaries have been maintained.
20.	**Need to Know Based Controlled Access**	Data Protect	Access control list is being maintained.
21.	**Wireless Access Control**	Network Protect	Advanced Encryption Standard (AES) is configured for wireless data.
22.	**Account Monitoring and Control**	Users -Respond	All un-necessary accounts have been disabled.
23.		Users Protect	All un-necessary accounts have been disabled.
24.		Users Protect	Session time out has been configured to log out user’s session after 15 minutes of inactivity.

25.	**Implement a Security Cognizance and Training Program**	-	Lectures on cyber security, data security and social engineering are regularly watched for awareness.
26.	**Application Software Protection**	-	All un-necessary accounts have been disabled.
27.	**Incident Response and Management**	-	Incident response procedures are defined with roles of personnel and actions to handle an incident.
28.		-	Management personnel nominated to support incident handling.
29.		-	Contact information has been maintained for reporting incidents.
30.	**Penetration Tests and Red Team Exercises**	-	Penetration test exercises are conducted to identify vulnerabilities.

4.3 ISO-27001

Ser	**Control**	**Action**
1.	**A.5.1.1 Information security policies** **A.5.1.2 Review the policies** **A.6.2.1 Mobile device policy** **A.6.2.2 Teleworking**	Policy is to protect the internal network at all costs. All defined security measures are to be taken as documented. No storage device will be connected to the network until it is sanitized through antivirus.
2.	**A.6.1.1 Information security roles and responsibilities** **A.6.1.2 Segregation of duties** **A.7.1.2 Terms and conditions of employment**	Responsible, Accountable, Supportive, Consulted, Informed (RASCI) Chart is prepared to define the job description of all the individuals.
3.	**A.6.1.3 Contact with authorities** **A.6.1.4 Contact with SIGs**	RASCI Chart Contact Details
4.	**A.6.1.5 InfoSec in projects**	Documentation

5.	**A.7.1.1 Screening**	RASCI Chart Contact Details
6.	**A.7.2.1 Management responsibilities**	Not applicable - All employees are mandated to comply with the management security policies
7.	**A.7.2.2 Security awareness and training**	Regular lectures of cyber security, social engineering and data security are watched.
8.	**A.8.1.1 Asset inventory** **A.8.1.2 Asset owners**	Inventory Management has been prepared to maintain an updated list of all hardware and other IT eqpt in home inventory.
9.	**A.8.2.1 Information classification** **A.8.2.2 Classification labelling** **A.8.2.3 Handling of assets**	Not applicable, however still information is classified as need to know basis.
10.	**A.9.1.1 Access control policy** **A9.1.2 Network access**	Access management policy is defined with details of role-based access to user accounts on different devices in the network.
11.	**A9.2.3 Privileged user management** **A9.4.4 Use of privileged utilities**	Privileged controls records are made when administrative tasks are performed in the network.
12.	**A9.2.4 Password management**	Password management policy is made for ensuring password security.
13.	**A9.2.5 Access rights reviews** **A9.2.6 Access rights adjustment**	Being maintained.
14.	**A9.3.1 Password security** **A9.4.3 Password management**	Password management policy is made for ensuring password security.
15.	**A9.4.1 Information access restriction**	Change management records are also maintained and updated for any change made in the system.

16.	**A12.2.1 Antivirus**	An updated antivirus has been deployed in the network and being regularly updated.
17.	**A12.4.1 Event logs** **A12.4.2 Log security** **A12.4.3 Admin and operator logs**	Event logs have been configured to be saved for suitable time to detect any untoward event.
18.	**A12.4.4 Clock synch**	All system clocks are synched and regularly monitored for any time difference.
19.	**A12.7.1 Systems audit controls**	An audit of system is conducted and all configuration including security aspects are checked.
20.	**A13.1.1 Network security** **A13.1.2 Network service security** **A13.1.3 Network segregation**	Not applicable.
21.	**A16.1.1 Incident management responsibilities** **A16.1.2 Incident reporting** **A16.1.3 Vulnerability reporting** **A16.1.4 Incident assessment** **A16.1.5 Incident response** **A16.1.6 Learning from incidents** **A16.1.7 Forensics**	In case of any incident, proper incident management guidelines have been formulated to be followed.

4.4 INVENTORY MANAGEMENT

Following systems are the part of proposed Home Energy Management System (HEMS):

Table 4.1: List of Inventory

Ser	Device	Code	Remarks
a.	Laptop – HP Core i-5	HEMS/1/001	
b.	Virtual Machine – 1	HEMS/1/002	
c.	Virtual Machine – 1	HEMS/1/003	
d.	Air Conditioner	HEMS/1/004	
e.	Fridge	HEMS/1/005	
f.	Mobile Phone – Huawei	HEMS/1/006	
g.	Network Adapter	HEMS/2/001	

4.5 RASCI MATRIX

A matrix defining responsibilities as “Responsible-R, Accountable-A, Supportive-S, Consulted-C, Informed-I” as mentioned below:

Table 4.2: List of Responsibilities

	Pers-1	Pers-2	Pers-3
Asset marking	C/I	S	R/A
Inventory management	C/I	R/A	S
Network maintenance	I	S	R/A
Antivirus update	I	R/A	S
Documentation	C/I	S	R/A

4.6 IMPLEMENTATION RESULTS

The appropriate controls have been applied to implement various cybersecurity frameworks in the home-based network. In this study, each framework's strengths and weaknesses were evaluated taking into account factors such as compatibility, cost and practicality to determine its suitability for the home energy management network's specific requirements. The study also identified any gaps in the standards and recommended ways to address them. The report evaluates the extent of cybersecurity risk according to specific standards and presents a summary of various standards capable of safeguarding against cyber threats. Stakeholders have been educated on the significance of cybersecurity standards and their role in preventing cyber-attacks. The frameworks were compared based on their relevance, simplicity, technical granularity and ease of implementation with the metrics presented in the table below. After conducting the assessment, the study concludes that NIST 800-30 is the most suitable framework for small networks. This framework covers all the necessary requirements including security measures, risk management and mitigation measures, and satisfies the network's security standards.

Table 4.3: Comparison of Frameworks

Ser	Category	Metric	NIST	CIS-20	ISO-27000
a.	Relevance & Simplicity in Understanding	Documentation	1	0	0
b.		Software List	1	1	1
c.		Hardware List	1	1	1
d.	Technical Granularity & Ease of Implementation	Risk Management	1	1	1
e.		Protections (Antivirus, Firewall etc.)	1	0	1
f.		Password Management	1	0	1
g.		Role Based Access Management RASCI Matrix	1	0	1
h.		Security Awareness	1	0	1
i.		Change Management	1	0	1
j.		HR Management	1	0	1

Conclusions

This chapter is aimed to implement the best cyber security standards for evaluation of a home energy management network. First of all, three security standards namely NIST, CIS Top 20 and ISO 27001 are implemented based on the specific requirements of the home energy management network considering their strengths and weaknesses as well as its practicality compatibility. Subsequently, findings of the evaluation are analyzed and different standards are compared against each other based on the evaluation criteria and the network's specific requirements. Three chosen standards are implemented for the evaluation of the home energy management network and to monitor the network's performance to ensure that it meets the required cybersecurity standards.

CHAPTER-5

CONCLUSIONS AND FUTURE WORK

HEMS is a technology that enables homeowners to effectively monitor, control, and optimize their energy usage within their homes. It has gained recognition as an efficient system for promoting energy conservation and reducing electricity consumption. However, due to the reliance on interconnected devices and online connectivity, it is crucial to prioritize the security of HEMS to protect home appliances from potential cyber-attacks. Security evaluations play a vital role in assessing and analyzing vulnerabilities and risks associated with the system. These evaluations aim to identify weaknesses in HEMS infrastructure, protocols, and devices that could make them susceptible to cyber threats. By conducting security evaluations, homeowners, manufacturers, and service providers can implement appropriate security measures to safeguard the system and its connected appliances.

HEMS systems, like any other interconnected devices, are attractive targets for hackers. Unauthorized access or control of home appliances through HEMS can lead to severe consequences such as privacy breaches, device manipulation, or physical damage. Security evaluations are essential for identifying vulnerabilities and potential attack vectors to mitigate these risks. HEMS collects sensitive data on energy consumption patterns within a home, which can reveal insights into residents' daily routines, occupancy, and lifestyle. Security evaluations ensure that this data is adequately protected against unauthorized access, preserving homeowners' privacy. As the system relies on multiple devices and communication protocols to function seamlessly, evaluating their security is crucial to maintaining the integrity of the overall system. By identifying vulnerabilities, weaknesses, and potential entry points for attackers, security evaluations enable the implementation of appropriate security controls and countermeasures.

To enhance the security of HEMS, several measures can be implemented based on the findings of security evaluations. These include the use of secure communication protocols with encryption and authentication mechanisms to protect data transmission between devices and the HEMS infrastructure. Strong access control mechanisms can be implemented to restrict unauthorized access to the system, and user authentication can ensure that only authorized individuals can control the HEMS. Regular software updates and patches should be applied to address known vulnerabilities. Separating HEMS devices from the main home network and implementing firewalls or network segmentation can isolate the system from potential threats.

Intrusion detection systems and monitoring tools should be deployed to detect and respond to potential cyber-attacks or anomalies in real-time.

In the context of assessing network security, this study evaluates an HEMS using three recognized standards: NIST, CIS Top 20 and ISO 27001. Applying these standards allows the research project to identify potential threats and vulnerabilities within the network. The study aims to understand the system's security posture and identify areas that require improvement. The study identified potential threats and vulnerabilities and recommended measures to mitigate them. By evaluating adherence to established security controls and industry best practices, significant insights into the network's security are provided. The ultimate goal of the research project is to improve the security and reliability of households. By identifying vulnerabilities and recommending mitigation measures, the study aims to enhance the network's ability to safeguard home appliances and protect against cyber-attacks. Additionally, the research highlights the importance of energy conservation and emphasizes how a secure network contributes to efficient energy use within households. Ultimately, the project aims to enhance homeowners' overall quality of life by providing a safe and reliable environment for their daily activities.

Future work involves expanding the HEMS by connecting more home appliances and devices to the home network. This expansion aims to broaden the scope of energy monitoring and control within the household. By integrating additional appliances like HVAC systems, lighting fixtures, or smart plugs, the HEMS can gather more comprehensive data on energy consumption and enable homeowners to optimize their energy usage further. To ensure the security of the expanded HEMS, the focus will be on analyzing network traffic. This involves closely monitoring data packets and communication patterns within the home network to detect potential security threats or anomalies. Analyzing network traffic allows for the identification of suspicious activities, unauthorized access attempts, or abnormal behavior that may indicate a cyber-attack.

References

[1] STJEPAN GROŠ, "A CRITICAL VIEW ON CIS CONTROLS" ARXIV:1910.01721V2 [CS.CR], 2 MAY 2020.

[2] AHMED IBRAHIM, CRAIG VALLI, IAN MCATEER, JUNAID CHAUDHRY, "A SECURITY REVIEW OF LOCAL GOVERNMENT USING NIST CSF: A CASE STUDY" THE JOURNAL OF SUPERCOMPUTING (SPRINGER SCIENCE+BUSINESS MEDIA, LLC, PART OF SPRINGER NATURE), 2018.

[3] MANISH SHRESTHA, CHRISTIAN JOHANSEN, JOSEF NOLL, "CRITERIA FOR SECURITY CLASSIFICATION OF SMART HOME ENERGY MANAGEMENT SYSTEMS" RESEARCH REPORT 492, JULY 2019.

[4] MUHAMMAD YASIN, ARRY AKHMAD ARMAN, IAN JOSEPH M. EDWARD, WERVYAN SHALANNANDA, "DESIGNING INFORMATION SECURITY GOVERNANCE RECOMMENDATIONS AND ROADMAP USING COBIT" 2019 FRAMEWORK AND ISO 27001:2013 (CASE STUDY DITRESKRIMSUS POLDA XYZ), 2019.

[5] FOTIS KITSIOS, ELPINIKI CHATZIDIMITRIOU AND MARIA KAMARIOTOU "DEVELOPING A RISK ANALYSIS STRATEGY FRAMEWORK FOR IMPACT ASSESSMENT IN INFORMATION SECURITY MANAGEMENT SYSTEMS" A CASE STUDY IN IT CONSULTING INDUSTRY, 2022.

[6] AHMAD NURUL FAJAR, HENDY CHRISTIAN, ABBA SUGANDA GIRSANG, "EVALUATION OF ISO 27001 IMPLEMENTATION TOWARDS INFORMATION SECURITY OF CLOUD SERVICE CUSTOMER IN PT. INDODEV NIAGA INTERNET" INTERNATIONAL CONFERENCE ON COMPUTATION IN SCIENCE AND ENGINEERING, IOP CONF. SERIES: JOURNAL OF PHYSICS: CONF. SERIES 1090, 2018.

[7] USMAN ZAFAR, SERTAC BAYHAN AND ANTONIO SANFILIPPO, "HOME ENERGY MANAGEMENT SYSTEM" DIGITAL OBJECT IDENTIFIER 10.1109/ACCESS.2020.3005244, 2020.

[8] ISABEL MARIA LOPES, PEDRO OLIVEIRA AND TERESA GUARDA," HOW ISO 27001 CAN HELP ACHIEVE GDPR COMPLIANCE" 14TH IBERIAN CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGIES (CISTI), 2019.

[9] RICHARD PRESTON, MARK DUCK, COLIN FINNEGAN, RODRIGO MUNOZ, "INTEGRATING CYBER SECURITY REQUIREMENTS INTO A POWER MANAGEMENT SYSTEM" PAPER NO. PCIC-2019-14, 2019.

[10] IBRAHIM AL-MAYAHI, SA'AD P. MANSOOR, "ISO 27001 GAP ANALYSIS - CASE STUDY"

[11] DEDY ACHMADI, YOHAN SURYANTO, KALAMULLAH RAMLI, "ON DEVELOPING INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FRAMEWORK FOR ISO 27001-BASED DATA CENTER" 978-1-5386-5525- 2/18/$31.00 C_ 2018 IEEE IWBIS, 2018.

[12] EMMA SCOTT, SAKSHYAM PANDA, GEORGE LOUKAS, EMMANOUIL PANAOUSIS, "OPTIMISING USER SECURITY RECOMMENDATIONS FOR AI-POWERED SMART-HOMES"

[13] DAMIAN SHAW-WILLIAMS, "THE EXPANDING ROLE OF HOME ENERGY MANAGEMENT ECOSYSTEM: AN AUSTRALIAN CASE STUDY" CHAPTER 7, BEHIND AND BEYOND THE METER, 157-175, 2020.

[14] ZHOU, J., & WANG, L. (2017). AN EVALUATION FRAMEWORK FOR SECURITY AND PRIVACY OF HOME ENERGY MANAGEMENT SYSTEM. ENERGY PROCEDIA, 105, 4047-4052.

[15] ZENG, Y., DONG, Y., & XIAO, Y. (2018). SECURITY ANALYSIS OF HOME ENERGY MANAGEMENT SYSTEMS. IN PROCEEDINGS OF THE 3RD INTERNATIONAL CONFERENCE ON ELECTRICAL AND INFORMATION TECHNOLOGIES FOR RAIL TRANSPORTATION (EITRT) (PP. 1104-1109). IEEE.

[16] AMIN, S. M., & WANG, X. (2013). EVALUATING THE SECURITY OF ADVANCED METERING INFRASTRUCTURE NETWORKS. IEEE TRANSACTIONS ON SMART GRID, 4(2), 983-990.

[17] XIE, W., & ZHANG, R. (2015). EVALUATING THE SECURITY OF SMART HOME AUTOMATION SYSTEMS. IEEE TRANSACTIONS ON SMART GRID, 6(2), 831-840.

[18] JIANG, Z., LI, Y., & WU, H. (2014). SECURITY AND PRIVACY EVALUATION FOR HOME ENERGY MANAGEMENT SYSTEM BASED ON CLOUD COMPUTING. IN PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE ON INTERNET MULTIMEDIA COMPUTING AND SERVICE (ICIMCS) (PP. 279-282). ACM.

[19] ZHANG, Z., LI, X., & WANG, H. (2019). SECURITY EVALUATION OF SMART HOME ENERGY MANAGEMENT SYSTEMS BASED ON SCADA. IN PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE ON ELECTRICAL AND ELECTRONICS ENGINEERING (ICEEE) (PP. 118-121). IEEE.

[20] YOUSSEF, A. E. (2017). EVALUATING THE SECURITY OF HOME ENERGY MANAGEMENT SYSTEM USING SECURITY AUTOMATION FRAMEWORK. IN PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE ON RENEWABLE ENERGY RESEARCH AND APPLICATIONS (ICRERA) (PP. 121-127). IEEE.

[21] LI, C., LI, X., & LI, Z. (2020). SECURITY EVALUATION OF RESIDENTIAL SMART ENERGY MANAGEMENT SYSTEMS BASED ON CYBER-PHYSICAL SYSTEMS. IEEE ACCESS, 8, 23195-23207.

[22] AOUN, R., & NAJA, N. (2019). EVALUATING THE SECURITY OF SMART HOME ENERGY MANAGEMENT SYSTEMS USING AN ATTACK TREE METHODOLOGY. JOURNAL OF AMBIENT INTELLIGENCE AND HUMANIZED COMPUTING, 10(9), 3349-3361.

[23] WANG, J., LU, J., & WU, Z. (2018). AN EVALUATION FRAMEWORK FOR THE SECURITY OF HOME ENERGY MANAGEMENT SYSTEMS. IN PROCEEDINGS OF THE 3RD INTERNATIONAL CONFERENCE ON CONTROL SCIENCE AND SYSTEMS ENGINEERING (ICCSSE) (PP. 341-345). IEEE.

[24] ZHAO, Y., LIU, Y., & LUO, X. (2017). SECURITY EVALUATION OF HOME ENERGY MANAGEMENT SYSTEMS BASED ON RISK ANALYSIS. JOURNAL OF RENEWABLE AND SUSTAINABLE ENERGY, 9(5), 053705.

[25] WANG, L., & ZHOU, J. (2018). AN EVALUATION FRAMEWORK FOR SECURITY AND PRIVACY OF HOME ENERGY MANAGEMENT SYSTEM BASED ON ATTACK GRAPH. JOURNAL OF RENEWABLE AND SUSTAINABLE ENERGY, 10(6), 063703.

[26] ZHANG, Z., LI, X., & WANG, H. (2018). AN EVALUATION FRAMEWORK FOR SECURITY AND PRIVACY OF SMART HOME ENERGY MANAGEMENT SYSTEMS. JOURNAL OF RENEWABLE AND SUSTAINABLE ENERGY, 10(3), 033701.

[27] WANG, Y., ZHU, H., & CUI, J. (2017). AN EVALUATION MODEL FOR SECURITY OF HOME ENERGY MANAGEMENT SYSTEM. IN PROCEEDINGS OF THE 36TH CHINESE CONTROL CONFERENCE (CCC) (PP. 5107-5111). IEEE.