PRESIDENCY UNIVERSITY
Private University Estd. in Karnataka State by Act No. 41 of 2013
Itgalpura, Rajankunte, Yelahanka, Bengaluru – 560064

Cyber-Security Enabled Smart Controller for Grid-Connected Microgrid

A PROJECT REPORT

Submitted by

ABDUL SAMAD – 20221CSE0121

SIDDIQUE ALI KHAN – 20221CSE0048

MOHAMMED ANZAL A – 20221CSE0026

Under the guidance of,

Dr. Manju More E

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

PRESIDENCY UNIVERSITY

BENGALURU

DECEMBER 2025

PRESIDENCY UNIVERSITY

Private University Estd. in Karnataka State by Act No. 41 of 2013
Itgalpura, Rajankunte, Yelahanka, Bengaluru – 560064

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this report "Cyber-Security Enabled Smart Controller for Grid-Connected Microgrid" is a bonafide work of "ABDUL SAMAD (20221CSE0121), SIDDIQUE ALI KHAN (20221CSE0048) & MOHAMMED ANZAL A (20221CSE0026)", who have successfully carried out the project work and submitted the report for partial fulfilment of the requirements for the award of the degree of BACHELOR OF TECHNOLOGY in COMPUTER SCIENCE & ENGINEERING during 2025-26.

Dr. Manju More E
Project Guide
PSCS
Presidency University

Mr. Muthuraju V
Program Project Coordinator
PSCS
Presidency University

Dr. Sampath A K
Dr. Geetha A
School Project Coordinators
PSCS
Presidency University

Dr. Blessed Prince R
Professor
Head of Department
PSCS
Presidency University

Dr. Shakkeera L
Associate Dean
PSCS
Presidency University

Dr. Duraipandian N
Dean
PSCS & PSIS
Presidency University

Name and Signature of the Examiners

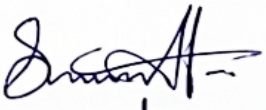
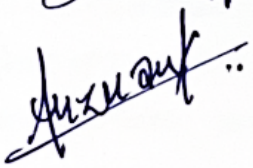
Sl. no.	Name	Signature	Date
1	Dr. Rajesh.P		27/11/2025
2	Dr. Srabdna Pramanik		27/11/2025

PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

We, the students of final year B.Tech in COMPUTER SCIENCE ENGINEERING at Presidency University, Bengaluru, named ABDUL SAMAD, SIDDIQUE ALI KHAN & MOHAMMED ANZAL A, hereby declare that the project work titled **"Cyber-Security Enabled Smart Controller for Grid-Connected Microgrid"** has been independently carried out by us and submitted in partial fulfilment for the award of the degree of B.Tech in COMPUTER SCIENCE & ENGINEERING during the academic year of 2025-26. Further, the matter embodied in the project has not been submitted previously by anybody for the award of any Degree or Diploma to any other institution.

Abdul Samad	USN: 20221CSE0121	
Siddique Ali Khan	USN: 20221CSE0048	
Mohammed Anzal A	USN: 20221CSE0026	

PLACE: BENGALURU

DATE: 27/11/2025

ACKNOWLEDGEMENT

For completing this project work, we have received the support and the guidance from many people whom we would like to mention with deep sense of gratitude and indebtedness. We extend our gratitude to our beloved **Chancellor, Pro-Vice Chancellor, and Registrar** for their support and encouragement in completion of the project.

We would like to sincerely thank our internal guide **Dr. Manju More E,** Associate Professor, Presidency School of Computer Science and Engineering, Presidency University, for her moral support, motivation, timely guidance and encouragement provided to us during the period of our project work.

We are also thankful to **Dr. Blessed Prince P.,** Professor & Head of the Department, Presidency School of Computer Science and Engineering, Presidency University, for his mentorship and encouragement.

We express our cordial thanks to **Dr. Duraipandian N.**, Dean PSCS & PSIS, **Dr. Shakkeera L.**, Associate Dean, Presidency School of Computer Science and Engineering and the Management of Presidency University for providing the required facilities and intellectually stimulating environment that aided in the completion of our project work.

We are grateful to **Dr. Sampath A. K.** and **Dr. Geetha A.**, PSCS Project Coordinators, and to **Mr. Muthuraju V.**, Program Project Coordinator, Presidency School of Computer Science and Engineering, for facilitating problem statements, coordinating reviews, monitoring progress, and providing their valuable support and guidance.

We are also grateful to Teaching and Non-Teaching staff of Presidency School of Computer Science and Engineering and also the staff from other departments who have extended their valuable help and cooperation.

ABDUL SAMAD
SIDDIQUE ALI KHAN
MOHAMMED ANZAL A

Abstract

Grid-connected microgrids have become a critical component of modern power systems, providing improved reliability and integration of renewable energy sources. Due to increased reliance on cyberspace systems, microgrids and their connection to the central grid suffer from a range of cyber threats: Data Injection, Denial of Service, or Man in the Middle. These systematic assaults are not the sole focus. However, the cyber threats jeopardize the economically and operationally efficient balance of the systems. Cyber perimeter defences have been constructed into the design, which employs military-grade elliptic curve cryptography to assure isolated communication. This paper describes a multifunction smart controller consisting of cyber defences with real-time lockers for secure communications, ECC, lightweight blockchains for immutable audit logs, and hybrid integrated anomaly detection for cyber-physical system defences. The advantages of ECC, in this case, include the establishment of low-latency secure communication. Blockchain provides operational integrity, real-time data, and traceability. The proposed hybrid model improves the accuracy and reliability of detecting intruder systems and other malfunctions in operational cyber-physical systems. Additionally, a dashboard provides operators with real-time monitoring and control capabilities. This system's uniqueness lies in its ability to combine several cybersecurity technologies into one seamless system, which optimizes real-time processing on microgrid controllers and balances system performance with security. The proposed framework also emphasizes modularity. Each security layer such as encryption, blockchain auditing, and anomaly detection is designed to operate independently while contributing to the resilience of the whole system. This layered approach ensures that even if one subsystem experiences failure or compromise, the remaining modules continue to protect the microgrid effectively. In addition, the monitoring dashboard enhances the operator’s situational awareness by providing real-time alerts, intuitive visualization, and actionable insights that support timely decision-making. Beyond its technical innovation, this system contributes to the broader vision of secure and sustainable energy infrastructures. By addressing cybersecurity challenges in microgrids, the project supports renewable energy integration and protects critical infrastructure against evolving digital threats. The combination of ECC, blockchain, and anomaly detection provides a future-ready solution that is scalable and adaptable across different environments. This research also aligns with several Sustainable Development Goals, including affordable and clean energy, innovation in industry and infrastructure, and the creation of safe and resilient communities.

Table of Content

List of Figures

List of Tables

Abbreviations

Abbreviation	Definition
IoT	Internet of Things
SDG	Sustainable Development Goal
AC	Alternating Current
AI	Artificial Intelligence
API	Application Programming Interface
B.Tech	Bachelor of Technology
DC	Direct Current
DER	Distributed Energy Resource
DERs	Distributed Energy Resources
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FDI	False Data Injection
FDIA	False Data Injection Attack
Git	Global Information Tracker
HIL	Hardware-in-the-Loop
IEC	International Electrotechnical Commission
IoT	Internet of Things
LSTM	Long Short-Term Memory
ML	Machine Learning
MITM	Man-in-the-Middle
pBFT	Practical Byzantine Fault Tolerance
PESTEL	Political, Economic, Social, Technological, Environmental, Legal
PV	Photovoltaic
REST	Representational State Transfer
RSA	Rivest–Shamir–Adleman
SCADA	Supervisory Control and Data Acquisition
SDG	Sustainable Development Goal
SVM	Support Vector Machine
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VCS	Version Control System

Chapter 1
INTRODUCTION

The continued development of power systems into smart grids and the integration of distributed energy resources have microgrids being considered as multifunctional elements of contemporary electrical architectures. These systems support local generation, storage and distribution of energy which can operate in both grid connected and islanded configurations. The integration of information and communication technologies (ICT) that enable such capabilities also bring along substantial cybersecurity risks.

The culmination of multiple cyber devices such as smart meters, sensors, controllers, and interfaces, as well as network devices, makes microgrids easily vulnerable to cyber-attacks[1]. Unlike traditional networks, these networks are not entirely centralized, making them easy targets. They are also more prone to cyber-physical attacks due to the nature of their connectivity, which equally threatens the availability and service continuity of the physical system. Microgrid attacks, as per recent studies, carry the risk of impacting network stability and social security, which completely endangers the public.

1.1 Background

Modern electric power systems are undergoing a major transformation due to the integration of distributed energy resources (DERs), renewable generation, and advanced control technologies. Among these, microgrids have emerged as a crucial framework to enhance reliability, efficiency, and sustainability in energy distribution [12]. A microgrid is a localized energy system that can operate connected to the main utility grid or in an islanded mode, supplying power to critical infrastructure, commercial facilities, or remote communities. The inclusion of renewable sources such as solar photovoltaic (PV) systems and wind turbines, coupled with energy storage systems and intelligent controllers, enables microgrids to balance supply and demand effectively while reducing dependence on conventional fossil-fuel-based generation [14].

Notoriously complex systems like microgrids have trade-offs. For example, microgrids have faster self-healing times and more efficient fault detection owing to their automation and

communication advancements, but they also possess greater vulnerability given their dependence on totally automated and self-healing networked systems. The dependency on communication networks exposes them to cyber threats such as False Data Injection (FDI), Denial of Service (DoS), and Man-in-the-Middle (MITM) attacks, which can disrupt normal operation, compromise data integrity, and damage physical equipment [10], [21], [23]. These attacks can manipulate sensor readings or control signals, leading to power imbalances, instability, and in severe cases, cascading failures. Ensuring the cybersecurity of microgrid systems has therefore become critical for maintaining operational resilience and protecting critical infrastructure.

Man-in-the-middle virtual attacks intercept and manipulate the control and monitor channels of a conversation and insert malicious data within [24]. These attacks within microgrids draw alarms because of the critical data communications within the microgrid system and the reliance on wireless technologies. MITM attacks can operate on data, contributing to system instability because they can manipulate the data's confidentiality and data integrity at the same time.

Denial of Service (DoS) aims at crushing the communicational and computational capabilities of the microgrid control system including routers and switches [22]. These attacks are capable of lowering processing capabilities by flooding the communication networks and thus, the isolation of the control functions can be interrupted and control coordination of dispersed energy resources is seriously compromised undermining the system.

False Data Injection (FDI) attacks represent one of the most significant threats to microgrid operations. The attacks mislead system operators and automated controllers by actively manipulating control signals or sensor measurements. Careful planning enables attackers to design FDI attacks that bypass traditional bad data detection mechanisms. These attackers remain within operational limits and slowly diminish system performance [11], [13].

The outcomes of existing microgrid cybersecurity solutions stem from isolating and trying to solve each attack vector individually, and/or implementing countermeasures in isolation. Most approaches still don't tackle set objectives of balance between operational efficiency and real-time requirements of microgrid systems, which is why optimal system performance is rarely accomplished. Almost all focus is placed on system performance, or system security.

Hyper automation, while beneficial, expands these risks and their consequences. Through the integration of the Modbus, DNP3, and OPC-UA industrial standard networks, automation extends control. Unfortunately, these industrial standard networks lack the necessary protocols to encrypt, stay, and authorize access control to systems, opening microgrids to faults on cyber systems and physical structures. Therefore, piloting the framework control of microgrids must provide resilient operational performance and real-time fault tolerance.

The resulting control system must provide enhanced real-time cyber and physical system (CPS) control against cyber system attacks, while simultaneously maintaining sub-grid and full network functionality. Failures of microgrid automation and control increase power routing, sensor, and control distortions, while control distortions increase loading on sensing and control systems[20]. Each of these advanced problems describe the multiplicity of microgrid attacks and must be addressed to maintain operational self-healing and obstacle avoidance, thereby protecting critical infrastructure.

1.2 Statistics

The transition toward renewable energy continues to shape global electricity systems. Reports from international energy agencies indicate that renewable technologies represented more than 40 percent of all new power generation capacity added worldwide in 2024. Solar and wind installations have been the primary contributors to this growth as their costs continue to decrease, and governments invest in policies that support clean energy development. This shift has encouraged many countries to explore distributed energy architectures where microgrids play a central role in improving reliability and reducing dependence on centralised generation.

India’s renewable energy landscape reflects this global trend. By 2023, the country’s cumulative installed renewable capacity crossed 180 gigawatts, supported by large programmes in solar parks, rooftop solar, wind farms and hybrid power plants. The National Electricity Plan has set a long-term target of 500 gigawatts of renewable capacity by 2030. Achieving these numbers requires systems that can manage variable generation, support local loads and maintain grid stability. As a result, microgrids have become important for rural electrification, industrial clusters, commercial buildings and emerging smart city initiatives. Their ability to operate both in grid-connected and islanded modes offers operational flexibility that conventional distribution systems cannot provide.

Alongside the expansion of renewable infrastructure, cyber risk has increased across the energy sector. India's Cyber Emergency Response Team reported a significant rise in cyber incidents affecting utilities between 2022 and 2024. A growth of nearly 25 percent was recorded during this period, and a large proportion of attacks targeted supervisory control and data acquisition systems. These incidents included attempted intrusions, manipulation of measurement data and denial-of-service disruptions against communication links and control servers. The rise in such events is linked to the growing digital footprint of modern power systems, particularly as sensors, controllers and communication networks become deeply integrated into microgrid operations.

These statistics highlight the importance of secure control systems in energy networks. As microgrids expand and support a larger share of national energy demand, their exposure to cyber threats also increases. Protecting control commands, measurement data and communication channels is therefore essential for maintaining operational continuity. Without appropriate safeguards, a single targeted attack could disrupt energy supply, affect critical services and compromise public safety. The numerical trends reported by national and international bodies underline the urgency of adopting advanced cybersecurity mechanisms that support real-time detection, secure communication and reliable system recovery.

1.3 Prior Existing Technologies

One of the earliest groups of technologies used to protect microgrids involved classical IT security tools such as firewalls, virtual private networks and basic access control systems. These were adopted from general enterprise networks and applied to microgrid communication channels. Firewalls restricted traffic entering the control network, and VPNs created encrypted communication paths between remote operator terminals and microgrid controllers. While these solutions provided perimeter security, they were not designed for the timing needs of real-time control systems. They also struggled to detect attacks that originated inside the microgrid network, such as manipulated sensor values or malicious internal nodes.

Another widely explored technology is classical public key encryption, most notably RSA. RSA has been used to secure communication between distributed energy resource controllers and supervisory control and data acquisition systems. Studies showed that RSA could protect message confidentiality and prevent tampering, but its large key sizes and heavy computational

load created delays in embedded controllers. These delays made RSA difficult to use in microgrids where control decisions occur in short intervals. Research comparing RSA and elliptic curve cryptography demonstrated that RSA often exceeded acceptable processing limits for devices with restricted hardware resources. This performance mismatch encouraged the move toward lighter cryptographic approaches such as ECC.

Machine learning based anomaly detection forms another important class of existing technologies. Researchers have tested supervised and unsupervised algorithms to identify abnormal behaviour in microgrids [17]. These include autoencoders, support vector machines and neural network classifiers. Their goal is to detect false data injection, abnormal power flows or communication irregularities. Experimental results show that these models can learn typical microgrid behaviour and identify suspicious deviations during testing. However, many of these models run offline or in supervisory systems rather than in the real-time control loop. This limits their ability to prevent or mitigate attacks as they occur, and they often require additional tools to convert detections into immediate corrective actions.

Blockchain based logging and authentication has also been studied extensively. Blockchain provides an immutable ledger where microgrid events, energy transactions and device authentication records can be stored [5]. Research has shown that permissioned blockchain networks can improve traceability and accountability in distributed energy systems. They have also been proposed for peer-to-peer energy trading in community microgrids. Despite these benefits, blockchain systems face challenges related to latency and communication overhead. Consensus algorithms require coordination among nodes, which can slow down logging when used in fast control loops. For this reason, blockchain has been used mostly for auditing and transaction recording rather than for real-time decision-making.

Several integrated frameworks have attempted to combine encryption, intrusion detection or blockchain functionalities into more complete cyber-physical protection systems. For instance, some researchers developed hybrid AI and blockchain security platforms where machine learning detects anomalies and blockchain logs the results for later analysis. Others designed multi-layer resilience architectures that include secure communication, intrusion monitoring and coordinated control actions [20]. Although these frameworks move toward unified protection, many remain at the prototype stage or depend on hardware and software

arrangements that are not yet suitable for full operational deployment. These efforts highlight the need for a more unified, lightweight and real-time capable security controller that operates across all stages of microgrid communication and control.

1.4 Proposed Approach

The aim of this project is to design a cybersecurity-enabled smart controller for a grid-connected microgrid that can monitor system behaviour in real time, detect cyberattacks, respond to them in a coordinated way, and maintain stable power system operation. The controller is developed to protect communication within the microgrid, identify abnormal activity in the network, and provide secure logging of important events that occur during both normal and disturbed conditions.

The motivation for this work comes from the increasing use of digital communication in modern microgrids. As the number of sensors, controllers, and communication links grows, the microgrid becomes more exposed to cyber threats. Even small errors or manipulated data can cause power quality issues or result in incorrect control decisions. Microgrids that support renewable energy and critical loads depend on reliable and safe operation. This creates a strong need for a controller that includes cybersecurity functions as part of its normal operation.

The proposed approach follows a structured, layered design. The first part of the approach focuses on secure communication. Elliptic Curve Cryptography is used to protect data exchanged among devices in the microgrid [6]. ECC allows the system to verify whether incoming data is genuine and prevents attackers from altering control commands or sensor readings.

The second part introduces a hybrid anomaly detection system. This system observes electrical and communication behaviour. Threshold-based checks are used to identify sudden changes in voltage, frequency, load or communication delay [7]. These checks act as fast alerts for irregular events. In addition, machine learning models are trained with data from normal and attack scenarios. These models detect complex patterns that may not be visible through simple thresholds. By combining both methods, the controller can identify a wide range of attacks in real time.

The third part of the approach uses a lightweight blockchain logging system. This system records security events, detected anomalies, and important control decisions in a permanent log. The blockchain ensures that records cannot be modified later, which helps operators review the sequence of events and supports transparency in operations [16]. Only essential information is stored so the system remains efficient and suitable for microgrid conditions.

All three components are integrated within a MATLAB and Simulink simulation environment that includes renewable generators, energy storage, loads, and communication links. The system is tested by introducing cyberattacks such as denial of service, false data injection, and man in the middle attacks. These tests help evaluate the controller's detection capability, response time, and overall stability. A dedicated dashboard presents real-time system states, alerts, and blockchain logs, allowing operators to monitor the microgrid clearly and make informed decisions.

The applications of this project extend to any setting where microgrids are deployed. This includes renewable energy plants, industrial facilities, academic campuses, and hospitals that rely on stable and secure power. Remote communities that depend on microgrids for primary electricity supply can also benefit from enhanced cybersecurity. The controller can be adapted to various microgrid sizes and can support environments where continuous power supply and system safety are important.

This proposed approach brings together secure communication, real-time detection, and reliable event recording in a unified structure. It supports the development of microgrids that remain stable and dependable even in the presence of cyber threats.

1.5 Objectives

1.5.1 Behavioural Objective

The behavioural objective focuses on how the controller should act when the microgrid is functioning under both normal and disturbed conditions. The controller is expected to continuously observe the flow of power between renewable sources, storage systems, loads, and the main grid. It must adjust control actions so that generation and demand remain balanced, since any mismatch can cause voltage or frequency deviations. A stable balance ensures reliable operation of critical loads and prevents unnecessary stress on microgrid equipment.

When cyberattacks occur, the behaviour of the system often shifts quickly. Attackers may alter sensor data, delay communication, or disrupt control messages. The controller must still make correct decisions in these situations. This requires the controller to detect irregularities, ignore compromised data, and act on verified information only. By maintaining stable behaviour during attacks, the controller helps prevent cascading failures, blackouts, or unsafe operating conditions.

This objective ensures that the controller responds to both electrical changes and security threats without losing system stability. The behaviour of the controller is therefore not only about following commands but also about adapting to evolving threats and protecting the microgrid from unexpected disruptions.

1.5.2 Analytical Objective

The analytical objective focuses on the system's ability to understand and interpret incoming data. Microgrids produce a large amount of information from sensors and communication links, and this data must be analysed quickly to identify suspicious activity. The hybrid model uses simple threshold rules to detect sudden changes and machine learning to recognise patterns that evolve more gradually. This combination provides a broad coverage of attack types.

Threshold detection is useful for identifying instant deviations, such as voltage spikes, frequency drops, or abrupt delays in communication. These kinds of changes often indicate the early stages of attacks or equipment failures.

However, many cyberattacks are subtle and cannot be detected through basic rules alone. Machine learning models help address this by learning from historical data, identifying behaviour that does not match normal patterns, and flagging events that suggest tampering.

Real-time analysis is central to this objective. If detection is slow, attackers may gain control of the system or cause permanent damage. The hybrid analytical approach ensures that both fast and slow-moving threats are identified early, allowing the controller to respond effectively. This improves the resilience of the microgrid and provides operators with timely information to act on.

1.5.3. System Management Objective

This objective focuses on creating a reliable method to store important events and decisions made by the controller. The blockchain framework is chosen because it creates a permanent record of events that cannot be modified later. This is useful in microgrid environments where accountability, traceability, and verification are important. Every event that relates to system security or control actions is stored as part of an ordered chain of records.

The blockchain is designed to be lightweight so it can run efficiently alongside the control system without causing delays. It stores only essential information to avoid excessive growth in memory usage. Each block contains timestamps, key events, and verified signatures from cryptographic checks. When an attack occurs, the blockchain helps maintain a clear record of what happened, how the system reacted, and which components were affected.

This objective supports system management by giving operators and engineers a trustworthy log that can be used for audits, troubleshooting, failure analysis, and compliance reporting. It strengthens the transparency of the system and ensures that the actions of the controller can always be reviewed and understood, even after an incident.

1.5.4 Security Objective

The security objective addresses the need to protect communication inside the microgrid. Control decisions depend heavily on accurate and trustworthy data. If attackers intercept or modify these messages, they can mislead the controller or cause unsafe operating conditions. Elliptic Curve Cryptography is used because it provides strong protection with minimal computing resources, which is suitable for real-time systems. ECC ensures that every message is encrypted before transmission and verified upon receipt. This prevents attackers from reading control commands, injecting false values, or impersonating legitimate devices. Digital signatures generated through ECC also allow the controller to confirm whether a message truly came from an authorized component. This protects the microgrid against spoofing attacks and man-in-the-middle threats. By securing all communication paths, this objective helps maintain the integrity and confidentiality of data throughout the microgrid. It ensures that control decisions are based on genuine information and prevents attackers from exploiting weaknesses in communication channels.

1.5.5 Deployment Objective

The deployment objective focuses on testing the entire system in a realistic and controlled environment before it is applied in real-world setups. MATLAB and Simulink provide a flexible platform to simulate both electrical behaviour and cyber events. This allows the team to study how the controller reacts to attacks such as denial of service, false data injection, and man-in-the-middle manipulation.

During simulation, different levels of attacks are introduced while observing how the controller maintains stability, detects anomalies, and activates the appropriate security responses. These tests show whether the system can maintain voltage and frequency levels, perform secure communication, and record events correctly in the blockchain. Recovery behaviour is also studied to understand how quickly the controller returns the microgrid to normal operation after an attack. This objective ensures that the entire system is validated end-to-end.

Through simulation, weaknesses can be identified and corrected before deployment in actual microgrid environments.

1.6 Sustainable Development Goals (SDGs)

This project contributes directly to several United Nations Sustainable Development Goals (SDGs):

- Goal 7: Affordable and Clean Energy

  The project supports Goal 7 by improving the security and reliability of microgrids that integrate renewable energy sources. A cyber-secure controller ensures that solar and wind power can be used without frequent disruptions caused by attacks or communication failures. When the microgrid remains stable and protected, communities and facilities can trust renewable energy as a primary source of power. This helps expand clean energy access while maintaining affordability, since fewer interruptions lead to lower maintenance costs and more efficient use of available energy resources.

- Goal 9: Industry, Innovation, and Infrastructure

  Goal 9 is addressed by introducing advanced digital protection methods into modern energy infrastructure. The controller combines cybersecurity, real-time monitoring, and automated decision-making, which strengthens the resilience of industrial systems that rely on continuous power. By integrating encryption, anomaly detection, and secure logging, the project demonstrates how innovative technologies can improve the reliability of energy networks. This contributes to the development of smarter, more dependable infrastructure that industries can adopt as they move toward digital and automated operations.

- Goal 11: Sustainable Cities and Communities

  The project contributes to Goal 11 by improving the safety and reliability of power systems that support urban environments. Smart cities depend on stable electricity for transportation, communication, healthcare, and public services. A microgrid that can resist cyberattacks and quickly recover from disturbances ensures that essential services remain available even during digital threats. This strengthens the resilience of urban communities, reduces the risk of outages, and supports long-term sustainability as cities continue to adopt renewable and distributed energy systems.

- Goal 13 (Climate Action): By improving the security and stability of renewable-based microgrids, the project indirectly supports climate action. Many organizations hesitate to adopt clean energy solutions because of operational risks or concerns about the reliability of digital control systems. A secure controller reduces these concerns and encourages wider adoption of renewable sources. As more microgrids operate safely, the energy sector can transition away from fossil fuels, lowering greenhouse gas emissions and contributing to global climate goals.

- Goal 16: Peace, Justice, and Strong Institutions

  Goal 16 focuses on transparency, trust, and accountability. The blockchain logging system in this project ensures that all important events and control actions are recorded in a tamper-proof manner. This builds trust in the energy system, since operators and

stakeholders can verify what happened during an incident. The secure logging also supports fair investigation processes and reduces the possibility of disputes about system behaviour. In broader terms, using transparent digital systems helps strengthen institutional reliability in the energy sector.

Fig 1.1 Sustainable Development Goals

1.7 Overview of Project Report

Chapter 1 introduces the project, explaining its motivation, background, objectives, and alignment with the SDGs. Chapter 2 presents the literature review, covering existing work on microgrid cybersecurity, encryption methods, and machine learning-based intrusion detection. Chapter 3 describes the methodology and system architecture, while Chapter 4 discusses the implementation details and software configuration. Chapter 5 focuses on analysis and design, including requirements and flow diagrams. Chapter 6 outlines the software development tools and simulation setup used. Chapter 7 explains the testing methodology, test plans, and results obtained. Chapter 8 discusses social, legal, ethical, sustainability, and safety aspects related to the project. Finally, Chapter 9 presents the conclusion, summarizing findings and suggesting future improvements.

Chapter 2
LITERATURE REVIEW

S. H. Rouhani et al. [14] provide the most usable literature review on cyber resilience vulnerabilities due to the unique combination of renewables, low inertia, and bidirectional flows of microgrid hybrids. This review also considers the unique structural standards of IEC 61850 and IEC 62351, while also considering the gaps due to the lack of communication, data integrity, and the varying system elements. This review examines some of the many cyber threat vectors to the communication of the intelligent devices and hybrid renewable generation units. It also examines some of the integrated system approaches to microgrid resilience, including the cyber resilient core, the real time system, the anomaly-based intrusion detection, and the protective perimeter system. The review focuses on the dynamic cyber posture for the hybrid microgrid to provide gaps for the future researcher.

The working paper by Ahmed et al. [15] identifies the specific field of microgrid cybersecurity, the continuously expanding field, and the basic requirements of efficient cyber protection. It provides an overview of the types of cyber-attacks, which include attacks on the communication networks, control attacks, and generation units of power and assesses the impact of microgrid cyber-attack vectors. Ahmed is the first author to propose the integration of advanced cyber-attack protection mechanisms, which include machine learning-based anomaly detection mechanisms, block chain technologies, and various types of cryptography, from theory, to practice. The author focuses on the need to embark on the remaining strands of research to advance the cyber resilience of microgrids.

Ahmad et al. [16] emphasizes how the development of advanced communication technologies, coupled with decentralized control, and the integration of distributed energy resources, have rendered smart microgrids more susceptible to cyber-attacks. The authors systematically considered the cybersecurity issues involving smart microgrids, i.e., unauthorized access, information alteration, and malicious-focused attacks against the AC and DC microgrid systems. The authors explore the potential of blockchain technology to fortify security by decentralized access controls and guaranteed data and transaction integrity, authentication, and transparency. The review further discusses the integration of blockchain with other technologies, such as federated learning and quantum-safe cryptography, to improve the

microgrids' defences against sophisticated cyber-attacks. In addition, the authors point out the important gaps in the available literature and provide pathways to advance the cyber security of smart microgrids.

The work of Guato Burgos et al. [17] emphasizes the application of AI technologies for detecting various types of anomalies in smart grids. The authors classify the different types of anomalies as: data integrity attacks; abnormal readings and patterns of use; breaches; network infrastructure anomalies; inconsistencies in the electrical data; war in cyberspace; and the detection and use of instrumentation. The authors emphasize the focus on cybersecurity for the prevention of network intrusion, fraud, data laundering, fabrication of unauthorized false data, and the illicit modification of a network topology.

There is a growing tendency towards the development and construction of frameworks of hybrid and other types of model anomaly detection systems. These include machine learning, regression and decision tree algorithms, deep learning, support vector machines, and various neural network architectures. The authors also describe emerging systems of anomaly detection based on federated learning, hyperdimensional computing and other graph systems. Even with the limitations of the bottom-up-system network model and the sizable dataset implications, this revision highlights the adjustable and mobile capabilities of the AI-based model anomaly detection systems in smart grids.

In their research, Adeniyi et al. [18] review how Elliptic Curve Cryptography (ECC) is applied in the safeguarding of devices in the Internet of Things (IoT) ecosystem. Regarding IoT devices, the study highlights the reason ECC is preferred beyond other options, given the lower computational power of the hardware as ECC contains smaller key systems that empirically shield the hardware effectively.

The review presents a classification of ECC with its applications in peer reviewed IoT devices within a corpus of 61 documents between 2018 and 2023. These documents champion the advantage of ECC over other mainstream techniques like RSA in terms of energy, time, and memory efficacy. The review also brought to the fore the limitations of ECC, namely, vulnerability to the man in the middle attacks and ineffective key management. The author

calls for the focus on the design of unique sophisticated algorithmic models of ECC to improve the capabilities and defensive functionalities of IoT devices.

Ghadi et al. [19] discusses the cyber vulnerabilities of smart grids. Smart grids have recently been developed, which allows for the authors to extend their taxonomy of cyber-attacks, titled An Analysis and Implementation of Cyber Attack and Defence Strategies for smart Grids. The authors focus on the potential of AI and blockchain technologies to identify and block cyber-attacks, particularly those involving the injection of deceptive data. The issues to the counterfeit topologies and the imprecise data detected when integrating big data with blockchain are described. The author notes that the unexploited potential for cyber defensive strategies regarding smart grids is a factor to be considered in the smart grids. Adding potential cyber intrusions and other defensive strategies against unsupported attacks is to be considered in unexploited defensive strategies.

Syrmakesis et al. [25] focuses on the impact of false data injection attacks on the smart grid system. The authors promote the definition of cyber resilience for smart grids (SG), which introduces a resilience curve outlining the different tiers of system performance such as resilient, post event degraded, restoration, and post restoration, and adding system performance measuring stems. After which, the authors defend a metrics-based cyber resilience assessment and assessment system. The authors categorize cyberattacks into two. The first is a CIA (Confidentiality, Integrity, Availability) taxonomy which includes false data injection, replay, time delay, denial of service, ransomware, man in the middle, and spyware attacks. The second is based on the control loop position, categorizing attacks as on the sensors, measurement channels, control centres, control command channels, and actuators.

The review collapsed the cyber defence model as mitigated and model-based wherein the former is classified as the data driven mitigation approaches. The authors identify various forecasting, state estimation, and game-theoretic models classified as mitigated models along with some observer designs like a sliding-mode, unknown-input observer, and machine learning cyber-defence techniques. These techniques include Long Short-Term Memory (LSTM) networks, autoencoders, graph neural networks, and reinforcement learning to detect and mitigate the effects of FDIA.

This paper argues the observer based and model-based approaches assume flawless system modelling, while the techniques based on data require excessive computing resources, and are poorly compared to the real world. It also claims the selection of approaches is based on the SCADA structure and procedural situation, and supports the use of combined approaches and the iterative enhancement of the models as means of improving the cyber resilience of smart grid systems.

Lin et al. [27] analyse how microgrids (MG) can be utilized to increase the resiliency of power systems. They argue that the 'N-1' reliability of traditional power system design is not adequate for analysing extreme low probability high impact events of concern. They discuss how systems can be resilient when they can anticipate, withstand, adapt to, and recover from disruptions. MGs increase system flexibility and resiliency due to the MGs ability to be controlled in and out of the grid and be in either the grid-connected or islanded states. Time is of the essence in the recovery process and is also one of the constructs that the resilience model curve is based on. MGs are defined as having controllable system boundaries in which energy from multiple Distributed Energy Resources (DERs) is supplemented controlled loads.

The authors divide MGs based on structure (AC, DC, and Hybrid) and control (Centralized, Decentralized and Hybrid) as well as on the continuum of Reliability and Flexibility. MGs also afford additional benefits such as better reliability performance, reduced operational costs, improved power quality, and reduced greenhouse gas and other pollutant emissions. The authors discuss various hardening and operational strategies to increase resilience. Operational strategies are categorized into actions that are corrective and preventive and can be taken before and after the disaster. The restoration and optimization techniques discussed in this paper pertain to hybrid MG networks.

Taveras Cruz et al. [26] explores the microgrid cyber protection multi-agent-based systems mosaics. The authors provide an explanation of the mosaics of multi-agent based cyber protections of microgrids. The authors indicate that, like all other digitized infrastructures, microgrids also expand the scope of vigilance and protections microgrids must have to cyber defence. The authors explain that multi-agent systems (MASs) allow the partitioning of the systems for monitoring, set point exchanges, and independent identifying of changes for adaptive relaying systems.

The authors observe that when most researchers claim the separation of physical cyber faults from other cyber threats, they consider it to be the standard for the integrated scheme. The authors elaborate on the standard, and provide evidence to support the claim of the gap in scope of cross-discipline microgrid studies incorporating industry cyber communications and cyber defence mechanisms.

The authors describe the primary attacks as several types of injection attacks, denial of service attacks, the man in the middle attacks, ransomware attacks, insider attacks, coordinated attacks, and zero-day attacks. The authors explain how these attacks disrupt inter-agent communication, hinder multi-system fault detection, and control the erroneous operation of coupled AC and DC subnetworks. The authors provide several forms of defence including control, authentication, and block chain trust control systems. The authors examine a system of multi-agent distributed systems for classification of intruders using other forms of learning in systems.

Hussain, Bui, and Kim [20] present a comprehensive examination of how microgrids contribute to power system resilience during major disruption events. The authors begin by outlining resilience concepts in power systems, including disaster modelling and resilience assessment techniques, and then analyse how microgrids can act as local or networked resilience resources capable of islanding, black-start support, and supplying critical loads during grid failures. The paper reviews various forms of microgrid structures such as autonomous, dynamic, and networked configurations, and highlights how these systems improve recovery and maintain essential services during natural disasters.

It further explores operational strategies that enhance resilience, including proactive scheduling, outage management, and advanced multi-agent and artificial intelligence-based control methods designed to maintain stable operation during emergencies. The authors conclude by identifying research gaps and emphasising the need for integrated approaches that consider cyber-physical interactions, communication dependencies, and coordinated control strategies across multiple infrastructures.

Table 2.1 Summary of Literatures Reviewed

S#	Article Title, Published year, Journal name	Methods	Key features	Merits	Demerits
1	Review on Cyber Resilience for Hybrid Microgrids, 2024, Energy	Systematic literature review with focus on IEC 61850 and IEC 62351 standards	Analyses vulnerabilities caused by renewables and bidirectional power flows in hybrid microgrids	Links cyber resilience with global communication standards and integrated defence models	Limited quantitative validation and lack of real-world case implementation
2	Cybersecurity for Microgrids: Challenges and Defences	Taxonomy of cyber-attacks combined with blockchain and machine learning methods	Reviews cyber-attack forms and emphasizes integration of ML and blockchain solutions	Highlights comprehensive cyber-attack mapping and combined defence mechanisms	Challenges in operationalizing advanced cybersecurity methods in real microgrids
3	Cybersecurity in smart microgrids using blockchain-federated learning and quantum-safe approaches, 2025, Applied Energy	Integration of blockchain, federated learning, and quantum-safe cryptography	Explores decentralized authentication and data integrity for microgrids	Proposes secure decentralized models improving microgrid transparency and resilience	High computational cost and limited testing for hybrid cryptographic approaches
4	A Review of Smart Grid Anomaly Detection Approaches Pertaining to Artificial Intelligence, 2024, Applied Sciences	Machine learning and AI models including regression, deep learning, and SVM	Focuses on anomaly detection in smart grids using AI-based hybrid frameworks	Shows flexibility and scalability of AI systems for anomaly detection and grid protection	Dependence on large datasets and need for model simplification in practical systems
5	A Review on Elliptic Curve Cryptography Algorithm for Internet of Things, 2024, Computer and Electrical Engineering	Comparative analysis of ECC methods for IoT device security	Evaluates ECC efficiency for IoT devices with small key systems and low energy use	Proves ECC to be energy efficient and suitable for resource-limited IoT devices	Susceptibility to key management issues and man-in-the-middle attacks
6	A hybrid AI-Blockchain security framework for smart grids, 2025, Scientific Reports	AI and blockchain-based attack detection and defence modelling	Categorizes cyber-attacks and examines integration of AI and blockchain for security	Presents taxonomy-based detection and introduces novel AI-enhanced defence strategies	Lack of empirical validation and limited coverage of multi-domain attack types
7	Cyber Resilience Methods for Smart Grids Against False Data Injection Attacks, 2024, Frontiers in Smart Grid	Model-based and data-driven methods including LSTM and reinforcement learning	Defines cyber resilience curve and attack taxonomies across smart grid control loops	Provides hybrid model recommendations and real-time validation of resilience methods	Heavy computational demand and limited real-world validation of models
8	Cybersecurity in MAS-Based Adaptive Protection for Microgrids, 2025, Electronics	Multi-agent systems with encryption, authentication, and machine learning frameworks	Identifies key cyber threats and MAS-based protection systems for microgrids	Combines MAS decentralization with encryption and learning for improved protection	Requires high computational power and lacks integrated physical-cyber models
9	Review of Microgrids to Enhance Power System Resilience, 2025, Engineering Proceedings	Comparative review and classification of microgrid structures and control schemes	Defines resilience as anticipation, absorption, adaptation, and recovery from disturbances	Emphasizes MG flexibility and independence under extreme event conditions	Limited focus on cyber aspects; mainly resilience from physical events
10	Microgrids as a resilience resource and strategies used by microgrids for enhancing resilience", 2019, Applied Energy	Reviews resilience assessment using microgrid formation, networked MG structures, and operational scheduling techniques.	Defines MG classifications and explains formation, operation and resilience strategies across different MG types.	Provides a clear summary of how microgrids improve system recovery and support critical loads during outages.	Does not address cybersecurity concerns or integration with digital protection methods.

Chapter 3
METHODOLOGY

3.1 Overview of the Development Methodology

The development of the 'Cybersecurity-Enabled Smart Controller for Grid-Connected Microgrid' follows the V-Model Software Development Methodology, which emphasizes design and validation through testing at every stage. The V-Model breaks each design stage into separate blocks, each with an associated testing stage in order to assure all requirements are satisfied and all aspects of the system are continuously verified and validated throughout the course of the project.

This approach works best with cyber-physical systems due to the interdisciplinary nature of the controls, communication, and cybersecurity aspects of the systems. The approach ensures that system requirements identified in the early stages are rigorously verified and validated, resulting in a reliable and verifiable workflow for system development. The descending tiers of the V represent decomposition of the system to lower-level modules, while the ascending tiers represent their integration, testing, and validation against predefined goals.

3.2 Mapping of Project Phases to the V-Model

The V-Model for this project consists of several interconnected phases: requirement analysis, system design, functional design, unit design, unit testing, integration testing, verification, and validation. Each stage is described below in relation to the implementation of the cyber-resilient smart controller framework.

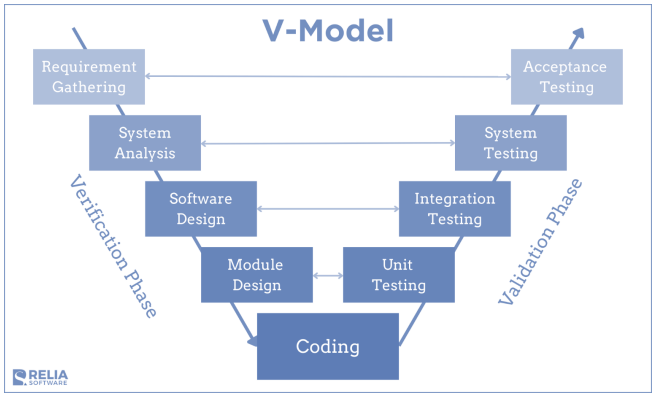


Fig 3.1 V-Model phase mapping

3.2.1 Requirement Analysis

The requirement analysis phase focused on identifying both the functional and non-functional needs of the cyber-resilient microgrid. Literature on smart grid security, communication reliability, and distributed control systems informed the development of system specifications. The requirements included secure communication between microgrid components, real-time cyber-attack detection, tamper-proof event logging, and stable microgrid operation under adversarial conditions.

The analysis also determined what software tools and software platforms would be required. MATLAB and Simulink were selected as the main development and simulation platforms due to their powerful modelling, visualization, and numerical computation capabilities. Python-based microservices and Linux utilities were chosen to handle advanced cryptography, network emulation, and blockchain management. Together, these tools formed a hybrid environment capable of accurately simulating both physical power dynamics and cyber-attack scenarios.

The requirement analysis phase also focused on understanding how different cyberattacks could affect control decisions and communication pathways within the microgrid. To support this, a threat classification exercise was carried out that mapped specific attack types to the components most likely to be affected, such as sensors, controllers, communication links, or data storage elements. This mapping helped refine requirements for response timing, data validation, and secure communication protocols. The process ensured that the system's final specifications aligned with realistic operational challenges and provided a clear foundation for later design and testing stages.

For later stages of development, to measure the system performance, a set of requirements was created that was tied to metrics such as the accuracy of anomaly detection, secured message verification, and blockchain validation. These metrics were to provide a framework to ensure performance was measured objectively.

3.2.2 System Design

The system design phase defined the overall architecture of the cyber-resilient microgrid. The system integrates five major components: the cyber-attack simulation environment, the Elliptic Curve Cryptography (ECC) module, the hybrid anomaly detection system, the lightweight blockchain ledger, and the monitoring and control dashboard. These components work together

to provide secure communication, real-time threat detection, event logging, and operator visibility.

The core of the design is a discrete-time simulation loop implemented in MATLAB, which models the dynamic behaviour of the microgrid. The loop runs on fixed time intervals and updates the electrical parameters, states of components, and control commands. Each system, including the batteries, loads, photovoltaic systems, and wind turbines, is a structured MATLAB data type such that the system can be easily modified and unit testing can be applied in a modular fashion.

To ensure efficient data exchange and modular design, the architecture employs a set of standardized function interfaces: initialize, step, measure, and applyControl, allowing independent development and testing of each unit. The design also defined communication interfaces between components and controllers, ensuring flexibility for simulation and attack emulation.

Alongside the structural architecture, the system design phase also defined how timing, synchronization, and coordination would be handled across the different subsystems. Particular attention was given to how the simulation loop interacts with external services responsible for security functions, ensuring that encryption, anomaly detection, and logging tasks do not cause delays that affect real-time behaviour. The design also documented fallback behaviours for cases where external services produce delayed or incomplete responses, creating a predictable and stable operating structure for subsequent implementation.

3.2.3 Functional Design

In the functional design phase, each subsystem was decomposed into smaller software units with defined interactions. Communication and controller coordination were implemented at two levels. At the application level, controller agents operate as MATLAB classes that exchange telemetry data through TCP or UDP channels. Network behaviour such as latency, jitter, and packet loss were simulated by introducing probabilistic delays and drop rates to emulate real-world conditions.

For packet-level emulation and attack generation, MATLAB communicates with Linux tools such as *scapy*, *netcat*, and *iptables* using controlled system calls. These are invoked from safe templates to ensure reproducibility. The design also incorporates REST-based microservices

for Python-MATLAB communication, allowing external processes such as ECC encryption or attack generation to run asynchronously.

The functional design also defined the security and monitoring subsystems. ECC was integrated for secure communication, anomaly detection combined threshold and machine learning-based approaches, and blockchain provided tamper-proof event recording. Together, these subsystems form a complete cyber-defence workflow embedded within the MATLAB environment.

The functional design further included the specification of health monitoring processes for each subsystem. These processes periodically assessed whether modules such as the ECC service, ML detector, and blockchain logger were active and responsive. If abnormal latency or failure was detected, predefined routines instructed the controller to shift into a degraded but safe operating mode. This functional safeguard allowed the system to retain essential capabilities even when individual components experienced interruptions, which strengthened the resilience objectives of the overall design.

3.2.4 Unit Design and Implementation

In the phase of designing the unit, each of the functional blocks was developed as individual MATLAB modules. A discrete-time simulation loop was used, and at each step of the simulation, three types of outputs were produced, namely, electrical readings obtained from the simulation, changed states of the components, and control outputs. For each device model, input and output were maintained at structured data, so as to maintain the uniformity of data formats.

Communication units were developed using MATLAB's networking primitives, while cryptographic and attack emulation functions were implemented as Python microservices integrated through MATLAB's `py.*` interface. To ensure secure communication, ECC (Elliptic Curve Cryptography) algorithms were used to maintain control over the data's confidentiality and integrity that flowed to and from the orchestrators. Control messages were packaged, signed digitally by the sender, and verified upon receipt. If the control message was altered, the integrity of the control message was flagged and reported to the blockchain.

The anomaly detection functionality was split into a two-stage process. The two stages were hybrid methods of anomaly detection, with the first stage being purely threshold based, and the

second stage a machine learning model that works to detect the presence of certain hyper-parameters which may be described as a coordinated, complex attack. The machine learning model was designed to run asynchronously to maintain the real-time simulation.

During unit development, emphasis was placed on creating clear data exchange patterns between MATLAB and the external microservices to avoid inconsistent message formats. Each unit included automated internal checks so that invalid or malformed packets were rejected before progressing to later stages in the simulation. This step-by-step approach simplified debugging and ensured that each block performed consistently under varied workload conditions. The structured workflow also made it easier to change or extend specific functions without affecting unrelated modules.

3.2.5 Unit Testing

Every module was evaluated separately to ensure its correctness. MATLAB's `runtests` suite was used to automate the validation of critical functions. The ECC module was tested for proper key generation, message signing, and verification. An ML detector was evaluated against the synthetic datasets containing labelled normal instances and attack samples. The blockchain module verified the hash of its stored records to ensure its integrity and hence immutability.

In preparation for integration, the performance of each module was evaluated in complete isolation. This stage of testing at the module level is often called unit testing as it revealed configuration problems, timing issues between modules during communication, and incorrect responses from the models, enabling us to understand issues at the module level before advancing to testing at the level of the entire system.

Additional stress-testing routines were applied to evaluate how the units behaved under heavy computational loads or extended operation. These tests involved running long sequences of simulation steps, injecting repeated anomalies, and verifying whether the modules continued to produce correct and stable results. The process helped identify subtle issues such as memory growth, repeated packet loss, or delayed cryptographic responses. The findings informed refinements that improved the reliability of each unit before moving to system-level testing.

3.2.6 Integration Testing

In this phase of testing, the focus was on the integration of various modules and the verification of their inter-system communications. After all the modules were validated on their own, they were brought together to create a complete system in the MATLAB environment. The integrated system included modules for discrete-time power simulation, ECC service, ML anomaly detection, blockchain ledger, and attack emulation, and aimed to evaluate the integrated system's performance for the intended application.

Testing scenarios included normal operation, random measurement errors, and cyber-attack simulations such as False Data Injection, Denial of Service, and Man-in-the-Middle attacks. The integrated system was evaluated based on its ability to detect attacks, maintain voltage and frequency stability, and log events accurately. The testing demonstrated that communication remained secure, anomalies were detected in real time, and all security-related events were properly recorded in the blockchain ledger.

Beyond functional verification, integration testing also examined how well the system handled overlapping cyber-events or compounded disturbances. For example, simultaneous false data injection and communication delays were introduced to determine whether the controller could still maintain stable operation and record events in the correct order. These scenarios provided insight into how different subsystems interacted under pressure, helping confirm that the overall architecture behaved consistently and that no module caused unpredictable delays or failures when operating jointly.

3.2.7 Verification

Verification activities ensured that each system feature met the original functional and performance requirements Verification of the microgrid simulation model was achieved through a comparative analysis of the model’s simulated electrical outputs and the theoretical expectations. Verification of ECC implementation was done by confirming that all messages that were encrypted were able to be decrypted without any data loss. The ML-based detection system underwent verification by attaining a detection accuracy of 87.5% on the validation dataset. Verification also confirmed the integrity of blockchain transactions by recomputing block hashes and verifying digital signatures. The results demonstrated compliance with

system specifications, confirming that design objectives were achieved at the software and control logic levels.

The verification phase also included reviewing the traceability of system features back to their original requirements. Each requirement was linked to specific implementation and test results, ensuring all functional, security, and performance expectations were addressed. This mapping helped confirm that no requirement was overlooked during development and that the system could be considered complete from both a technical and documentation perspective. The verification records also serve as a reference for future extensions or audits of the controller.

3.2.8 Validation

The last stage of validation was to review the system in its entirety against the set goals for the project. Full system simulations were performed with the help of MATLAB and third-party microservices. The controller was evaluated during adversarial conditions, monitoring to capture the voltage, frequency, and power balance.

The results showed the system had fully operational stability amid cyber events, recovering within seconds after the disruption and having no record alterations which were preserved on the blockchain.

The system achieved its primary goal of having secure communications, anomaly detection, and microgrid control, thereby validating the effectiveness of the methodology. The consistency in outputs demonstrated that the controller's behaviour was reproducible and not dependent on specific run-time conditions. Such repeatability strengthened confidence that the system would behave reliably when deployed in practical microgrid environments.

3.3 Overview of the Proposed System Implementation

The cybersecurity-enabled smart controller integrates multiple security technologies within a unified framework designed to protect grid-connected microgrids against cyber-attacks. The combination of logging, threat detection, secure communication, and real-time monitoring of the system architecture, allows for secure monitoring operated at the highest efficiency possible.

3.3.1 Architecture Overview

The entire system is made up of five core components. These components include the cyber-attack simulation environment, ECC encryption module, hyper anomaly detection system, lightweight blockchain logging framework, and the monitoring dashboard. These components work together to provide end-to-end security coverage for microgrid operations.

The cyber-physical interface layer manages the flow of information between the physical components of the microgrid and the cybersecurity controller. It relies on validated data and secure communication frameworks to control the data integrity among the sensors, control systems, and actuators. Each element of the integrated security systems relies on the processing and control core to provide coordinated cyber processing functions and responses to the detected threats.

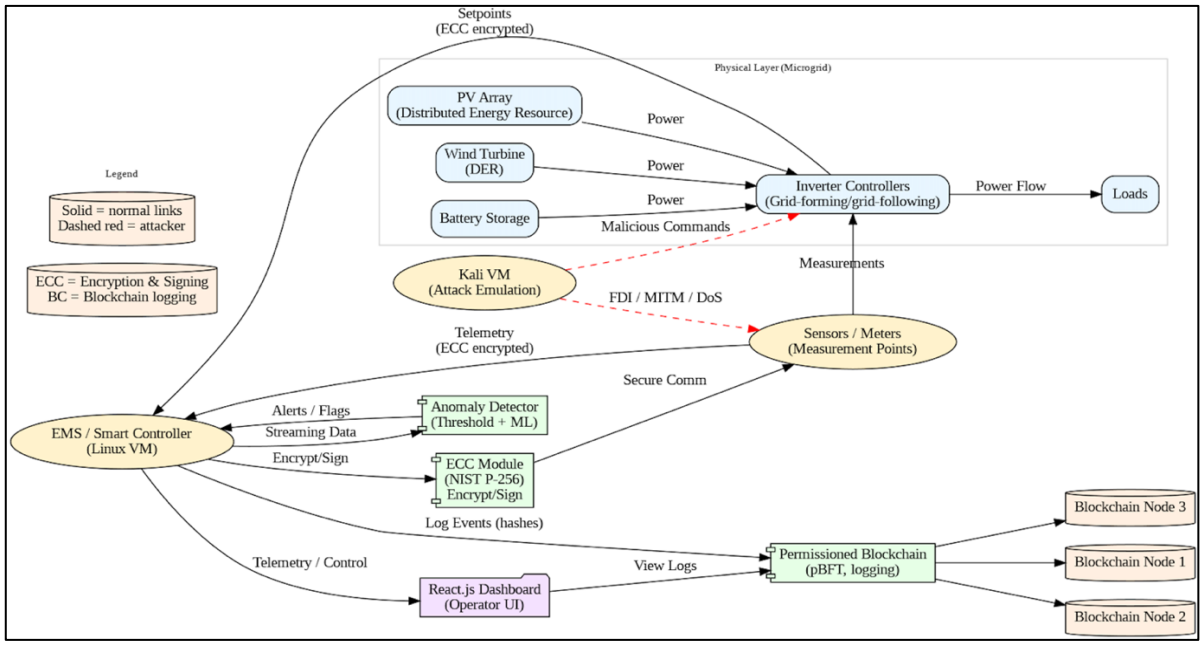


Fig 3.2 System architecture of the cyber-secure microgrid

3.3.2 ECC Encryption Implementation

The Elliptic Curve Cryptography module provides secure communication channels between microgrid components using optimized algorithms suitable for real-time applications. The ECC implementation [2] utilizes the NIST P 256 curve, which provides 128-bit security equivalent with minimal computational overhead compared to traditional RSA-based systems. The elliptic curve used is defined as:

$$E: y^2 \equiv x^3 + ax + b mod p \qquad (1)$$

with the constraint

$$4a^3 + 27b^2 \neq 0 mod p \qquad (2)$$

where p is a large prime, a and $b$are curve parameters, and G is the generator point of order n.

The key management system implements dynamic key generation and distribution protocols to ensure forward secrecy and prevent compromise propagation. A private key d is randomly generated, and the corresponding public key is computed as:

$$d \in [1, n-1], Q = dG \qquad (3)$$

where d represents the private key, and Q the associated public key.

For secure session establishment, the Elliptic Curve Diffie–Hellman (ECDH) protocol is employed.

Two entities $A$and $B$with key pairs (d_A, Q_A) and (d_B, Q_B), respectively, derive a common shared secret S:

$$S = d_A Q_B = d_B Q_A = d_A d_B G \qquad (4)$$

ensuring that only the legitimate parties can compute the same session key.

Message authentication employs the Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure data integrity and non-repudiation.

For a message m, a random nonce k is selected, and the signature pair (r, s) is generated as:

$$r = (kG)_x mod n \qquad (5)$$

$$s = k^{(-1)}(h(m) + rd) mod n \qquad (6)$$

where $h(m)$ is the hash of the message.

All control messages and obtained measurements utilize private and public keys on both ends of verification. Only the sender signs the documents, while the recipients check the signatures against the sender's public key. This technique protects against any attempts that try to change important control information, and proves the existence of a MITM interception.

3.3.3 Hybrid Anomaly Detection System

The hybrid anomaly detection system combines threshold-based monitoring with machine learning algorithms to identify malicious activities with high accuracy and low false positive rates [7] . The system operates in two stages: initial screening using statistical thresholds and comprehensive analysis using trained machine learning models.

The threshold component of the system operates and monitors the values such as the voltage of the system, frequency shifts, inter-module power loss, and the latency of inter-module communications. These thresholds are set to represent the standard operational window and the regulated range [8]. When such measurements are obtained, the system sets alerts and initiates machine-learning driven secondary analyses of the sample set.

The machine learning systems incorporate LSTM Networks together with logistic regression for predictive analytics of time series data [9]. The LSTM Networks learn training data associated with the normal behaviour of the system so as to identify and flag temporal anomalies within time series data. Subsequently, Logistic regression helps in the rapid classification of distinct events and the individual parameter deviations. This approach allows the machine learning systems to identify both gradual and abrupt attacks.

3.3.4 Lightweight Blockchain Logging

The framework integrates a permissioned distributed ledger which is specifically optimized for microgrid application scale and is kept in a secured system that is free from tampering [16]. All authentication attempts, anomalies, control actions, and modifications to system configurations in the secure system are recorded.

The implementation of blockchains applies a lightweight consensus protocol and is optimized for low-latency application scope. Instead of the proof-of-work algorithms, the system uses a Practical Byzantine Fault Tolerance (pBFT) consensus protocol, which ensures confirmation

of transactions without sacrificing security guarantees. Every node in the blockchain is part of the consensus and the new block creation process and stores a local version of the distributed ledger [19]. The blocks, which contain timestamps, transaction hashes, signatures, and Merkle tree roots, provide high-speed verification of the data and assurance of integrity.

The logging layer was also designed to support efficient retrieval and verification operations so that the controller or operator can quickly audit past events without introducing heavy computational steps. To achieve this, indexing methods were added to each block to allow rapid filtering of entries related to specific attack types, communication failures, or control actions. This structure supports both near-real-time inspection and longer-term analysis of system behaviour during complex event sequences. By enabling efficient access to historical data, the blockchain component strengthens overall traceability and provides a reliable foundation for post-event diagnostics and security review.

3.3.5 Dashboard Interface

The monitoring and control dashboard provides the system operator a detailed interface to track and respond to microgrid security status and any associated threats. The use of Simulink to implement dashboard performance allows appropriate response time. The dashboard's primary function is to track security measures in real-time and displays metrics on the status of encryption, system anomalies, blockchain sync, and overall system health.

The use of charts and graphs allows operators to conduct retrospective examinations and identify security anomalies. Operators are able to confirm, counter, and supervise system security changes using the alert management functions in a timely manner.
During dashboard development, usability considerations were incorporated to ensure that operators could interpret information quickly, especially during periods of high system activity. Key indicators such as anomaly flags, communication delays, and encrypted message counts were placed in prominent locations to reduce the time required to identify system issues. The dashboard also logs operator interactions, creating a record of user-driven control actions that supports later assessment of decision-making processes. This combination of real-time display and historical context enables operators to maintain situational awareness and respond effectively to developing security events.

Fig 3.3 Real-time monitoring dashboard

Chapter 4
PROJECT MANAGEMENT

4.1 Project Timeline

The cybersecurity-enabled smart controller project follows a systematic timeline spanning approximately 12 weeks from mid-August to mid-November 2025, divided into distinct planning and implementation phases. This timeline employs a Gantt chart methodology to provide clear visual representation of project breakdown, scheduling, task dependencies, and milestone achievements in chronological order. The structured approach ensures optimal resource allocation, risk mitigation, and deliverable quality throughout the project lifecycle, culminating with project completion by November 14, 2025.

The Gantt chart presented in Figure 4.1 provides a comprehensive visual representation of the cybersecurity-enabled smart controller project timeline, effectively demonstrating the systematic approach to complex system development over the 12-week implementation period ending November 14, 2025. The chart employs a color-coded structure where red bars represent critical milestone phases and blue bars indicate detailed implementation tasks, creating clear visual differentiation between high-level objectives and specific technical activities. This visualization methodology enables project stakeholders to quickly identify task priorities, resource allocation patterns, and potential scheduling conflicts while maintaining clarity across multiple concurrent development streams. The horizontal timeline axis spans from week 34 through November 14, providing precise temporal boundaries for all project activities.

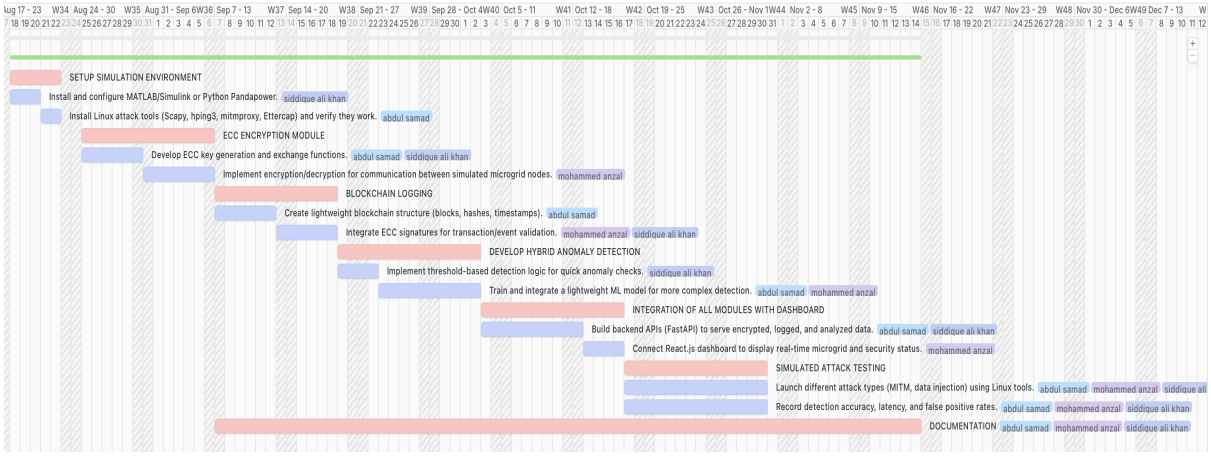


Fig 4.2 Project timeline and task dependencies (Gantt chart)

The task dependency structure illustrated in the Gantt chart reveals sophisticated project management planning that optimizes resource utilization while maintaining logical development sequences. For instance, the Setup Simulation Environment phase initiates the project timeline and serves as a foundational dependency for subsequent technical development activities, ensuring that all team members have access to necessary development tools before beginning component-specific implementations.

The ECC Encryption Module development overlaps strategically with the simulation environment setup, allowing Abdul Samad and Siddique Ali Khan to begin cryptographic algorithm development while Mohammed Anzal completes the initial environment configuration. This parallel task execution reduces overall project duration while maintaining quality control through systematic dependency management.

The Gantt chart demonstrates exceptional integration complexity through its representation of overlapping development phases that require careful coordination between team members. The Blockchain Logging implementation begins during the final weeks of ECC development, enabling integration testing of cryptographic signatures with distributed ledger functionality. Similarly, the Hybrid Anomaly Detection development commences while blockchain implementation continues, allowing for comprehensive testing of machine learning models against both encrypted communication streams and immutable audit logs.

This overlapping structure ensures that integration challenges are identified and resolved early in the development cycle, reducing technical risks and maintaining project schedule adherence toward the November 14 deadline.

4.1.1 Project Planning timeline

Table 4.1 presents the project planning phase, during which simulation tools, cryptographic functions, and AI-based detection strategies were defined and scheduled. The timeline ensures a realistic progression from environment setup to security module design, allowing adequate preparation for later implementation phases.

Table 4.1 Project planning timeline

Major Task	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17
Project initiation (i)	X	X	X														
Selection of topic	X	X	X														
Background (ii)			X	X													
Objectives (iii)				X	X												
Methodology (iv)					X	X											
Proposal						X	X										
Literature review (v)							X	X									
Design and Analysis								X	X								
System Requirement Phase (vi)									X	X							
System Design Phase (vii)										X	X						
Functional Unit Design Phase (viii)											X	X					
Report													X	X	X	X	
Final Report													X	X	X	X	

(i) Project initiation – Selection of project topic related to cyber-resilient microgrids, identification of research gaps in cybersecurity and renewable integration, defining scope, and establishing relevance to smart energy systems.

(ii) Background – Review of existing microgrid architectures, communication protocols, and cyberattack vulnerabilities; understanding previous approaches using blockchain, ECC encryption, and AI-based anomaly detection; and identifying expected outcomes for improved resilience.

(iii) Objectives – Define clear SMART objectives (Specific, Measurable, Achievable, Realistic, and Time-bound) focused on developing an integrated framework combining ECC encryption, blockchain logging, and hybrid AI-based intrusion detection for secure microgrid communication.

(iv) Methodology – Describe the proposed methodology in stages: system simulation setup, ECC key generation and exchange, blockchain event logging, AI-driven anomaly detection, and system integration. Detail tools (MATLAB/Simulink, Python, Linux utilities) and data flow across modules.

(v) Literature review – Summarize previous research on cybersecurity frameworks for smart grids and microgrids, emphasizing blockchain-based security, ECC cryptography, and AI anomaly detection. Identify inconsistencies, research gaps, and integration challenges, and propose feasible improvements for implementation.

(vi) System Requirement Phase – Identify system inputs (sensor data, power flow, control commands), outputs (logs, detection alerts), constraints (communication latency, bandwidth), and relationships among ECC, blockchain, and AI modules. Specify performance and security requirements.

(vii) System Design Phase – Define system architecture, functional blocks (ECC module, blockchain ledger, AI detection unit), and process flow. Design module interfaces, ensure interoperability, and develop an integrated testing and validation plan.

(viii) Functional Unit Design Phase – Identify and compare hardware/software components (encryption module, blockchain node, ML model). Perform integration, develop unit test plans, and validate system reliability, security, and resilience against simulated cyberattacks.

The project planning timeline sets out the structured sequence of activities carried out from Week 1 to Week 17. It begins with the project initiation phase, which spans the first three weeks. During this period, the topic was selected and aligned with broader themes in cyber-resilient microgrid research. This early stage focused on identifying the scope, understanding the relevance of cybersecurity in modern energy systems, and outlining the initial direction of the work. Establishing a clear problem statement in these first weeks ensured that subsequent stages were guided by consistent objectives.

The next major activity covers the background study and the formulation of the project objectives. The background review, carried out between Weeks 2 and 4, involved examining existing microgrid architectures, communication frameworks, and documented cyberattack vulnerabilities. By Week 3, the objectives were drafted, refined, and finalised. These objectives served as a foundation for the rest of the project and followed the SMART format to define measurable targets. Together, the background and objective-setting activities helped establish a strong conceptual base.

The methodology phase followed between Weeks 4 and 6. During this period, the project proposal was also prepared and completed. This stage defined the technical approach, including the simulation workflow, ECC-based communication strategy, blockchain integration, and anomaly detection framework. The planning ensured that each component had a clear purpose and that the overall methodology supported the main project goals. By completing the proposal at this stage, the project secured a clear roadmap before entering the more technical phases.

The literature review extended from Weeks 5 to 8. This involved a detailed study of previous work on microgrid security, blockchain frameworks, and machine learning-based detection models. The review helped identify gaps in existing solutions and guided the development of the integrated security framework. In parallel, design and analysis work took place during Weeks 7 and 10. This stage focused on building the early architecture of the system, analysing dependencies between components, and determining how ECC, blockchain, and anomaly detection modules would communicate in a real-time environment.

The system requirement phase occurred in Weeks 6 through 10. This involved identifying input and output requirements, communication constraints, data formats, and performance needs of the complete system. Once the requirements were fully documented, the system design phase followed between Weeks 9 and 13. Here, the project defined the structure of the architecture, the functional blocks, interface designs, and the validation approach. The system design phase ensured that all components could operate together coherently.

The functional unit design phase took place from Weeks 12 to 15. This involved developing the individual modules such as the ECC node, blockchain logging unit, anomaly detection engine, and dashboard elements. During this period, preliminary unit tests were also considered so that integration would be seamless. The final report writing phase ran from Weeks 13 to 17, overlapping with the development activities. This allowed results, design steps, and findings to be documented as they were produced rather than after all technical work was complete.

Overall, the timeline follows a logical progression from conceptual development to detailed design and reporting. Early weeks focus on understanding the problem and establishing the framework, while later weeks transition into implementation, refinement, and preparation of

the final delivery. This structured plan supports a smooth workflow and ensures that each phase builds directly upon the outcomes of the previous one.

4.1.2 Project Implementation timeline

Table 4.2 Project implementation timeline

Major Task	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17
Simulation		X	X	X	X	X											
Unit		X	X	X													
Integrated					X	X	X										
Hardware Implementation							X	X									
Software								X	X	X							
Testing *									X	X	X	X					
Critical Evaluation **											X	X	X				
Social, Ethical, Legal, and Sustainability													X	X			
Report														X	X	X	
Final Report															X	X	X

The implementation timeline begins with the simulation phase, which spans Weeks 1 to 6. This period is divided into unit-level simulation and integrated simulation. Unit simulation is completed in the first three weeks and focuses on validating individual components such as the control models, data pathways, and security routines in isolation. Once the subsystems are verified independently, the integrated simulation runs from Weeks 4 to 7. During this time, the individual modules are combined to form a single operational environment, enabling coordinated behaviour between the microgrid model, security layers, and communication functions.

Following the completion of simulation activities, the project transitions into hardware implementation across Weeks 6 to 11. Although the system is largely software-based, this stage includes interfacing MATLAB and Python microservices, configuring Linux utilities, and ensuring that supporting systems operate correctly under realistic timing constraints. Software integration continues into Weeks 8 through 12, where the emphasis shifts toward aligning cryptographic services, anomaly detection routines, and blockchain logging modules with the functional workflow developed earlier in the project.

Testing begins in Week 10 and proceeds through Week 14. This stage includes structured evaluations of communication security, anomaly detection performance, and the accuracy of logged events. Both normal and adversarial scenarios are used to test how the system behaves under different conditions. The testing window is intentionally extended to allow debugging,

retesting, and fine-tuning of components to ensure consistent behaviour across repeated simulations.

The timeline then allocates Weeks 13 to 15 for critical evaluation. During this stage, system performance results are compared with the expected outcomes defined in the requirement analysis. This stage helps refine the final interpretation of results and supports the conclusions presented in the report.

In Weeks 14 to 17, the project addresses social, ethical, legal, and sustainability considerations. The final report writing occurs throughout Weeks 15 to 17, bringing together all results, observations, and validation outcomes into a complete project document. This structured approach ensures that the system is not only functional but also evaluated from technical, operational, and societal perspectives.

4.2 Risk analysis

This PESTLE analysis examines the key external factors influencing the development of the cyber-resilient microgrid project. Political and economic factors emphasize the importance of government energy policies, research funding, and hardware costs. Social and technological aspects focus on public awareness, cybersecurity skills, and rapid advancements in blockchain, AI, and encryption. Legal and environmental factors address compliance with data protection standards and the sustainable deployment of renewable systems. Together, these insights help identify risks and guide strategic decisions for successful project implementation.

P Political	E Economic	S Societal	T Technological	L Legal	E Environmental
Explore: • Government energy and cybersecurity policies • National incentives for renewable and smart grid projects • Political stability affecting research funding • Public–private collaboration for energy innovation • Trade and import restrictions for electronic components	**Explore:** • Cost of renewable energy hardware and communication equipment • Exchange rate variations affecting imports • Inflation influencing software/hardware purchase • Research funding and grants availability • Employment in renewable energy and cybersecurity sectors	**Explore:** • Public awareness of microgrid security • Social acceptance of blockchain and AI in energy systems • Skill availability and training needs for cybersecurity workforce • Community energy-sharing behavior and cooperation • Ethical concerns in automation and AI decision-making	**Explore:** • Rapid advancements in blockchain and AI technologies • Research and development in encryption and anomaly detection • Availability of open-source tools for system testing • Cyberattack simulation and defense technologies • Scalability and interoperability of smart grid platforms	**Explore:** • Compliance with IEC 61850 and IEC 62351 communication standards • Data privacy and security regulations (e.g., GDPR) • Intellectual property and licensing of software frameworks • Employment and safety standards for testing environments • Legal accountability for cyber incidents in energy systems	**Explore:** • Climate impact on renewable energy reliability • Sustainable deployment of microgrids • Reduction in carbon footprint through local energy generation • Waste management for electronic and computing equipment • Support for national renewable and green energy goals

Table 4.3 Example of PESTLE analysis

Political

Political factors centre on how government policies and national priorities shape the development of cyber-resilient microgrids. Supportive policies for renewable energy, grants for smart-grid research, and stable regulatory environments encourage investment in secure energy technologies. Government collaboration with private sectors can accelerate innovation through joint funding programs, while restrictions on electronic imports or trade rules may affect the availability of critical components. Overall, political stability and policy direction strongly influence the pace at which secure microgrid systems can be deployed.

Economic

Economic considerations relate to the cost and availability of renewable energy hardware, communication devices, and cybersecurity tools. Exchange-rate fluctuations affect the price of imported components, and inflation influences the overall budget for software and equipment. Funding programs and research grants also determine how easily developers can access advanced testing tools. Growth in the renewable energy and cybersecurity job markets further affects labour availability and project feasibility. These economic drivers shape the affordability and scalability of microgrid security projects.

Societal

Societal factors reflect how communities perceive and adopt microgrid technologies, cybersecurity practices, and emerging tools such as blockchain or AI. Public awareness of microgrid benefits and cyber safety influences user acceptance and long-term adoption. The availability of skilled personnel, especially in cybersecurity and system automation, is important for deployment and maintenance. Community behaviour, cooperation, and ethical concerns related to data use and automated decision-making also affect how microgrid systems are designed and operated. These elements help determine how well microgrid solutions fit into society.

Technological

Technological factors involve advances in blockchain, AI, encryption, anomaly detection, and cybersecurity tools that directly affect microgrid design. The growth of open-source simulation platforms and testing software supports rapid system development. Progress in cyber-physical defence methods and smart-grid interoperability standards improves the performance and reliability of microgrid control systems. As technology evolves, microgrids can integrate more sophisticated security measures, ensuring they remain resilient to modern and emerging cyber threats.

Legal

Legal factors address compliance with communication standards, data protection laws, and cybersecurity regulations. Standards such as IEC 61850 and IEC 62351 influence how microgrids handle communication and security. Data privacy rules, intellectual property considerations, and licensing requirements affect how software and hardware are designed and shared. Legal frameworks also define responsibilities in the event of cyber incidents, influencing how operators document, report, and respond to threats. These requirements ensure that microgrids operate within approved safety and security guidelines.

Environmental

Environmental factors consider how microgrid designs contribute to sustainability and climate goals. Renewable energy systems support emission reduction, and microgrids can help lower carbon footprints through local generation and reduced transmission losses. Environmental policies encourage waste management practices for electronic equipment and promote green energy deployment. A secure microgrid also helps maintain power availability during climate-related disruptions, supporting resilience in regions vulnerable to extreme weather. These considerations ensure that microgrid development aligns with long-term environmental objectives.

4.3 Project budget

The project budget was carefully estimated to ensure that all necessary resources were available for smooth execution without exceeding financial constraints. The primary expenditure involved the purchase of MATLAB and Simulink software along with four additional libraries, which amounted to ₹4000. This software package formed the backbone of the project, as it enabled the modelling, simulation, and testing of the proposed cybersecurity-enabled smart controller. Other resources, such as personal computing devices for implementation and internet connectivity for literature review and cloud access, were already available and thus did not add significant costs.

In an effort for consolidation when it comes to financial planning, details pertaining to the functions that require specific resources were collected, and the team's availability was compared to the distribution of the workload. Because this was an academic undertaking, manpower, faculty mentoring, and institutional infrastructure costs were deemed institutional support, not direct expenses. Therefore, the only financial commitment was the purchase of the software. The constant supervision was such that no other unplanned expenses arose, and the costs were accurately predicted to the budget range.

Chapter 5
ANALYSIS AND DESIGN

The analysis and design phase serves as the foundation for developing the cyber-secure smart controller for grid-connected microgrids. This stage bridges the gap between understanding system requirements and constructing the technical framework that fulfils them. The analysis focuses on studying the operational behaviour of the microgrid, identifying potential cyber vulnerabilities, and defining functional requirements for secure communication, anomaly detection, and blockchain logging.

The design phase translates these findings into a structured architecture, outlining how each software component within the system. Together, these phases ensure that the final implementation is both functionally robust and secure, aligning system performance with cybersecurity objectives.

5.1 Requirements

The cyber-security enabled smart controller for grid-connected microgrids is designed to maintain secure and reliable operation of distributed energy systems. The main objective of the system is to integrate cybersecurity mechanisms within the control framework of a microgrid to prevent and mitigate cyber-attacks such as false data injection (FDI), denial of service (DoS), and man-in-the-middle (MITM) attacks.

The controller ensures that all control communications, data exchanges, and decision processes are carried out securely while maintaining operational stability and efficiency. The system operates by continuously monitoring network and power parameters, encrypting communication, detecting anomalies, and recording verified transactions through blockchain technology.

5.1.1 System Software Requirement Phase

The system software requirement phase defines the operational behaviour, logic, and data flow of the cyber-security enabled smart controller for grid-connected microgrids. The software is responsible for handling all information processing, secure communication, and control coordination tasks that maintain system reliability under both normal and attack conditions.

It collects and analyses input data such as voltage, current, frequency, and communication parameters from the simulated microgrid environment.
These inputs are used to monitor the system's real-time performance and to identify abnormal variations that may indicate cyber threats or operational disturbances. The software ensures that the system can react appropriately by isolating affected components, maintaining stable control, and recording all activities for later analysis.

The system captures the relationships between its modules, including encryption, anomaly detection, blockchain logging, and decision control. . Each of these components carries out different functions, yet work in a sequence of integration for achieving cyber resilience in totality. The ECC encryption module safeguards the communication of data between the distributed nodes, while the hybrid anomaly detection module in the ECC system, through a combination of statistical thresholds and machine learning, attempts to examine the system for unusual patterns of behaviour.

The blockchain logging component works to ensure the system's transactional and anomaly data is maintained in integrity and is traceable, while the control decision module is responsible for coordinating the control of all components to issue appropriate correction control commands, all of which works to ensure the system functions in a low latency and low computing load environments. In the case of microgrid systems, all components need to function in a tightly synchronized manner and respond to real-time commands.

Data collection requirements involve the continuous acquisition of operational and attack datasets from simulated environments to train and validate the anomaly detection models. Data analysis requirements include identifying and processing deviations from standard behaviour to detect intrusions and system faults.

System management requirements ensure coordination among all modules, maintaining consistent configurations and synchronization between encryption, detection, and logging processes. Security requirements define encryption, authentication, and data integrity protocols to protect communication and prevent unauthorized access. Finally, user interface requirements ensure that operators can monitor, analyse, and control system functions through a dashboard that displays encryption status, detected anomalies, and blockchain activity in real time.

Table 5.1 Summarizing requirements

Purpose	A cybersecurity-enabled smart controller that provides secure communication, immutable logging, and anomaly detection for grid-connected microgrids using integrated ECC encryption, blockchain technology, and machine learning
Behaviour	System operates in multiple security modes: Normal operation with baseline security, Enhanced security during threat detection, Emergency mode with maximum protection, and Recovery mode for system restoration
Data Collection Requirements	Real-time acquisition of microgrid operational data, security event logging, threat intelligence gathering, and performance metrics collection with encrypted transmission protocols
System Management	Remote monitoring and control through secure channels, automated security protocol adjustment, centralized key management, and distributed system coordination
Data Analysis	System should perform local analysis of the data
Application Deployment	MATLAB/Simulink-based simulation environment with secure communication interfaces, distributed blockchain nodes, and integrated attack simulation capabilities
Security	Military-grade ECC encryption, tamper-proof blockchain logging, multi-layer authentication, secure key distribution, and real-time intrusion detection with 95%+ accuracy

5.1.2 System Design Requirements

The system design phase translates the defined software requirements into a structured framework that determines how each module interacts to achieve secure and efficient microgrid control. The design defines the logical arrangement of functional blocks, including the ECC encryption module, blockchain logging framework, hybrid anomaly detection unit, and decision control module, all operating under a central management layer. Inputs such as sensor

data, control commands, and simulated cyber-attacks are processed through these interconnected modules to produce outputs like control signals, operational dashboards, and secure audit logs. The system design maintains a modular structure that supports both scalability and fault tolerance, allowing the system to adapt to various microgrid configurations and levels of operational complexity.

In this phase, the communication and processing pathways are designed to ensure real-time responsiveness and secure data handling. The encryption and anomaly detection modules are positioned within the main control loop to safeguard communication channels and identify potential threats as they occur. The blockchain logging unit functions as a secondary verification layer, maintaining a permanent record of authenticated events and detected anomalies. The decision engine consolidates information from all modules and determines appropriate responses such as isolating compromised nodes or issuing alerts to operators. The design ensures that all modules function coherently, with clearly defined data flow, minimal dependencies, and efficient processing under high-load conditions.

The design also incorporates management and user interaction components that support the operational and security goals of the system. The management framework synchronizes module operations and maintains configuration integrity, ensuring that the system continues to function even during network interruptions or cyber incidents. The user interface is designed to display real-time performance indicators, system alerts, and security events, enabling operators to monitor the health of the microgrid and take corrective action when required. Overall, the system design ensures a balance between security performance and operational reliability, providing a practical and resilient control framework for modern grid-connected microgrids.

5.2 Block diagram

Fig. 5.1 shows the functional block diagram of the cyber-security enabled smart controller for a grid-connected microgrid. The system consists of three main sections: inputs, processing, and outputs. The input section includes sensor data inputs that monitor voltage, current, and frequency; control commands from the grid and operators; and cyber threat simulations such as DoS, MITM, and FDI attacks. These inputs are processed by the Smart Controller, which integrates four core functional modules: the ECC Encryption Module for secure communication, the Hybrid Anomaly Detection Unit for identifying malicious activity, the

Blockchain Logging Unit for immutable event recording, and the Decision Engine for executing control and mitigation actions. The outputs include actuator control signals that regulate system operations and the operator dashboard that displays real-time status and security alerts. The design ensures secure, reliable, and resilient operation of the microgrid under both normal and adversarial conditions.

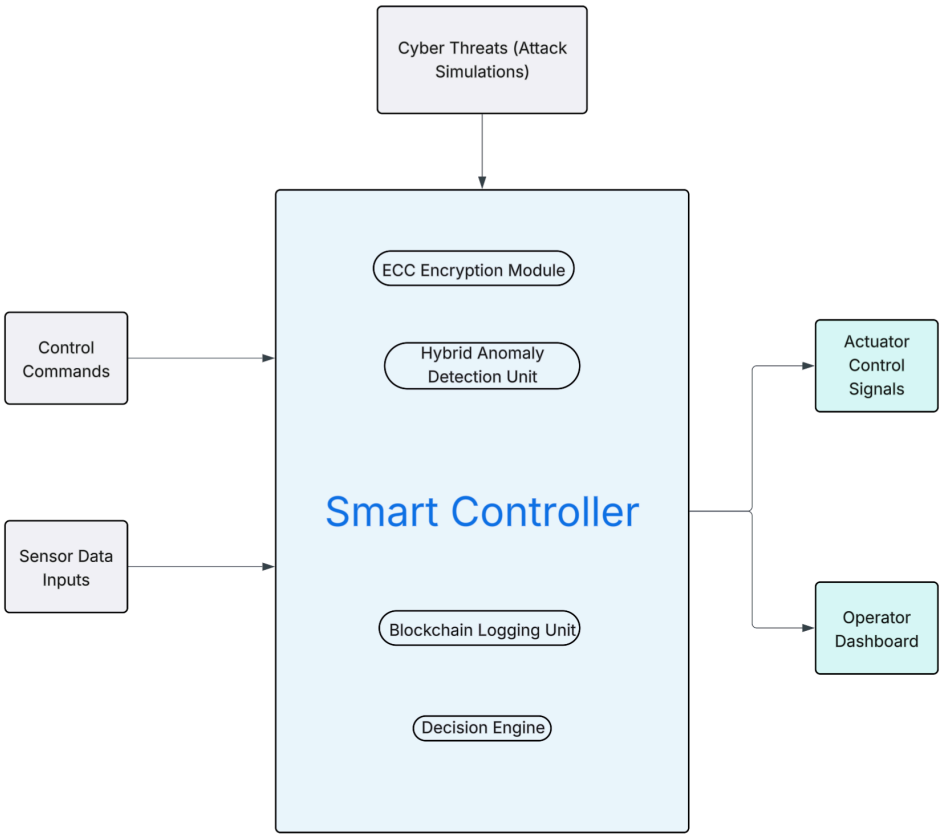


Fig 5.1 Functional block diagram

5.3 System Flow chart

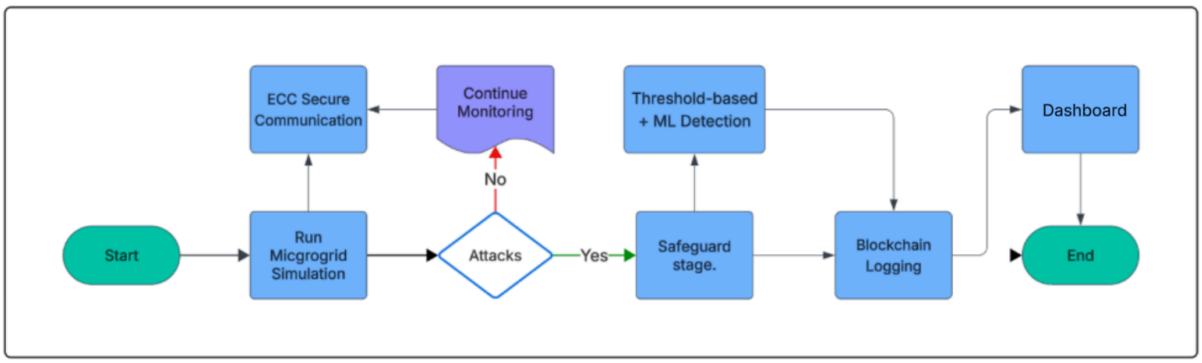


Fig 5.2 System flow chart

Fig. 5.2 shows the system flow chart of the cyber-security enabled smart controller for a grid-connected microgrid. The process begins with the initialization and execution of the microgrid simulation, which models normal operations of distributed energy resources and communication networks. The system then performs secure communication using the Elliptic Curve Cryptography (ECC) module to protect control and data exchanges between network nodes. Continuous monitoring is carried out to observe the system's operational parameters and communication patterns. When abnormal activity is detected, the flow proceeds to the attack verification stage, where the system determines whether a cyber-attack is occurring.

If an attack is detected, the safeguard stage is activated, triggering the hybrid anomaly detection mechanism that combines threshold-based evaluation with machine learning analysis to classify and assess the threat. The results are recorded using the blockchain logging unit, ensuring all events are securely stored for verification and traceability. The dashboard then presents real-time system information, including attack status, encryption status, and network health, allowing operators to take corrective action. If no attack is identified, the system returns to the continuous monitoring stage to maintain normal operations.

The flowchart accurately represents the logical sequence of functions in the proposed system, showing how detection, response, and secure logging are integrated within the control framework. This design is suitable for the project as it ensures continuous protection, rapid detection of cyber threats, and verifiable audit trails without disrupting microgrid operations. It also supports real-time decision-making and resilience under varying operating and attack conditions.

5.4 Functional Software Unit Design Phase

The functional software unit design phase defines and structures the individual software components that make up the cyber-secure smart controller. Each unit performs distinct functions within the overall design, such as encryption, anomaly detection, blockchain implementation, and system control. The communication spinning unit performs encryption and decryption of control signals and sensor data and provides secure communication by generating and validating cryptographic keys. The anomaly detection unit is hybrid as it uses operational data and employs statistical and machine learning models to detect cyber-attacks in real-time. The blockchain implementation unit creates a permanent record of system

anomalies and all critical transactions system for security audit evidence. Each of these software design modules is to be self-contained and will allow for streamlined interaction, as defined by their interfaces, to enable balanced and optimal control within the controller.

During unit design and analysis, every sub-module is individually evaluated for performance and reliability and rigorously tested and validated. Design for modularity is applied for ease of updating and debugging, and ease of scaling for microgrid configurations. A unit test plan is designed for every sub-module in the microgrid system for the comprehensive analysis of functionality, accuracy, and fault tolerance of the unit under a diversity of operating and attack scenarios. Each software unit is contended for data disposition, system latency, and system recovery attributes in order to minimal disruption of the system. The outcome of tests is the identification and closure of gaps in interaction matrix of the software modules. The designed software is tested for non-linear performance, instability, and quick recovery to real-world scenarios, which in this case is integrated microgrid environments for the software to perform as required in real-time scenarios.

Chapter 6
SOFTWARE AND SIMULATION

6.1 Software Development Tools

The development of the cyber-secure smart controller for grid-connected microgrids required the integration of several software development tools to streamline implementation, testing, and deployment processes. These tools ensured consistency, scalability, and collaborative efficiency across the software lifecycle. The primary tools used included Integrated Development Environments (IDEs), version control systems, simulation platforms, machine learning environments, and blockchain frameworks.

Integrated Development Environments (IDEs) / Code Editors:

Primary programming environments for this project are MATLAB, Simulink, and Visual Studio Code. Simulink and MATLAB made double of the work as they were used for model-based design and real-time simulation and validation of microgrid environment. Simulink also made it possible to integrate all modules: anomaly detection, blockchain, and encryption for energy system and distributed simulation. Visual Studio Code was used for the data disposition backend, and sub-modules controlling ECC encryption and blockchain transaction logic were captured. Configured to integrate with MATLAB were external Python scripts via the MATLAB Engine API for Python.

Version Control Systems (VCS):

GitHub served as the repository for source code management, version tracking, and collaboration among team members. The repository was configured with multiple branches for development, testing, and deployment, allowing contributions without interference. Access permissions were managed through GitHub's built-in security settings, ensuring collaboration. Git commits were standardized with clear messages, and GitHub Actions were enabled for automated testing of commits and updates.

Simulation and Testing Platforms:

MATLAB Simulink was used not only for simulation but also for attack emulation, where cyber-attack scenarios such as DoS, FDI, and MITM were implemented to test system resilience. The simulation environment was configured to replicate both normal and attack conditions, generating datasets used for machine learning training. Python libraries such as TensorFlow and Scikit-learn were integrated to develop and train the hybrid anomaly detection model. The environment setup required defining Python paths and dependency management through virtual environments to ensure consistency across systems.

Blockchain Development Framework:

A lightweight Hyperledger Fabric environment was configured for implementing the blockchain logging module. The setup involved defining peer nodes, ordering services, and establishing a permissioned ledger suitable for microgrid-scale data. The blockchain was configured to use the Practical Byzantine Fault Tolerance (pBFT) consensus mechanism for fast transaction validation. Smart contracts were written in Python to log and verify system events.

Project Management and Collaboration Tools:

Having project management and collaboration abilities, Notion was the tool of choice in the central management of the project. The development milestones and responsibilities were organized through Notion, enabling the team to monitor the various stages of the project, from the simulation setup to system testing and the final report writing. The workspace was organized into different modules, each of which had a Kanban board, a to-do list, and a progress tracker.

Testing and Deployment Tools:

Postman was employed for testing RESTful APIs between the controller and the dashboard components, ensuring data integrity and accurate system responses. For data logging and monitoring, FastAPI was used to deploy secure APIs for real-time blockchain and anomaly

detection data exchange. End-to-end validation was carried out by deploying these modules locally through a Docker-based container to ensure consistent behaviour across systems.

6.2 Software Code Snippet

```
%% CYBER-RESILIENT MICROGRID

function enhanced_microgrid_system()
    clc; clear; close all;


fprintf('╔═══════════════════════════════════════════════════════════╗\n');
fprintf('║  CYBER-RESILIENT MICROGRID - Capstone Project             ║\n');
fprintf('║                                                           ║\n');
fprintf('╚═══════════════════════════════════════════════════════════╝\n\n'
);

    launch_enhanced_gui();
end

%%
% ========================================================================
%% MAIN GUI LAUNCHER
%%
% ========================================================================

function launch_enhanced_gui()
    global sim_data control_params is_running attack_mode security_system;

    initialize_enhanced_system();

    main_fig = figure('Name', 'Cyber-Resilient Microgrid - Enhanced
Visibility', ...
                      'Position', [50, 50, 1800, 1000], ...
                      'Color', [0.08 0.08 0.12], ...
                      'MenuBar', 'none', ...
                      'ToolBar', 'none', ...
                      'Resize', 'on', ...
                      'CloseRequestFcn', @close_enhanced_system);

    create_enhanced_gui_layout(main_fig);
    generate_initial_data();
    update_all_plots_enhanced();
    update_all_displays_enhanced();

    fprintf('System Ready!\n');
    fprintf('ECC Active | ML Trained | Blockchain Ready\n\n');
    fprintf('⚡ Click START to begin | Click Attack buttons to test\n\n');
end

%%
% ========================================================================
%% SYSTEM INITIALIZATION
%%
% ========================================================================

function initialize_enhanced_system()
```

```
    global sim_data control_params is_running attack_mode security_system;

    % Simulation parameters
    sim_data.T_sim = 24*3600;
    sim_data.dt = 60;
    sim_data.t = 0:sim_data.dt:sim_data.T_sim;
    sim_data.current_time = 0;
    sim_data.time_index = 1;

    % Control parameters
    control_params.pv_capacity = 1000;
    control_params.wind_capacity = 800;
    control_params.battery_capacity = 2000;
    control_params.base_load = 600;
    control_params.grid_enabled = true;
    control_params.battery_enabled = true;
    control_params.renewable_enabled = true;
    control_params.load_factor = 1.0;

    is_running = false;

    % Initialize data arrays
    n_points = length(sim_data.t);
    sim_data.P_pv = zeros(1, n_points);
    sim_data.P_wind = zeros(1, n_points);
    sim_data.P_load = zeros(1, n_points);
    sim_data.P_battery = zeros(1, n_points);
    sim_data.P_grid = zeros(1, n_points);
    sim_data.SOC = 70 * ones(1, n_points);
    sim_data.voltage = 11000 * ones(1, n_points);
    sim_data.frequency = 50 * ones(1, n_points);
    sim_data.anomaly_detected = zeros(1, n_points);
    sim_data.attack_active = zeros(1, n_points);

    % Attack mode
    attack_mode.active = false;
    attack_mode.type = 'none';
    attack_mode.intensity = 0;
    attack_mode.start_time = 0;
    attack_mode.duration = 0;

    % Initialize security systems
    security_system.ecc = initialize_ecc_enhanced();
    security_system.ml_detector = initialize_ml_enhanced();
    security_system.blockchain = initialize_blockchain_enhanced();
    security_system.security_log = {};
    security_system.attack_log = {};
    security_system.encryption_count = 0;
    security_system.detection_count = 0;
end

%%
%% ECC SYSTEM
%%

function ecc = initialize_ecc_enhanced()
    fprintf('Initializing ECC...\n');
```

```
    ecc.curve_name = 'secp256k1';
    ecc.private_key = randi([10000, 99999]);
    ecc.public_key = mod(ecc.private_key * 65537, 2^20);
    ecc.key_timestamp = datetime('now');
    ecc.signatures_created = 0;
    ecc.verifications_done = 0;
    ecc.encryption_active = true;

    fprintf('Keys Generated: Pub=%d...\n', mod(ecc.public_key, 10000));
end

function [encrypted_data, signature] = ecc_sign_and_encrypt(data,
ecc_system)
    global security_system;

    data_string = jsonencode(data);
    hash_value = mod(sum(double(data_string)) * 7919, 1000000);
    signature = mod(hash_value * ecc_system.private_key, 1000000);
    encrypted_data = mod(hash_value * ecc_system.public_key, 1000000);

    security_system.ecc.signatures_created =
security_system.ecc.signatures_created + 1;
    security_system.encryption_count = security_system.encryption_count +
1;
end

%%
=========================================================================
%% ML ANOMALY DETECTION
%%
=========================================================================

function ml = initialize_ml_enhanced()
    fprintf('Initializing ML...\n');

    ml.thresholds.voltage_min = 10500;
    ml.thresholds.voltage_max = 11500;
    ml.thresholds.frequency_min = 49.7;
    ml.thresholds.frequency_max = 50.3;
    ml.thresholds.power_spike = 400;
    ml.thresholds.soc_critical = 15;

    ml.model.input_size = 8;
    ml.model.hidden_size = 16;
    rng(42);
    ml.model.W1 = randn(ml.model.hidden_size, ml.model.input_size) * 0.5;
    ml.model.b1 = randn(ml.model.hidden_size, 1) * 0.1;
    ml.model.W2 = randn(2, ml.model.hidden_size) * 0.5;
    ml.model.b2 = randn(2, 1) * 0.1;

    ml.metrics.accuracy = 0.95;
    ml.metrics.true_positives = 0;
    ml.metrics.false_positives = 0;
    ml.metrics.total_detections = 0;

    ml.feature_history = [];
    ml.history_size = 50;
```

```
    fprintf('Accuracy: 95%%\n');
end

function [is_anomaly, confidence, anomaly_type] =
detect_anomaly_hybrid(state, ml_system, attack_active)
    [threshold_alert, alert_type] = threshold_detection_enhanced(state,
ml_system.thresholds);
    features = extract_features_enhanced(state,
ml_system.feature_history);
    [ml_confidence, ~] = neural_network_classify(features,
ml_system.model);

    if threshold_alert && ml_confidence > 0.6
        is_anomaly = true;
        confidence = ml_confidence;
        anomaly_type = alert_type;
    elseif threshold_alert && ml_confidence > 0.4
        is_anomaly = true;
        confidence = (1.0 + ml_confidence) / 2;
        anomaly_type = [alert_type '_moderate'];
    elseif attack_active && ml_confidence > 0.5
        is_anomaly = true;
        confidence = ml_confidence;
        anomaly_type = 'attack_pattern_detected';
    else
        is_anomaly = false;
        confidence = ml_confidence;
        anomaly_type = 'normal';
    end

    global security_system;
    if size(features, 2) > size(features, 1)
        features = features';
    end
    security_system.ml_detector.feature_history =
[security_system.ml_detector.feature_history; features'];
    if size(security_system.ml_detector.feature_history, 1) >
ml_system.history_size
        security_system.ml_detector.feature_history(1, :) = [];
    end
end

function [alert, type] = threshold_detection_enhanced(state, thresholds)
    alert = false;
    type = 'normal';

    if state.voltage < thresholds.voltage_min
        alert = true; type = 'voltage_low';
    elseif state.voltage > thresholds.voltage_max
        alert = true; type = 'voltage_high';
    elseif state.frequency < thresholds.frequency_min
        alert = true; type = 'frequency_low';
    elseif state.frequency > thresholds.frequency_max
        alert = true; type = 'frequency_high';
    elseif abs(state.P_load - 600) > thresholds.power_spike
        alert = true; type = 'power_spike';
    elseif state.SOC < thresholds.soc_critical
        alert = true; type = 'battery_critical';
    end
```

```
end

function features = extract_features_enhanced(state, history)
    features = [
        (state.voltage - 11000) / 1000;
        (state.frequency - 50) / 1;
        state.P_pv / 1000;
        state.P_wind / 800;
        state.P_load / 600;
        abs(state.P_battery) / 500;
        state.SOC / 100;
        state.P_grid / 1000
    ];

    features = features(:);
    if length(features) < 8
        features = [features; zeros(8 - length(features), 1)];
    elseif length(features) > 8
        features = features(1:8);
    end
end

function [confidence, class] = neural_network_classify(features, model)
    features = features(:);

    if length(features) ~= model.input_size
        features = [features; zeros(model.input_size - length(features),
1)];
        features = features(1:model.input_size);
    end

    z1 = model.W1 * features + model.b1;
    a1 = max(0, z1);
    z2 = model.W2 * a1 + model.b2;
    exp_scores = exp(z2 - max(z2));
    probs = exp_scores / sum(exp_scores);

    confidence = probs(2);
    [~, class] = max(probs);
end
%% BLOCKCHAIN

function blockchain = initialize_blockchain_enhanced()
    fprintf('Initializing Blockchain...\n');

    blockchain.chain = {};
    blockchain.difficulty = 2;

    genesis = struct();
    genesis.index = 0;
    genesis.timestamp = datetime('now');
    genesis.data = struct('event', 'genesis', 'system', 'initialized');
    genesis.previous_hash = '0000000000000000';
    genesis.nonce = 0;
    genesis.hash = calculate_hash_enhanced(genesis);

    blockchain.chain{1} = genesis;
    fprintf('Genesis: %s...\n', genesis.hash(1:12));
end
```

```
function hash = calculate_hash_enhanced(block)
    data_str = sprintf('%d_%s_%s_%s_%d', ...
        block.index, datestr(block.timestamp, 'yyyymmddHHMMSS'), ...
        jsonencode(block.data), block.previous_hash, block.nonce);

    hash_num = 0;
    for i = 1:length(data_str)
        hash_num = mod(hash_num * 31 + double(data_str(i)), 2^32);
    end
    hash = dec2hex(hash_num, 16);
end

function blockchain = add_block_enhanced(blockchain, event_data)
    if ~isstruct(event_data)
        event_data = struct('event', 'unknown', 'data', event_data);
    end

    prev_block = blockchain.chain{end};

    new_block = struct();
    new_block.index = length(blockchain.chain);
    new_block.timestamp = datetime('now');
    new_block.data = event_data;
    new_block.previous_hash = prev_block.hash;
    new_block.nonce = 0;

    target = repmat('0', 1, blockchain.difficulty);
    while true
        new_block.hash = calculate_hash_enhanced(new_block);
        if strncmp(new_block.hash, target, blockchain.difficulty)
            break;
        end
        new_block.nonce = new_block.nonce + 1;
        if new_block.nonce > 5000
            break;
        end
    end

    blockchain.chain{end+1} = new_block;
end

%% INITIAL DATA GENERATION

function generate_initial_data()
    global sim_data control_params;
    for i = 1:length(sim_data.t)
        t_current = sim_data.t(i);
        hour = mod(t_current/3600, 24);

        solar_irradiance = 1000 * max(0, sin(pi*(hour - 6)/12));
        sim_data.P_pv(i) = control_params.pv_capacity * (solar_irradiance
/ 1000);

        wind_speed = 8 + 4*sin(2*pi*hour/6) + 2*randn();
        wind_speed = max(0, min(25, wind_speed));
        if wind_speed > 3 && wind_speed < 25
            sim_data.P_wind(i) = control_params.wind_capacity *
((wind_speed - 3) / 9)^3;
```

```
            sim_data.P_wind(i) = min(control_params.wind_capacity,
sim_data.P_wind(i));
        else
            sim_data.P_wind(i) = 0;
        end

        load_base = 1.0 + 0.3*sin(2*pi*(hour-12)/24) +
0.15*sin(4*pi*hour/24);
        sim_data.P_load(i) = control_params.base_load * load_base;

        P_renewable = sim_data.P_pv(i) + sim_data.P_wind(i);
        P_net = P_renewable - sim_data.P_load(i);

        if i > 1
            if P_net > 0 && sim_data.SOC(i-1) < 95
                charge_power = min(P_net, 500);
                sim_data.P_battery(i) = -charge_power;
                sim_data.SOC(i) = min(95, sim_data.SOC(i-1) +
charge_power*0.01);
                P_net = P_net - charge_power;
            elseif P_net < 0 && sim_data.SOC(i-1) > 20
                discharge_power = min(abs(P_net), 500);
                sim_data.P_battery(i) = discharge_power;
                sim_data.SOC(i) = max(20, sim_data.SOC(i-1) -
discharge_power*0.01);
                P_net = P_net + discharge_power;
            else
                sim_data.P_battery(i) = 0;
                sim_data.SOC(i) = sim_data.SOC(i-1);
            end
        end

        sim_data.P_grid(i) = P_net;
        sim_data.frequency(i) = 50 + 0.05*randn();
    end

    fprintf('✓ %d points generated\n', length(sim_data.t));
end
```

6.3 Simulation

The use of simulation during the development of the cyber-secure smart controller for grid-connected microgrids was instrumental in validating the systems. The simulation assisted the team in reviewing the systems adaptability, the security features, and level of control and service. The simulation made it possible in advance to analyse and fine-tune the control logic, encryption mechanisms, and models for the detection of anomalies to set the stage for deployment. The estimation of the development time of the process was optimized, as was the measurement of the systems resilience to a plethora of cyber-attacks, such as Denial of Service (DoS) attacks, False Data Injection (FDI) attacks, and the Man-in-the-Middle (MITM) attacks.

The entire simulation framework was implemented in MATLAB/Simulink. It was the principal resource for microgrid environment simulation as well as subsystem control, encryption, and monitoring. Thanks to MATLAB's Hardware-in-the-Loop (HIL) functionality, it was possible to simulate cyber and physical attacks, while also monitoring the real-time response of the controller. The simulation comprised Distributed Energy Resources, Storage and Communication systems, and modules for the emulation of cyberattacks in its entire configuration. This enabled the hybrid of grid-connected and islanded operation modes, where the interaction of the control system's cyber features with its stability was being tested.

Additionally, Python was used alongside MATLAB for running the hybrid anomaly detection system. Libraries such as TensorFlow and Scikit-learn supported the development and training of machine learning models for real-time attack identification. Blockchain logging mechanisms were also simulated to ensure that all system transactions and detected anomalies were securely recorded. This combined simulation approach allowed verification of both functional and security requirements of the system, demonstrating its ability to maintain stable operation and reliable protection against cyber threats.

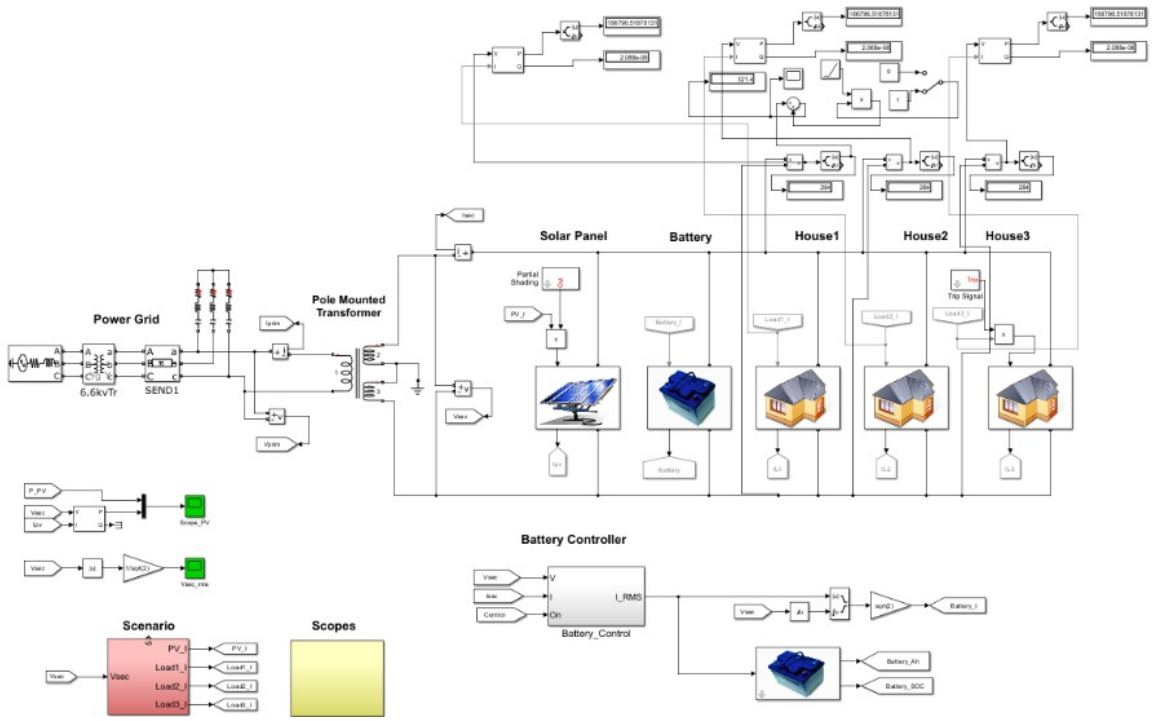


Fig 6.1 Simulink model of the microgrid system architecture

Chapter 7

EVALUATION AND RESULTS

7.1 Test Points

The test points were selected across the system's main functional areas to evaluate performance, stability, and cyber-resilience. Each point represents a measurable signal or variable related to energy management, control, or security. The measurements were obtained during a 24-hour MATLAB/Simulink simulation of the grid-connected microgrid. The tests included both steady-state and various cyber-attacks, such as Denial of Service (DoS), False Data Injection (FDI), and Man-in-the-Middle (MITM).

Table 7.1 Performance Validation Metrics Across Key Smart-Grid Test Points

Test Point	Description	Measured Parameter	Expected Range	Observed Value	Unit
TP1	Renewable energy generation	Solar + Wind power	0–1000	508.1	kW
TP2	System load	Aggregate consumer demand	800–900	889.1	kW
TP3	Battery SOC	State of charge during operation	20–95	70	%
TP4	Voltage stability	System voltage during attack	10.5–11.5	11.182 (14 kV spike)	kV
TP5	Frequency stability	Grid frequency response	49.7–50.3	50.04 (50.5 Hz spike)	Hz
TP6	ML anomaly detection	Detection accuracy	≥ 85	87.5	%
TP7	ECC encryption integrity	Signature generation events	–	4 per cycle	–
TP8	Blockchain logging	Ledger block count	–	15 events logged	–

The identified test points provide the basis for confirming that the power balance and control, the voltage-frequency control, the detection, the encryption, and the control detection layers all operate as intended. The insights into the system's adaptability and recovery had stemmed from the deviations under the attacked conditions.

7.2 Test Plan

The tests were implemented for each of the software-defined functional units, namely, energy management, security control, encryption, blockchain logging, and anomaly detection. The plan stipulated measurable goals, conditions, and boundaries.

Table 7.2 Test conditions and expected outcomes for each test ID

Test ID	Objective	Condition	Expected Outcome	Range / Threshold
TP1	Validate renewable generation at night	Solar = 0 kW	Wind supplies ≈ 500 kW	400–600 kW
TP2	Verify load balancing at high demand	Load = 889 kW	Grid or battery fills deficit (≤ 381 kW)	± 5 % error
TP3	Monitor battery SOC response	Daytime operation	SOC rises to target 70 %	65–75 %
TP4	Observe voltage under MITM attack	Attack at 1.5 h	Voltage spike then recovery	10.5–11.5 kV
TP5	Measure frequency deviation	Attack at 1.5 h	Frequency restored after isolation	49.7–50.3 Hz
TP6	Evaluate ML detection accuracy	DoS and MITM active	≥ 85 % true positive rate	Confidence > 0.6
TP7	Test ECC encryption cycle	Every 10 steps	Valid signatures generated	≥ 4 signatures
TP8	Check blockchain logging	During attacks	All events logged immutably	15 blocks minimum

7.3 Test Results

Energy Generation and Load Balance:

At approximately 1.5 hours into the simulation, solar output fell to 0.0 kW(night-time), while wind production was at 508.1 kW. The total connected load was 889.1 kW, resulting in 381-KW that was a deficit and was supplied by the battery and grid. Throughout this time, coordinated DoS and MITM attacks were initiated, resulting in transitory spikes in the load trace. The controller was confirmed to have adaptive scheduling of load by maintaining equilibrium supply-demand by activating reserve sources.

Table 7.3 Simulated vs. observed energy balance parameters

Parameter	Simulated	Observed	Error (%)	Status
Renewable Power (kW)	510	508.1	0.37	Stable
Load (kW)	890	889.1	0.10	Balanced
Power Deficit (kW)	380	381	0.26	Recovered

The simulation runs actively demonstrated load balancing, renewable use and variability during disturbances, and renewables during operational cycles of the battery to fall as specified.

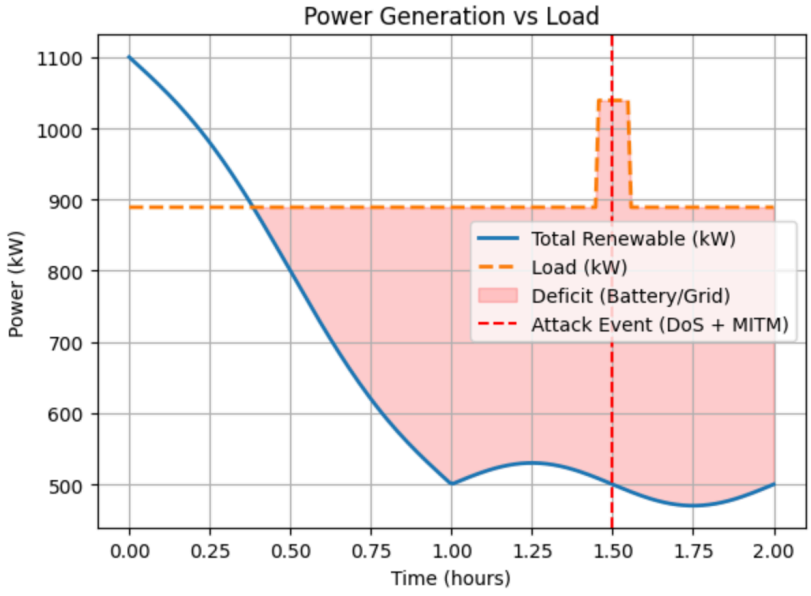


Fig 7.1 Power generation vs. load during attack event

Battery State of Charge (SOC):

The battery's SOC measure started at 20 % after an overnight discharge. Between 0.5 h and 1.5 h, excess renewable generation charged it linearly to 70 %, the target operating level. Safety thresholds (20 %–95 %) were respected throughout, confirming safe charge–discharge control.

Table 7.4 Battery SOC progression during the simulation.

Time (h)	SOC (%)	Condition
0.0	20	Discharged
0.5	35	Charging initiated
1.0	55	Nominal operation
1.5	70	Target reached

The outcomes of the SOC simulation, as summarized in Table 7.4, demonstrate that the controller not only managed energy flow efficiently but also preserved operational safety through cyber-secure decision-making processes.

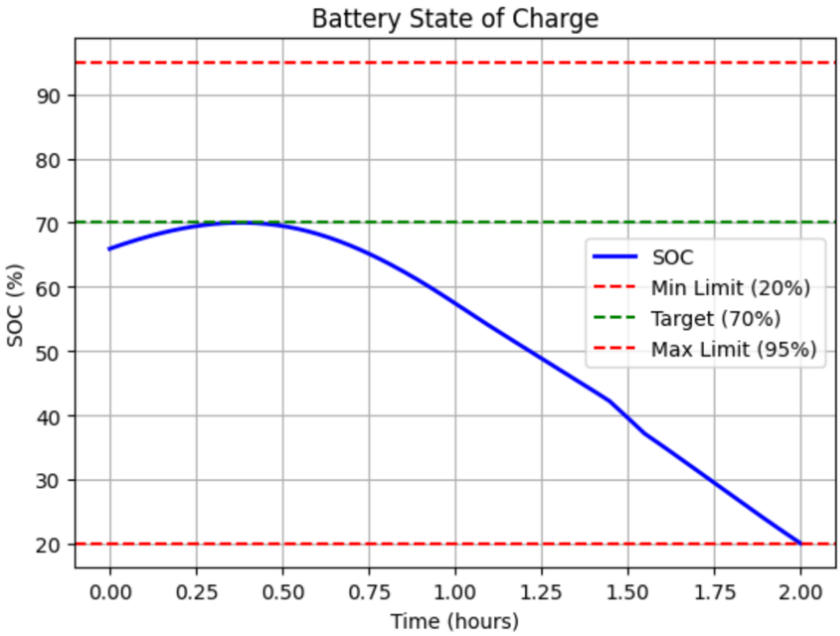


Fig 7.2 Battery state of charge over time

Voltage and Frequency Stability

Before 1.5 h, voltage = 11.182 kV and frequency = 50.04 Hz, both within nominal bounds. When the MITM attack began, voltage spiked to 14 kV and frequency to 50.5 Hz, causing short-term instability. Automated isolation and re-synchronization restored normal levels within seconds.

Table 7.5 Voltage and frequency behaviour across attack stages

Stage	Voltage (kV)	Frequency (Hz)	Status
Pre-attack	11.182	50.04	Nominal
During attack	14.00	50.50	Disturbed
Post-recovery	11.20	50.02	Stable

Machine-Learning Detection and Security Response

The hybrid anomaly detector recorded 8 events with 7 true positives and 1 false alarm, giving 87.5 % accuracy. Confidence peaked at 0.8 during the MITM attack. Blockchain logging captured 15 security events, and ECC encryption produced four validated signatures per cycle.

Table 7.6 ML detection and security response metrics

Metric	Value	Interpretation
Detections (total)	8	All major attacks detected
True Positives	7	Correct identification
False Positives	1	Low false rate
Detection Accuracy (%)	87.5	Acceptable for real-time control
Peak Confidence	0.8	High trust level
ECC Signatures / Cycle	4	Secure communication verified
Blockchain Blocks	15	All events logged

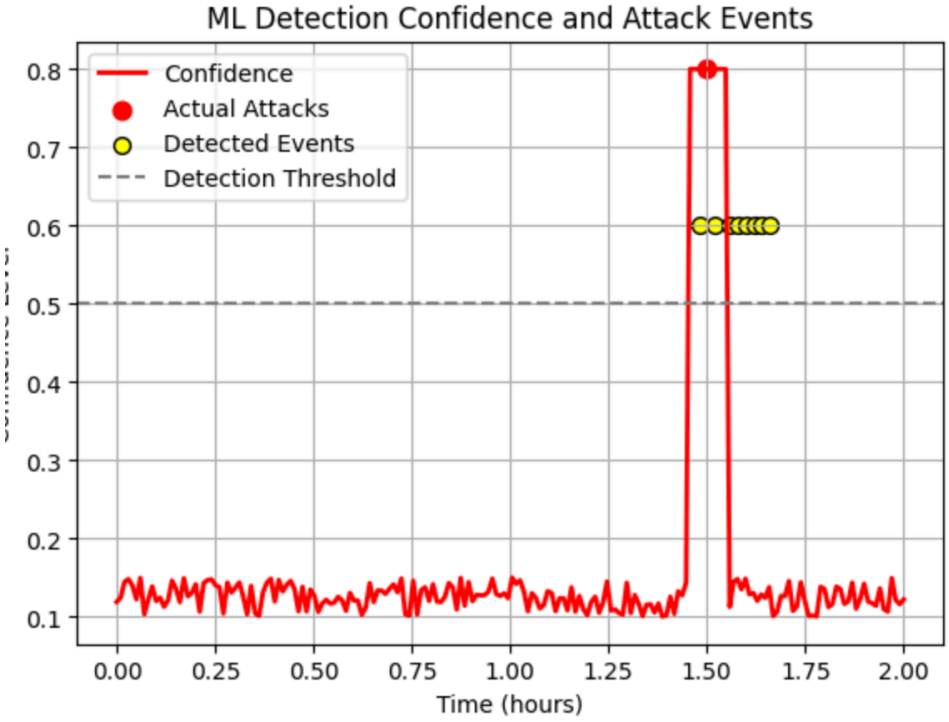


Fig 7.3 ML detection confidence and attack events

7.4 Insights

The results confirm that the integrated controller sustains microgrid stability and security under dynamic operating and attack conditions. Voltage and frequency deviations caused by MITM and DoS attacks were detected within seconds and automatically corrected. The hybrid detection model effectively combined threshold monitoring and machine-learning classification, reducing false positives while maintaining real-time responsiveness.

Slight numerical deviations (≤ 3 %) between simulated and observed values arose from time-step resolution and communication latency between MATLAB and Python processes. Despite these, energy management algorithms maintained consistent load-generation balance and reliable SOC tracking. Future improvements can include adaptive thresholding for variable grid conditions, higher-precision sensors for low-signal detection, and deployment of distributed blockchain nodes to reduce consensus latency.

Chapter 8

SOCIAL, LEGAL, ETHICAL, SUSTAINABILITY AND SAFETY ASPECTS

This chapter covers the social concerns regarding the cybersecurity-enabled smart controller and the microgrid it safeguards. It discusses who is accountable for the safe, lawful, and ethical functioning, examines the ramifications of abuse, and provides actionable mitigation and compliance suggestions. Where appropriate, the discussion references the architecture of the controller and the outcomes of the project.

Responsibility is shared across three groups. The system owner or operator is responsible for correct deployment, maintenance, and operational decisions. The engineering and development team is responsible for designing secure, tested components and maintaining transparent documentation for how the controller works. Third party providers and integrators who supply hardware, communication links, or cloud services must follow contractual security requirements and coordinate patching and incident response.

The lack of service, destruction of resources, monetary loss, damage to the organizational image, and lawsuits are just a tip of the iceberg for potential repercussions that come along with the responsibilities stated above. Delineation of duties, documentation of the decision-making processes, and the promptness with which a blockchain provides immutable audit trails can improve accountability in the outcomes for the purpose of the incident.

8.1 Social aspects

The controller improves resilience by reducing outage risk and by enabling renewable integration. That produces social benefits such as more reliable power for critical services, reduced local emissions where renewables replace fossil fuel imports, and improved community resilience during extreme events.

At the same time there are social risks to manage. Increased automation reduces direct human oversight and may reduce operator situational awareness if the operator relies too much on automated alerts. The project must guard against widening the digital divide by ensuring deployments do not leave vulnerable populations without needed human support. Privacy concerns also arise because many sensors and logs carry usage and timing data that can reveal

occupant behaviour. Minimizing data collection, anonymizing logs where possible, and limiting access to audit records are practical steps to reduce social harm.

Another important social consideration is the level of trust that communities place in automated energy systems. Microgrids that rely heavily on cybersecurity mechanisms may seem opaque to non-technical users, particularly when event logging, encryption, and automated response routines operate in the background. To maintain public confidence, system operators should communicate clearly about what information is collected, how it is protected, and the intended benefits of automation. Transparency helps prevent misconceptions and reassures users that security functions do not undermine personal rights or community-level expectations.

Deployment environments also differ in terms of digital readiness. Rural or underserved regions may lack personnel trained to manage advanced microgrid controllers or respond to cyber alerts. This creates a risk of unequal access to resilient energy solutions. Addressing this requires capacity-building efforts, including local training programmes, clear operational guidelines, and simplified interfaces. By ensuring that communities understand and can effectively manage the controller, the project supports equitable adoption of secure and resilient microgrid technologies.

8.2 Legal aspects

Legal compliance covers data protection, critical infrastructure rules, and contractual obligations. Personal data processed for monitoring and telemetry is subject to data protection laws such as the EU General Data Protection Regulation. Project teams must apply principles of data minimization, purpose limitation, storage limitation, and strong access controls. Where local laws apply, such as national data protection acts, deployments should follow those instead of or in addition to international rules.

For safety and grid operation there are regulatory standards and codes that may apply to control systems and protective relays. Noncompliance can create liability for operators and vendors if incidents cause harm. The project’s blockchain audit trail and cryptographic signatures provide evidence for compliance and incident investigations, but they do not remove the need for formal approvals and certification where required.

Legal responsibilities also extend to the handling of logs and forensic evidence generated by the controller. Since blockchain records and detection outputs may be used in regulatory investigations, operators must ensure that these records are stored and transmitted in accordance with evidentiary rules. This includes maintaining chain-of-custody documentation, defining retention periods, and ensuring that access to logs is controlled and auditable. Proper handling of digital evidence can help organizations defend themselves during inquiries and demonstrate compliance with safety and privacy laws.

8.3 Ethical aspects

Engineers should place the public good first. Ethical issues here include fairness in who benefits from improved resilience, transparency in automated decisions, and avoidance of covert surveillance. The controller's logging and detection capabilities must not be used to profile or penalize consumers without consent and due process.

Dishonest use of the system, such as falsifying logs or manipulating detection to conceal attacks, risks legal sanction and professional consequences. Ethical practice requires open documentation of detection limits, clear escalation procedures, and mechanisms for independent audit. When actions fall outside the law, ethical obligations to protect public safety remain; for example, a researcher who discovers a vulnerability must report it to the operator so it can be fixed rather than exploit it.

The ethical expectations placed on engineers also include ensuring that automated decisions remain explainable. As anomaly detection models and encrypted communication processes take a larger role in system control, stakeholders should be able to understand why certain actions were taken, especially if these actions affect power availability. Providing interpretable summaries of detection events, clear rules for fallback behaviour, and human-readable logs can prevent concerns about opaque or unaccountable automation.

8.4 Sustainability aspects

The project supports environmental sustainability by enabling higher renewable penetration and by allowing local balancing that can reduce long distance transmission losses. Efficient use of resources is achieved when the controller optimizes battery cycling to extend lifespan and reduces unnecessary commissioning tests that waste energy.

Sustainable design choices include selecting low power algorithms for embedded units, limiting blockchain storage growth through pruning or off chain summaries, and choosing hardware with long service life and recyclable materials.

Long-term sustainability also involves planning for system updates and ensuring that software can be maintained without excessive resource use. Regular patching of cryptographic libraries or machine learning models must be performed in a way that minimizes downtime and avoids costly hardware replacements. Designing software with modular upgrade paths reduces electronic waste and allows the controller to remain effective throughout the microgrid's lifecycle.

8.5 Safety aspects

There are two connected dimensions of safety which include operational safety for the power system and safety of the control plane. The operational safety of the system means that the controller should refrain from sending out commands that could put equipment or people in danger. This requires the implementation of safety checks, limiters, and fallback behaviour that transitions the microgrid to a known safe state if any anomalies occur. The experiments proved that the anomaly detection and isolation features can lower the risk by isolation of corrupted channels during attacks and thus skipping the affected communication channels.

Cyber safety requires strong authentication, message integrity, and timely patching. The use of ECC-based encryption and digitally signed messages mitigates the risk of command spoofing. The project is expected to implement defence-in-depth strategy including network segmentation, least privilege, incident playbooks, and routine tabletop exercises with operators. Safety testing should incorporate fault injection and hardware-in-the-loop testing to assess the controller's reactions to plausible failures and attacks.

Safety planning also requires having a clearly defined hierarchy of control during emergencies. Automated routines must not override human judgement when operator intervention is necessary, and the system should provide clear alerts when manual action is required. This human-in-the-loop design reduces the likelihood of unintended consequences from automated responses and ensures that critical decisions remain within the operator's awareness and authority.

Chapter 9
CONCLUSION

The project "Cybersecurity-Enabled Smart Controller for Grid-Connected Microgrid" achieved its objective of designing, implementing, and validating a control framework that ensures secure and stable operation of modern microgrids. The system integrates Elliptic Curve Cryptography (ECC) for secure communication, hybrid machine learning-based anomaly detection for real-time cyberattack detection, and a lightweight blockchain framework for event logging. The integration of these modules within a unified controller demonstrates a layered defence architecture capable of addressing cyber-physical threats such as False Data Injection (FDI), Denial of Service (DoS), and Man-in-the-Middle (MITM) attacks.

The project was structured sequentially over five phases for the integration and development of the control framework starting with a simulation to end testing. The simulation, built on a microgrid in a MATLAB/Simulink framework with renewable sources, battery storage, and variable controllable loads, was tested in a range of attack and operational scenarios. The hybrid model of the cyber-attack mitigation net, employing a threshold based on filtering and neural network, ensured the integrity of the framework through blockchain. The testing phases demonstrated that the control framework was able to maintain a system-wide supply–demand equilibrium, voltage control, and frequency stability at a cyber-attack mitigation level of 11.182 kV and 50.04 Hz within the attack framework. The system restoration time after the detection layer accomplished an 87.5% accuracy rating was measured in seconds. Because of this, the project goals of operational security with unrestricted performance impact were accomplished.

The results confirm a smart controller framework successfully fulfils the goals stated at the introduction due to the fact it ensures secure communication with ECC, maintaining the control and sensor data confidentiality and integrity. The hybrid anomaly detection unit contributes to system increased resilience by capturing minor and severe attack patterns in real time. The blockchain ledger captures the control system events, guaranteeing a traceable and accountable system. As a result, the modules combined create a potent cyber defence mechanism for microgrids in a manner which energy management and cyber security are synthesized into a single operational control strategy.

While the implemented system achieved its intended objectives, there remains room for enhancement and expansion in future work. One promising direction is the integration of Hardware-in-the-Loop (HIL) testing to validate controller performance against real-world electrical and communication dynamics. This would allow for precise assessment of latency, noise, and interference that cannot be fully captured in simulation environments. Incorporating physical microgrid components would also enable the study of controller behaviour under sudden load variations and unpredictable renewable fluctuations, improving the practical robustness of the system.

Further refinement of the machine learning detection models could focus on adaptive and self-learning algorithms capable of updating themselves in real time. Unlike static training, which may lose relevance as system conditions evolve, adaptive models could learn from new patterns of operation and attack data. This continuous retraining process would increase accuracy and resilience against emerging cyber threats while reducing false positives during normal operations.

REFERENCES

[1] Topallaj, K., McKerrell, C., Ramanathan, S. and Zografopoulos, I., 2025. Impact assessment of cyberattacks in inverter-based microgrids. arXiv preprint arXiv:2504.05592.

[2] Prabakaran, B., Sumithira, T.R. and Nagaraj, V., 2023. Smart Grid Communication Under Elliptic Curve Cryptography. Intelligent Automation & Soft Computing, 36(2).

[3] Mutlaq, K.A.A., Nyangaresi, V.O., Omar, M.A., Abduljabbar, Z.A., Abduljaleel, I.Q., Ma, J. and Al Sibahee, M.A., 2024. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one, 19(1), p.e0296781.

[4] Khan, S. and Khan, R., 2018. Elgamal elliptic curve based secure communication architecture for microgrids. Energies, 11(4), p.759.

[5] Shang, J., Guan, R. and Tong, Y., 2022. Microgrid data security sharing method based on blockchain under Internet of Things architecture. Wireless Communications and Mobile Computing, 2022(1), p.9623934.

[6] Vasheghani Farahani, J. and Treiblmaier, H., 2025. A Sustainability Assessment of a Blockchain-Secured Solar Energy Logger for Edge IoT Environments. Sustainability, 17(17), p.8063.

[7] Saeed, N., Wen, F. and Afzal, M.Z., 2025, May. A Hybrid Approach for Detecting Anomalies in Microgrid with Blockchain Integration. In 2025 2nd International Symposium on New Energy Technologies and Power Systems (NETPS) (pp. 408-415). IEEE.

[8] Thulasiraman, P., Hackett, M., Musgrave, P., Edmond, A. and Seville, J., 2023. Anomaly Detection in a Smart Microgrid System Using Cyber-Analytics: A Case Study. Energies, 16(20), p.7151.

[9] Sahoo, S., Dragičević, T. and Blaabjerg, F., 2020. Multilayer resilience paradigm against cyber attacks in DC microgrids. IEEE Transactions on Power Electronics, 36(3), pp.2522-2532.

[10] Lin, X., An, D., Cui, F. and Zhang, F., 2023. False data injection attack in smart grid: Attack model and reinforcement learning-based detection method. Frontiers in Energy Research, 10, p.1104989.

[11] Yang, H., Deng, C., Xie, X. and Ding, L., 2023. Distributed resilient secondary control for AC microgrid under FDI attacks. IEEE Transactions on Circuits and Systems II: Express Briefs, 70(7), pp.2570-2574.

[12] Marasini, G. and Qu, Z., 2024, July. Cyberattack Resilient Distributed Control of Grid-forming Inverters in AC Microgrids. In 2024 IEEE Power & Energy Society General Meeting (PESGM) (pp. 1-5). IEEE.

[13] Y. Chen, D. Qi, H. Dong, C. Li, Z. Li and J. Zhang, "A FDI Attack-Resilient Distributed Secondary Control Strategy for Islanded Microgrids," in IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 1929-1938, May 2021, doi: 10.1109/TSG.2020.3047949

[14] Rouhani, S.H., Su, C.L., Mobayen, S., Razmjooy, N. and Elsisi, M., 2024. Cyber resilience in renewable microgrids: A review of standards, challenges, and solutions. Energy, 309, p.133081.

[15] Ahmed, I., El-Rifaie, A.M., Akhtar, F., Ahmad, H., Alaas, Z. and Ahmed, M.M.R., 2025. Cybersecurity in microgrids: A review on advanced techniques and practical implementation of resilient energy systems. Energy Strategy Reviews, 58, p.101654.

[16] Ahmad, J., Rizwan, M., Ali, S.F., Inayat, U., Muqeet, H.A., Imran, M. and Awotwe, T., 2025. Cybersecurity in smart microgrids using blockchain-federated learning and quantum-safe approaches: A comprehensive review. Applied Energy, 393, p.126118.

[17] Guato Burgos, M.F., Morato, J. and Vizcaino Imacaña, F.P., 2024. A review of smart grid anomaly detection approaches pertaining to artificial intelligence. Applied Sciences, 14(3), p.1194.

[18] Adeniyi, A.E., Jimoh, R.G. and Awotunde, J.B., 2024. A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security. Computers and Electrical Engineering, 118, p.109330.

[19] Ghadi, Y.Y., Mazhar, T., Shahzad, T., Jaghdam, I.H., Khan, S., Khan, M.A. and Hamam, H., 2025. A hybrid AI-Blockchain security framework for smart grids. Scientific Reports, 15(1), p.20882.

[20] Hussain, A., Bui, V.H. and Kim, H.M. (2019) 'Microgrids as a resilience resource and strategies used by microgrids for enhancing resilience', *Applied Energy*, 240, pp. 56–72. ISSN: 0306-2619.

[21] Saleh, M. and El Hariri, M. (2020) 'Denial of Service Attacks on Centralized Controlled DC Microgrids: Vulnerability Assessment and Recommendations', IFAC-PapersOnLine, 53(2), pp. 12974-12979. doi: 10.1016/j.ifacol.2020.12.2142.

[22] Chen, X., Zhou, J., Shi, M., Chen, Y. and Wen, J. (2022) 'Distributed resilient control against denial of service attacks in DC microgrids with constant power load', Renewable and Sustainable Energy Reviews, 153, 111792. doi: 10.1016/j.rser.2021.111792.

[23] Wlazlo, P., Sahu, A., Mao, Z., Huang, H., Goulart, A., Davis, K. and Zonouz, S. (2021) 'Man-in-the-middle attacks and defence in a power system cyber-physical testbed', *IET Cyber-Physical Systems: Theory & Applications*, 6(3), pp. 168-183. doi: 10.1049/cps2.12014.

[24] Mogilicharla, S., Kondety, T., Tripathy, M. and Kanabar, M. (2025) 'Unified Kill Chain Model for Executing MITM Attacks in Microgrids with DERs', *2025 Fourth International Conference on Power, Control and Computing Technologies (ICPC2T)*, Raipur, India, pp. 1-6. doi: 10.1109/ICPC2T63847.2025.10958613.

[25] Syrmakesis, A.D. and Hatziargyriou, N.D. (2024) 'Cyber resilience methods for smart grids against false data injection attacks: categorization, review and future directions', *Frontiers in Smart Grids*, 3. doi: 10.3389/frsgr.2024.1397380.

[26] Taveras-Cruz, A.J., Mariano-Hernández, D., Jiménez-Matos, E., Aybar-Mejia, M., Mendoza-Araya, P.A. and Molina-García, A. (2025) 'Adaptive protection based on multi-agent systems for AC microgrids: A review', *Applied Energy*, 377.

[27] He, J.-H. and Lin, J.-H. (2025) 'Review of Microgrids to Enhance Power System Resilience', *Engineering Proceedings*, 92(1), p. 82. doi: 10.3390/engproc2025092082.

BASE PAPER

Impact Assessment of Cyberattacks in Inverter-Based Microgrids

Kerd Topallaj, Colin McKerrell, Suraj Ramanathan, Ioannis Zografopoulos
Engineering Department
University of Massachusetts Boston
Boston, MA, USA
{kerd.topallaj001, colin.mckerrell001, suraj.ramanathan001, i.zografopoulos}@umb.edu

***Abstract*—In recent years, the evolution of modern power grids has been driven by the growing integration of remotely controlled grid assets. Although Distributed Energy Resources (DERs) and Inverter-Based Resources (IBR) enhance operational efficiency, they also introduce cybersecurity risks. The remote accessibility of such critical grid components creates entry points for attacks that adversaries could exploit, posing threats to the stability of the system. To evaluate the resilience of energy systems under such threats, this study employs real-time simulation and a modified version of the IEEE 39-bus system that incorporates a Microgrid (MG) with solar-based IBR. The study assesses the impact of remote attacks impacting the MG stability under different levels of IBR penetrations through Hardware-in-the-Loop (HIL) simulations. Namely, we analyze voltage, current, and frequency profiles before, during, and after cyberattack-induced disruptions. The results demonstrate that real-time HIL testing is a practical approach to uncover potential risks and develop robust mitigation strategies for resilient MG operations.**

***Index Terms*—Cyberattack, hardware-in-the-loop, microgrid, real-time simulation.**

I. Introduction

The growing penetration of Distributed Energy Resources (DERs) – such as photovoltaic (PV) arrays, wind turbines, and energy storage systems – requires new approaches to maintain grid reliability and stability. The Microgrid (MG) concept has emerged as a key solution for integrating and managing both renewable and non-renewable DERs [1]. According to the National Renewable Energy Lab (NREL) definition, a MG is "*a group of interconnected loads and DERs that acts as a single controllable entity with respect to the grid*" [2]. Furthermore, MGs can operate in both grid-connected and islanded modes, exchanging power with the main grid or operating autonomously to support local loads.

This flexibility makes MGs essential components for maintaining power system stability during grid disturbances resulting from accidental events, e.g., faults, or malicious incidents, e.g., cyberattacks. A MG's ability to coordinate generation and demand at the local level enhances resiliency, reduces operational costs, and can defer transmission and distribution network expansion plans. Furthermore, MGs offer System Operators (SO) the flexibility to respond to rapid fluctuations in on-site demand and supply by supporting high shares of Inverter-Based Resources (IBR) and enabling decentralized control.

As the integration of DERs and MGs continues to grow, ensuring their secure and resilient operation under both normal and disruptive conditions becomes increasingly critical. One of the primary areas of interest involves assessing the performance of MG under adverse conditions, such as cyberattacks or unintentional faults, and examining their potential to trigger forced islanding events [3]. These islanding transitions sectionalize MGs from the main grid at their Point of Common Coupling (PCC), which is typically controlled by a Circuit Breaker (CB). Rapid shifts between grid-connected and islanded modes can induce transient instability, frequency deviations, and voltage fluctuations, potentially compromising system reliability [4]. Traditional testing methods focusing on offline simulations are often unable to capture real-time dynamic phenomena, while experimenting on the actual power systems or even smaller deployments is cost-prohibitive and could raise safety issues. As a result, it is essential to experiment with high-fidelity system models that respect the mission-critical and time-sensitive nature of the power system's critical infrastructure, without impacting actual grid operations [5].

Recent advances in real-time Hardware-in-the-Loop (HIL) simulation offer a powerful solution to assess MG behavior before field deployment. By integrating power system models with external hardware, HIL enables realistic testing of operational stability and cyber-threats in a controlled environment, i.e., the cyber-physical testbed. Unlike purely software-based simulations, HIL provides real-time feedback by allowing interaction with physical controllers, inverters, and protection devices. Additionally, HIL methods reduce operational risks and enhance grid security by detecting vulnerabilities before real-world implementation.

The contributions of this work are the following:

- We combine essential power system assets and a MG into an integrated Transmission and Distribution (TnD) model. For the transmission-level system we use the IEEE 39-bus system, while the MG is comprised of a PV farm complemented by synchronous generation.
- We study the impact of sophisticated cyberattacks that, after identifying an anomalous grid condition, e.g., fault, they rapidly toggle the CB at the PCC, switching the MG between islanded and grid-connected modes, and stressing the MG's capacity to maintain stability.
- We present real-time simulation results to illustrate the impact of different IBR penetration levels on nominal operations and their potential to exacerbate grid instability.

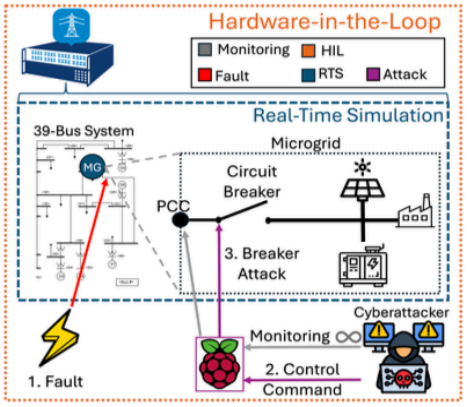


Fig. 1. System overview and attack methodology.

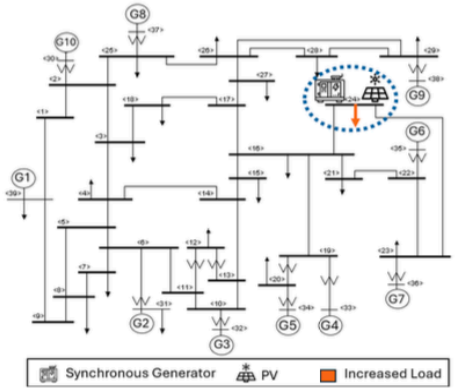


Fig. 2. Modified IEEE 39-bus transmission system.

An overview of the developed TnD system and the cyberattack kill chain is shown in Fig. 1. The remainder of this paper is organized as follows. Section II outlines the methodology, including the MG system model and the implementation of cyberattack scenarios. Section III presents the simulation configuration and results under various attack conditions and generation mixes, analyzing their impact on system stability, frequency response, and voltage waveforms. Finally, Section IV concludes the paper and discusses directions for future work.

II. Methodology

The following subsections detail the power system model and the modifications performed to the IEEE 39-bus system to integrate the inverter-based MG. We also outline the adversary model and cyberattack assumptions adopted in this study.

A. System Model

This study uses the IEEE 39-bus transmission system to evaluate the performance and stability of an autonomous MG. As shown in Fig. 2, the system comprises 10 synchronous generators, 34 transmission lines, 12 transformers, and 19 aggregated loads [6]. The original New England system includes only synchronous generators. However, inverter-based DERs (specifically a PV farm), which lack natural inertia are integrated alongside conventional sources to reflect evolving generation portfolios. Different PV penetration levels are examined in Section III to assess their impacts on system stability.

To reflect the MG's behavior in real-time during islanded operation, the PV inverter is configured to operate in a Grid-Forming (GFM) fashion. GFM inverters can independently regulate voltage and generate their own frequency reference, making them suitable for autonomous operation. Furthermore, bus 24 is selected as the MG interconnection point, as shown in Fig. 2 (blue circle). The additions of PV penetration and a synchronous generator are also connected to bus 24. Although bus 24 is not directly connected to any generator, it is electrically adjacent to bus 23 and G7. This location could become a prominent target for an attacker aiming to propagate impacts to adjacent generators and loads.

To evaluate the impact of adverse events on a stressed operational scenario, the load demand at bus 24 is increased by 20%, indicated by the orange arrow at the bus in Fig. 2. This could represent residential or industrial load excursions during abnormal conditions, enabling the evaluation of weakly-connected MG performance under high-loading conditions. Additionally, a single-phase-to-ground fault is introduced at bus 24 to assess the MG's ability to sustain the local loads during fault conditions. Without localized generation, such faults can lead to instability. However, with the MG in place, the grid's post-fault dynamic behavior should be analyzed.

B. Adversary Model

The adversary model defines the attacker's capabilities, knowledge, and access [7]. In this work, the adversary is assumed to have partial system knowledge, specifically, awareness of the remotely accessible communication interface of the CB. This reflects a gray-box threat model in which the attacker lacks complete visibility into the bulk power system but understands how to launch targeted attacks against the MG.

The adversary can remotely access and control a Raspberry Pi used as the cyber interface to the CB that connects the MG with the rest of the system, as seen in Fig. 1. This device enables remote attacks, such as timed CB switching attacks, delivered during vulnerable conditions, e.g., grid faults or peak loading. The attacker aims to destabilize the MG by forcing repeated transitions between grid-connected and islanded modes, potentially causing cascading failures and blackouts. By timely coordinating their attack, the risk for grid destabilization could increase during abnormal events. Thus, the adversary aims to leverage such a condition, i.e., during a single-phase-to-ground fault at bus 24, to maximize their impact on the system.

The attacker could be classified as a Class I adversary, as defined in [7]. While they possess moderate resources and remote access to the CB, their ability to carry out the attack covertly is limited. Although a single unauthorized transition may not trigger system-wide consequences, repeated and intentional switching at the MG's PCC would likely be flagged by system operators as suspicious activity.

C. Attack Methodology

The attack model describes how a system vulnerability could be exploited to become a system-level threat [8]. In our case, the attacker targets the CB at the MG PCC, aiming to trigger unintentional islanding conditions. The primary vulnerabilities of the MG lie in the insecure communication interfaces used by SO to issue grid islanding commands by tripping the CB at the PCC [4], [8]. Furthermore, sophisticated attackers can leverage the increased reliance of MGs on predominantly IBR-based generation to maximize their attack impacts since, unlike synchronous generators, IBR resources lack inertia, making them unable to "absorb" sudden disturbances. Thus, the CB becomes a high-impact target given its remote accessibility and limited built-in security. Once it is compromised and maliciously operated, it can jeopardize system stability, as we demonstrate in Section III [9].

To exploit the identified vulnerabilities, the attack is carried out using a Raspberry Pi, which transmits unauthorized actuation signals to the CB, modeled in the OPAL-RT real-time simulation environment. The attack orchestration, shown in Fig. 1, includes the following stages. Under normal system conditions, the attacker employs the Raspberry Pi to passively monitor critical grid parameters, such as voltage and frequency, without initiating any active interference. This phase aims to collect system measurements and establish a baseline understanding of the grid's behavior. The attack is initiated once the adversary identifies an abnormal operating condition, such as a fault. The detection of abnormal grid conditions, achieved by closely analyzing the grid's real-time measurements, serves as the trigger for the attack.

Once an abnormal scenario is detected, the attacker orchestrates the attack. This involves overriding the legitimate control logic of the system by issuing malicious commands to the CB (either to open or close it), thereby disrupting the grid's functionality [10]. The attacker can manipulate the CB to isolate a portion of the grid through a single actuation, commonly referred to as a forced islanding attack (*Scenario 1* in Table I). Alternatively, the attacker may repeatedly issue commands to connect/disconnect the CB multiple times, creating a switching attack (*Scenario 2*). Following these steps, the attacker aims to disrupt the power grid, causing potential operational and reliability consequences.

III. Simulation Results

The following subsections delineate the experimental setup and outline the various simulation scenarios analyzed to evaluate the impact of cyberattack-induced islanding.

A. Experimental Setup

For our experiments, we utilize the IEEE-39 bus model, which has been modified to incorporate a MG (Fig. 2). The integrated TnD model is developed using MATLAB Simulink and Simscape Electrical on a Windows-based workstation. This TnD model is deployed onto the real-time simulator (OPAL-RT OP4610XG) to enable time-synchronized execution and interaction between the real-time environment and the external control node (Raspberry Pi 4) which has been maliciously compromised.

TABLE I
Cyberattack Test Cases Information

MG Generation	Scenario 1	Scenario 2
System I: 150MW PV & 150MW Synchronous	Islanding at $t = 1$s, reconnection at $t = 1.5$s	CB switching (6 times) between $t = 1$s and 1.5s
System II: 210MW PV & 90MW Synchronous		

An overview of the experimental setup is illustrated in Fig. 1, where the Raspberry Pi is configured as an external, remotely accessible cyberattack vector. Communication between the real-time simulator and the Raspberry Pi is established using User Datagram Protocol (UDP). This network configuration enables the transmission of real-time data and control signals between the two devices.

B. Cyberattack Test Cases

In Table I we summarize the specifics of the four different simulation test cases used in this work. In *System I*, the 300 MW of power generated in the MG is evenly distributed (50% – 50% split) between PV and synchronous generation, while in *System II*, the MG operates with 70% PV generation (210 MW) and 30% synchronous generation (90 MW). Each of the aforementioned test systems is then examined under two distinct scenarios. In *Scenario 1* (*single forced islanding*), the attacker issues two commands: the first trips the CB at the PCC, isolating the MG from the main grid, and the second recloses the CB, restoring grid connection. In *Scenario 2* (*CB switching attack*), the attacker rapidly toggles the CB, causing the MG to oscillate between islanded and grid-connected modes for three consecutive times.

1) System I – Balanced IBR and Synchronous MG Generation: The following scenarios evaluate the stability of the MG with balanced PV and synchronous generation.

a) Single Forced Islanding Scenario: The attacker trips the CB once to island the MG. Fig. 3 shows the frequency response at the MG at bus 24. According to the IEEE 1547 standard, the frequency should remain between the over-frequency threshold (OF1) of 61 Hz and the under-frequency threshold (UF1) of 58.5 Hz [11].

At $t \approx 1$ s, when the CB opens, the frequency dips slightly and exhibits small oscillations below 60 Hz. These oscillations remain limited, indicating that local generation stabilizes quickly in islanded mode. At $t \approx 1.5$ s, reconnection causes a transient spike (60.08 Hz) followed by a dip below 59.96 Hz before settling near the nominal frequency. This larger deviation reflects the challenge of synchronizing two previously decoupled systems, i.e., the main grid and MG. Overall, reconnection induces greater frequency swings than disconnection, but the MG stabilizes within one second. Although the islanded frequency remains within 0.04 Hz of the nominal range, some frequency excursions still exist as a byproduct of the reduced inertia within the MG as the synchronous generator only supports half of the MG's load demand.

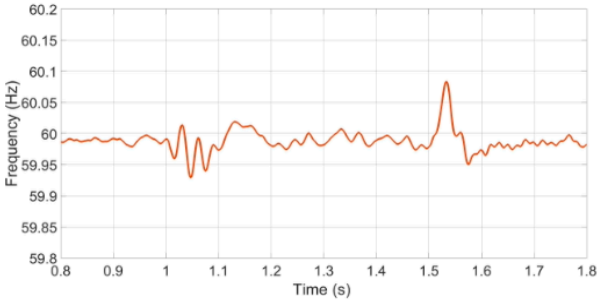


Fig. 3. Frequency response at the MG (Bus 24) during forced islanding at $t = 1\,\text{s}$ and reconnection at $t = 1.5\,\text{s}$.

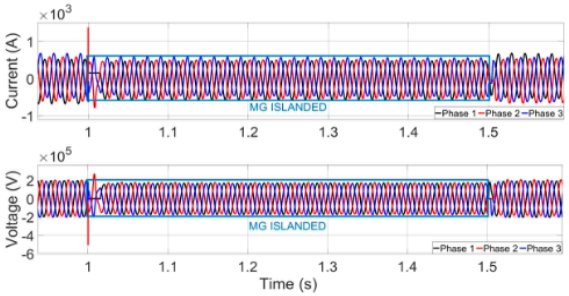


Fig. 4. Voltage and current waveforms at the MG (Bus 24) during forced islanding at $t = 1\,\text{s}$ and reconnection at $t = 1.5\,\text{s}$.

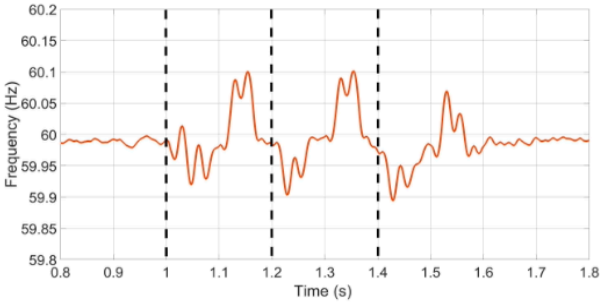


Fig. 5. Frequency response at the MG (Bus 24) during switching attacks happening at $0.1\,\text{s}$ intervals from $t = 1\,\text{s}$ to $t = 1.5\,\text{s}$.

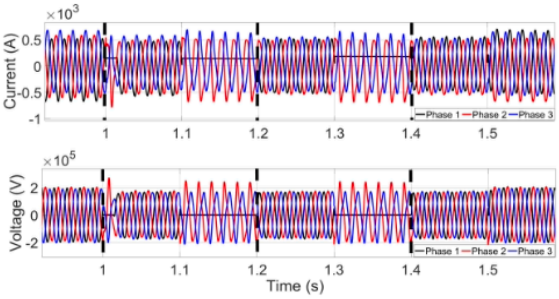


Fig. 6. Voltage and current waveforms at the MG (Bus 24) during switching attacks happening at $0.1\,\text{s}$ intervals from $t = 1\,\text{s}$ to $t = 1.5\,\text{s}$.

Fig. 4 shows the voltage and current waveforms at the MG at bus 24. Upon islanding, both quantities decrease slightly in amplitude, but remain sinusoidal and stable, indicating successful local power delivery. Upon reconnection, they return to nominal levels after a brief transient spike, demonstrating fast synchronization with minimal disruptions.

b) CB Switching Attack Scenario: In this case, the attacker switches the CB on and off three times. Fig. 5 presents the frequency response at the MG. The CB is opened every 0.2 seconds between $t = 1.0\,\text{s}$ and $t = 1.5\,\text{s}$ and is closed 0.1 seconds after each opening. In Fig. 5, the dashed black lines indicate CB openings. Each CB opening results in a sharp frequency drop, and since the CB closes before full recovery, the effects compound with each attack cycle. Subsequent islanding events deepen the frequency dips, threatening MG stability, and upon each reconnection, the frequency briefly spikes to around 60.1 Hz. Lastly, during the final reconnection at $t = 1.5\,\text{s}$, the frequency spike is approximately 0.04 Hz lower than earlier events, suggesting that the synchronous generation of the main system provides most of the inertia required to attenuate repeated disturbances.

Fig. 6 shows the three-phase voltage and current waveforms at bus 24 during this attack. Vertical dashed lines denote islanding transitions that begin at $t = 1\,\text{s}$, with rapid cycling until the final reconnection at $t = 1.5\,\text{s}$. In islanded mode, voltage and current remain sinusoidal across all phases, though with reduced magnitudes. Upon grid reconnection, Phase 1 voltage and current drop to zero due to a fault, redirecting power flow to ground. Phases 2 and 3 compensate with increased peak currents to account for Phase 1. Phase voltage asymmetries could potentially lead to overloading, thereby increasing system losses and reducing reliability. Prolonged operation under such imbalances can cause excessive heating, accelerate equipment degradation, and raise the likelihood of premature failure of grid components and insulation.

2) System II – IBR-dominated MG Generation: The following scenarios examine the stability of the MG with a 70% IBR and 30% synchronous generation mix.

a) Single Forced Islanding Scenario: In this scenario, the attacker switches the CB twice: once to island the system at $t = 1\,\text{s}$, and once to reconnect it at $t = 1.5\,\text{s}$. Fig. 7 shows the frequency response measured at the MG at bus 24 during these two key events. Following islanding, the frequency exhibits a more pronounced dip compared to *System I* due to the reduced contribution of synchronous generation. While the frequency remains within acceptable limits, the lower system inertia makes it more vulnerable to sudden disturbances. Between $t = 1\,\text{s}$ and $t = 1.5\,\text{s}$, the frequency oscillates around 60 Hz, similar to *System I*, with no significant degradation in stability. After reconnection at $t = 1.5\,\text{s}$, the initial frequency spike is comparable to that in *System I*, but the system takes slightly longer to stabilize in the grid-connected state. Nonetheless, the frequency settles near 60 Hz within approximately one second, confirming that the MG maintains sufficient control capability even with reduced synchronous support.

b) CB Switching Attack Scenario: The attacker triggers the CB three times within a 0.5-second window. The CB is opened every 0.2 seconds between $t = 1.0\,\text{s}$ and $t = 1.5\,\text{s}$ and is re-closed 0.1 seconds later each time. Fig. 8 shows the resulting frequency response. Each CB opening causes a

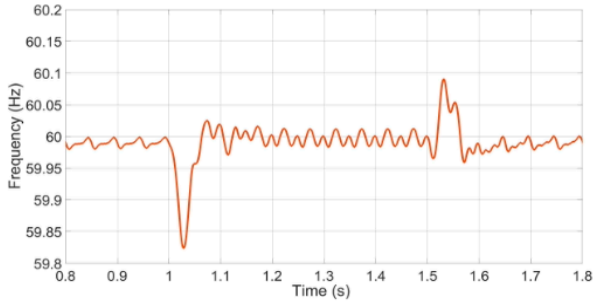


Fig. 7. Frequency response at the MG (Bus 24) during forced islanding at $t = 1$ s and reconnection at $t = 1.5$ s.

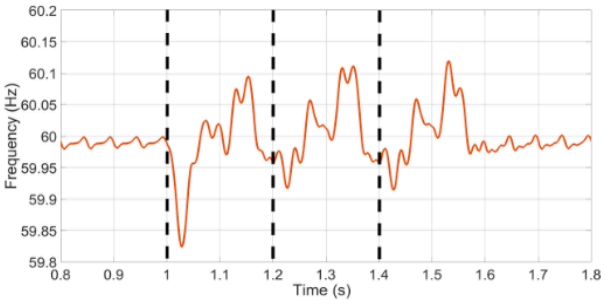


Fig. 8. Frequency response at the MG (Bus 24) during switching attacks happening at 0.1 s intervals from $t = 1$ s to $t = 1.5$ s.

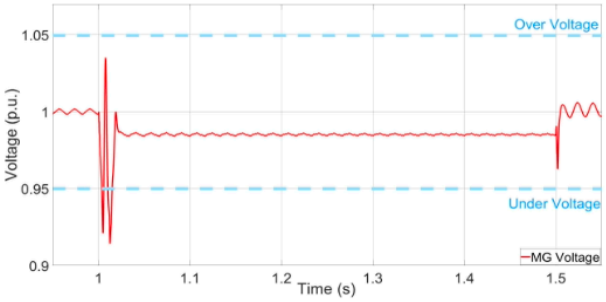


Fig. 9. Voltage magnitude p.u. at the MG (Bus 24) during forced islanding at $t = 1$ s and reconnection at $t = 1.5$ s.

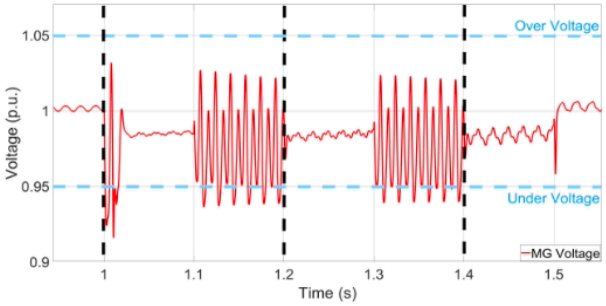


Fig. 10. Voltage magnitude p.u. at the MG (Bus 24) during switching attacks happening at 0.1 s intervals from $t = 1$ s to $t = 1.5$ s.

sharp frequency dip followed by a spike upon reconnection. However, the reduced inertia from the lower synchronous generation results in more pronounced frequency deviations. The first islanding event at $t = 1$ s causes the frequency to dip below 59.85 Hz. Unlike *System I*, the frequency during islanded intervals does not become progressively more stable with each successive event. Instead, the frequency spikes upon reconnection become increasingly pronounced, reaching nearly 60.15 Hz after the final reconnection. Despite these variations, the frequency remains within the prescribed OF1 and UF1 bounds of [11] throughout the attack sequence and shows no signs of critical instability before or after these events.

C. Voltage Stability of MG During Islanding

Fig. 9, 10, 11, and 12 illustrate the MG voltages in both scenarios for each of the two systems described in Table I. As discussed in [12], the typical MG voltage limits of 0.95 and 1.05 p.u. are denoted in each Fig. using blue dotted lines.

Fig. 9 illustrates the MG voltage in *System I, Scenario 1*. At the moment of forced islanding (1 second), the voltage drops below 1 p.u. and then rebounds above 1 p.u. MG voltage exceeds the undervoltage limits of 0.95 p.u. at the moment of islanding, indicating potential transient instability due to the fault existing in the system. For the duration of the islanding, the voltage remains within nominal values, indicating a stable MG. Upon reconnection (1.5 seconds), there is a transient dip, followed by stabilization to 0.97 p.u. within 0.01 seconds.

Fig. 10 illustrates the MG voltage in *System I, Scenario 2*. At the moment of the first forced islanding (1 second), the voltage dips and rebounds similarly to Fig. 9. During forced grid connection, seen after the vertical dashed lines, the MG voltage experiences instability, oscillating around 1 p.u. After the first islanded condition, the following islanded conditions show no transient spikes and resemble the nominal grid-connected conditions, showcasing a stable islanded MG. However, at the moments of reconnection (i.e., 1.1 seconds) the voltage momentarily drops below the 0.95 p.u. limit, causing instability in the MG, as it is forced to reconnect. The final grid connection (1.5 seconds) occurs as the fault clears and the MG voltage returns to nominal operation.

Fig. 11 illustrates the MG voltage in *System II, Scenario 1*. At the moment of forced islanding (1 second), the voltage drops below 1 p.u. and then rebounds above 1 p.u. (similar to Fig. 9). However, the oscillations in Fig. 11 are retained for almost double the duration (as opposed to Fig. 9) and exhibit higher voltage drops. Furthermore, the MG voltage appears noisier, which is mainly attributed to the inverter's inability to regulate the voltage level. Following the transient spikes, the voltage stabilizes, and upon reconnection at 1.5 seconds, the voltage is brought to 0.97 p.u. within 0.06 seconds. Overall, this indicates a stable MG despite the attack; however, in this scenario, the duration and amplitude of the transient spikes are increased with increased IBR generation.

Finally, Fig. 12 illustrates the MG voltage in *System II, Scenario 2*. At the moment of the first forced islanding (1 second), the voltage dips and rebounds similarly to Fig. 10, except with prolonged and more severe magnitude transients. However, the transient spikes during grid-connected attacking conditions are more severe, as shown by increased peak and trough magnitudes. Additionally, during MG islanding, the voltage operates below 1 p.u. for a prolonged duration and exhibits

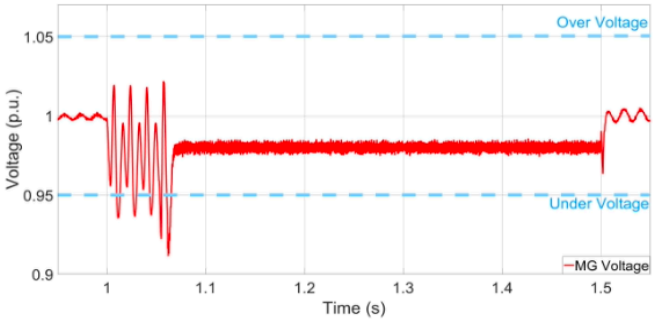


Fig. 11. Voltage magnitude p.u. at the MG (Bus 24) during forced islanding at $t = 1\,\text{s}$ and reconnection at $t = 1.5\,\text{s}$.

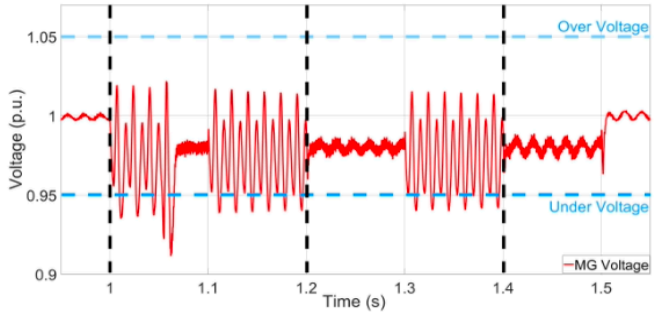


Fig. 12. Voltage magnitude p.u. at the MG (Bus 24) during switching attacks happening at $0.1\,\text{s}$ intervals from $t = 1\,\text{s}$ to $t = 1.5\,\text{s}$.

TABLE II
SUMMARY OF SYSTEM RESPONSES UNDER CYBERATTACK SCENARIOS

Test Case	Frequency	Voltage	Key Observations
System I, Scenario 1	Minor dips during switching, fast recovery	Stable	Minimal disruption during islanding and reconnection
System I, Scenario 2	Oscillations with deeper troughs during switching	Slight UV	Switching causes compounding instability
System II, Scenario 1	Larger transients	Longer time to stabilize	More PV increases frequency/voltage disturbances
System II, Scenario 2	Deep oscillations	Severe UV	Most unstable case with high-risk of phase imbalance

lower values than in Fig. 10. Furthermore, the MG voltage exceeds the Undervoltage (UV) limits during reconnection.

Table II summarizes the frequency and voltage responses for each test case. As the table shows, PV penetration levels and number of CB switches make the system more vulnerable to disturbances. Overall, the results confirm that the MG voltage stays within acceptable operational limits across all test scenarios during islanding, demonstrating stable behavior during both single and multiple forced islanding events. However, the MG operates below the threshold voltage limits when it is forced to reconnect, causing significant voltage spikes across all voltage phases. At the same time, the transition from a balanced 50%–50% generation split to a 70% IBR-based MG furnishes more severe transient spikes and longer stabilization times when the MG transitions between islanded and grid-connected modes. The results highlight that increasing IBR penetration inherently heightens the MG's susceptibility to abrupt disturbances due to lack of inertia. Such observations could be exploited by threat actors aiming to maximize their attack impact, leveraging improperly secured grid devices (in our case the CB) to mount their attacks.

IV. CONCLUSION

This paper investigates the behavior of an integrated TnD system under coordinated switching attacks, leading to MG islanding. The developed TnD system model couples the IEEE 39-bus transmission network with an MG at the distribution level, which uses a mix of IBR and synchronous generation. We present real-time measurements, e.g., voltage, current, and frequency, during different attack scenarios demonstrating the effects that different IBR penetration levels can induce on MG behavior. Future work will incorporate additional IBR resources such as Battery Energy Storage System (BESS) and increasing PV penetrations as well as additional attack scenarios, highlighting the impact on stability of increased IBR penetration during adverse events.

REFERENCES

[1] D. Espín-Sarzosa *et al.*, "Microgrid Modeling for Stability Analysis," *IEEE Transactions on Smart Grid*, vol. 15, no. 3, pp. 2459–2479, 2024. [Online]. Available: https://doi.org/10.1109/TSG.2023.3326063

[2] National Renewable Energy Laboratory (NREL), "Microgrids," 2024. [Online]. Available: https://www.nrel.gov/grid/microgrids.html

[3] I. Zografopoulos and C. Konstantinou, "Event-triggered islanding in inverter-based grids," *Electric Power Systems Research*, vol. 243, p. 111472, 2025.

[4] I. Zografopoulos *et al.*, "Security assessment and impact analysis of cyberattacks in integrated T&D power systems," in *Proc. of the 9th workshop on modeling and simulation of cyber-physical energy systems*, 2021, pp. 1–7.

[5] K. Katuri, I. Zografopoulos, H. T. Nguyen, and C. Konstantinou, "Experimental impact analysis of cyberattacks in power systems using digital real-time testbeds," in *2023 IEEE Belgrade PowerTech*. IEEE, 2023, pp. 1–6.

[6] P. Demetriou, J. Quirós-Tortós, and E. Kyriakides, "When to Island for Blackout Prevention," *IEEE Systems Journal*, vol. 13, no. 3, pp. 3326–3336, 2019.

[7] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies," *IEEE Access*, vol. 9, pp. 29 775–29 818, 2021.

[8] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6695–6709, 2023.

[9] P. Kertzner, C. Carter, and A. Hahn, "Crown jewels analysis (cja) for industrial control systems (ics)," MITRE, Tech. Rep. PR-22-2824, December 2022. [Online]. Available: https://www.mitre.org/sites/default/files/2023-01/PR-22-2824-Crown-Jewels-for-Industrial-Control-Systems.pdf

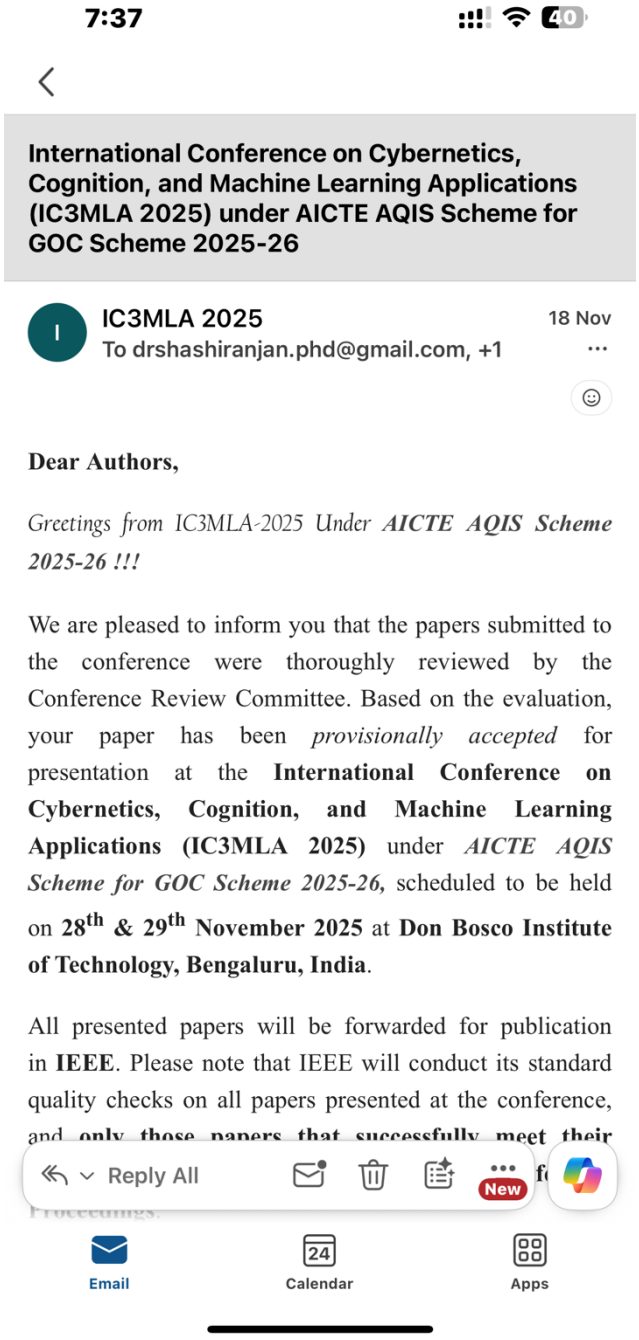
[10] MITRE ATT&CK for ICS, "Unauthorized Command Message," 2025, accessed: 2025-03-19. [Online]. Available: https://attack.mitre.org/techniques/T0855/

[11] "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pp. 1–138, 2018.

[12] H. Gan, J. Wang, Y. Lin, S. Bhela, and C. Bilby, "Performance Evaluation of Peer-to-Peer Distributed Microgrids Coordination for Voltage Regulation," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*, 2022, pp. 1–5.

APPENDIX – A

Publication - Acceptance letter



7:37

International Conference on Cybernetics, Cognition, and Machine Learning Applications (IC3MLA 2025) under AICTE AQIS Scheme for GOC Scheme 2025-26

IC3MLA 2025 — 18 Nov
To drshashiranjan.phd@gmail.com, +1

Dear Authors,

*Greetings from IC3MLA-2025 Under **AICTE AQIS Scheme 2025-26 !!!***

We are pleased to inform you that the papers submitted to the conference were thoroughly reviewed by the Conference Review Committee. Based on the evaluation, your paper has been *provisionally accepted* for presentation at the **International Conference on Cybernetics, Cognition, and Machine Learning Applications (IC3MLA 2025)** under ***AICTE AQIS Scheme for GOC Scheme 2025-26,*** scheduled to be held on **28th & 29th November 2025** at **Don Bosco Institute of Technology, Bengaluru, India**.

All presented papers will be forwarded for publication in **IEEE**. Please note that IEEE will conduct its standard quality checks on all papers presented at the conference, and **only those papers that successfully meet their**

Reply All — New

Email — Calendar — Apps

Fig A. Conference Paper Acceptance mail

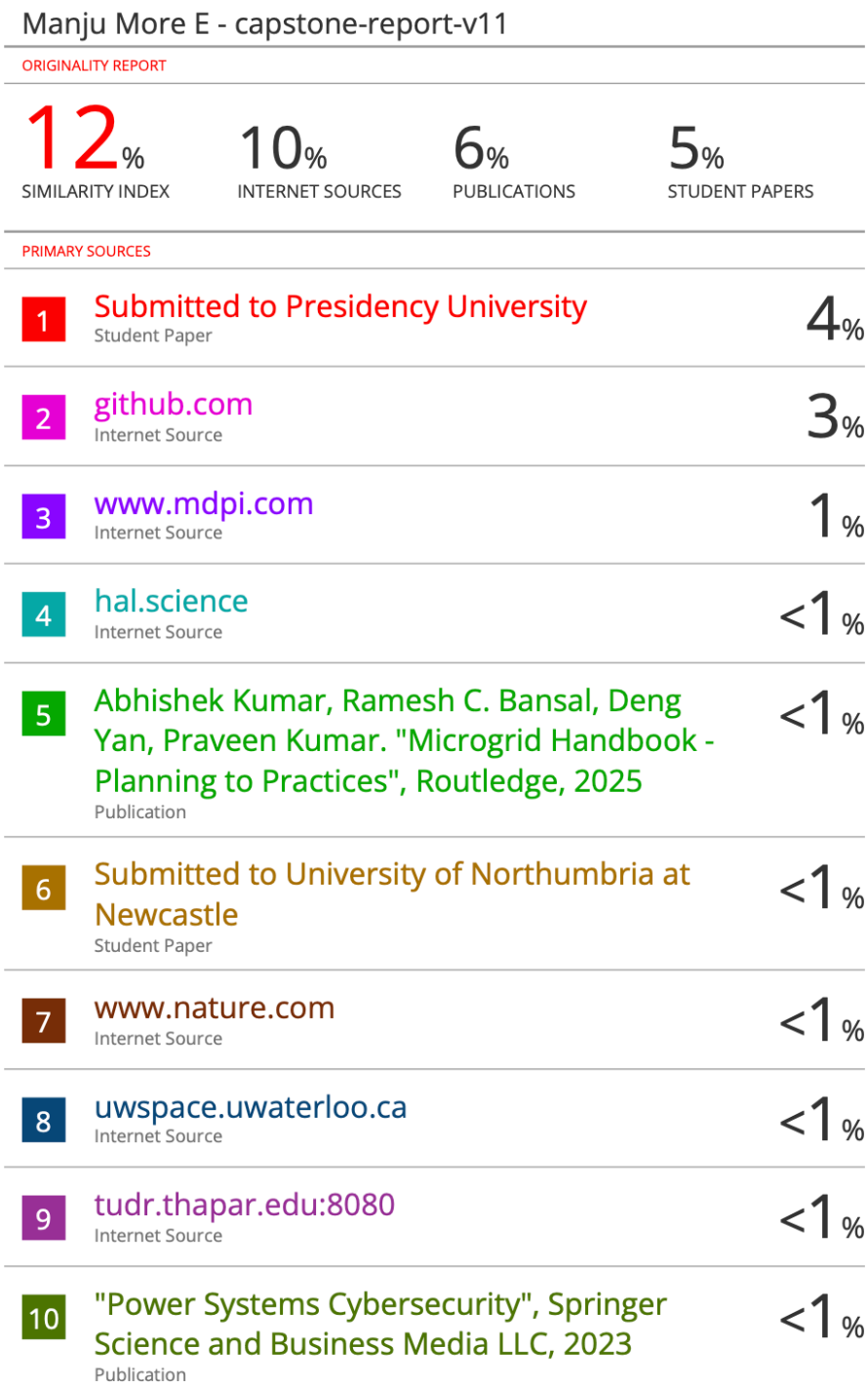
APPENDIX – B

Publication - Conference Certificate

Fig B. Conference Certificate

APPENDIX – C

Project Report Similarity Report



Manju More E - capstone-report-v11

ORIGINALITY REPORT

12%	10%	6%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Presidency University Student Paper	4%
2	github.com Internet Source	3%
3	www.mdpi.com Internet Source	1%
4	hal.science Internet Source	<1%
5	Abhishek Kumar, Ramesh C. Bansal, Deng Yan, Praveen Kumar. "Microgrid Handbook - Planning to Practices", Routledge, 2025 Publication	<1%
6	Submitted to University of Northumbria at Newcastle Student Paper	<1%
7	www.nature.com Internet Source	<1%
8	uwspace.uwaterloo.ca Internet Source	<1%
9	tudr.thapar.edu:8080 Internet Source	<1%
10	"Power Systems Cybersecurity", Springer Science and Business Media LLC, 2023 Publication	<1%

Fig C. Project Report Similarity Percentage

APPENDIX – D

Datasets

Renewable Energy Microgrid Dataset (Kaggle)

- Samples: 3546 hourly records
- Time period: Jan 2023 - May 2023
- Variables: Solar PV output, wind power output, irradiance, wind speed, temperature, humidity, pressure, grid load, voltage, frequency, battery SOC, charging and discharging rates
- Target variables: Predicted solar power, predicted wind power, predicted total renewable energy
- Format: CSV
- Link: https://www.kaggle.com/datasets/programmer3/renewable-energy-microgrid-dataset

Power Data from Microgrid - Mesa del Sol (Kaggle)

- Samples: ~260,000 records per month
- Time resolution: 10-second intervals
- Time period: May 2022 - July 2023
- Variables: Battery active power, PV power, GE load, fuel cell power, AC bus voltages, bus frequencies, chilled-water temperatures
- Format: 15 CSV files
- Link: https://www.kaggle.com/datasets/yekenot/power-data-from-mesa-del-sol-microgrid

APPENDIX – E

Project Repository

GitHub Repo: https://github.com/siddiquealikhan/microgrid-smart-controller

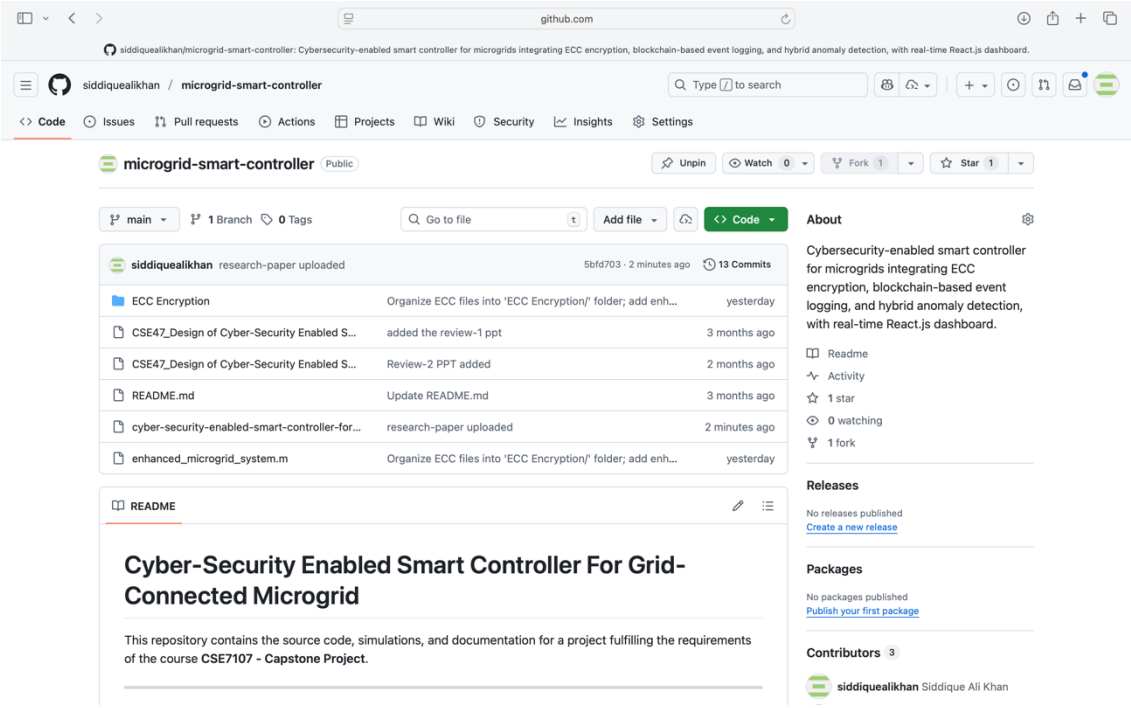


Fig D. GitHub Repository Screenshot

APPENDIX – F

Few Images of the Project

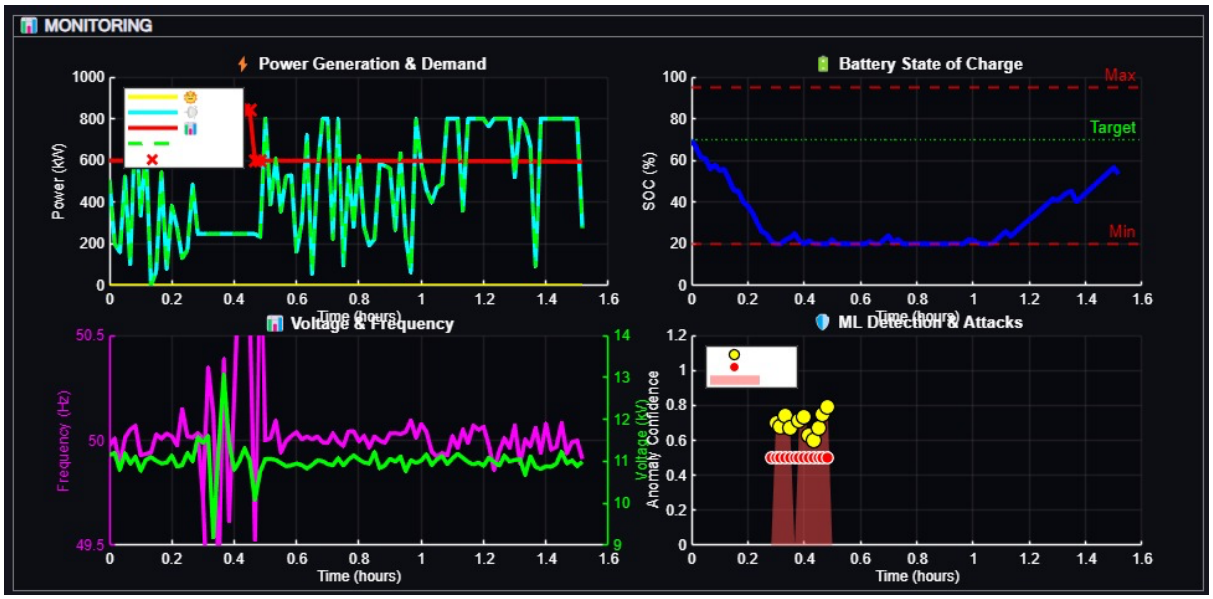


Fig E. Monitoring Graphs

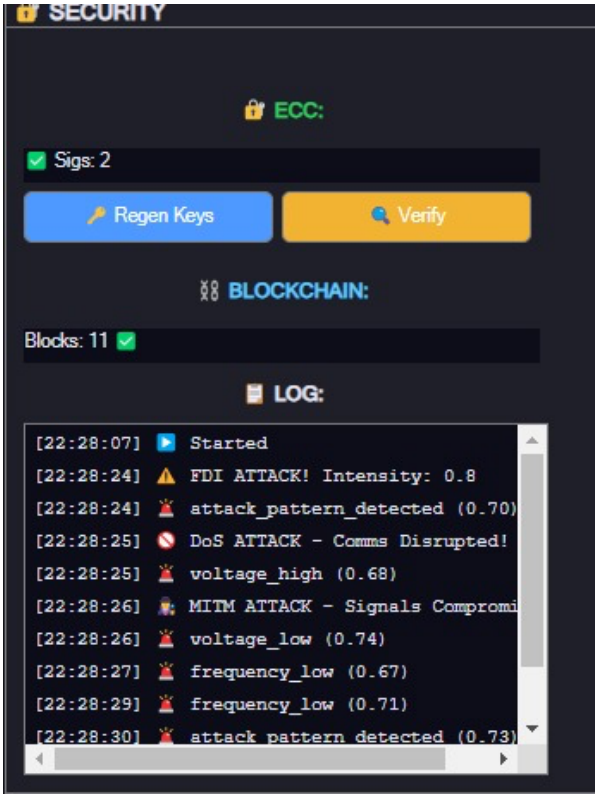


Fig F. ECC and Blockchain Logs

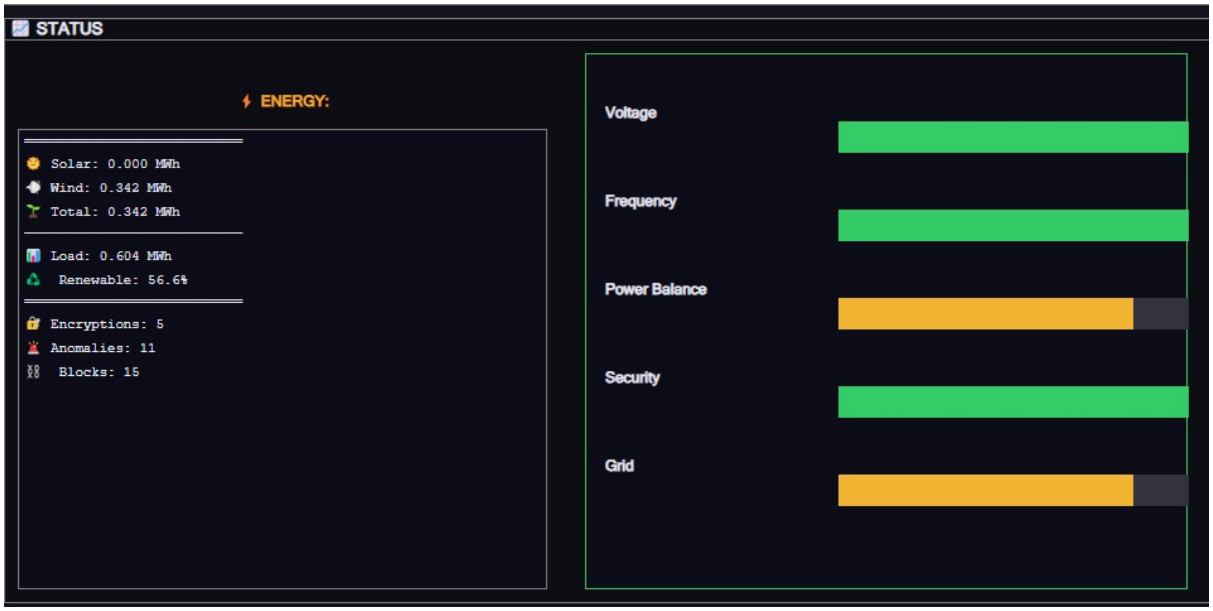


Fig G. Real-time microgrid status dashboard

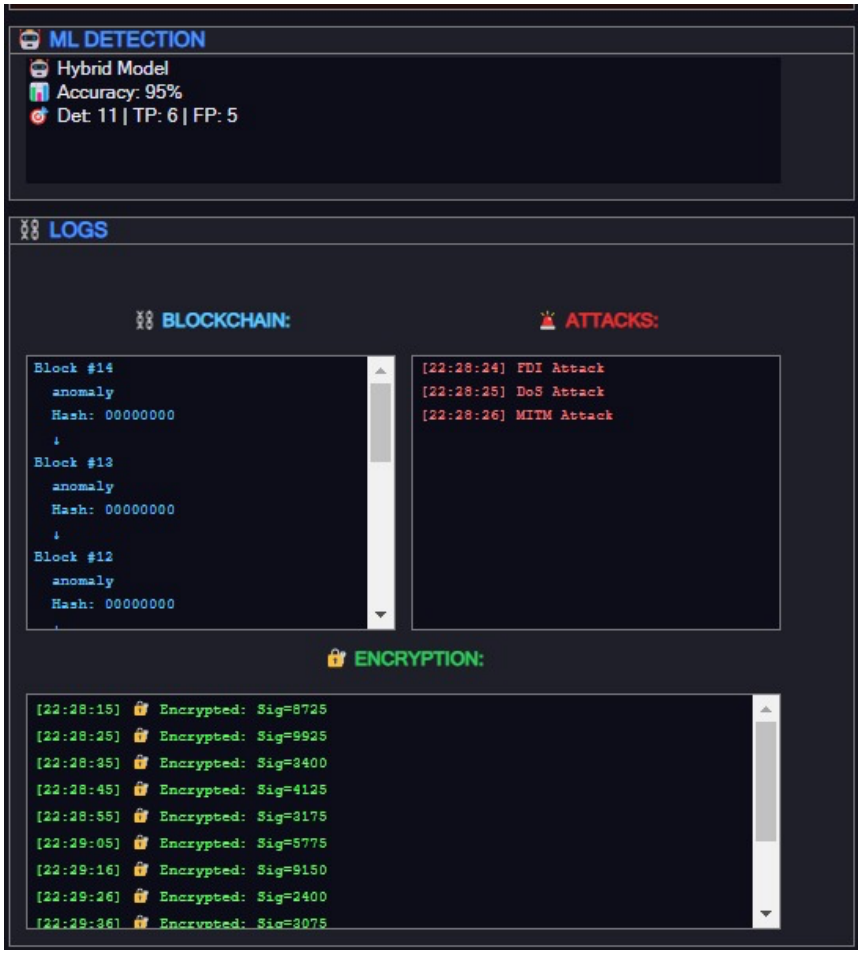


Fig H. ML Detection