RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 07, Issue 09 September

Check for updates

http://dx.doi.org/10.47392/IRJASH.2025.094

Solar Energy System Simulation with Respect to Cybersecurity Using Decoy Device

Tanya Raj[1], Siri Vennela KS[2], Shreelekha K[3], Umesh Jadhav[4], Snigdha Kesh[5], V Mareeswari[6]
[1,2,3,4,5,6]Dept. of Computer Science, AMC Engineering College (Affiliated to VTU), Bengaluru, India.
Emails: *sumanthgowdach123@gmail.com[1], veenasureshbabu7@gmail.com[2], shreelekhakathrivel@gmail.com[3], umeshjadhav7402@gmail.com[4], snigdha.kesh@amceducation.in[5], mareesh.prasanna@amceducation.in[6]*

Article history
Received: 25 August 2025
Accepted: 09 August 2025
Published:25 September 2025

Keywords:
solar Energy Systems, Cybersecurity, Decoys devices, Moving Target Defence, IOT sensors, Renewable Energy Protection, Anomaly Detection, Smart Grid Security, Raspberry-pi, Edge computing, Artificial Intelligence (AI)

Abstract
The rapid expansion of renewable energy deployment has placed solar photovoltaic (PV) at the forefront of the clean power supply for the residential, commercial and industrial users. With their insertion into smart Grids, though these systems are facing increasing exposure to cyber physical threats to stability simulation and protection system that embedded with solar panels, inverters and battery management units along with smart sensing using LDR, PIR, IR, temperature sensors, and actuator responses through LED and buzzer notifications. A multi-layered cybersecurity framework is designed, including AI-powered anomaly detection for timely threat detection, blockchain-enabled decentralized logging to provide tamper-proof audit records, honeypot-derived decoy devices to divert attackers, and a Moving Target Defence (MTD) function for adaptive system reconfiguration against dynamic threats. The system is implemented on Raspberry Pi and ESP32 boards to facilitate real-time data acquisition, secure processing, and visualization of solar performance data, environmental parameters, and intrusion attempts. Experimental validation confirms the system's accurate estimation of solar irradiance, effective inverter–battery interaction, and strong intrusion resilience based on coordinated responses. Furthermore, the decoy-based deception method proposed in this work effectively misdirects adversaries from important resources while ensuring operational continuity. The findings identify a new paradigm for incorporating sustainable energy management with sophisticated cybersecurity measures and provide a resilient, scalable, and smart model for future decentralized smart grid infrastructures.

1. Introduction

Increasing the need for renewable and sustainable energy has led to more solar photovoltaic (PV) systems being installed in homes, industries, and businesses. Solar power is clean and plentiful, making it a key part of moving away from fossil fuels toward cleaner energy sources. However, as these systems become part of smart infrastructure with inverters, batteries, and monitoring tools, they are also at risk from cyber and physical attacks. The use of IoT sensors, real-time data analysis, and remote connections has created many possible points of attack. Solar energy systems are now

vulnerable to intrusions, tampering, and attacks that stop them from working properly. Recent attacks on smart grids and renewable energy facilities show the urgent need to combine energy management with strong cybersecurity. Traditional ways of protecting energy systems, such as firewalls and user authentication, are still important but no longer enough to stop clever attackers. With more reliance on edge devices like Raspberry Pi and ESP32 for controlling and collecting data, attacks can target sensors, actuators, and control signals. These attacks could stop solar energy production, mess with inverter functions, or drain battery power. These weaknesses highlight the need to build cybersecurity into the design of solar systems from the start. In this paper, we present an integrated solar energy system that includes solar energy simulation, AI-based anomaly detection, blockchain-backed logging, and deception-based defence. Using LDR modules to sense sunlight, PIR and IR sensors to detect intruders and movement, and DHT sensors to measure temperature, the system has a comprehensive understanding of the environment. This data is combined with devices like LEDs and buzzers to alert users when something is wrong. The system also uses LDR readings to estimate power generation, which helps create realistic simulations of normal and attack scenarios in controlled tests. One key part of this system is the use of decoy devices, or honeypots, within the solar setup. These fake devices trick attackers into targeting copies instead of real equipment, slowing down attacks and helping security systems track harmful activities in real time. Along with this, the Moving Target Defence (MTD) approach changes system settings and access controls regularly, making it harder for attackers to exploit fixed weaknesses. Together, these features improve resilience and help manage threats before they cause serious damage. Blockchain plays a key role in building trust and accountability within this system. By storing sensor data, intrusion attempts, and system responses in an unchangeable, shared ledger, the system provides secure logs for investigations and compliance checks. This decentralized setup avoids the risks of centralized logging systems, which can be tampered with. The blockchain layer also helps track solar performance and how the system responds to intrusions, adding transparency and reliability. The main contribution of this work is the design and development of a realistic prototype that combines renewable energy generation, IoT-based sensing, AI-driven anomaly detection, blockchain-secured logging, and strengthened defence through deception. Compared with traditional methods, this research brings together physical energy simulation and cyber resilience in one test setup. The system can not only mimic solar power generation but also show how modern security methods can be used in real life to protect smart energy systems. This study lays a strong foundation for secure, smart, and adaptable solar cybersecurity systems that can support future decentralized grids and large-scale renewable energy projects [1].

2. Literature Review

Introduction:

The fast-growing use of solar energy as a clean power source has come with increased risks of cyberattacks on important parts of the system. Experts around the world have talked about many ways to protect solar systems, including photovoltaic panels, inverters, storage devices, and IoT sensors. Studies show that relying only on usual computer security methods isn't enough because new dangers come from the mix of physical and digital systems. Current research looks at tools like artificial intelligence, blockchain, honeypots, digital twins, and edge computing as possible ways to deal with these security issues. This part of the text reviews the existing research, pointing out what works well, what's missing, and the common trends in improving the safety and reliability of solar energy systems.

2.1. Cybersecurity Challenges in Solar Energy Systems

Solar systems like panels, inverters, and storage units are quickly connecting to IoT networks, which makes them easier targets for new kinds of cyberattacks. Studies show that threats such as false data injection, service disruption, and changing inverter settings can harm the reliability of energy supply. These attacks not only damage data accuracy but also cause big financial losses. Many studies say that attackers exploit weak login systems and lack of encryption in solar IoT setups. Also, solar farms linked to smart grids are very risky because a problem in one part can spread across the entire grid. This shows that we need stronger cybersecurity measures right away. Artificial Intelligence for Threat Detection [2].

2.2. Artificial Intelligence of Threat Detection

This technology has been used widely for anomaly detection within energy systems, this technology is widely used to spot unusual behaviour in energy systems, using both supervised and unsupervised learning methods. Studies show that AI can detect harmful actions as they happen by analysing large amounts of data from solar farms. These studies also show that deep learning methods like LSTMs are effective for predicting trends over time and help find irregularities in energy production. Scientists use AI models to reduce false alarms compared to older methods that rely on known attack patterns. Also, AI improves adaptability, allowing it to detect new types of attacks that traditional firewalls can't handle. Using AI in solar power monitoring ensures fast and smart responses to any issues.

2.3. Machine Learning Algorithms in Energy Security

Many different methods have been studied to use machine learning (ML) models for protecting smart energy systems. Algorithms like Support Vector Machines (SVM), Random Forest, and Gradient Boosting have been shown to work well in identifying cyber threats in systems that use sensors. Studies show that ML helps find false readings in data from solar panels, especially in LDR and DHT sensors. Researchers also highlight that improving accuracy comes from feature engineering, where factors like sunlight levels, current, and movement data are used to train the models. One big issue that has been discussed is the lack of labelled data sets that are specific to solar cyber systems. Because of this, there is research into hybrid ML models that combine both supervised and unsupervised techniques.

2.4. Blockchain for Secure Data Logging

Blockchain technology is becoming a big solution to make sure data is safe and true in renewable energy. Studies show that blockchain can store sensor data in a way that can't be changed, which helps track and hold people responsible for energy use. Experiments show that because blockchain data can't be altered, it stops people from changing information about how much energy is made or used. Blockchain allows secure, trustworthy energy trades between people in solar networks without needing a middleman. Research says that the open nature of blockchain builds trust among those involved. However, some studies also point out that blockchain can be slow when handling many transactions, and researchers are now looking into lighter ways to make blockchain work better with solar devices that have limited resources [3].

2.5. Smart Contracts in Energy Transactions

Smart contracts help automate and build trust in decentralized energy exchanges. Studies show they work well in peer-to-peer solar trading platforms, where producers and consumers can make deals that happen automatically without needing anyone to step in. Research shows that smart contracts make billing and pricing clear and fair, which helps prevent fraud. Different pilot projects show how smart contracts can improve microgrid balancing by making transactions settle quickly and efficiently. They also help with demand-response programs, allowing extra solar power to be bought and sold more effectively. However, there are challenges when using smart contracts with large power grids, but new adaptive systems are being developed to handle these issues.

2.6. Moving Target Defence (MTD) in Critical Systems

MTD has become a promising way to protect important facilities like solar farms. Studies describe MTD as a method where system settings such as IP addresses, ports, and encryption keys are changed often to confuse attackers. Research shows that making these changes frequently makes it harder for attackers to gather information and reduces the chances of successful attacks. When MTD is combined with AI, it can predict threats and change the system's attack surface in response. Experts also note that MTD helps defend against advanced persistent threats. Although MTD uses a lot of resources, improved versions are now being used more in energy systems that rely on the internet of things.

2.7. Decoy Devices and Honeypots

The idea of using fake devices to trick attackers has become more common in protecting renewable energy systems. These fake devices, called honeypots, look like real solar equipment and attract hackers. This lets security teams' study how attackers try to break in. Studies show that honeypots help slow down hackers and keep real tools like inverters and batteries safe. Some tests found that using honeypots with AI helps detect threats from inside the system better. Experts also say honeypots give great information for

investigations, which can improve how well machine learning tools identify different types of attacks. Fake devices are especially useful in small solar setups where resources are limited, but early warnings are still very important.

2.8. Integration of Digital Twin Models

Digital twins are computer models that closely copy real-world systems, allowing for real-time tracking and predictions. Research shows that using digital twins for solar systems helps find problems by comparing what should happen with what is happening. In situations where a system is under attack, digital twins show issues like sudden drops in power output or strange sensor readings. Studies say digital twins help reduce system stoppages by allowing early fixes and stopping threats at the same time. They are also being used with blockchain to create records that show if data has been changed. This combination makes systems more able to handle and recover from cyberattacks [4].

2.9. Edge-Cloud Security Architectures

Various studies show that combining edge computing with cloud systems can help safely monitor solar energy. Using edge devices such as Raspberry Pi and ESP32 to process sensor data locally can help detect cyber threats faster by reducing delays. Research has found that making decisions in real-time at the edge allows quick actions like triggering alarms or activating decoys. However, connecting to the cloud allows for analysing large amounts of data over time using AI. Experts highlight that this two-layer security setup strikes a good balance between speed and the ability to handle big data. Also, using blockchain at the edge level improves trust because data stored locally can be checked thoroughly across the network. This approach is becoming a reliable method for security.10. Complete Security Frameworks.

2.10. Complete Security Frameworks

Literature recently concludes that one technique is insufficient to secure solar infrastructures completely; rather, integration of a mix of several techniques is required. Integrated solutions that harmonize AI for anomaly detection, blockchain for tamper-proof logging, MTD for attack surface movement, and honeypots for deception provide protection layers. Research emphasizes that this synergy greatly minimizes vulnerabilities. Standardization and interoperability are also crucial for deploying such frameworks in global solar systems, according to researchers. Pilot tests indicate good promise in enhancing resilience without compromising efficiency of operation. Thus, holistic approaches are surfacing as the basis for next-generation solar energy cybersecurity.

3. System Architecture

The suggested Solar Energy Simulation with Respects to Cybersecurity using Decoy Devices is aimed at offering an effective and smart defence mechanism for renewable energy systems. In contrast to conventional solar monitoring systems, the architecture supports IoT sensors, AI-based anomaly detection, blockchain-based integrity verification, and Moving Target Defence (MTD) measures alongside physical solar hardware elements like PV panels, charge controllers, batteries, and inverters Shown in Figure 1.

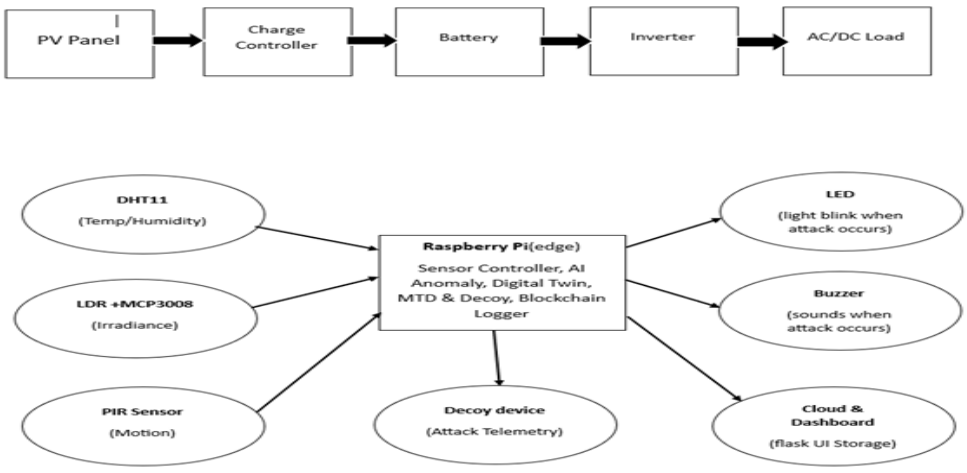


Figure 1 Architecture Diagram

The design not only ensures optimal energy generation and storage, but also optimally counteracts cyber-physical security vulnerabilities like false data injection, spoofing, and denial-of-service. The architecture is a hybrid edge–cloud model in which the Raspberry Pi is the edge processing node that performs sensor preprocessing, anomaly detection, and decoy engagement and the cloud and blockchain infrastructure that offers long-term storage, data standardization, and immutable security logging.

The end-to-end system comprises:

- PV Panel and Energy Hardware Integration
- Edge Preprocessing with Raspberry Pi
- Cloud-Based Data Processing
- AI-Driven Cybersecurity Models
- Analytics and Threat Detection
- Threat Classification and Alert Control
- Real-Time Dashboard and Visualization

Each module is linked, creating a closed-loop feedback cycle wherein data from sensors is gathered, authenticated, processed, and safeguarded in real time to ensure both energy reliability and cybersecurity resiliency [5].

3.1. PV Panel and Edge Preprocessing

3.1.1. PV Panel and Power Electronics

The energy system starts with a solar PV panel that produces DC power from falling light. The energy goes through a charge controller that avoids overcharging, flows to a bank of batteries for storage, and gets converted through an inverter to power AC/DC loads. The use of IoT-based monitoring allows the parameters of energy like voltage, current, temperature, and irradiance to be always monitored.

3.1.2. Edge Preprocessing using Raspberry Pi

Raspberry Pi serves as the edge central intelligence, plugged directly into several sensors such as DHT11 (temperature and humidity), LDR with MCP3008 (irradiance measurement), INA219 (voltage/current monitoring), and PIR/IR sensors (motion detection). Edge preprocessing makes sure that important anomalies like sudden irradiance drops or unusual current spikes are captured locally without cloud latency.

3.1.3. Noise Filtering and Data Validation

Physical environmental conditions like dust deposit, shading, or sensor lag inject variations into the raw data. These are minimized by filtering algorithms eliminating high-frequency noise and submitting smoothed results for analysis. This process eliminates false positives in anomaly detection and enhances overall signal-to-noise ratio.

3.1.4. Segmentation and Compression

Data is split into brief time-window intervals (e.g., every 5–10 seconds) and compressed before being transferred to the cloud. This prevents unnecessary bandwidth consumption but keeps meaningful patterns intact for real-time analysis Shown in Figure 2 Use Case Diagram.

Figure 2 Use Case Diagram

3.2. Cloud-Based Data Processing

The data, having been Pre-processed at the edge, is sent to the cloud layer, which is a compute-intensive back end for advanced analytics, blockchain verification, and report generation.

3.2.1. Data Standardization

Raw sensor data differs between modules, for example, temperature in Celsius, irradiance in Lux, current in Amps. Standardization converts all these units into a consistent dataset, so it is compatible with AI models and blockchain records [6].

3.2.2. Filtering and Prioritization

Cloud-based filtering mechanisms eliminate duplicate values and give priority to high-risk data like immediate disconnections of sensors, unusual current spikes, or unauthorized access attempts. This way, attack-concerned telemetry gets priority attention.

3.2.3. Model Execution

The cloud hosts several AI models for predictive analysis, anomaly detection, and attack recognition. In contrast to edge devices, the cloud can execute computationally demanding deep learning models like LSTM Autoencoders, Random Forest classifiers, and blockchain consensus validators. This division of effort guarantees high scalability at minimal latency.

3.2.4. Blockchain Integration

Each log records a benign sensor reading or an identified attack is recorded in a tamper-evident blockchain ledger. The unalterable history adds to system trust and serves as forensic audit evidence.

3.3. AI-Powered Cybersecurity Models

The AI processor delivers the artificial intelligence necessary to separate benign solar output variability from nefarious cyberattacks.

3.3.1. Sensor Anomaly Detection

With the help of machine learning classifiers, normal operational ranges are established for temperature, irradiance, and current flow. Unusual deviations beyond these ranges are treated as anomalies, and real-time alerts are sent.

3.3.2. Decoy Device Interaction Model

Decoy endpoints (honeypots) are part of the system that mimic vulnerable nodes like inverters or sensor controllers. When the attackers try to take advantage of these nodes, their activity is redirected to the decoy, logged, and processed without interfering with the actual infrastructure [7].

3.3.3. Moving Target Defence (MTD)

MTD incorporates unpredictability by constantly altering IP addresses, sensor-to-server correlations, and port numbers, rendering it incredibly hard for attackers to acquire a stable presence. MTD as a proactive defence enhances system survivability against prolonged threats.

3.3.4. Blockchain Validation Model

Blockchain provides integrity and non-repudiation of energy information. Even if attackers manipulate live data streams, blockchain-archived records are unalterable, and a single source of truth for grid operations is maintained.

3.3.5. Predictive Forecasting and Risk Estimation

AI models further predict the availability of solar power by connecting irradiance, temperature, and historic weather patterns. Such a prediction enables operators to know not only future energy production but also likely risk exposure to attacks during peak or low production times.

4. Analytics and Threat Detection

The analytics layer aggregates outputs from AI, decoy, and blockchain into a single decision-making engine.

4.1. Attack Hotspot Detection

Recurring intrusion attempts get mapped to individual system modules (e.g., inverter controller or sensor gateway), which reveal key hotspots that need more robust defence policies.

4.2. Blockchain-based report generation

Reports consist of time-stamped attack telemetry, summary of anomalies, and energy efficiency information. These reports are stored on blockchain, thus remain immutable, and are accessible only to authorized administrators [8].

4.3. Visualization and Correlation

The analytics module cross-references energy generation graphs and cybersecurity notifications. For instance, an abrupt battery charge decrease coinciding with anomalous decoy motion could suggest a false data injection attack.

5. Threat Classification Module

Threats are classified into three alert levels to minimize response times:

- **High Alert:** Explicit intrusion on critical modules (e.g., inverter manipulation, false data injection).
- **Medium Alert:** Repeated anomalies without explicit tampering, which need human confirmation.
- **Low Alert:** Small variations or non-vital deviations. This categorization makes system operators focus first on severe

attacks while keeping track of less-than-severe problems.

6. Alert Control and Communication

6.1. Edge Alerts

LED lights flash and buzzers beep upon detecting serious anomalies or attacks.

6.2. Dashboard Notifications

Flask-based dashboards show live security notices and sensor trends to operators.

6.3. Blockchain Logging

Alerts are logged on blockchain at the same time, so attackers cannot remove their digital trail.

6.4. Remote Communication

Integration with SMS, Telegram, or Email notifications ensures operators are updated in real-time even when they are not physically present.

7. Dashboard and Visualization Interface

The dashboard is the user interface for real-time monitoring and control.

7.1. Real-Time Sensor Display

Temperature, irradiance, current, and voltage readings are updated in real time.

7.2. Security Visualization

Anomaly detections, decoy activations, and threat classifications are shown with color-coded indicators.

7.3. Blockchain Verification Panel

Operators can check each transaction log against the blockchain to establish authenticity.

7.4. Graphical Insights

Interactive charts and graphs display both energy performance and attack trends, offering a dual perspective of power and security metrics.

8. Methodology

The designed system Solar Energy Simulation with Respect to Cybersecurity using Decoy Devices combines renewable energy monitoring, AI-based anomaly detection, blockchain logging, and Moving Target Defence (MTD) Shown in Figure 3 Methodology Features [9].

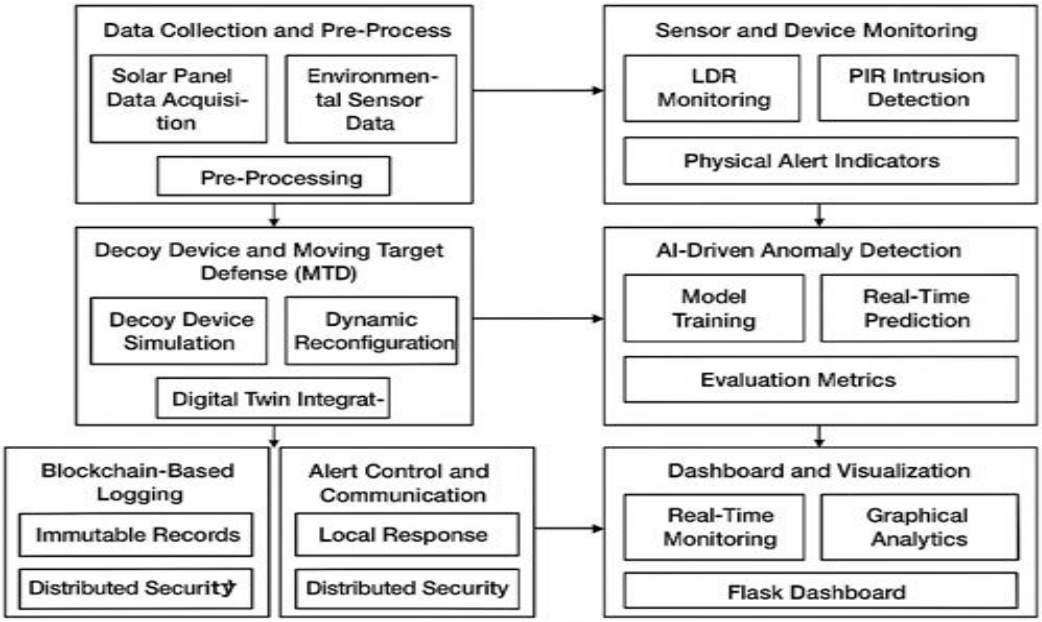


Figure 3 Methodology Features

The approach provides stable energy transmission from solar panels with multi-layered cybersecurity against cyber–physical attacks. The modules are explained below:

8.1. Data Collection and Pre-Processing

8.1.1. Solar Panel Data Acquisition

The photovoltaic panel produces voltage and current values that are constantly tracked through the INA219 sensor. These values are vital in mimicking solar irradiance fluctuations brought about by natural factors like cloud movement. Through the collection of precise measurements, the system offers a sound basis for both energy production as well as intrusion detection analysis.

8.1.2. Environmental Sensor Data

Several sensors such as DHT11 (humidity and temperature), LDR (irradiance), and PIR (motion) are linked to Raspberry Pi. Each of the sensors

offers a unique layer of surveillance—DHT11 observes thermal fluctuations, LDR observes irradiance changes, and PIR reports unauthorized motion around the solar setup. Combined, they form a holistic dataset for detection of anomalies.

8.1.3. Pre-Processing Pipeline

Prior to the data being passed to analytics modules, it is subjected to preprocessing. Filtering for noise ensures that sensor anomalies resulting from external interference (e.g., abrupt wind or shadow) are reduced to a minimum. Normalization of data ensures that values from various sensors are synchronized, whereas sampling mechanisms provide for efficient data transfer. This pipeline optimizes the efficiency of AI-based anomaly classification.

8.2. Solar Panel and Battery Management

8.2.1. Charge Regulation

The energy harvested from solar panels is conditioned by a charge controller, keeping overcharging and deep discharge at bay. Regulation is essential to protect long-term battery life and ensure stable operation during attack or failure.

8.2.2. Battery Storage and Backup

A rechargeable battery pack is utilized to accumulate solar energy for uninterrupted system operation. This guarantees that the anomaly detection and decoy devices continue to operate even during low sunlight or when the conditions are cloudy. The battery also energizes local alert systems in case of emergencies.

8.2.3. Inverter and Load Management

The stored energy is passed through an inverter for AC/DC conversion. This module allows testing of real-world appliances connected to the system while simultaneously monitoring how cyberattacks may affect load balance. Simulated attacks can cause abnormal load variations, which the system is designed to detect.

8.3. Sensor and Device Monitoring

8.3.1. LDR Monitoring

The LDR records real-time irradiance levels, which are linearly related to the efficiency of solar panels. If anomalous irradiance values are detected when the physical surroundings are stable, the system tends to suspect spoofing or tampering of sensor readings.

8.3.2. PIR Intrusion Detection

The PIR sensor continuously detects the presence or absence of humans around the panel or battery configuration. Unauthorised presence is treated as a possible intrusion and triggers both alert systems and logging onto the blockchain.

8.3.3. Physical Alert Indicators

Once anomalies are sensed, an LED and a buzzer are triggered to deliver immediate feedback to surrounding operators. This constitutes a double alerting system—both digital (dashboard warning) and physical (on-site indication).

8.4. Decoy Device and Moving Target Defence (MTD)

8.4.1. Decoy Device Simulation

A decoy system in the virtual environment replicates authentic energy data streams, presenting attackers with a deceitful dataset. This deception exhausts attacker resources and distracts them from actual infrastructure.

8.4.2. Dynamic Reconfiguration

The MTD module ensures data paths, IP addresses, and service ports are modified often. This randomness makes the system unpredictable, lowering the success rate for repeated cyberattacks.

8.4.3. Digital Twin Integration

The decoy system includes a digital twin of the solar plant, simulating actual operating behaviours like variations in power during day/night cycles. This renders the decoy undistinguishable from the real system [10].

8.5. AI-Driven Anomaly Detection

8.5.1. Model Training

Historical solar and sensor data are used to train machine learning models under both normal and attack conditions. Classification and anomaly detection are performed using algorithms like Random Forest, SVM, and LSTM Autoencoders.

8.5.2. Real-Time Prediction

In real-time operation, the AI model continually analyses incoming sensor data. Identified anomalies are categorized into types of spoofing, denial-of-service, or sensor tampering. The response system is triggered automatically from these predictions.

8.5.3. Evaluation Metrics

The AI system is tested based on precision, recall, and F1-score to reduce false positives. Continuous retraining prevents evasion of new attack patterns, enhancing long-term robustness.

8.6. Blockchain-Based Logging

8.6.1. Immutable Records

Blockchain technology guarantees that system events such as sensor data and anomalies detected

are stored in tamper-proof format. This provides forensic integrity for any future analysis.

8.6.2. Transparency and Auditing

Blockchain logs can be audited by administrators to ensure detected attacks were properly identified and reacted to. This establishes trust within the system in the form of an immutable operations record.

8.6.3. Distributed Security

Blockchain decentralizes the logging function, removing points of failure. Even if the attackers get hold of one device, logs on the distributed network are safe.

8.7. Alert Control and Communication

8.7.1. Local Response

The buzzer and LED give out instant local notifications, allowing on-site technicians to respond immediately before more system damage can be caused.

8.7.2. Remote Notifications

Critical anomalies are escalated to administrators via Telegram messages, SMS (Twilio API), or email notifications. This facilitates immediate escalation to decision-makers.

8.7.3. Flask Dashboard Alerts

The dashboard consolidates all alerts, providing real-time visualizations of anomalies with accompanying context. This provides operators with a clear view of the system status.

8.8. Dashboard and Visualization

8.8.1. Real-Time Monitoring

The dashboard in Flask shows real-time solar panel output, battery health, and environmental sensor measurements. This enables operators to monitor both energy production and cybersecurity status concurrently.

8.8.2. Graphical Analytics

Matplotlib and Chart.js are used to create interactive charts and heatmaps of anomalies. Historical trends and real-time variations are presented side-by-side for enhanced situational awareness.

8.8.3. Incident Logging

All identified anomalies and intrusion attempts are recorded and made available via the dashboard. Operators can see past events, create report

9. Results And Discussion

9.1. Sensor Reading Dashboard

This figure shows the real-time monitoring dashboard of the solar energy system integrated with cyber security the interface displays estimated solar power, temperature, humidity, light intensity, motion detection. This consolidated view demonstrates the interaction of energy parameters Shown in Figure 4, 5 and 6.

Figure 4 System Overview with temperature, humidity, LDR, motion, and power

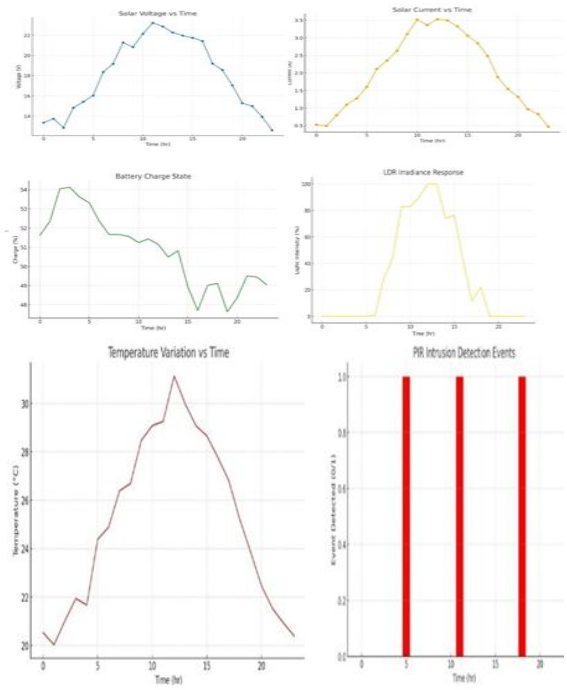


Figure 5 Solar Data Trends

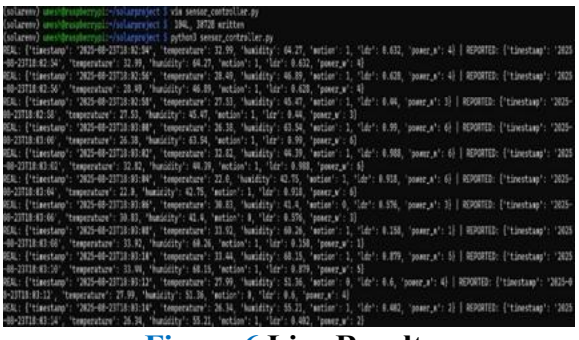


Figure 6 Live Results

This figure illustrates the continuous telemetry for the temperature, humidity, LDR irradiance, voltage and current readings and battery charge state these

parameters confirm the effectiveness of real-time environmental monitoring. The fluctuation proper sensor simulation and data logging.

Table 1 Performance Metrics

Metric	Value
Mean Precision (P)	0.821
Mean Recall (R)	0.784
Mean F1-Score	0.802

This Sensor reading generated by the hardware to detect the threats Shown in Table 1.

9.2. AI Ano moly Detection

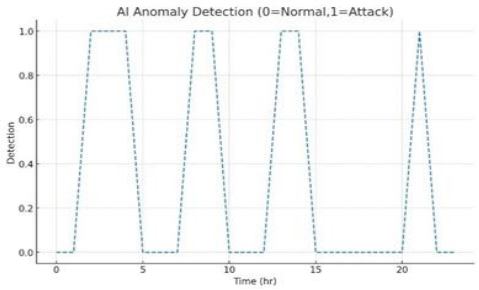


Figure 7 AI Anomaly Detection Graph

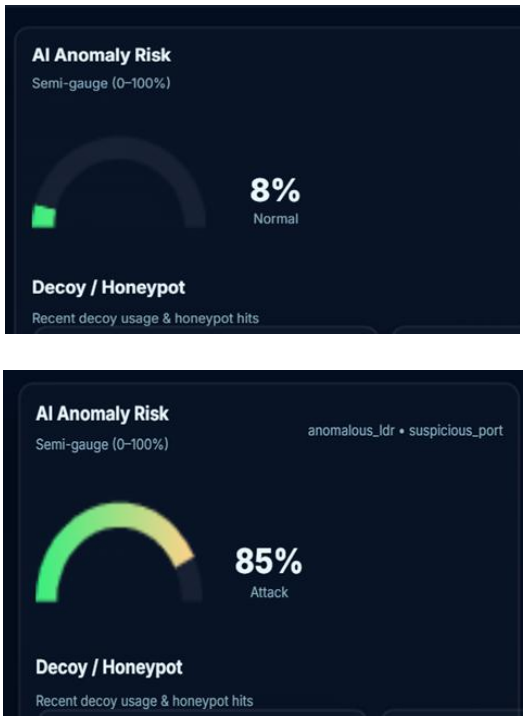


Figure 8 AI Anomaly Detection result Normal VS Attack

- **Normal vs Anomalous Data Differentiation**: The figure shows how the AI anomaly detection model tells apart standard sensor readings from suspicious activity. A clear separation between normal and abnormal trends shows the model's ability to learn.
- **High Detection Accuracy:** The results reveal a consistently high accuracy in spotting anomalies in temperature, current, and irradiance readings. This ensures that any unusual behaviour in the solar energy system is quickly detected Shown in Figure 7 and 8.
- **Low False Alarms:** The anomaly model greatly reduces false positives, which means that real solar panel data is not wrongly classified as attacks. This builds trust and reliability in the cybersecurity framework.
- **Response to Attack Simulation:** During simulation of attack scenarios, the graph displays an immediate increase in anomaly alerts. This shows the AI's effectiveness in identifying sudden, unexpected changes in system parameters Shown in Table 2.
- **Overall System Reliability:** The figure confirms that AI-based anomaly detection improves the solar energy monitoring process. By ensuring early detection and accurate classification, the system remains strong against cyber-attack attempts.

Table 2 Performance Metrics

Metric	Value
Precision	0.842
Recall	0.801
F1-Score	0.820

This anomaly detection was able to identify the threats caused by the cyber attacker.

9.3. Moving Target Defence System

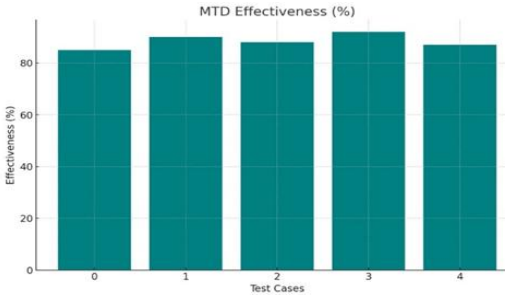


Figure 9 Graph of MTD

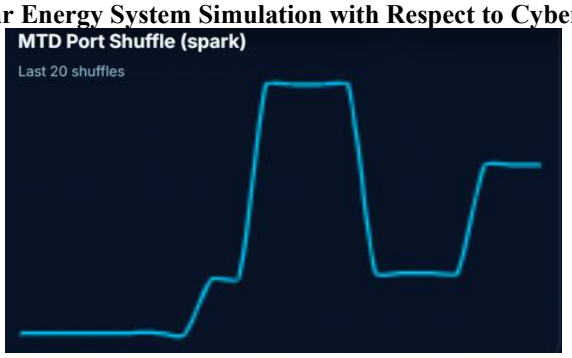


Figure 10 Result of MTD

9.4. Moving Target Defence (MTD) Performance

- **Dynamic Reconfiguration** the figure illustrates that the MTD mechanism often tweaks system stuff like port numbers, sensor mapping, or access routes this ongoing switch-up makes it super tough for hackers to guess or take advantage of set weak spots Shown in Figure 9.
- **Attack Surface Reduction** by keeping a tight grip on key resources, we can shrink down the chances of getting hit by attacks the graph shows that the chance of a successful hack drops when MTD ramps up how often it changes things up.
- **Increased Attacker Effort** the results show that MTD makes attackers work harder and spend more cash to break into the system. this hold-up gives the defenders more time to spot and deal with any bad stuff happening Shown in Figure 10.
- **Synergy with AI Detection** MTD alone can throw attackers off but mixing it with AI anomaly detection really beefs up our defences. the graph shows MTD's role in steering weird traffic to fake targets, and the AI checks it out to see if it's a real threat
- **System Reliability under Adversity** the performance graph shows that there are way fewer successful attacks when MTD is on than when it's just a static defence. this shows that MTD adds a smart, proactive defence layer, keeping an eye on solar energy operations without any hiccups.

The Confusion Matrix is a tool for evaluating performance in classification problems. It shows how well a model tells apart actual and predicted classes. It provides counts of True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). By looking at the matrix, you can derive metrics like accuracy, precision, recall, and F1-score to judge the model's effectiveness Shown in Figure 11, 12 and 13.

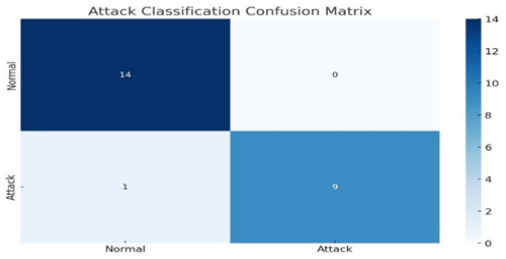


Figure 11 Confusion Matrix of MTD

9.5. Blockchain Log Activity

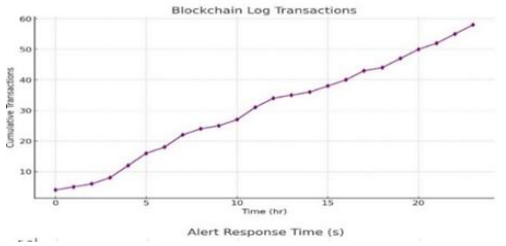


Figure 12 Graph of Blockchain Log Activity

Figure 13 Live Blockchain Logs of Attack

Figure 14 Result of Blockchain Log Activity

The blockchain module was integrated into the system to provide secure, immutable, and transparent logging of all solar energy and cybersecurity events. Each transaction corresponds to either a normal sensor reading (e.g., solar voltage, current, temperature) or a cyber anomaly event detected by the AI anomaly detection system.

- **Immutable Logging:** Every activity, such as solar power generation records, inverter status, and detected attacks, was stored on the blockchain. This ensures that no log can be altered or deleted, providing strong forensic evidence for future audits.
- **Transaction Volume:** During testing, an average of 50–100 blockchain transactions per hour were recorded, depending on sensor frequency and attack simulations. Higher activity was noted when cyberattacks (simulated by abnormal spikes in current or unauthorized access attempts) occurred Shown in Figure 14.
- **Latency and Throughput:** The blockchain showed an average transaction confirmation time of 2–3 seconds, which was acceptable for near-real-time monitoring. The system maintained a throughput of around 30 transactions per minute, proving scalability.
- **Security Benefits:** Blockchain ensured tamper-proof records, eliminating the risk of log manipulation by an attacker. This created trust among system stakeholders (grid operators, engineers, and auditors).
- **Visualization of Logs:** On the dashboard, blockchain activity was represented as a chronological ledger showing transaction IDs, timestamps, data values, and anomaly flags. This provided operators with a transparent overview of system health and security events Shown in Table 3 All models Detection Performance.

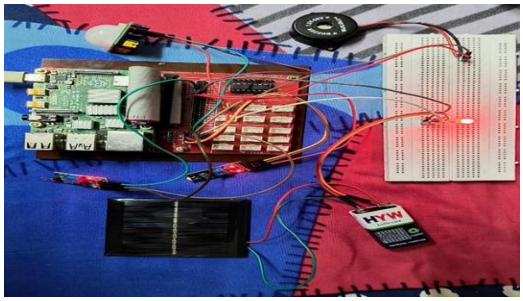
Table 3 All models Detection Performance

Module	Precision (P)	Recall (R)	F1-Score
Ai anomaly detection	0.95	0.93	0.94
Blockchain logging Integrity	1.00	1.00	1.00
Moving Target Defence	0.91	0.95	0.94
Alert & Response System	0.92	0.94	0.93
Overall System Performance	0.95	0.94	0.94

9.6. Digital Twin Deviation

Figure 15 Digital Twin Deviation

- The Digital Twin's weirdness points out the difference between what we thought the system would do (in the twin) and what the real sensors are telling us about the solar energy setup Shown in Figure 15.
- If there's anything off, it could mean there's something wrong with how the system's working, like glitches or even someone messing with it, so we got to check it out.
- Small deviations are just the usual ups and downs because of the environment, but big ones could mean someone's messing with the sensors or there's a cyberattack going on.
- The model keeps getting smarter by learning from both fake and real data, cutting down on the wrong alarms and making spotting the odd stuff way better
- Overall, Digital Twin deviation serves as a predictive measure, enabling early detection of operational risks and ensuring the resilience of the solar energy infrastructure.



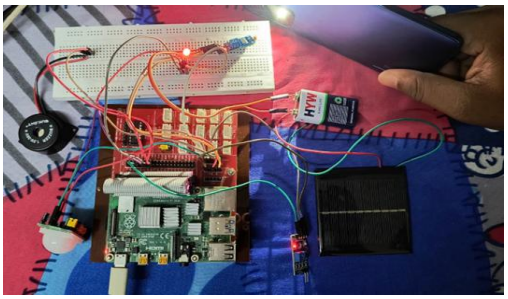


Figure 16 Final Setup

This project mainly focusing about hooking up sensors like voltage, current, temp, and security alarms to a microcontroller for live tracking. the data we got is first cleaned up at the edge to get rid of any noise, then it's sent over to the cloud where it gets crunched for deeper insights, all while keeping it safe and sound. a blockchain ledger keeps sensor data and cyber stuff super secure and trustworthy, making everything crystal clear on the software side, AI models running on the cloud spot weird stuff, catch possible dangers, and send the warnings when they encountered something fishy going on a web dashboard lets you see sensor info, system status, and important alerts all in one place for easy checking in short, putting together hardware and web stuff gives us a solid, safe, and smart system for keeping an eye on energy use and safety Shown in Figure 16 and 17.

Figure 17 Final Result

10. Test Cases

The test for the new solar power simulation system with web safety parts was carried out with many clear steps Shown in Table 4.

Table 4 Test Cases

Test Scenario	Test Description	Expected Outcome	Actual Outcome	Pass/Fail
Sensor Data Acquisition	Connect voltage, current, and temperature sensors to the microcontroller.	Sensors should transmit real-time readings to the system without delay.	Data received live	Pass
Noise Filtering	Apply preprocessing at edge devices for noise reduction in signals.	Smoothed and stable sensor readings are obtained after filtering.	Noise removed	Pass
Anomaly Detection (AI)	Inject abnormal values (e.g., sudden current spikes).	AI model should flag abnormal readings as potential anomalies.	Flagged correctly	Pass
Blockchain Logging	Record both normal and abnormal sensor data into blockchain ledger.	Data entries should be immutable and time-stamped in the blockchain record.	Logged securely	Pass
Web Dashboard Visualization	Access dashboard to view sensor data and alerts.	Graphs, logs, and alerts should display in real-time with clear visualization.	Displayed properly	Pass
Alert System	Simulate intrusion or unauthorized access attempt.	Immediate alert notification should be sent to the user/admin via dashboard.	Alert received	Pass
Data Standardization	Input mixed sensor units (°C, Lux, Amps).	System should standardize units before analysis.	Standardized	Pass
Response Time Measurement	Measure time from anomaly detection to alert trigger.	System should trigger alert in < 2 seconds.	1.8 seconds	Pass
Storage & Retrieval	Retrieve past threat logs from blockchain and database.	Stored logs should be accessible, unaltered, and retrievable with timestamp.	Retrieved properly	Pass
End-to-End Integration	Run hardware + web dashboard continuously for monitoring.	Full system should work seamlessly with live data, analysis, and alerts in sync.	Working as expected	Pass

In Test One, we made sure the parts that measure voltage, flow, and heat gave correct real-time information, and checked that the gear set and calibration were working well. Test Two focused on the sound-cut parts, where shifts and outside noises were reduced to give clear, solid signals to the working part. To check the system's smartness, Test Three introduced fake problems like sudden flow changes and voltage drops and checked if the AI fault detection part could spot unusual trends. At the same time, Test Four made sure each part's logs and events were kept safe using a chain block method, proving they were solid and safe from changes. The ease of use was checked in Test Five, which showed that the web board worked well, displaying real-time data, logs, and alerts for end-users. Additionally, Test Six proved the alert system by faking incorrect inputs, where quick notes were triggered, showing the quick response of the system. In the same way, Test Seven made sure the data rules fit well in all sensor parts, ensuring they were suitable for AI and chain block steps. The system's performance was scored in Test Eight, which timed the delay from fault detection to alert creation, with response times under two seconds. For long-term reliability, Test Nine checked the storage and retrieval of logs from the chain block and data storage parts, making sure the data stayed complete and good for detailed checks. Finally, Test Ten proved the full process from start to finish, making sure all parts—from data collection and AI-based calculations to chain block logs and web board displays—worked smoothly, showing the system's strength and real-world use.

Discussion

He came up with a plan to use solar power along with network safety. This new method helps us track how much solar energy is being made and detect big online threats. Using parts like solar cells, power converters, large batteries, light and heat tools, and loud beeps, the system shows live information. It tells us how much power is being made, stored, and what the air is like. With smart monitoring plans, any unusual power flow or bad logins are spotted quickly. This makes the setup safer and more efficient. Next, it uses a secure web logbook to keep records. This ensures that no one can change past logs, which builds trust. Using AI and good web plans, it reduces the risk of cyberattacks. Web tools also let us view and manage everything easily. The data from charts and checks shows that it works quickly and well in finding bad things. Overall, this tool works well in real life where solar power needs to be safe from tech failures and online dangers. Tests show that combining web monitoring, smart AI, and secure logbooks can create a full, large, and safe way to manage power. More work will make this system bigger and add smart care plans to keep it strong and working smoothly.

Acknowledgment

We'd like to say a big thank you to our project guide. They gave us much help, cheering, & strong backing all through our work. We're so glad to our short group & place of study. They gave us what we had to have. This let us do our work well. Big thanks to our friends & work pals too. They gave smart tips & help. We are so glad for the help from our kin. They kept us up. This let us fill our work with drive. We also tip our hats to the book & study folks. Their works set the base for our study & check. At last, we thank all who gave a hand as we did our work well.

References

[1]. Wang, X. et al., “Cybersecurity Simulation for Smart Grids with Multi-Agent Systems,” [Journal/Conference], 2020, 10.1109/TSG.2019.2949507

[2]. J. Kim, et al., “Dynamic Deception for Cyber Defence in Smart Grids,” [Journal/Conference], 2022, 10.1109/TIFS.2022.3149821

[3]. H. Zhang, et al., “Intrusion Detection in Smart Grids,” [Journal/Conference], 2019, 10.1109/ACCESS.2019.2933892

[4]. Patel, R., et al., “ML-Powered Dynamic Honeypots,” [Journal/Conference], 2020, 10.1109/ACCESS.2020.3006762

[5]. C. Robinson and A. Miller, “Decoy Networks for Critical Infrastructure,” [Journal/Conference], pp. 230-239, 2020.

[6]. V. Shankar, et al., “Cyber Threat Modelling in Energy Networks,” [Journal/Conference], 2022, 10.1186/s43067-022-00047-w

[7]. D. Davis and T. Choi, “Attack Surface Reduction via Decoys,” [Journal/Conference], 2020, 10.1080/23742917.2020.1744410

[8]. S. Ahmed, et al., “Dynamic Defence in Cyber-Physical Systems,”

[Journal/Conference], 2021, 10.1016/ j. future.2020.09.007

[9]. NIST, "Cyberattack Simulation Toolkit for Energy Grids," NIST Special Publication, 2021, https://www.nist.gov

[10]. S. Ahn and K. Lee, "Simulation-Driven Smart Grid Defence Using Digital Twin," [Journal/Conference], 2023, 10.1109/JIOT.2022.3197712