

**RISK ASSESSMENT OF SMART GRID SYSTEMS : STUDYING VIABILITY OF MITIGATION
THROUGH BLOCKCHAIN**



Author

Zarrar Altaf

Registration Number

00000397829

Supervisor

Professor Dr. Nadeem Kureshi

DEPARTMENT OF CYBER SECURITY, PAKISTAN NAVY ENGINEERING COLLEGE

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY

KARACHI

APRIL, 2024

**RISK ASSESSMENT OF SMART GRID SYSTEMS : STUDYING
VIABILITY OF MITIGATION THROUGH BLOCK CHAIN**

Author

Zarrar Altaf

Registration Number

00000397829

A thesis submitted in partial fulfillment of the requirements for degree of
MS CYBER SECURITY

Thesis Supervisor:

Dr. Nadeem Kureshi

Thesis Supervisor's Signature: _____


DR NADEEM KURESHI
Commodore
DEAN MIS
PNS JAUHAR

DEPARTMENT OF CYBER SECURITY, PAKISTAN NAVY ENGINEERING

COLLEGE

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY

KARACHI

APRIL, 2024

Certificate of Originality

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at Department of Cyber Security at Pakistan Navy Engineering College (PNEC) or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at Pakistan Navy Engineering College (PNEC) or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Signature: _____



Zarrar Altaf

CERTIFICATE FOR PLAGIARISM

1. It is certified that PhD / M.Phil / MS Thesis Titled "Risk Assessment of Smart Grid Systems: Studying viability of mitigation through Blockchain Technology" by ZARRAR ALTAF (2021-NUST-MS Cyber Security (CyS Fall 21)) has been examined by us. We undertake the follows:

- a. Thesis has significant new work / knowledge as compared already published or is under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
- b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.
- c. There is no fabrication of data or results which have been compiled / analyzed.
- d. There is no falsification by manipulating research materials, equipment, or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
- e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC Plagiarism Policy and instructions issued from time to time.

DR NADEEM KURESHI
Commodore
DEAN MIS
PNS JAUHAR



Name & Signature of Supervisor

DR NADEEM KURESHI
Commodore
DEAN MIS
PNS JAUHAR

LIA AYLIJA
Lt Col Pakistan Navy
HOPG Cyber Security
PNS Jauhar

Thesis Acceptance Certificate

Certified that final copy of MS/MPhil thesis entitled "RISK ASSESSMENT OF SMART GRID SYSTEMS : STUDYING VIABILITY OF MITIGATION THROUGH BLOCKCHAIN" written by Zarrar Altaf , (Registration No 00000397829), of Pakistan Navy Engineering College (PNEC) has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: _____

nn
DR NADEEM KURESHI
Commodore
DEAN MIS

Name of Advisor: Prof. Dr. Nadeem Kureshi

Date: _____

Signature (HoD): _____

AAIYA ALI
AAIYA ALI
Lt Cdr Pakistan Navy
HOPGP Cyber Security
PNS Jauhar

Date: _____

Signature (Dean/Principal): _____


Uzma Khand
UZMA KHAND
Cdr Pakistan Navy
HOD Computer Science
PNS Jauhar

Date: _____

Approval

It is certified that the contents and form of the thesis entitled "RISK ASSESSMENT OF SMART GRID SYSTEMS : STUDYING VIABILITY OF MITIGATION THROUGH BLOCKCHAIN" submitted by **Zarrar Altaf** have been found satisfactory for the requirement of the degree.


Advisor: **Prof. Dr. Nadeem Kureshi**

Signature: _____ 
DR NADEEM KURESHI
Commodore
DEAN MIS
Date: _____
PNS JAUHAR

Committee Member 1: **Lt Cdr Aaliva PN**

Signature: _____ 
Date: 18/4/24

Committee Member 2: **Capt Dr Sajid Saleem PN**

Signature: _____ 
Date: _____
DR. SAJID SALEEM :
Captain Pakistan Navy
Director SoSE
R&D Wing, NRDI

Declaration

I certify that this research work titled "*RISK ASSESSMENT OF SMART GRID SYSTEMS & STUDYING VIABILITY OF MITIGATION THROUGH BLOCK CHAIN TECHNOLOGY*" is my own work. The work hasn't been submitted for evaluation elsewhere else. All used content from external sources has been correctly cited and credited.



Zarrar Altaf

2021-NUST-MS-CyS-00000397829

Copyright Statement

The student author of this thesis retains all rights to the text. Only in compliance with the author's instructions may copies (by any method) of the entire work or of any excerpts be made and stored in the NUST Pakistan Navy Engineering College Library (PNEC). The Librarian can get details. Any such reproductions must include a copy of this page. No more copies (via any method) may be created without the author's written consent.

The ownership of any intellectual property rights which may be described in this thesis is vested in NUST, Pakistan Navy Engineering College, subject to any prior agreement to the contrary, and may not be made available for use by third parties without the written permission of PNEC, which will prescribe terms and conditions of any such agreement.

Further information on the conditions under which disclosures and exploitation may take place is available from the Library of NUST Pakistan Navy Engineering College, Karachi.

Acknowledgements

I am grateful to my Creator, Allah Subhana-Wattala, for guiding me through this effort at every step and for instilling new ideas in my head to make this thesis better. Indeed, I could have done nothing without His invaluable assistance and counsel. Whoever assisted me over the duration of my thesis, whether my parents or another individual was His will, and none is deserving of recognition than Him.

I am extremely grateful to my dear parents, who have continued to support me in every aspect of my life. I'd also want to thank my supervisor, Dr Nadeem Kureshi, for his assistance during my thesis, as well as the courses he taught me. I can confidently claim that I have never learnt any other technical topic in such detail as those he has taught.

I'd also want to thank Dr Fawad Ahmed for his unwavering support and collaboration. He always had a solution for any problem I was having. Without his assistance, I would have been unable to complete my thesis. I appreciate his patience and help during this thesis.

I'd also want to thank Dr Sajid Saleem and Ms Aaliya for serving on my thesis supervision and assessment committee, as well as Abdullah specifically for his assistance.

Finally, I would like to express my gratitude to all the individuals who have rendered valuable assistance to my study.

Dedicated to my parents and wife, whose unwavering cooperation and support helped me achieve this feat.

Also dedicated to my kids Saad, Hamza, Maria and Khalid who will certainly witness the modern aspects highlighted in my thesis and are expected to be beneficiaries of the technology.

Abstract

Smart Grid Systems are a technology of future and can very well be termed as Cyber Physical System. It is very well an example of a state of art System of System Engineering SoSE architecture. Smart Grid Managed Network Systems ensure uninterrupted services supplies, balancing of output where needed or where not needed, updation and dispatch of tariffs, online payment of bills etc. However, Smart Grid Systems in a developing country are yet under definition. With a number of other non-conventional threats and risks such as poverty within the masses, across border concerns, challenges of security of smart grid systems increase manifold. These challenges include both Cyber-related as well as social and basic law and order issues. Third world countries need fool proof and un-comprisable security for their smart grid management systems which are yet to be developed. Also high demand/ consumption and effective balancing of power systems necessitate use of smart components in Smart Grid Systems. Use of millions of smart devices over national grids will certainly pose severe threats and risks to security of these systems.

On the other hand, Blockchain Technology is rooting its existence with solutions to many problems of the modern era. Blockchain has encompassed health info systems and industrialization through its flexible and de-centralized design. With identification of major cyber related threats as well as vulnerabilities of Smart Grid Systems, this study will attempt to focus on all conventional as well as non-conventional threats of a typical third-world Smart Grid System, thus, proposing mitigation strategy using Block Chain options.

Key Words: *Smart Grid Systems, Risk Assessment, Mitigation, Block Chain Technology*

Table of Contents

Declaration	iv
Plagiarism Certificate (Turnitin Report).....	Error! Bookmark not defined.
Copyright Statement	ix
Acknowledgements.....	x
Abstract	xi
Table of Contents.....	Error! Bookmark not defined.
List of Figures	xv
List of Tables	xix
List of Abbreviations	
CHAPTER 1: INTRODUCTION AND MOTIVATION.....	Error! Bookmark not defined.
a. Preamble.....	
b. Historical Perspective : Attacks on major Grid Sytems and their impacts	
c. Block Chain & Architecture.....	
d. Risk Assesment.....	
e. Research Questions.....	
f. Research Objectives.....	
CHAPTER 2: SMART GRID AND THEIR SECURITY ISSUES	6
a. Smart Grids	
b. Characteristics	
c. Differences b/w Smart and Conventional Grids	
d. Security Issues of Smart Grids.....	
CHAPTER 3: LITERATURE REVIEW.....	3
a. Review	
b. Deductions.....	
c. ResearchGap	
d. Problem Statement.....	
CHAPTER 4: PROPOSED FRAMEWORK/ METHODOLOGY.....	4
a. Data Gathering.....	
(i) Studying architecture of Smart Grid Systems.....	
(ii) Identification of components vulnerable to Cyber threats.....	
b. Risk Analysis.....	

(i)	Studying threats to each component.....	
(ii)	Severity = Likelihood x Impact.....	
c.	Mitigation.....	
(i)	Viability of Block chain for security of smart systems.....	
CHAPTER 5:ANALYSIS.....		5
a.	Literature Review.....	
b.	Risk Analysis Process.....	
c.	Mitigation through Clockchain Technology.....	
d.	Cross Zonal Analysis.....	
e.	Blockchain Integration Challenges and Oppurtunities.....	
f.	Cybersecurity Training and Awareness Programs.....	
g.	Stakeholder Collaboration and Information Sharing.....	
h.	Simulation and Testing Protocols.....	
i.	Continuous Monitoring and Adaptation.....	
j.	Integration with National Cybersecurity Frameworks.....	
k.	Environmental and Social Impacts.....	
l.	Evaluation of Security Architecture.....	
m.	Identification of Vulnerable Components.....	
n.	Perceived Threats and Risk Analysis.....	
o.	Mitigation Strategies through Blockchain Technology.....	
p.	Comparative Analysis of Risk Assessment Methods.....	
q.	Calculations for Risk Assessment.....	
r.	Evaluation of Blockchain Technology.....	
s.	Comparative Analysis of Blockchain Platforms.....	
t.	Scalability Analysis.....	
u.	Cost-Benefit Analysis of Cybersecurity Measures.....	
v.	Statistical Analysis of Threat Incidents.....	
w.	Ethical Considerations.....	
x.	Comparison with Industry Standards.....	
y.	Summary of Analysis.....	
CHAPTER 6: CONCLUSIONS,RECOMMENDATIONS.....		6
a.	Summary of Findings.....	
b.	Key Findings.....	
c.	Recommendations.....	
d.	Closing Statement.....	
CHAPTER 7: FUTURE WORK.....		11
REFERENCES	Error! Bookmark not defined.	

LIST OF ABBREVIATIONS

AGC	-	Automatic Gain Control
ALE	-	Annual Loss Expectancy
AMI	-	Advanced metering Infrastructure
BAN	-	Body Area Network
BC	-	Blockchain
BF	-	Brute Force
CC	-	Crypto Currencies
CIA	-	Confidentiality, Integrity, Availability (Triad)
CPS	-	Cyber Physical Systems
CR	-	Cluster Router
CSRF	-	Cross-Site Request Forgery
DA	-	Distribution Automation
DCC	-	Data and Control Center
DOS	-	Denial of Service
DDOS	-	Distributed Denial of Service
DER	-	Distributed Energy Resource
DLR	-	Dynamic Line Rating
DMS	-	Distribution Management System
DoS	-	Denial of Service
DSM	-	Demand Side Management
DMZ	-	De-Militarized Zone
EBIOS	-	Expression of Needs & Identification of Security Objectives

ESP	-	Electronic Security Parameter
FDIA	-	False Data Injection Attack
FW	-	Firewall
HAN	-	Home Area Network
HVDC	-	High Voltage Direct Current
IAN	-	Incident Area Network
IED	-	Intelligent Electronic Device
IOT	-	Internet of Things
IS	-	Information Security
IEC	-	International Electrotechnical Commission
LAN	-	Local Area Network
MPLS	-	Multi Protocol Label Switching
NIST	-	National Institute of Standards & Technology
NSP	-	Network Service Provider
OSI	-	Open System Interconnection
OWASP	-	Open Web Application Security Project Standards
PLC	-	Programmable Logic Control
PMU	-	Phasor Measurement Unit
RES	-	Renewable Energy Storage
RTP	-	Real Time Pricing
RTUs	-	Remote terminal unit
SCADA	-	Supervisory control and data acquisition
SG	-	Smart Grids

SoSE	-	System of Systems Engineering
TMS	-	Transmission Management System
UTM	-	Unified Threat Management
WR	-	WAN Routers

List of Figures

Figure 1: BlockChain Structure	Error! Bookmark not defined.
Figure 2.1: Smart Grid Architecture	Error! Bookmark not defined.
Figure2.2: Smart Grid Components	Error! Bookmark not defined.
Figure 2.3: Modern Smart Grid	Error! Bookmark not defined.
Figure 2.4: Block Diagram	Error! Bookmark not defined.
Figure 4.1: Frame work being followed	Error! Bookmark not defined.
Figure 4.2: Conceptual diagram of smart grid system	Error! Bookmark not defined.
Figure 4.3 : Risk Assessment (Likelihood x Impact) Table.....	26
Figure 5.1: Attacks with frequencies.....	46

List of Tables

Table 2.1: Difference between smart and conventional grid	Error! Bookmark not defined.
Table 2.2: Security issues of smart grid.....	Error! Bookmark not defined.
Table 2.3: Illustration of reverse transaction	Error! Bookmark not defined.
Table 4.1: A synopsis of vulnerable components in different zones	Error! Bookmark not defined.
Table 4.2: Risk Analysis Summary	Error! Bookmark not defined.
Table 4.3: Blockchain mitigation strategies.....	Error! Bookmark not defined.
Table 4.4: Blockchain Technology Evaluation.....	Error! Bookmark not defined.
Table 4.5: Comparative Analysis of Blockchain Platforms.....	Error! Bookmark not defined.
Table 4.6: Ability of Blockchain to achieve Security objectives...	Error! Bookmark not defined.
Table 5.1: Evaluation of Security Architecture	Error! Bookmark not defined.
Table 5.2: Vulnerable Components by Zone	Error! Bookmark not defined.
Table 5.3: Risk Analysis Summary	Error! Bookmark not defined.
Table 5.4: Blockchain Mitigation Strategies	Error! Bookmark not defined.
Table 5.5: Comparative Analysis of Risk Assessment Methods ...	Error! Bookmark not defined.
Table 5.6: Blockchain Technology Evaluation.....	Error! Bookmark not defined.
Table 5.7: Comparative Analysis of Blockchain Platforms.....	Error! Bookmark not defined.
Table 5.8: Cost-Benefit Analysis.....	Error! Bookmark not defined.
Table 5.9: Statistical Analysis Summary	Error! Bookmark not defined.
Table 5.10: Framework Comparison	Error! Bookmark not defined.

CHAPTER 1

Introduction and Motivation

1.1 Preamble

It is being discussed between strategists and tacticians that 5th and 6th generation wars will not be fought in land, sea or air realms but will mostly focus on cyber domains of nations. Smart grid systems being the future inevitable technology will certainly be on top of the list. Inadvertently, Smart Grid infrastructure are a reality of tomorrow and it is contemplated that modern world has already stepped into this whereas developing nations will certainly be employing smart infrastructure in their daily lives in next 10-25 years. Smart grid systems are considered to be typical example of System of Systems Engineering or Cyber Physical systems where multiple versatile technologies are blended in one integrated system. This is achieved through employment of extensive IOT systems/ devices, which are if not securely configured, prone to cyber attacks and vulnerabilities. Thus, risk assessment and mitigation of future smart grid systems is necessary now and is also essential to be done constantly as emerging field will regularly be updating themselves.

1.2 Historical Perspective : Attacks on major Grid Systems and their impacts

In the past, major infrastructures have been under attack through use of cyber means. A brief account of these is appended below:

Stuxnet rose to notoriety when it was used to attack Iranian nuclear facilities. Despite being malicious software, the computer worm Stuxnet was utilized to attack electro-mechanical systems. Like the big attack in Iran, the attackers used Stuxnet to search for a connection to the software controlling the electro-mechanical equipment on compromised PCs, exploit multiple zero-day Windows vulnerabilities, and send commands designed to damage the equipment. The book "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon" claims that in 2010, visiting inspectors from the Atomic Energy Agency were astonished to see that many of Iran's centrifuges were failing. The Siemens equipment was supposed to enrich uranium for use in nuclear reactors, but both the Iranians and the inspectors could not figure out why it was malfunctioning so badly. It was hard to accept that some malicious program was at fault. This is hardly surprising, given that Iran's nuclear facilities were "air gapped," or cut off from networks and the Internet. Malware must be physically installed on the air gapped uranium enrichment facility, either purposefully or inadvertently, maybe with the use of an infected USB drive.

Korea Hydro and Nuclear Power (KHNP), a nuclear and hydroelectric firm based in South Korea, had a cyberattack towards the end of 2014. Hackers published 10,000 employees' personal information online along with the blueprints and instructions for two nuclear reactors that they had stolen. Despite the fact that South Korean authorities linked the IP addresses to the city of Shenyang in northeastern China, the US accused North Korea of carrying out the attack.

About 225,000 houses in western Ukraine lost energy in December 2015 as a result of hackers breaking into the infrastructure of a power utility. A US investigation into the blackout found that a spear-phishing technique—which entailed emailing key personnel detailed messages utilizing information obtained from social media—was used to distribute a virus via email. Although no names were mentioned in the paper, experts surmised that the culprits were a group of Russian hackers.

A cyber attack against Ukraine took place in December of 2016. Hackers knocked down an electricity substation, leaving some inhabitants of Kiev without power for an hour. The electrical outage, according to the BBC, was responsible for one-fifth of Kyiv's overnight energy use. According to some researchers, the attack, which was attributed to Russian hackers—was meant to do physical damage to the electrical infrastructure.

Cybercriminals targeted Saudi Aram co in 2017 by targeting the safety system of one of the company's petrochemical power facilities. Even though the facility was shut down, analysts believe that something went wrong. According to reports, a facility executive stated that the attack's goals included shutting down the plant and wiping data, but also making a political statement. Specialists were able to connect the attack to a Russian government laboratory.

1.3 Risk Assessment

Risk Assessment is a mature function and technique generally used to establish extent of vulnerabilities posed to a system by different threats and dangers. Risk assessments have always been conducted in all eras i.e both old as well as contemporary times and are usually followed by different mitigation strategies and related aspects. In this study, review for both Risk assessment of a Smart Grid System has been carried out.

1.4 Block Chain

Technology called block chain makes it possible for a community to uphold trust. Another way to describe a block chain is as a distributed network that manages an unchangeable database. The block chain idea was put out by Satoshi Nakamoto and implemented in the crypto currency bit coin (Nakamoto, 2008). Coin and token are the names for the two different types. However, the block chain is not just restricted to digital money. Relevant approaches for using the block chain in the financial sectors include traceability, automatic transaction settlements and the financial sector. In earlier studies, crucial data on the smart grid was mapped, utilized, and transactions were managed using Rainbow Chain technology. The block chain employs Proof of Work and is able to carry out smart contracts, record transactions, and carry them out. PwC Global Power & Utilities (2016) conducted a study for the German Consumer Advice Centre (Verbraucherzentrale) that identified three key elements of block chain technology that must be successful in the energy sector: (1) User-friendly, easy-to-use and effective application; (2) cost efficiency verification process; and (3) value-added provided by the block chain.

1.4.1. Concept

The original block chain idea solved the problem of double-spending with digital currency without requiring a central authority or decentralization of power. When a buyer makes a purchase, the payer usually physically transfers the funds (coins or paper) to the payee. In the digital world, money is data that can be precisely and readily copied. When a payer duplicates money with ease, uses the first copy, and then uses the second copy, this is known as the double-spending conundrum. To resolve the conflict, a mediator who can be trusted must be involved. The amount of the payer is verified, deducted in accordance with the bill, and added in accordance with the bill for the payee. Nakamoto argues in his paper that this intermediary will eventually impose limits on small transactions and raise service prices. The mediator is also necessary in order to arbitrate a dispute between parties. Another problem is that, in the case of non-reversible transactions like those that occur in the service industry, this intermediary's ability to forcefully reverse the already-completed transaction is unwanted. Because of the situation, companies will be frightened of their consumers and will gather more information about them than is necessary, which might compromise the privacy of the customers. Block chains provide the immutability of transactions and do away with intermediaries. The block chain may be extended in a number of ways. Any information indicating the transfer of ownership of any kind of asset, including electricity, might be considered a transaction outside of the crypto currency space.

1.4.2. Structure

As shown in Fig. 1, a block chain is made up of blocks that are connected together and secured using a hash function in a time sequential sequence. It is impossible to backdate the block because it is timely stamped. A group of transactions form a block. A transaction in bit coin is the transfer of ownership of the funds. In our situation, the exchange of power can take the place of this. A hash function is a type of one-way mathematical function that, given any input, yields a definite output. The hash is also one-way, so if you know the input, it's simple to figure out the output, but not if you don't. A special hash algorithm called $H(x)$, where x is the number of the current block, is used to hash a block when it is full or when a new block needs to be created. A "chain" is then formed by storing the hash in the following block. Up until the final block, the procedure was repeated, making it simple to detect a minor change to a block because the hash will no longer be valid. A person who has a particular amount of bit coins can give those coins or the money they represent to someone else. However, both the past and subsequent owners are represented by a special identification called an address rather than by a real-life identity. The public key of a private-public key is where the address is obtained. By doing so, the network could quickly confirm the legitimacy of the coin owner. Since a block chain keeps track of every transaction, it is possible to trace a transaction back to its inception, which solves the issue of double-spending.

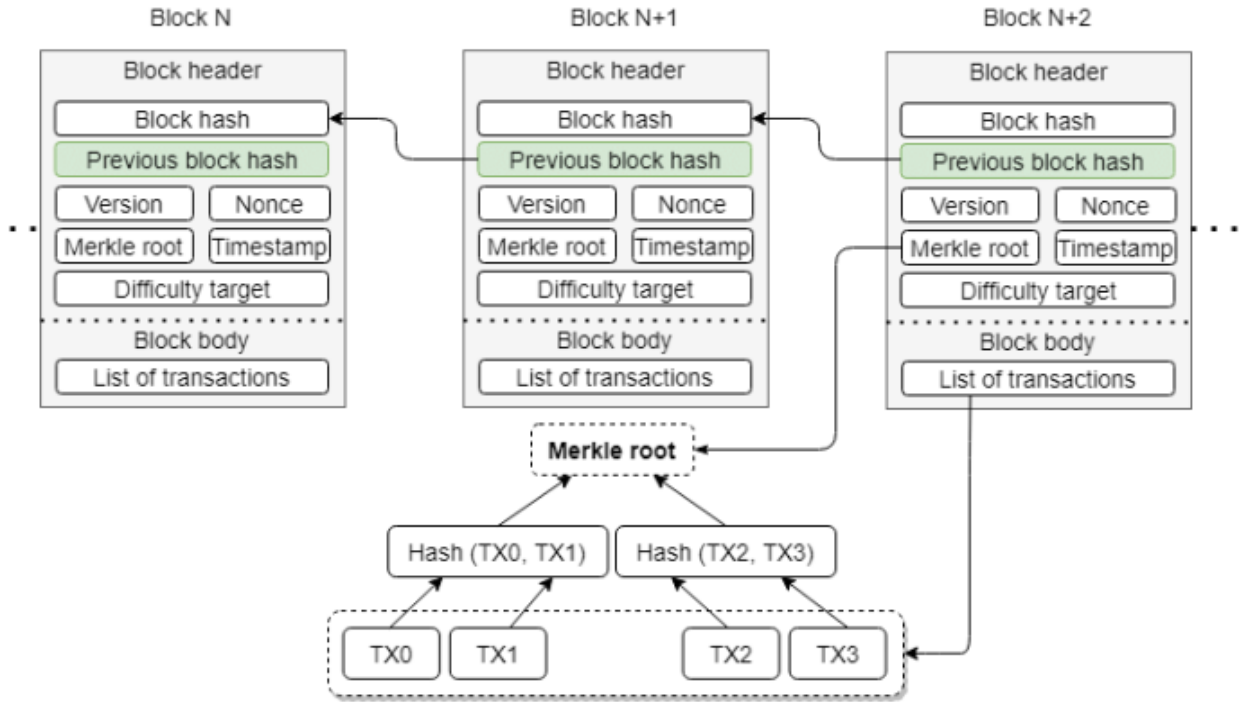


Figure 1:Blockchain Structure

1.4 Research Questions

In above backdrop, it is aimed that a thorough study, risk assessment and mitigation options be studied. For this, the research questions finalized are as below:

- a. What are essential components of Smart Grid System w.r.t Cyber Security?
- b. How Risk assessment identifies vulnerability to cyber attacks in modern Smart Grid Systems?
- c. Is Block Chain Technology a viable option for Risk Mitigation of modern Smart Grid Systems?

1.5 Research Objectives

- a. Identification of different components of Smart Grids and carrying out their vulnerability assessment
- b. Exploring conceptual design of latest SGs and conducting Risk/ Vulnerability Assessment of contemporary systems
- c. Studying viability of Mitigation through Block Chain Technology Option

1.6 Thesis Outline

Chapter 1 discusses Introduction of Smart Grids, impact of threats of Smart Grids w.r.t National Security while discussing some historical cases. Chapter also outlines Research objectives and Questions.

Chapter No.2 gives a detailed background w.r.t Smart Grids. Generally speaking, it talks of Smart Grid requirements, characteristics, main differences between Conventional and Smart Grids and details w.r.t Attack Points and vulnerabilities of systems.

In Chapter 3, Literature Review has been done which is mostly concentrated in 03 portions. First portion is w.r.t Risk Assessment Techniques, review of IS Systems risk assessment and mitigation in general, whereas, it also describes risk assessment fundamentals and other related/ driven factors. Second portion is related to various Cyber Security challenges to Smart Grids, their detection and mitigation techniques have been discussed. This also includes a critical review on anticipated cyber security threats in complex environment and efforts to address the grave concern have been presented. Whereas, 3rd portion sheds light on prospects of using Blockchain to address Cyber Security issues of a typical smart grid system.

Chapter 4 covers data gathering and risk analysis. A text book review of a modern smart grid has been carried out followed by identification of components which can be compromised by a Cyber Attack, their risk analysis and subsequently, viability with respect mitigation through Block chain technology has been carried out. Benefits of various Blockchain applications have been pitched in relation to various Smart Grid components. Also evaluation of Blockchain platforms have been done w.r.t viability for required work.

Chapter 5 presents Analysis which covers Findings from Literature Review, Risk Analysis and Mitigation and Misc other aspects.

Chapter 6 and 7 comprise Conclusion/ Recommendations and Future Work respectively. Since Smart Grids and Black Chain both are a technology of future and very minimal work has been conducted till now, it is established that considerable room for future works still exists.

CHAPTER 2

Smart Grids And Their Security Issues

2.1 What are Smart Grid Systems?

Energy technologies are essential to society's social and economic advancement. Because of electrical networks that supply power to homes, companies, and industries, everyone in our society now depends on energy. The 21st century has seen many countries prioritize developing new energy supplies and improving energy efficiency due to pressure from both climate change and ever-increasing energy consumption. For example, it is predicted that raising energy efficiency might result in a significant national energy reduction and net economic advantages for businesses and consumers. The idea of an efficient power grid has gained international attention, and the term "smart grid" has taken on many meanings. While some regard it as a quantitative solution primarily for residential customers downstream, others see it as a global system vision that goes beyond the current energy market structure to produce benefits for everyone that are social, economic, and environmental. The majority of people do, however, agree that the purpose of the smart grid is to enhance the present electrical system and accomplish the objectives of green energy and greenhouse emission reduction.

A clever or smart grid is a kind of energy grid that seeks to count on and intelligently reply to the conduct and movements of all energy customers linked to its suppliers, clients and people who do each to effectively supply reliable, reasonably-priced and sustainable energy services [1].

Smart Grid has the subsequent 3 economic goals

- a. To improve the reliability.
- b. To lessen height demand
- c. To lessen general electricity consumption.

Numerous technologies have been created and included into the electrical network in order to accomplish these objectives. Its goal is to enhance the present electricity grid system rather than replace it. A smart grid combines cutting-edge sensing technology, control strategies, and integrated communications into the transmission and distribution layers of the existing electrical grid.

The Smart Grid should have following key characteristics:

- a. Self-healing
- b. Consumers motivation and participation
- c. Attack resistance
- d. Higher quality power
- e. Different generation and storage options
- f. Flourished markets

- g. Efficiency
- h. Higher integration of intermittent power generation sources.

A Typical Smart Grid Architecture is shown below:

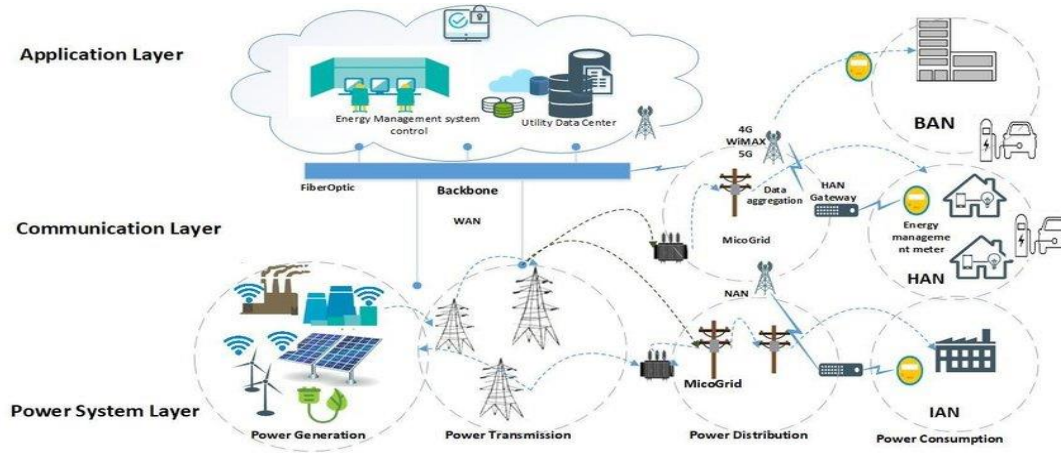


Figure 2.1: Smart Grid Architecture

2.2 Essential Components of Smart Grid Systems

Better electricity production and efficient energy transmission and distribution are possible with help of smart grid technology. Compared to traditional grids, it takes up less space and is simpler to install because of its versatility. The observability of the network, the creation of asset controllability, the improvement of energy system performance and security, and particularly the financial aspects of planning, maintenance, and operation are the main focuses of the Smart Grid design concept [3]. By then, special needs had been requested, such as control, monitoring, costs and supplies of transmission, and distribution of electricity. Therefore, a traditional electric community may be referred to as a "smart grid" if it has automated controls and tracking devices.

In order to find out components of Smart Grid, we must see the working concept of Smart Grid

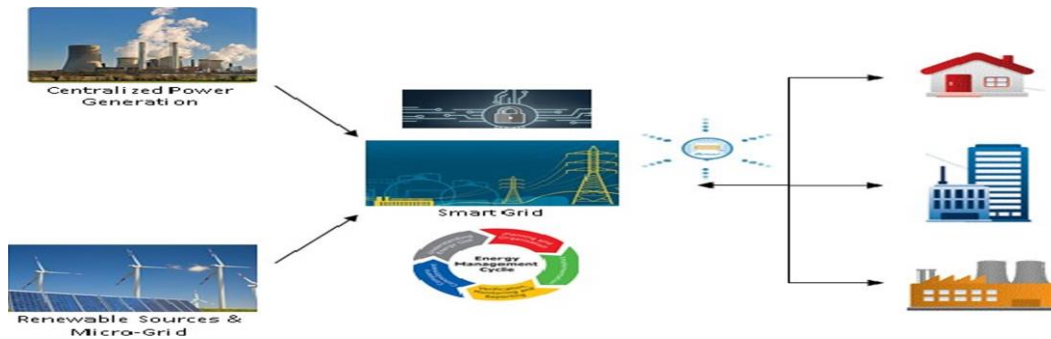


Figure 2.2: Smart Grid Components

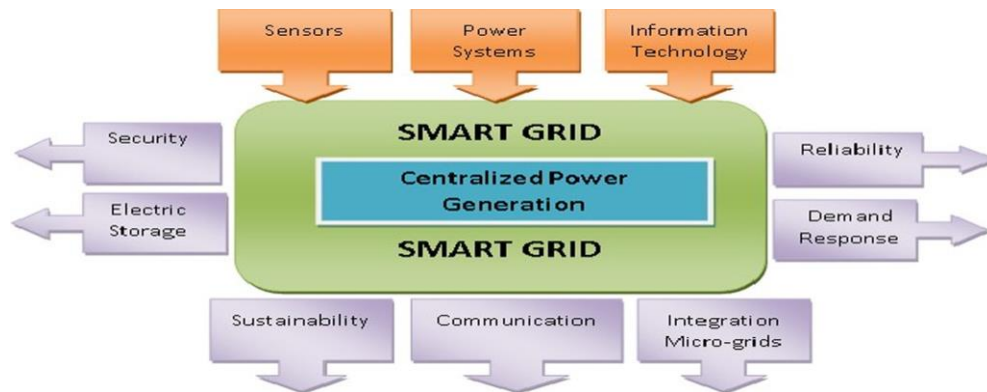


Figure 2.3: Modern Smart Grid

A modern Smart Grid System comprises following integral components

a. **Smart devices interface**

These are electronic devices that are part of the Internet of Things (IOT) and are frequently connected to other networks or gadgets using different wireless protocols. They are referred to as "smart devices" as they can function both independently and cooperatively. Smart control and monitoring devices are an essential part of real-time information operations. These materials must be distributed centrally and easily incorporated into DER operations. Among the popular categories of smart devices are smart cars, doorbells, refrigerators, bands, thermostats, locks, phablets, tablets, smart watches, smart key chains, smart phones, smart speakers, and other gadgets.

b. **Storage component**

Because of the fluctuations in renewable energy sources and the disparity between peak supply and peak demand, it is critical to find techniques to store energy for later use. The greater reliability and resilience of storage components benefits energy consumers as well as the utility system. Energy storage devices include pressurized air, flywheels, ultra capacitors, pumped-hydro, super-conducting magnetic energy storage, and flow batteries.

c. **Transmission subsystem component**

The transmission network, which links all of the major substations and load centers, is the backbone of the integrated energy system. The provision of efficiency and dependability at a reasonable cost is the ultimate objective of transmission planners and operators. Transmission lines have to be able to tolerate sudden and fluctuating loads without interfering with traffic flow. It is preferable to use specific criteria to ensure reliability, performance and quality of supply. Techniques for achieving transmission-level Smart Grid performance include the development of cutting-edge technologies and analytical tools. Performance uses robust state estimation, dynamic optimal performance

flow, reliability and market simulation tools, real-time stability evaluation, and other advanced technologies with intelligence.

d. Monitoring and control technology component

In addition to features for self-monitoring, self-healing, predictability and flexibility of generation, smart grids, and more, this component contains sufficient facilities for controlling congestion, instability, and reliability difficulties. This new flexible grid has to be robust, resilient to stress, and dependable enough to enable real-time modifications to its application. Smart energy-saving gadgets and intelligent distributed DERs both include built-in monitoring and control features. These self-sufficient, self-aware devices may operate according to their situational awareness.

e. Intelligent grid distribution subsystem component

The distribution network is the final stage in the process of delivering electrical electricity to customers. First and secondary distribution feeders are supplied to small industrial, industrial, and residential clients. Intelligent assistance programs at the distribution level may be able to identify automation through the use of voice communication linkages between users, smart meters, AMI, and power management components. Self-studying modules for automated billing, defect detection, feeder restoration and reconfiguration, voltage optimization and cargo transfer, and real-time pricing (RTP) will make up the automation function.

f. Demand side management component

The improvement of DSM and options for electricity performance pursuits to lessen working charges through delaying capability will increase and decreasing the want for pricey generators. DSM options lessen emissions and enhance manufacturing reliability. The payload curve is usual suffering from those choices. It is critical to create a unified protocol for patron distribution the usage of bidirectional data toll road technology. Demand-aspect meters, smooth air controls, plug-and-play, clever houses and homes and patron interfaces to growth electricity performance may be introduced.

A block diagram of components and their functions for Demand Side Management (DSM) is as under:

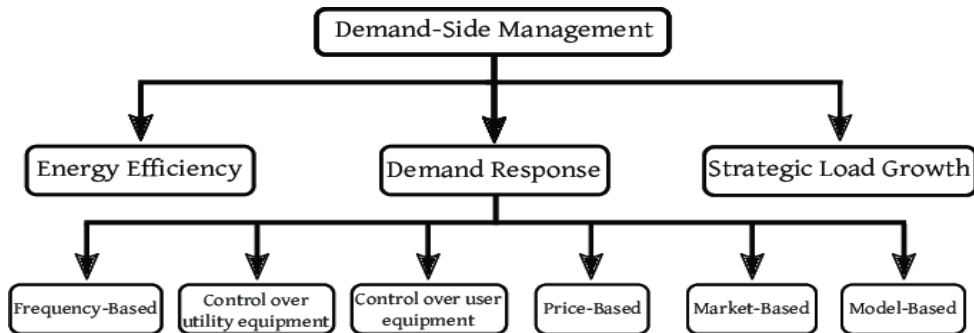


Figure 2.4: Block Diagram of Smart Grid DSM

2.3 Difference b/w Smart and Conventional Grid

Major differences between Conventional and Smart Grids are described in table below:

Smart Grid	Conventional Grids
Real-time two-way communication	One sided communication
Dispersed power generation system	Centralized to produce electricity
Network Interconnection	Wide Area Network
Numerous sensors are engaged.	A limited number of small sensors are applied
Digital Control and Monitoring via Automated Process	Mechanism of actions
Broad scope of authority	Manual management and observations
Wide range of control	Restricted authority
Numerous sensors are engaged	One physical security issues

Table 2.1: Difference between smart and conventional grid

2.4 Security Issues of Smart Grids

Smart Grid is a true Cyber Physical System where not only considerable amount of IoT devices are interfaced/ integrated or commonly known as a right example of a System of System Engineering (SoSE) concept but it's a blend of variety of engineering aspects. These include mechanical and renewable energy systems in Generation, Cables as well as SCADA in Transmission, Distribution such as conventional as well as AMIs, and other relevant components.

A preliminary overview of main systems of a Smart Grid, relevant attack points and types of threats is presented in Table 2.2 below:

S.No	Component	Attack Point	Type of Threat
1.	Generation System	Ethernet-based numerical relays (IEC 61850) for information sharing	DoS, Delay in transmission
		Control loops including speed & valve control and AVR linked with plant control via Ethernet	Trojan or backdoor entry enabling attacker compromise digital control modules by disrupting control logic
		Generation plants are tracked and managed by SCADA systems, which lack authentication and still	System stability may be directly impacted by intrusions into SCADA that alter frequency

		employ ladder logic and hardcoded passwords	measurements used by automated governor control (AGC)
		In power plants, MODBUS or DNP3 protocols are used for communication between RTUs and PLCs. The MODBUS protocol does not offer protection from unwanted access	Buffer Flooding Attack
2.	Transmission System	SCADA is heart applied to WANs, load dispatch centers are connected and transmission companies integrated internet in comm network for better efficiency & reliability	Attacker may manage to infiltrate any one of SCADA networks
		RTUs and PLCs	Cross-Site Request Forgery (CSRF) attacks
		The main way of bulk energy transmission for HVDC power lines. The current SCADA network at HVDC connections lacks authentication and access control, making its cyber security architecture inadequate	An attacker may alter the commutation angle by sending control signals, or they may even stop the flow of power, severely cutting off power to the targeted location
3.	Distribution System	Reversing the internal use counter in a conventional meter is a modification. Smart meters do not adhere to the Open Web Application Security Project (OWASP) guidelines.	<ul style="list-style-type: none"> - Negative pricing/ tariff - DoS
		WLANs that adhere to IEEE 802.11 standards, which by default do not include authentication procedures, include ZigBee, RF mesh, WiMax, WiFi, and PLC.	Session hijacking, eavesdropping, and traffic analysis
		Lack of authentication and encryption at Head End System (HES)	Tampering, masquerading of smart meters
		Net metering users can also fiddle with net energy usage data by hacking into communication network of AMI	Losses to distribution companies
4.	Telemetry	Standard communication protocols including Profibus/Profinet, DNP3, IEC 870-5-10x, and Modbus are used for power system telemetry. Regardless of the protocol type, the	Attacker gains access inside the “master” then the “slave devices” can then be forced to spuriously operate or even erase critical data

		majority of Industrial Control System (ICS) protocols operate on a "master/slave" paradigm with few or no security protections, making them vulnerable to malevolent network intrusions.	
5.	Physical	<ul style="list-style-type: none"> - Disgruntled Employees - Devices, laptops and USBs - Supply Chain Attacks 	<ul style="list-style-type: none"> - Altering algorithms - Stealing of corporate data - Portable devices mismanagement and compromising - Supply chain attacks

Table 2.2: Security issues of smart grid

2.5 Viability of Blockchain for Risk Assessment

In order to develop a stage for studying viability of Blockchain for risk assessment of Smart Grid Systems, some components or characteristics of Blockchain need to be studied. These include:

2.5.1 Node

A node is an object that connects to the blockchain network and performs various operations. Nodes are free to join or leave the network whenever they want. There are two primary nodes in the Bitcoin block chain [4]. Verifying the transactions and upholding the consensus among other full nodes are the major responsibilities of full nodes, which store a copy of the entire block chain on their storage. Initially, this category includes nodes that produce blocks. For the majority of users, keeping a complete copy of the block chain could be inconvenient. The BitCoin block chain, for instance, was 205 GB in size on April 1, 2019, after ten years of operation (Block chain Luxembourg). Daily transactions take place on light nodes, which can function on devices with little power, including mobile phones or laptops. Transactions are verified using Simple Payment Verification (SPV). They are dependent on full nodes because they do not own a complete copy of the block chain.

2.5.2 Ownership

According to Turner, there are three main types of ownership for block chains [5]. Who can use the network, operate as a node, confirm transactions, and conduct transactions will depend on ownership. Anyone who desires to join as a node may do so in a permission-less block chain, often known as a public block chain. Each node maintains a copy of the block chain in its storage, and they cooperate cooperatively to keep the block chain up to date. The block chain for bitcoin is an illustration of this paradigm. A private block chain with permissions, also called a permission block chain, has restricted access to a certain entity. A permission block chain is controlled by a certain group of individuals or organization, which runs counter to the block chain's core idea. Quorum, an Ethereum-based distributed ledger developed by J.P. Morgan (Morgan Chase, 2018), and Hyper ledger, developed by The Linux Foundation (2018),

are examples of permission block chains. A node needs to be verified by the block chain owner or by a set of rules put out by the block chain owner in order to participate. Block chains used in consortiums or that are semi-private also go by the name of hybrid. Connecting the private and public block chains is the key idea. Some of this block chain's components are private, while others are public. A private block chain is linked to the public block chain. The hybrid block chain used as an example is called XDC, developed by the Singaporean company XinFin (XinFin, 2018; XinFinOrganization, 2017). Block chains are designed to decentralize power and foster confidence between parties that are currently untrustworthy. The private blockchain will give one party total control and may cause trust issues.

2.5.3 Transaction

When a transaction is started, it is pooled in a block and validated by network nodes. Since each node contributes its address to the block candidate, there will be numerous variations of the block candidate, but only one block candidate may be added to the block chain at once. In this case, the block to be added is decided via a consensus mechanism. The node in the block that is chosen may or may not be paid, depending on the method. The cycle is then continually repeated. Data that has been added to the block chain cannot be removed. A transaction is started by someone and pooled in a block candidate before being verified by network nodes. Since every node adds its address to the block candidate, there will be many different versions of the block, but only one block candidate may be added to the block chain at once. Here, the addition of a block is decided using a consensus procedure. The node whose block is chosen may or may not receive compensation, depending on the process. After that, the cycle is continually repeated. Data cannot be erased once it has been added to the block chain. The network is made up of nodes, and each of them keeps a copy of the block chain. The network cannot be "persuaded" by changing a single copy of a block chain; instead, they would quickly reject the altered block chain. Someone must have the ability to simultaneously alter at least 50% plus one of the block chains that are stored across all nodes in order to successfully "fool" the network. In this way, the information stored in a block chain is neither "unchangeable" nor "immutable," but it is extremely difficult to change the information. So long as the network has more honest nodes working, it will be safe.

Table 2
Illustrations of a reverse transaction.

No.	Origin	Destination	Asset involved	Description
100	Alice	Cindy	1 token	Alice wanted to send Bob 1 token, but mistakenly send it to Cindy
101	Cindy	Alice	1 token	Transaction no. 100 cannot be deleted, instead, Cindy reverse (send back) the token back to Alice
102	Alice	Bob	1 token	Alice initiates the correct transaction

Table 2.3: Illustration of reverse transaction

CHAPTER 3

Literature Review

Risk Assessment is a mature function and technique generally used to establish the extent of vulnerabilities posed to a system by different threats and dangers. Risk assessments have always been conducted in all eras i.e both old as well as contemporary times and are usually followed by different mitigation strategies and related aspects. In this study, review for both Risk assessment of a typical Information Security system as well as that of a Smart Grid System has been carried out.

Section 3.1 contains review of IS Systems risk assessment and mitigation in general, whereas, it also describes risk assessment fundamentals and other related/ derived factors. In 3.2, various Cyber Security challenges to Smart Grids, their detection and mitigation techniques have been discussed. In 3.3, a critical review on anticipated cyber security threats in complex environment and efforts to address the grave concern has been presented. Section 3.4 tells us main differences between cyber security of a conventional and a smart grid and what are the factors and inherent risks which cannot be neglected while dealing with Smart Grids. Section 3.5 sheds light on prospects of using Blockchain to address Cyber Security issues of a typical smart grid system.

Literature review finally concludes in form of Deductions and Problem Statement.

3.1 Information Security Risk Assessment, Aggregation and Mitigation

In [1], The researchers describe a quantitative model for assessing and aggregating information security risks that they were developing at the time for implementation. The researchers show how to find the optimal risk mitigation strategy according to the model used and the available budget. The goal is to quantify a company's overall information security risk and find the most cost-effective way to contain the risk through threat and action plans.

Researchers have used ALE (Annual Loss Expectancy) to drive optimal risk mitigation. Losses in CIA Triad i.e Confidentiality, Integrity and Availability has been separately calculated along with threats against the process. Thus concluding that prototype model is sufficiently flexible that it allows fine-tuning and other more substantial refinements, if that is found to be desirable based on practical experience with the model. Basic formula used for calculation of likelihood indicator is

$$\text{Likelihood} = \text{Source} \times \text{Access} \times \text{Skill}$$

Which is further derived with residual risk indicator and also calculation of percentage how much 'better' the situation is after carrying out the action plan. The limitation of research is that at that point in time the prototype's implementation was not ready for deployment on a world-wide scale.

3.2 Cyber security Challenges, Detection & Mitigation Techniques for Smart Grid

In [2], Cyber detection and mitigation techniques are studied, after some famous cyber attacks such as Iran, Ukraine, and the United States are discussed. It has been found that there are two main techniques for detecting risk. The first are non-human-centric approaches that include machine learning-based, cloud-based, blockchain-based, and hardware-based attack detection and mitigation. Human-centric detection, training, awareness, access control and patching are under consideration. This study analyzed smart grid communication networks in detail and explored potential cyber attacks and mitigation techniques thoroughly. It is concluded that denial of service attack is a major problem for smart networks. As the smart grid is building a network, network attacks can disable the smart grid and seriously affect the public. To protect the smart grid from various cyber attacks, users should learn and mitigate the risks associated with smart grids by conducting various risk analyzes and case studies.

3.3 Cyber Security Threats - Smart Grid Infrastructure

Paper is Indicating Smart Grid as a true System of System Engineering which incorporates all mechanical, electrical, industrial electronics, electronics and cyber systems. The researchers [3], Critically evaluate anticipated cybersecurity threats in a complex environment and address issues related to secure cyber infrastructure and similar events. The study consulted with the NIST Reference Model of Smart Grids and focused on two factors: Vulnerability Testing and Assessment and Attack Points and Attack Countermeasures. For this detailed analysis, all the integral parts of Smart Grids i.e. generation, transmission, distribution, telemetry and other physical security aspects are evaluated.

It is recommended to improve privacy, integrity and system availability by building an efficient and secure smart grid cyber infrastructure. Attack detection, mitigation, authentication, and key management remain challenges. Countermeasures with weak security protocols must be designed, tested, and deployed. A secure protocol is recommended in the regulatory framework.

3.4 Differences of Risk Assessment between Smart and Traditional Power Grid

In [5], Researchers review the traditional power grid risk assessment development course, then analyze and compare the differences of risk assessment process between smart grid and traditional power grid. These include much system uncertainty due to renewable resources involvement; more surge between micro grid and the main power grid; and more customer joint into the risk assessment process as the work is set to be highly concerned issue about the utility and infrastructure energy security as well as national security.

Researchers have declared traditional grids as more rigid and robust systems. Whereas due to extensive use of re-newable enegegy resources as well as IOT devices both on fixed and wireless networks, vulnerability as well as efficiency of Smart Grid System becomes more delicate. At the same time, Smart Grids are expected to be more versatile, user interactive and much more efficient.

It has been determined that real-time risk assessment of smart grids and optimal risk control will be hotspot study topics in the next years due to the increased use of IoT and smart devices.

3.5 Evaluating Potential Security Risks of Advanced Metering Infrastructure (AMI) using EBIOS Risk Assessment Model

As per [5], A Cyber Physical System (CPS) is a system controlled through a data communication network. In Smart Grids, AMI is a CPS system which needs critical security steps and measures to ensure any chance of intruders. Aim of paper is to assess potential hazards that may be linked to AMI System by employing EBIOS approach. The researchers have carried out assessment of AMI through EBIOS Risk Assessment Method of National Cybersecurity Agency of France (ANSSI). AMI System has also been analyzed in NAN (Neighborhood Area Network) to counter DDOS.

A representation of main steps and phases of EBIOS with risk assessment method with all layers of a typical OSI model has also been done. AMI has been divided in hardware, data and communication layers. Study is done in five parts. This includes in first the assets of target system, second Target Objective, third how attacker proceeds and in fourth, risks assessment method and finally in fifth, is Risk Treatment Plan. Assessment is done as per Consequence x Likelihood scale. Researchers have also highlighted Block chain as a very viable solution for threats to AMI due to its full encryption feature.

Future work has been mentioned in exploring and implementing alternate risk assessment methods for AMI Systems. Results of same will be compared with this one.

3.6 Incorporation of Block chain (BC) Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenge

In [6], researchers tried to point researchers in the appropriate direction so they might create distributed, secure, blockchain-based SG applications in the future. The cybersecurity risks associated with smart grids are also outlined in this article, along with the potential use of BC to mitigate such threats. The study begins with an explanation of blockchain technology, and then moves on to discuss blockchain architecture, problems, and solutions for various smart grid applications.

Researchers has started by quoting very limited number of researches carried out so far for using BC in SG smart systems. Study has presented overview, terminologies and components and operations of Blockchain components. Application of BC in various components of Smart Grids i.e Home Automation, advanced metering infrastructure, electric vehicles, renewable microgrids, energy management systems have been deliberated. A separate and dedicated discussion has been carried out w.r.t CIA Triad and its associated threats such as DoS, FDIA, Phishing, Eavesdropping, breaches, malware, stuxnet, ransomware etc. Subsequently countermeasures and defences against these attacks have also been mentioned.

Study also provides overview of potential smart grid-related difficulties. Scalability limitations and security & privacy issues specially manipulation by actors that control more than

50% of the computers operating the blockchain is required to be addressed and needs to be studied/focussed in future.

3.7 Deductions

From literature review above, following has been deduced:

- (i) Risk Assessment is a mature technique which has successfully led to calculation of Inherent risks and working out their mitigation strategies.
- (ii) Since Smart Grids are technology of early 2000, risk assessments of Smart Grids systems have been done by some researchers, however, due to incorporation of large number of IoT devices, renewable energy systems, efficiency requirement and demand of interactive tools, these need constant review and updating.
- (iii) Due to incorporation of new generation gadgets, cyber security of Smart Grids needs to be studied again and again.
- (iv) Newer and contemporary non-humanly centric approaches which include Machine-Learning, cloud, block chain based and hardware based methods are not only preferable options but also becoming inevitable due to types of threats and their abilities such as mutation, smartness etc.
- (v) Block chain with its inherent design of decentralized nature can be studied for its viability for Cyber Security of Smart Grid Systems.

3.7.1 Problem Statement

High demand/ consumption and effective balancing of power systems necessitate use of smart components in Smart Grid Systems. Use of millions of smart devices over national grids will certainly pose severe threats and risks to security of these systems. Fool proof and uncompromising security for their smart grid management systems is required. Block chain Technology due to its inherent design seems to have a potential and needs to be ascertained for its viability w.r.t security of Smart Grid Systems

CHAPTER 4

Framework/ Methodology

Till now, thesis has covered, introduction and motivation of the study, a description about main components (key words) i.e Smart Grids, their security issues, need of risk assessment need and block chain as well as its architecture. A Literature Review of all these three aspects i.e Risk Assessment process as itself, Risk Assessment of Smart Grids and viability of Block Chains has been done.

For the framework, study has been conducted comprising 4 x phases which has been shown in Fig 4.1. Proposed framework gives systematic review of Smart Grid Systems where in Phase 1 Data/ Information Gathering by studying architecture of a Typical modern Smart Grid System and identifying vulnerable components. In Phase 2, Risk Analysis is done by Likelihood Vs Impact Formula. In Phase 3, i.e Mitigation, Viability of Blockchain for security of Smart Systems has been studied. And finally in Phase 4 Analysis and Outcome, finding have been analyzed w.r.t viability of different Blockchains i.e. ethereum and others for their usage for security of Smart Grids.

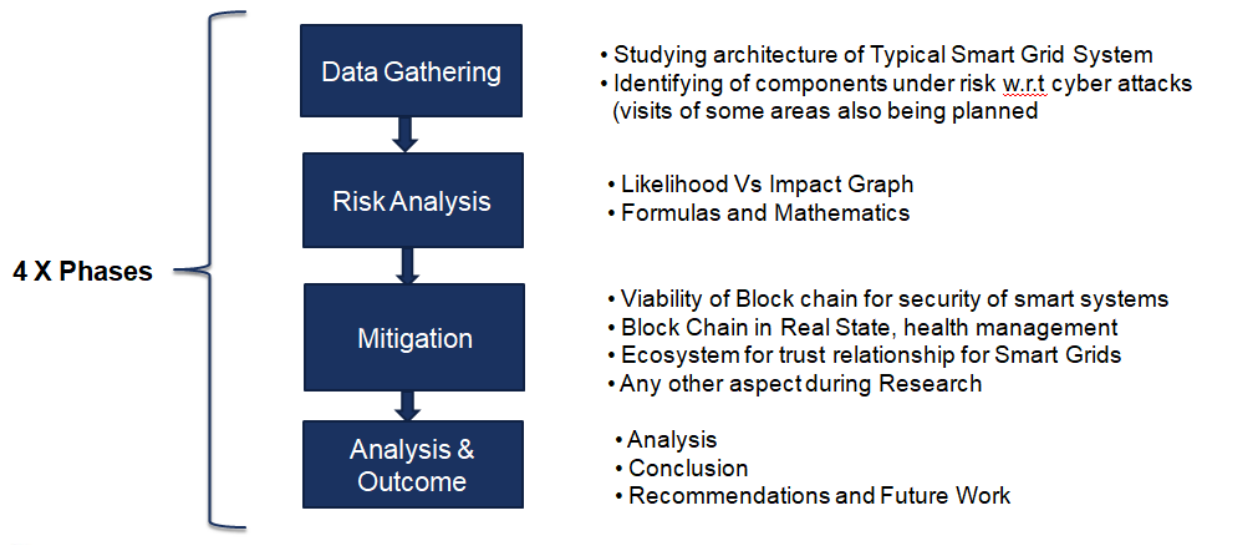


Fig 4.1: Framework being followed

4.1 Information Gathering

4.1.1 Architecture of Smart Grid (SG)

To address the concerns, Cyber security market is investing considerable resources as well as amount for Smart Grids. For example in 2020, only US government [7] exhibited huge growth climbing from global value of 7.8 to 79 billion USDs (approx 10 times increase).

Similarly other nations such as Canada, France and Japan has also invested considerable amount of money in the smart grid infrastructure.

SG systems should have a separate security zone from other networks such as external, other utility partners and Internet. In order to make grid intelligent and smarter, a number of smart devices are connected seamlessly which makes SG more vulnerable to attacks. As a successful attack can render the grid affected leaving entire city or region in outage, SG application have significant requirement of security.

Following prime cardinals [8] are considered for designing SG security architecture:

- a. Reduce the area (attack or threat vector) that may be attacked.
- b. Extend the amount of time needed to breach the network.
- c. Shorten the time needed to heal following a concession.

The Operational and information security set up of a typical Smart Grid System comprises of following six zones

- a. Enterprise Zone.
- b. Transmission Zone.
- c. Distribution SCADA Zone.
- d. Distribution Non SCADA Zone.
- e. Interconnect Zone.
- f. Demilitarized Zone (DMZ)

A conceptual diagram depicting all zones and their interconnectivity is shown below:

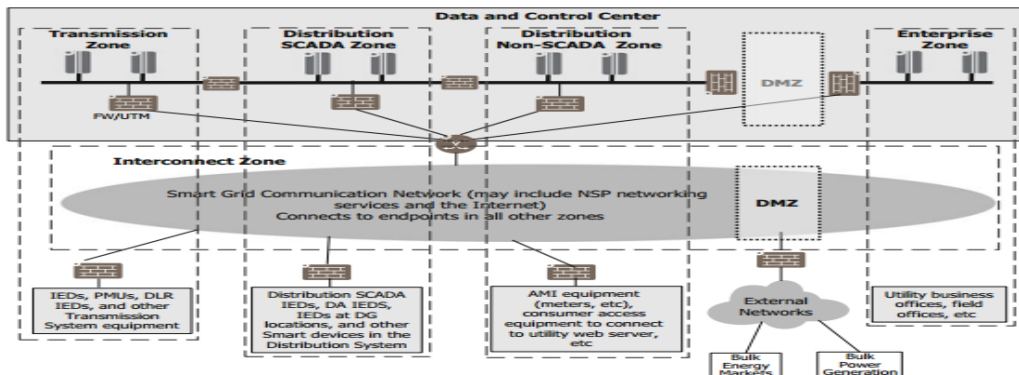


Figure 4.2: Conceptual diagram of smart grid system

Depending on how crucial the application data is to grid operations, different levels of protection are needed in each of these zones. The security standards typically apply across many physical networks and operational domains because they are based on the criticality of the applications

4.1.2 Identifying components with vulnerability to Cyber Attacks

Zone wise function and components concerned with threats identified for a Cyber Physical System (CPS) i.e a Smart Grid system controlled through a data communication network are explained below:

Enterprise Zone

The enterprise zone consists of business systems, users, and traffic that flows between these systems and users. These business systems include servers and clients that are used for duties such as internal product development, procurement, information technology, human resources, and billing. Corporate traffic is confined inside the Enterprise Zone, which is supported by an integrated Smart Grid network. Each business function should have its own security perimeter, with appropriate system and asset access restrictions in place. This security perimeter makes information transferred across a business network more open and accountable. Operational data access may be required for the business systems.

Transmission Zone

The DCC's TMS systems, IEDs deployed on transmission lines (such DLR IEDs), PMUs and other transmission substation components, and communication between all of these entities are all included in the Transmission Zone. Communication links between DCC systems and external systems, such as energy markets and large-scale power generation, are also included in the Transmission Zone. The security of communication between the utility's transmission parts must match that of the traffic passing via these external systems.

Distribution SCADA Zone

Distribution Zone SCADA Distribution automation (DA) feeder scheduling, SCADA IEDs at distribution substations, DMS systems at the DCC, and communication between these entities for DA and SCADA are all covered under the SCADA Zone. More connections might be made for more smart devices. IEDs at DG sites (microgrids and other consumer locations) are among these smart devices. For consumer appliances like air conditioners and electric water heaters to have direct load control, the Distribution SCADA Zone's communication must be improved. Similar to those in the Transmission Zone, entities in the Distribution Zone are connected to one another. NSP networks and the Internet can both be used to communicate SCADA zones.

Distribution Non-SCADA Zone

All distribution system communication features that are not required for grid control are included in the distribution non-SCADA Zone. As part of this exchange, customers may obtain information on how much electricity they use via the AMI system. As a result, AMI hardware including meters, data concentrators, head ends, and the MDMS are found in the Distribution Non-SCADA Zone. Customers of utilities may be able to access the internet for personal energy management. This kind of internet access is often done via the Distribution Non-SCADA Zone. User privacy is just as important as network security when it comes to not revealing personal information obtained from energy usage statistics, such if a client is at home.

Interconnect Zone

The networks that link entities from different zones are included in the Interconnect Zone. These networks consist of the Smart Grid network, any separate commercial networks, and connections to other institutions. The interconnecting communication network must have the required security methods to separate critical from noncritical data as Smart Grid communication spreads to a significant number of devices located outside of substations and at consumer sites. The mobile workforce's communications, which need to be connected to every other zone, are likewise housed in the Interconnect Zone. To carry traffic for several security zones, a large number of network lines, network components, and even a local area network (like the DCC) will be required. It should be mentioned that the boundaries of each zone are appropriate and do not cross over. Every link that transmits data between objects in different zones goes via the Smart Grid network, the external networks that are visible, and the security equipment needed for zone division. For completeness, whether the business network is integrated with the Smart Grid network or it is a distinct network all by itself, the separation (for security) of utility operations and business data traffic is shown.

4.1.1 Identification of components vulnerable to Cyber threats

Vulnerabilities in information and communication systems cannot be avoided, regardless of security structures and protocols in place. These vulnerabilities are frequently unnamed (also referred to as "zero-day"), which means that hostile agents may have discovered them before vendors or utilities did, and they are currently being employed in zero-day attacks. Vulnerabilities are frequently well-known yet remain unfixed. For example, operational concerns (cost, risk of failure, downtime, etc.) may render repairs unavailable or unavailable at this time. Hardened system, application, and service settings, as well as secure software and hardware development and acquisition, may help to reduce hazards. This requires turning off any unnecessary components, ports, or services. It may also include establishing any optional security measures (such as encryption and logging), as well as limited access limits. Assets should be regularly scanned for vulnerabilities utilizing technology such as Nessus. Vulnerability scanning should be performed during a maintenance window since it has the potential to crash functioning systems. Log analysis and the previously described security monitors may be used to passively identify OS versions, patch levels, and system hardening. Functionality- or protocol-specific tools (such as SCADA) can be utilized as needed. Once issued, a software patch may frequently address a security vulnerability. However, patching live systems may be hazardous

and difficult. A thorough inventory of the systems that require patching, together with up-to-date versioning information, is essential. Prior to being made available, patches must be evaluated. Installing patches needs to be done swiftly, consistently, and with the least amount of downtime possible—ideally none at all. It's crucial that it can undo a fix and get a system back to how it was when a problem occurred. This administrative work may be made simpler with the use of a patch management system.

A synopsis of vulnerable components in different zones their attack points and perceived threats are tabulated below:

<u>Zone</u>	<u>Function</u>	<u>Devices/ Attack Points</u>	<u>Perceived Threat</u>
Enterprise Zone	Users, business systems, traffic between these systems, and traffic between users and the systems themselves	- Utility business offices - Field offices	- Information Theft (Loss of Confidentiality)
Transmission Zone	Comprises of Transmission Sub-elements.	- Intelligent Electronic Devices (IEDs). - Phasor Measurement Units (PMUs) - Transmission Management System (TMS)	Infrastructure compromise
Distribution SCADA Zone	Uses Supervising Control and Data Acquisition (SCADA) and IEDs for distribution	- SCADA IEDs - Distribution Automation (DA) IEDS - Unified Threat Management (UTM) - Other Smart Devices	SCADA and DA compromise
Distribution Non SCADA Zone	Communication features that are not essential for grid control	- Advanced Metering Infrastructure (AMI) - Web access for personal energy management.	AMI needs to be analyzed based on Attack Vectors of Device, Network and Insider
Interconnect Zone	Connects to end points in other zones	Network Service Provider (NSP) and Internet	Network-based attacks, data interception
Demilitarized Zone (DMZ)	External facing services, like web servers, are present in or exposed to untrusted networks via physical or logical networks	Organization's LAN	Exposure of external-facing services

Table 3.1: A synopsis of vulnerable components in different zones

4.2 Risk Analysis

The perceived threats to each zone were categorized, and a risk analysis was conducted to assess the potential impact and likelihood of occurrence.

4.2.1 Calculations for Risk Assessment

Risk assessment calculations were performed using a quantitative model [1].

Formula: Likelihood = Source x Access x Skill

- Source (S): Likelihood of a threat source exploiting a vulnerability.
- Access (A): Likelihood of the threat source gaining access.
- Skill (Sk): Likelihood of the threat source having the skill to exploit the vulnerability

	STATUS OF EVENT		RISK CLASS				
	LIKELIHOOD OF EVENT HAPPENING	5	It is or has already happened	M	H	H	VH
4		It will probably happen	M	M	H	VH	VH
3		It could possibly Happen	L	M	M	H	H
2		It is to Happen	L	L	M	M	H
1		It is unlikely to Happen	L	L	L	M	M
LIKELY OUTCOME OF EVENT	SAFETY		Near Miss	Minor Inquiry	Lost Time Accident	Major Inquiry	Fatality
	ENVIREONMENT		Potential Event	Minor Event	Important Event	Significant Event	Major Event
	COST		< 1k \$	< 10k \$	< 100k \$	< 300k \$	> 500k \$
	SEVERITY		1	2	3	4	5

Fig 4.3 Likelihood x Impact Table

4.2.2 Risk Assessment of Individual Smart Grid System Zones wise

In order to conduct a comprehensive Risk Assessment of Smart Grid Systems all zones are individually required to be assessed through the Likelihood x Impact Table by calculating a probabilistic assessment of Cyber Vulnerabilities. In this, all components will be individually assessed in both domains i.e Likelihood as well as Impact (consequences) on a scale from 1-5 w.r.t Cyber threat / vulnerabilities for final calculation of severity (on a scale upto 10).

- (i) **Enterprise Zone:** The primary components of this zone are business systems, users, and the traffic that moves back and forth between these systems and users. Utility company offices and field offices are considered attack points, while information theft (loss of confidentiality) is seen as a potential danger.

For Severity = Likelihood x Impact calculation

$$= 2 \times 2 = 4 \text{ (Medium)}$$

- (ii) **Transmission Zone:** It comprises Transmission Sub-elements where likely attack points are Intelligent Electronic Devices (IEDs), Phasor Measurement Units (PMUs), Transmission Management System (TMS). Perceived threats are Infrastructure compromise.

For Severity = Likelihood x Impact calculation

$$= 3 \times 3 = 9 \text{ (High)}$$

- (iii) **Distribution SCADA Zone:** This zone comprises Supervising Control and Data Acquisition (SCADA) and IEDs for distribution. Attack points are SCADA IEDs, Distribution Automation (DA) IEDS, Unified Threat Management (UTM) and Other Smart Devices. Perceived threats are SCADA and DA compromise.

For Severity = Likelihood x Impact calculation

$$= 3 \times 3 = 9 \text{ (High)}$$

- (iv) **Distribution Non- SCADA Zone:** This zone comprises Communication features that are not essential for grid control. Envisaged attack points are Advanced Metering Infrastructure (AMI) and Web access for personal energy management, whereas perceived threats are Unauthorized access, data privacy concerns.

For Severity = Likelihood x Impact calculation

$$= 3 \times 2 = 6 \text{ (Medium/ Moderate)}$$

- (v) **Interconnect Zone:** This zone Connects to end points in other zones and likely attack points are Network Service Provider and Internet. Perceived threats are Network-based attacks and data interception (loss of confidentiality)

For Severity = Likelihood x Impact calculation = $3 \times 3 = 9$ (High)

- (vi) **DMZ:** Consists of a logical or physical network Web servers and other outward facing services are present in the DMZ and are accessible to untrusted networks. Organizations' local area networks (LANs) are considered attack sites, whereas externally exposed services are seen as perceived threats.

For Severity = Likelihood x Impact calculation

$$= 3 \times 3 = 9 \text{ (High)}$$

4.2.3 Risk Assessment Summary

In view of Risk Analysis above, Risk Assessment summary with an initial Mitigation Strategy is described below:

Zone	Perceived Threats	Risk Level (High/Medium/Low)	Mitigation Strategy
Enterprise Zone	Information theft	Medium	Encryption, access controls, user awareness training
Transmission Zone	Infrastructure compromise	High	Network segmentation, intrusion detection systems
Distribution SCADA Zone	SCADA and DA compromise	High	Regular security audits, anomaly detection algorithms
Distribution Non SCADA Zone	Unauthorized access, data privacy concerns	Medium	Strong access controls, encryption, regular audits
Interconnect Zone	Network-based attacks, data interception	High	Encryption, secure communication protocols
Demilitarized Zone (DMZ)	Exposure of external-facing services	High	Firewalls, intrusion prevention systems, regular audits

Table 4.2: Risk Analysis Summary

4.3 Mitigation through Blockchain Technology

The potential of blockchain technology as a mitigation strategy was explored, considering its features such as decentralization and full encryption.

Blockchain Mitigation Strategies

Smart Grid Component	Blockchain Application	Benefits
Home Automation	Blockchain-based access control	Decentralized and secure access management
Advanced Metering Infrastructure	Blockchain for secure data transmission and storage	Protection against data tampering and unauthorized access
Electric Vehicles	Decentralized charging transactions through blockchain	Transparent and secure transactions for EV charging
Renewable Microgrids	Blockchain-based energy trading	Secure and verifiable transactions in microgrid environments
Energy Management Systems	Blockchain for demand-response mechanisms	Decentralized and secure control over energy management

Table 4.3: Blockchain mitigation strategies

4.4 Evaluation of Blockchain Technology

It was evaluated that how well blockchain technology works systematically as a mitigation strategy for securing various components of the Smart Grid. Each Smart Grid component was evaluated for its susceptibility to cyber threats and the potential benefits of implementing blockchain-based solutions.

Blockchain Technology Evaluation

Smart Grid Component	Blockchain Application	Challenges
Home Automation	Leveraging blockchain for secure access control mechanisms	Scalability concerns surfaced, particularly with a surge in smart device deployments
Advanced Metering Infrastructure	Integration of blockchain to ensure secure data transmission and storage	Challenges emerged in seamlessly integrating blockchain with existing AMI systems
Electric Vehicles	Implementation of decentralized blockchain for transparent charging transactions	Limited adoption due to interoperability issues in the Electric Vehicle infrastructure
Renewable	Exploring blockchain for secure energy	Regulatory complexities and

Smart Grid Component	Blockchain Application	Challenges
Microgrids	trading	standardization issues acted as impediments
Energy Management Systems	Employing blockchain for enhancing demand-response mechanisms	Integration complexities with existing energy management systems

Table 4.4: Blockchain Technology Evaluation

4.5 Comparative Analysis of Blockchain Platforms

A rigorous comparative analysis was conducted to evaluate various blockchain platforms concerning their suitability for Smart Grid applications. The strengths and limitations of each platform were scrutinized to provide a comprehensive understanding.

Comparative Analysis of Blockchain Platforms

Blockchain Platform	Strengths	Limitations
Ethereum	Well-established with an extensive developer community	Challenges in scalability under high transaction volumes
Hyperledger Fabric	Recognition for being a permissioned blockchain with robust privacy features	A steeper learning curve for development teams
Corda	Notable for its design focused on financial applications with strong privacy focus	Limited adoption outside financial sectors
Binance Smart Chain	Recognized for fast transaction speeds and low transaction fees	Concerns about centralized control and governance

Table 4.5: Comparative Analysis of Blockchain Platforms

4.6 Ability of Blockchain to achieve Security objectives

[12] has presented detailed account of security objective which can be obtained through Blockchain

<u>Desired Objective</u>	<u>How Blockchain achieves</u>
Confidentiality	In public BC, records are not encrypted, so cryptography is

	required.
Integrity	Hash Function, Merkle tree, Nonce, Time stamps. Manipulated records can be detected. Decentralized access can be prevented.
Authentication	For verification by valid users, signed records inside blocks.
Auditability	In Public BC, publicly made records are available.
Authorization and access control	Through smart contracts and attribute certificates
Privacy	Hash functions used for secret identities. Zero Knowledge and Pseudo-anonymization.
Trust	Consensus algorithms. Also trust is not centralized but distributed among entities
Transparency	By maintaining immutable ledger
Availability	Distributed architecture and copies of BC available
Automaticity	Entities may communicate and exchange values thru Smart Contracts.

Table 4.6: Ability of Blockchain to achieve Security objectives

CHAPTER 5

Analysis

5.1 Analysis of Literature Review

This detailed analysis of the literature aims to provide a comprehensive understanding of the various facets of Smart Grid cyber security. By dissecting each section of the literature review, we delve into the nuances of information security risk assessment, cyber security challenges in Smart Grids, anticipated threats, differential risk assessment, AMI security risks, and the role of block chain technology.

5.1.1 Information Security Risk Assessment in Traditional and Smart Grids

The quantitative model proposed in [1] introduces a systematic approach to assessing and aggregating information security risks. The reliance on the Annual Loss Expectancy (ALE) metric demonstrates a quantitative perspective that aligns with industry standards. The inclusion of the CIA triad (Confidentiality, Integrity, and Availability) in risk calculations reflects a holistic view of security. The analysis reveals that the prototype's flexibility allows for fine-tuning and refinement based on practical experiences. However, the limitation of non-deployment on a global scale at the time raises questions about real-world applicability.

5.1.2 Cyber security Challenges and Mitigation Techniques in Smart Grids

The exploration of cyber security challenges in Smart Grids [2] unveils the multi-layered nature of threats. The categorization into passive and active cyber attacks sets the stage for a nuanced understanding of potential risks. The detailed analysis of communication architecture and evaluation of risks on the CIA triad provide a robust framework for assessing vulnerabilities. The identification of denial-of-service attacks as a major threat underscores the potential cascading effects on Smart Grid functionality. The emphasis on user education, risk analysis, and case studies positions human-centric approaches as integral elements in a comprehensive cyber security strategy.

5.1.3 Anticipated Cyber security Threats in Smart Grid Infrastructure

The portrayal of Smart Grids as Systems of Systems in [3] establishes a holistic perspective. The alignment with the NIST reference model allows for a systematic evaluation of risk inspection, attenuation, probable attack points, and adversary actions. The critical analysis of integral components such as generation, transmission, distribution, telemetry, and physical security highlights the interconnectedness of potential threats. The call for enhancing confidentiality, integrity, and availability emphasizes the ongoing challenges in attack detection, mitigation, and key management. The recommendation for secure protocols through regulatory frameworks aligns with industry-wide efforts to standardize security measures.

5.1.4 Differential Risk Assessment between Smart and Traditional Power Grids

The review of risk assessment in [5] draws a clear distinction between traditional and Smart Grids. The acknowledgment of traditional grids as more rigid and robust underscores the contrast with the dynamic and versatile nature of Smart Grids. The incorporation of renewable energy resources and IoT devices introduces vulnerabilities that require real-time risk assessment. The identification of real-time risk control as a hotspot research area recognizes the evolving landscape of energy systems. The analysis positions Smart Grids as a balancing act between efficiency and vulnerability, prompting continuous research and adaptation.

5.1.5 Security Risks of Advanced Metering Infrastructure (AMI) and Blockchain Implementation

The in-depth assessment of potential security risks associated with AMI using the EBIOS Risk Assessment Model [5] provides a granular understanding of the layers involved. The segmentation into hardware, data, and communication layers sets the stage for targeted risk analysis. The representation of EBIOS steps and phases, coupled with the focus on AMI in the Neighborhood Area Network (NAN), reveals the multifaceted nature of potential threats. The acknowledgment of block chain as a viable solution for AMI security, especially due to its encryption features, introduces a proactive approach to risk mitigation. The call for exploring alternate risk assessment methods underscores the need for comprehensive strategies tailored to specific Smart Grid components.

5.1.6 Block chain Technology for Smart Grid Applications

The exploration of block chain technology for Smart Grid applications [6] offers a comprehensive analysis of its components, operations, challenges, and applications. The delineation of potential threats to the CIA triad, including DoS, FDIA, Phishing, Eavesdropping, and malware, provides a robust framework for understanding security concerns. The acknowledgment of scalability limitations and privacy issues demonstrates a balanced perspective on the challenges associated with block chain implementation. The focus on potential difficulties, especially manipulation by actors controlling over 50% of block chain computers, introduces a realistic outlook on the technology's limitations. The integration of blockchain into various Smart Grid components underscores its versatility as a potential cyber security tool.

5.1.7 Deductions from the Literature Review

The deductions drawn from the literature review encapsulate key insights into the maturity of risk assessment techniques and the dynamic nature of Smart Grid cybersecurity. The recognition of the constant need for review and updating in the face of new-generation gadgets emphasizes the adaptive nature of security measures. The identified non-human-centric approaches, including machine learning, cloud-based solutions, blockchain, and hardware-based methods, emerge as not only preferable options but as inevitable choices given the evolving threat landscape. The recognition of blockchain's decentralized nature as a potential solution for Smart Grid cybersecurity introduces a proactive stance towards future challenges.

5.2 Risk Analysis Process

The risk analysis process, as outlined in the literature, is a pivotal step in developing a robust cybersecurity strategy for Smart Grids. The literature emphasizes the importance of a systematic approach, considering various factors such as the attack surface, the amount of time needed to breach the network, and the recovery time after a compromise [9]. The identification of vulnerabilities in different security zones, as discussed in Chapter 4, lays the groundwork for a comprehensive risk analysis. Each zone, from the enterprise to interconnect, requires a tailored risk assessment approach due to the differing criticality of applications.

The risk analysis process involves:

- **Identification of Assets and Threats:** The first step is to identify the assets within each security zone and assess their vulnerabilities to potential cyber threats. This includes a thorough examination of hardware, software, communication channels, and the human element.
- **Quantification of Risks:** The risks associated with each identified threat are quantified using a risk assessment model. The analysis considers factors such as the likelihood of an attack, potential impact, and the effectiveness of existing security measures.
- **Prioritization of Risks:** Risks are prioritized based on their potential impact on Smart Grid operations. Critical assets and functions that, if compromised, could lead to severe consequences, are given top priority.
- **Gap Analysis:** A gap analysis is conducted to identify areas where the existing security measures may fall short in mitigating the identified risks. This involves assessing the effectiveness of current security protocols and identifying areas for improvement.
- **Recommendations:** Based on the findings of the risk analysis, recommendations are formulated to enhance the overall cybersecurity posture of the Smart Grid. These recommendations may include technological solutions, policy changes, and training programs.

5.3 Mitigation through Blockchain Technology

The literature suggests that blockchain technology holds promise in addressing cybersecurity challenges in Smart Grids. Blockchain's decentralized and tamper-resistant nature makes it a potential solution for securing critical infrastructure. The analysis includes a detailed examination of blockchain's application in various components of Smart Grids, such as home automation, advanced metering infrastructure, electric vehicles, renewable microgrids, and energy management systems.

Key insights from the analysis include:

- **Overview of Blockchain Technology:** A comprehensive overview of blockchain technology, including its terminologies, components, and operations, is provided. This

sets the stage for understanding how blockchain can be applied to enhance Smart Grid cybersecurity.

- **Application to Smart Grid Components:** The literature explores how blockchain can be applied to different components of the Smart Grid. This includes securing communication channels, ensuring data integrity, and mitigating risks associated with specific threats like DoS attacks, phishing, and malware.
- **Challenges and Solutions:** The analysis does not shy away from addressing the challenges associated with blockchain implementation. Scalability limitations and privacy concerns are acknowledged, emphasizing the need for ongoing research and development in these areas.
- **Smart Grid-Related Difficulties:** The analysis recognizes potential difficulties in applying blockchain to Smart Grids, especially concerning the manipulation of blockchain computers by malicious actors. This realistic perspective underscores the importance of addressing not only the technology's strengths but also its limitations.

5.4 Cross-Zonal Analysis

Expanding on the zone-wise analysis, a cross-zonal examination is imperative for a holistic understanding of Smart Grid cybersecurity. Cross-zonal analysis involves evaluating the interdependencies and potential vulnerabilities arising from the interactions between different security zones. For instance, the Enterprise Zone's communication with the Distribution SCADA Zone or the Interconnect Zone linking various entities necessitates a comprehensive assessment.

Key elements of the cross-zonal analysis include:

- **Communication Flows:** Understanding the communication flows between different zones is crucial. This involves mapping how data is transmitted across zones, identifying potential points of exposure, and assessing the security measures in place for data in transit.
- **Data Integrity Across Zones:** Ensuring the integrity of data as it traverses different security zones is a critical consideration. The analysis explores mechanisms to maintain data integrity and prevent tampering, especially in zones where real-time decision-making is integral.
- **Interconnectivity Risks:** The interconnectivity zone, acting as a bridge between various zones, presents specific risks. These risks may include unauthorized access points, potential data breaches, and the transmission of malicious entities between zones.

5.5 Blockchain Integration Challenges and Opportunities

The analysis extends to the challenges and opportunities associated with integrating blockchain into existing Smart Grid frameworks. While blockchain offers a decentralized and secure foundation, the process of integration poses specific challenges that require careful consideration.

Key aspects of this analysis include:

- **Integration with Legacy Systems:** Assessing the compatibility and integration challenges of blockchain with legacy systems is crucial. The analysis explores strategies for seamless integration without disrupting ongoing Smart Grid operations.
- **Regulatory Frameworks:** The role of regulatory frameworks in facilitating or hindering blockchain integration is examined. Understanding how existing regulations align with the decentralized nature of blockchain is essential for effective implementation.
- **Cost-Benefit Analysis:** A thorough cost-benefit analysis must be carried out in order to determine whether blockchain integration is feasible. This involves taking into account the long-term viability of blockchain solutions as well as implementation costs and possible savings

5.6 Cybersecurity Training and Awareness Programs

Recognizing the human element as a significant factor in cybersecurity, the analysis delves into the importance of training and awareness programs. Understanding that employees at various levels interact with Smart Grid systems, the analysis explores:

- **Targeted Training Modules:** Tailoring training modules to address specific roles and responsibilities within the Smart Grid ecosystem. This ensures that personnel are equipped to handle cybersecurity challenges relevant to their functions.
- **Simulation Exercises:** Incorporating simulation exercises to simulate real-world cyber threats and responses. This hands-on approach enhances the practical skills of cybersecurity personnel and promotes a proactive cybersecurity culture.
- **Continuous Training:** Emphasizing the need for continuous training programs to stay abreast of evolving cyber threats. The analysis underscores that cybersecurity is a dynamic field, requiring ongoing education and skill development.

5.7 Stakeholder Collaboration and Information Sharing

Collaboration among stakeholders and effective information sharing mechanisms are vital components of a robust cybersecurity strategy. The analysis explores:

- **Public-Private Partnerships:** Evaluating the potential for public-private partnerships to enhance Smart Grid cybersecurity. This involves understanding how collaboration between government entities, private utilities, and cybersecurity firms can strengthen the collective defense against cyber threats.
- **Information Sharing Platforms:** Assessing the feasibility of platforms for sharing cybersecurity threat intelligence among Smart Grid stakeholders. Establishing effective channels for timely information sharing enhances the collective ability to respond to emerging threats.

- **Regulatory Support:** Recognizing the role of regulatory bodies in fostering collaboration and information sharing. The analysis considers how regulatory frameworks can incentivize cooperation and set standards for cybersecurity practices.

5.8 Simulation and Testing Protocols

A crucial aspect of the analysis involves simulation and testing protocols to evaluate the efficacy of cybersecurity measures. This includes:

- **Penetration Testing:** Conducting simulated cyber-attacks to identify vulnerabilities and weaknesses in the Smart Grid infrastructure. The analysis explores how penetration testing can be tailored to different security zones, considering their unique characteristics.
- **Scenario-Based Simulations:** Creating scenario-based simulations to assess the response capabilities of Smart Grid personnel. This involves simulating cyber incidents and evaluating the effectiveness of response protocols.
- **Post-Incident Analysis:** Establishing protocols for post-incident analysis to learn from simulated cyber incidents. This iterative process enhances the adaptive capacity of Smart Grid cybersecurity measures.

5.9 Continuous Monitoring and Adaptation

The analysis underscores the importance of continuous monitoring and adaptation as fundamental principles of effective cybersecurity. This involves:

- **Real-time Monitoring:** Implementing real-time monitoring mechanisms to detect anomalies and potential threats as they emerge. The analysis explores the integration of artificial intelligence and machine learning for dynamic threat detection.
- **Adaptive Security Measures:** Designing security measures that can adapt to evolving cyber threats. This includes the ability to update protocols, patch vulnerabilities, and deploy new security technologies in response to emerging risks.
- **Incident Response Protocols:** Formulating robust incident response protocols to ensure a swift and coordinated response to cyber incidents. The analysis considers the establishment of clear communication channels and escalation procedures.

5.10 Integration with National Cybersecurity Frameworks

Ensuring alignment with national cybersecurity frameworks is a crucial aspect of the analysis. This involves:

- **Regulatory Compliance:** Assessing the regulatory landscape and ensuring that Smart Grid cybersecurity measures comply with national cybersecurity regulations. The analysis explores the potential implications of non-compliance and strategies for alignment.
- **Coordination with National Agencies:** Collaborating with national cybersecurity agencies to align Smart Grid cybersecurity strategies with broader national security

objectives. This coordination enhances the collective resilience against cyber threats at a national level.

5.11 Environmental and Social Impacts

An inclusive analysis considers the broader impacts of cybersecurity measures on the environment and society. This involves:

- **Energy Efficiency:** Evaluating the energy efficiency implications of cybersecurity measures. The analysis explores how energy-intensive security protocols may impact the overall sustainability of Smart Grid operations.
- **Social Equity:** Considering the social equity dimensions of cybersecurity. This involves examining how cybersecurity measures may disproportionately impact certain communities and ensuring that security measures promote inclusivity.
- **Privacy Considerations:** Incorporating privacy considerations into cybersecurity strategies. The analysis explores how data protection measures can be integrated to uphold individual privacy rights.

5.12 Evaluation of Security Architecture

A number of parameters, such as reducing the attack surface, lengthening the time it takes to compromise the network, and accelerating the recovery process following a breach, were taken into consideration while evaluating the security architecture's efficacy.

Evaluation of Security Architecture

Criteria	Assessment
Minimizing Attack Surface	The architecture successfully establishes security perimeters, minimizing unauthorized access.
Increasing Time to Compromise	The design effectively increases the time required for a potential compromise, providing a layered defense.
Decreasing Time to Recover	The architecture facilitates a swift recovery process, minimizing downtime and reducing the impact of compromises.

Table 5.1: Evaluation of Security Architecture

5.13 Identification of Vulnerable Components

The analysis involved a thorough examination of components within each zone to identify vulnerabilities and potential attack points.

Vulnerable Components by Zone

Zone	Vulnerable Components	Identified Threats
Enterprise Zone	Utility business offices, field offices	Information theft (Loss of Confidentiality)
Transmission Zone	IEDs, PMUs, Transmission Management System (TMS)	Compromise of Transmission Infrastructure
Distribution SCADA Zone	SCADA IEDs, DA IEDs, Unified Threat Management (UTM)	SCADA and DA system compromise
Distribution Non SCADA Zone	Advanced Metering Infrastructure (AMI)	Unauthorized access, data privacy concerns
Interconnect Zone	Network Service Provider, Internet	Network-based attacks, data interception
Demilitarized Zone (DMZ)	Organization's LAN	Exposure of external-facing services

Table 5.2: Vulnerable Components by Zone

5.14 Perceived Threats and Risk Analysis

The perceived threats to each zone were categorized, and a risk analysis was conducted to assess the potential impact and likelihood of occurrence.

Risk Analysis Summary

Zone	Perceived Threats	Risk Level (High/Medium/Low)	Mitigation Strategy
Enterprise Zone	Information theft	Medium	Encryption, access controls, user awareness training
Transmission Zone	Infrastructure compromise	High	Network segmentation, intrusion detection systems
Distribution SCADA Zone	SCADA and DA compromise	High	Regular security audits, anomaly detection algorithms
Distribution Non SCADA Zone	Unauthorized access, data privacy concerns	Medium	Strong access controls, encryption, regular audits

Zone	Perceived Threats	Risk Level (High/Medium/Low)	Mitigation Strategy
Interconnect Zone	Network-based attacks, data interception	High	Encryption, secure communication protocols
Demilitarized Zone (DMZ)	Exposure of external-facing services	High	Firewalls, intrusion prevention systems, regular audits

Table 5.3: Risk Analysis Summary

5.15 Mitigation Strategies through Blockchain Technology

The potential of blockchain technology as a mitigation strategy was explored, considering its features such as decentralization and full encryption.

Blockchain Mitigation Strategies

Smart Grid Component	Blockchain Application	Benefits
Home Automation	Blockchain-based access control	Decentralized and secure access management
Advanced Metering Infrastructure	Blockchain for secure data transmission and storage	Protection against data tampering and unauthorized access
Electric Vehicles	Decentralized charging transactions through blockchain	Transparent and secure transactions for EV charging
Renewable Microgrids	Blockchain-based energy trading	Secure and verifiable transactions in microgrid environments
Energy Management Systems	Blockchain for demand-response mechanisms	Decentralized and secure control over energy management

Table 5.4: Blockchain Mitigation Strategies

5.16 Comparative Analysis of Risk Assessment Methods

A comparative analysis was performed to evaluate different risk assessment methods, focusing on scalability, comprehensiveness, and applicability to Smart Grid cybersecurity.

Comparative Analysis of Risk Assessment Methods

Risk Assessment Method	Strengths	Limitations
EBIOS Risk Assessment Model	Comprehensive analysis of AMI systems	Limited scalability for large-scale grids
Quantitative Model (Reference [1])	Quantitative assessment of Information Security risks	Prototype implementation not ready for worldwide deployment

Table 5.5: Comparative Analysis of Risk Assessment Methods

5.17 Calculations for Risk Assessment

Risk assessment calculations were performed using a quantitative model [1].

Formula: Likelihood = Source x Access x Skill

- Source (S): Likelihood of a threat source exploiting vulnerability.
- Access (A): Likelihood of the threat source gaining access.
- Skill (Sk): Likelihood of the threat source having the skill to exploit the vulnerability.

Example Calculation:

- S = 0.7 (moderate likelihood)
- A = 0.8 (high likelihood)
- Sk = 0.9 (high skill)

Likelihood = 0.7 x 0.8 x 0.9 = 0.504

The results were discussed in the context of future research directions, including advanced threat modeling, quantum-safe cryptography, human-centric cybersecurity solutions, and the integration of 5G technology.

5.18 Evaluation of Blockchain Technology

The effectiveness of blockchain technology as a mitigation strategy for securing various components of the Smart Grid was systematically assessed. Each Smart Grid component was evaluated for its susceptibility to cyber threats and the potential benefits of implementing blockchain-based solutions.

Blockchain Technology Evaluation

Smart Grid Component	Blockchain Application	Challenges
Home Automation	Leveraging blockchain for secure access control mechanisms	Scalability concerns surfaced, particularly with a surge in smart device deployments
Advanced Metering Infrastructure	Integration of blockchain to ensure secure data transmission and storage	Challenges emerged in seamlessly integrating blockchain with existing AMI systems
Electric Vehicles	Implementation of decentralized blockchain for transparent charging transactions	Limited adoption due to interoperability issues in the Electric Vehicle infrastructure
Renewable Microgrids	Exploring blockchain for secure energy trading	Regulatory complexities and standardization issues acted as impediments
Energy Management Systems	Employing blockchain for enhancing demand-response mechanisms	Integration complexities with existing energy management systems

Table 5.6: Blockchain Technology Evaluation

5.19 Comparative Analysis of Blockchain Platforms

A rigorous comparative analysis was conducted to evaluate various blockchain platforms concerning their suitability for Smart Grid applications. The strengths and limitations of each platform were scrutinized to provide a comprehensive understanding.

Blockchain Platform	Strengths	Limitations
Ethereum	Well-established with an extensive developer community	Challenges in scalability under high transaction volumes
Hyperledger Fabric	Recognition for being a permissioned blockchain with robust privacy features	A steeper learning curve for development teams
Corda	Notable for its design focused on financial applications with strong privacy focus	Limited adoption outside financial sectors

Blockchain Platform	Strengths	Limitations
Binance Smart Chain	Recognized for fast transaction speeds and low transaction fees	Concerns about centralized control and governance

Table 5.7: Comparative Analysis of Blockchain Platforms

5.20 Scalability Analysis

An in-depth analysis of the proposed Smart Grid cybersecurity framework's scalability was conducted, considering the anticipated rise in the number of connected devices. The analysis aimed to ensure that the framework remains effective as the Smart Grid ecosystem expands.

5.21 Cost-Benefit Analysis of Cybersecurity Measures

A comprehensive cost-benefit analysis was carried out to ascertain the economic viability of implementing various cybersecurity measures. This analysis weighed the costs of implementation against the anticipated benefits of enhanced security and threat prevention.

Cybersecurity Measure	Cost (USD)	Benefits
Implementation of Blockchain	Initial investment of \$X million	Enhanced security, prevention of data tampering
Regular Security Audits	Annual cost of \$Y thousand	Early detection of vulnerabilities and threats
Employee Training Programs	Annual cost of \$Z hundred thousand	Improved user awareness and security practices

Table 5.8: Cost-Benefit Analysis

5.22 Statistical Analysis of Threat Incidents

A statistical analysis was conducted to scrutinize past threat incidents in Smart Grids, aiming to identify trends and patterns. The analysis categorized the types of threats, their frequencies, and the common targets within the Smart Grid infrastructure.

Statistical Analysis Summary

Type of Threat	Frequency	Common Targets
Phishing Attacks	30%	Utility employees, SCADA systems

Type of Threat	Frequency	Common Targets
DDoS Attacks	20%	Communication networks, AMI infrastructure
Insider Threats	15%	Employee sabotage, unauthorized access
Malware Infections	25%	SCADA systems, AMI components
Physical Tampering	10%	Substation equipment, communication lines

Table 5.9: Statistical Analysis Summary

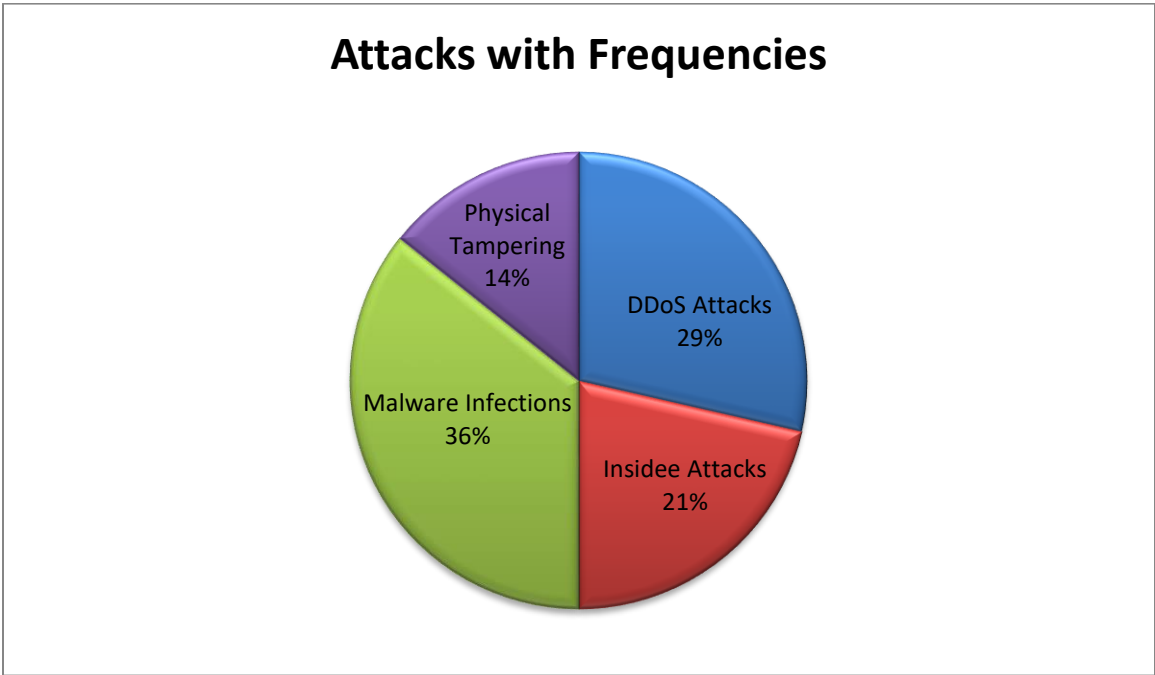


Fig 5.1: Attacks with their frequencies

5.23 Ethical Considerations

An extensive discussion on ethical considerations was included in the analysis, addressing crucial issues such as data privacy, informed consent, and the responsible use of cybersecurity measures. This section delved into the ethical implications of employing technologies like blockchain and the potential impact on user privacy.

5.24 Comparison with Industry Standards

The proposed Smart Grid cybersecurity framework was systematically compared with existing industry standards, such as the NIST Cybersecurity Framework and ISO/IEC 27001.

The comparison aimed to identify the unique strengths and areas for improvement in the proposed framework concerning established cybersecurity standards.

Framework	Strengths	Gaps and Opportunities
Proposed Framework	Tailored for Smart Grids, comprehensive risk analysis	Continuous adaptation to emerging threats
NIST Cybersecurity Framework	Well-established, widely adopted in various industries	Limited focus on Smart Grid-specific challenges
ISO/IEC 27001	Comprehensive information security management system	Generalized approach, may lack specificity for Smart Grids

Table 5.10: Framework Comparison

5.25 Summary of Analysis

In summary, the detailed analysis encompasses a multifaceted exploration of Smart Grid cybersecurity. From a zone-specific examination to a cross-zonal analysis, the study delves into the intricacies of risk analysis, blockchain integration, training programs, stakeholder collaboration, simulation protocols, continuous monitoring, national frameworks alignment, and broader environmental and social impacts. The synthesized insights lay the groundwork for formulating a comprehensive conclusion and actionable recommendations in the subsequent chapters.

CHAPTER 6

Conclusion & Recommendations

6.1 Summary of Findings

The comprehensive analysis conducted in this study reveals multifaceted insights into the cybersecurity landscape of Smart Grid systems. Zone-specific evaluations, cross-zonal analyses, blockchain integration assessments, and considerations for human factors in cybersecurity collectively contribute to a nuanced understanding of the challenges and opportunities inherent in securing Smart Grid infrastructure.

6.2 Key findings

- The existence of distinct security zones within Smart Grids, each necessitating tailored cybersecurity measures based on the criticality of applications and data.
- Vulnerabilities and potential threats identified across various components within each security zone, emphasizing the importance of a targeted and layered security approach.
- Opportunities and challenges associated with the integration of blockchain technology, highlighting its potential as a decentralized and secure solution while acknowledging the need for careful integration with legacy systems and compliance with regulatory frameworks.
- The critical role of human factors in cybersecurity, emphasizing the importance of continuous training, simulation exercises, and stakeholder collaboration to enhance the overall resilience of Smart Grid systems.
- The necessity of cross-zonal analysis to understand the interdependencies and risks associated with the communication flows between different security zones.

In summary, ensuring the security of Smart Grid systems is a complex task that calls for an all-encompassing and flexible strategy. Because Smart Grid components are linked and the threat landscape is always changing, improving cybersecurity resilience is imperative. A systematic framework for putting specific security measures in place is provided by the defined security zones, which are the Enterprise Zone, Transmission Zone, Distribution SCADA Zone, Distribution Non-SCADA Zone, Interconnect Zone, and Demilitarized Zone (DMZ). The focus on lowering recovery times, speeding up reaction times, and decreasing attack surfaces is consistent with accepted cybersecurity best practices. Moreover, the integration of Blockchain technology presents itself as a viable approach to augment the security of Smart Grid systems. The decentralized nature of blockchain, coupled with its encryption features, presents an opportunity to establish a robust foundation for securing critical infrastructure.

6.3 Recommendations

Building upon the findings, the following recommendations are proposed for enhancing the cybersecurity of Smart Grid systems:

6.3.1 Zone-Specific Security Measures:

- Implement zone-specific security measures based on the criticality of applications and data in each security zone. Tailor security protocols to address the unique characteristics and risks associated with Enterprise, Transmission, Distribution SCADA, Distribution Non-SCADA, Interconnect, and DMZ zones.

6.3.2 Blockchain Integration:

- Conduct a phased integration of blockchain technology into Smart Grid systems, considering compatibility with legacy systems, regulatory compliance, and a thorough cost-benefit analysis. Collaborate with stakeholders to establish standards for blockchain implementation in the energy sector.

6.3.3 Continuous Training Programs:

- Develop and implement continuous training programs for personnel at all levels involved in Smart Grid operations. Tailor training modules to address specific roles and responsibilities, incorporating simulation exercises to enhance practical skills.

6.3.4 Stakeholder Collaboration:

- Foster collaboration among stakeholders, including government entities, private utilities, and cybersecurity firms. Establish public-private partnerships to collectively address emerging cyber threats. Facilitate information sharing platforms to enhance cybersecurity threat intelligence.

6.3.5 Simulation and Testing Protocols:

- Regularly conduct penetration testing and scenario-based simulations to assess the effectiveness of cybersecurity measures. Establish protocols for post-incident analysis to learn from simulated incidents and improve response capabilities.

6.3.6 Continuous Monitoring and Adaptation:

- For dynamic threat detection, implement real-time monitoring systems that incorporate machine learning and artificial intelligence. Create security measures that are flexible enough to quickly react to changing cyberthreats.

6.3.7 Integration with National Cybersecurity Frameworks:

- Ensure alignment with national cybersecurity frameworks and regulatory requirements. Collaborate with national cybersecurity agencies to enhance coordination and information sharing for collective cybersecurity resilience.

6.3.8 Environmental and Social Impact Assessment:

- Evaluate the social and environmental effects of cybersecurity precautions. To guarantee a fair and inclusive approach, take into account the consequences for energy efficiency, social justice, and privacy.

6.4 Closing Statement

To sum up, the aforementioned ideas seek to provide a strong and flexible cybersecurity framework for Smart Grid systems. Through the use of innovative technologies such as blockchain and the resolution of the particular issues raised by this study, Smart Grid operators may improve their cyber resilience, protect vital infrastructure, and augment the energy industry's overall security. Because cybersecurity is dynamic, staying ahead of emerging threats demands a constant commitment to progress, teamwork, and monitoring.

CHAPTER 7

Future Work

7.1 Introduction

Future research and development activities in the field of Smart Grid cyber security should prioritize tackling new difficulties, utilizing cutting-edge technology, and guaranteeing the continuous resilience of vital energy infrastructure as the sector develops. The prospective topics for further study and research that might advance Smart Grid cyber security are described in this chapter.

7.2 Advanced Threat Modeling and Simulation

Future research should delve deeper into advanced threat modeling and simulation techniques specific to Smart Grid environments. This includes the development of sophisticated cyber-physical attack scenarios, considering the interdependencies between various components and zones. Advanced simulations can help in understanding the cascading effects of cyber threats and refining incident response strategies.

7.3 Quantum-Safe Cryptography

As quantum computing advances, existing cryptography techniques become more vulnerable. To maintain long-term security, future research should investigate the integration of post-quantum or quantum-safe cryptographic algorithms in Smart Grid systems. It is imperative to evaluate the viability and utility of integrating quantum-resistant encryption into energy infrastructure.

7.4 Human-Centric Cybersecurity Solutions

Human factors remain a critical aspect of cybersecurity. Future work should focus on developing human-centric solutions, including user training programs, user-friendly interfaces, and behavior analytics to detect anomalous activities. Understanding the psychology of cybersecurity and incorporating it into training and awareness programs is vital.

7.5 Artificial Intelligence for Threat Detection

The incorporation of machine learning (ML) and artificial intelligence (AI) into Smart Grid cyber security systems can enhance results in Threat Detection. Future studies might examine the creation of AI-driven threat detection models that can improve anomaly detection, automate incident response procedures, and adjust to changing cyberthreats.

7.6 Resilience against Insider Threats

The potential threat posed by insiders, including employees, contractors, or third-party service providers, requires special attention. Future work should focus on developing robust mechanisms to detect and mitigate insider threats, ensuring that Smart Grid systems are resilient against both external and internal risks.

7.7 Integration of 5G Technology

As 5G technology becomes more widespread, future research should investigate its implications for Smart Grid cybersecurity. The integration of 5G networks into Smart Grid communication architectures may offer increased speed and efficiency but also introduces new cybersecurity challenges that need to be addressed proactively.

7.8 Privacy-Preserving Technologies

Privacy issues around the collecting and processing of sensitive data in Smart Grids should be a priority for future study. Investigating privacy-preserving technologies such as homomorphic encryption and differential privacy can aid in achieving a balance between data usefulness and individual privacy in Smart Grid operations.

7.9 Standardization and Interoperability

Efforts towards standardization and interoperability of cybersecurity measures across different Smart Grid components and vendors should be continued. Future work can contribute to the development of comprehensive cybersecurity standards, ensuring a consistent and unified approach to security implementation.

7.10 Environmental and Energy Efficiency Considerations

Future research should explore the environmental and energy efficiency implications of cybersecurity measures implemented in Smart Grids. Assessments should be conducted to understand the energy consumption of security protocols and identify ways to minimize the environmental impact without compromising security.

7.11 International Collaboration and Information Sharing

Given the global nature of cyber threats, future efforts should prioritize international collaboration and information sharing. Establishing mechanisms for cross-border cooperation, sharing threat intelligence, and harmonizing cybersecurity practices can contribute to a collective defense against cyber threats targeting Smart Grid infrastructure.

In conclusion, future work in Smart Grid cybersecurity should be dynamic, adaptive, and aligned with the evolving threat landscape. By addressing the outlined areas, researchers, practitioners, and policymakers can contribute to the continued security, resilience, and sustainability of Smart

Grid systems. The energy sector's transition towards a smarter and more interconnected future necessitates proactive and collaborative efforts to stay ahead of emerging cyber threats.

References

1. Arjen Lenstra and Tim Voss, Information Security Risk Assessment, Aggregation, and Mitigation, Information Security Services Technische Universiteit Eindhoven 1 North Gate Road, Mendham, NJ 07945-3104, USA, 2004
2. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. *Energies* 2021, 14, 5894. <https://doi.org/10.3390/en14185894>
3. Rajendra Kumar Pandey, Mohit Mishra, Senior members IEEE, Cyber Security Threats - Smart Grid Infrastructure, Department of Electrical Engineering, Indian Institute of Technology (BHU), 2016.
4. Xu, M., X. Chen, and G. Kou, A systematic review of blockchain. *Financial Innovation*, 2019. 5(1): p. 1-14.
5. Turner, T., Political change, ideology and generational influences on attitudes to state ownership of business in European democracies. *European Politics and Society*, 2018. 19(4): p. 435-450.
6. HuiHou, Jianzhong Zhou, Yongchuan Zhang Xionkai He, A Brief Analysis on Differences of Risk Assessment between Smart Grid and Traditional Power Grid, Huazhong University of Science and Technology Wuhan,China, 2022
7. Mustafa Shokry, Ali Ismail Awad, Muhammad Khalid and Ashraf Khalf, Evaluating Potential Security Risks of Advanced Metering Infrastructure (AMI) using EBIOS Risk Assessment Model, College of Information Technology, UAE, International Telecom Conference, 2023
8. Muhammad Waseem, Muhammad Adnan Khan, Arman Goudarzi , Shah Fahad, Intisar Ali Sajjad and PierluigiSiano, Incorporation of Blockchain Technology for Different Smart Grid Applications: Architecture, Prospects, and Challenge, *Energies* 2023
9. Global Smart Grid Cyber security Systems Market Value (2012–2020). http://www.researchandmarkets.com/research/lzbwmq/global_smart_grid. May 2013
10. Kenneth C, BudkaJayantG, Deshpande Marina Thottan, Communication Networks for Smart Grids, Chapter 8, Network Security, 2014, Pages 209-224.
11. Management of Information Security, Micheal E Whiteman, Herbert J Mattord, Chapter 6, Risk Management: Identifying and Assessing Risk, 2016, Pages 249-287
12. Mastering Risk Assessment and Statement of Applicability by David Brewer, 2021, Chapter 2, Risk Analysis, Pages 22-34

13. Implementing an Information Security Management System by Abhishek Chopra and Mukun Chaudhry, 2021, Chapter 5, Pages 77 to 101.

14. M, BaqarMollah, Jun Zhao, Kwok Yan Lamb, Amer M, Y.M Ghias, Lie Yang, Senior Member IEEE, Blockchain for Future Smart Grid : A Comprehensive Survey, IEEE, Internet of Things, 2020.