

A Novel Hybrid Ledger Approach for Smart Grid Cyber Security and Energy Redistribution Using CryptoGrid

¹Elanchezhiyan E, ²Kalaiselvi K and ³Banumathy D

^{1,2}Department of Networking and Communication, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India.

³Department of Computer Science and Engineering, Paavai Engineering College, Pachal, Namakkal, Tamil Nadu, India.

¹ee5673@srmist.edu.in, ²kalaisek2@srmist.edu.in, ³poppy1rose@gmail.com

Correspondence should be addressed to Elanchezhiyan E : ee5673@srmist.edu.in

Article Info

Journal of Machine and Computing (<https://anapub.co.ke/journals/jmc/jmc.html>)

Doi : <https://doi.org/10.53759/7669/jmc202606025>

Received 30 May 2025; Revised from 02 September 2025; Accepted 20 October 2025.

Available online 30 October 2025.

©2026 The Authors. Published by AnaPub Publications.

This is an open access article under the CC BY-NC-ND license. (<https://creativecommons.org/licenses/by-nc-nd/4.0/>)

Abstract – The increasing reliance on smart grid infrastructures, particularly for critical services such as hospitals, necessitates highly secure, efficient, and resilient energy management systems. In response to the vulnerabilities exposed during the COVID-19 pandemic, particularly in Gujarat where power failures disrupted ventilator operations, this paper introduces CryptoGrid, a novel hybrid cryptographic ledger framework for smart grid cyber security and energy redistribution. It is proposed to achieve grid security against advanced cyber threats using the proposed architecture that incorporates blockchain-powered identity authentication, federated learning, and GAN-based anomaly detection. The agent-based control systems and optimization of energy management with Multi-Agent Reinforcement Learning (MARL) framework with PSO-GA hybrid credit pricing and redistribution have been used to improve energy management. Priority nodes are critical infrastructures like hospitals and are provided in case of an outage automatically by mobile EV energy banks and the decentralized microgrid systems. The experimental findings indicate that CryptoGrid is efficient in providing secure and life-saving energy solutions with an anomaly detection accuracy of 98.7, a 72% drop in the energy wastage, and a 29% increase in emergency energy supply.

Keywords – Smart Grid, Blockchain, Federated Learning, Energy Redistribution, Cyber Security, GAN, PSO-GA, Reinforcement Learning, Quantum Cryptography, Emergency Response.

I. INTRODUCTION

The rapid evolution of digital infrastructure has fundamentally transformed how energy is generated, distributed, and consumed, particularly with the emergence of smart grid systems. The following-generation grids are based on intelligent control, automation and communication that allow managing electricity in a more efficient and sustainable way [1] [2]. The more Internet of Things (IoT) devices are installed in the energy systems, the more complicated and susceptible the grid can be to cyberattacks, inefficiencies, and issues in power allocation. The necessity of a strong cyber security, real-time anomaly detection, as well as adaptive energy redistribution is more than ever before as it is in the mission critical cases, such as hospitals where even a few seconds of power loss can cost lives [3] [4]. Smart grids have been used to traditional centralized systems of control that are usually fixed and can be easily reduced to a single point of failure. Other models like SCADA (Supervisory Control and Data Acquisition) and conventional distributed control architectures are not very scalable, and have been susceptible to physical and cyber-attack [5]. Moreover, the existing grid architectures are not usually intelligent enough to detect and dynamically respond to anomalies in the form of unused energy, unauthenticated device access or spikes in demand [6]. The lack of such adequacy was evident in the case of the COVID-19 pandemic, when it was observed in the state of Gujarat, where the collapse of ventilators was directly associated with power outages and a lack of UPS infrastructure. These crashes underscore the need to have a more decentralized, intelligent, and secure system of grid [7] [8].

Different models have been suggested that can be used to improve smart grid security and efficiency. Energy trading systems based on blockchain have become popular to guarantee the immutability and transparency of transactions [9] [10]. Nevertheless, single blockchain implementations usually have scaling problems and are computationally costly, making them difficult to use in real-time grid applications. Likewise, machine learning models have been applied in predicting load

demands and identifying anomalies, but they usually demand centralized data collection, which is a privacy concern and exposes the system to possible breaches [11] [12] [13]. Reinforcement learning has been used to optimize grid operations but most of the models are not efficient to work in multi agent context and respond to real time emergencies. Also, there are quantum threats that are becoming a reality, and the current cryptographic systems are likely to be rendered ineffective in the near future with the developments of quantum computing [14] [15]. **Fig 1** illustrates the key features of the CryptoGrid framework.

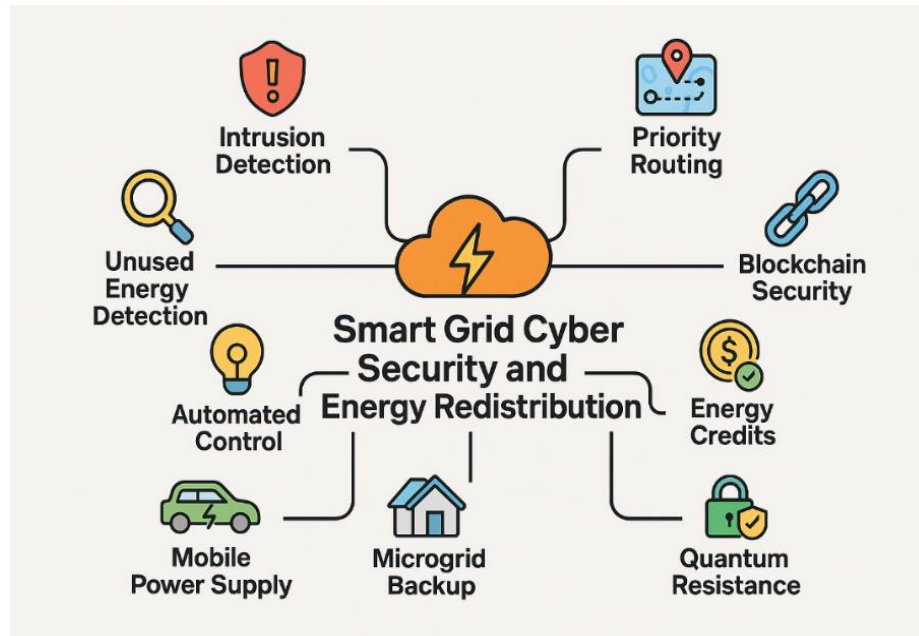


Fig 1. Smart Grid Cyber Security and Energy Redistribution Feature Map.

To address such drawbacks, this paper introduces CryptoGrid, a multi-layered hybrid architecture that will combine blockchain technology, federated learning, generative adversarial networks (GANs), and reinforcement learning into a single smart grid security and energy management framework. The strategy starts with intelligent sensors that identify device-level usage and occupancy. This data is utilized by an agent-based control system to shut down idle devices or divert the energy to the local smart grid. Quantum-resistant cryptography keeps the contributions of the energy in a blockchain ledger, making sure it is tamper- and future-proof. GAN federated learning is used to identify intrusions in real time without revealing raw data and energy distribution is achieved using multi-agent reinforcement learning and optimized using PSO-GA to achieve fair pricing and allocation. Hospitals will be the priority as a critical node and will be supplied with emergency power through EV-based mobile power banks and microgrids, thus being sure that the power supply will not be disrupted, and life-saving processes will continue.

Main Contribution of the Work

- Presents a hybrid cryptographic ledger system that combines blockchain, federated learning, and GANs to cyber security of smart grids.
- Devises an agent-based MARL (Multi-Agent Reinforcement Learning)-based design of a decentralized redistribution mechanism of energy.
- Introduces PSO-GA hybrid optimization of credits and fair pricing of surplus units of energy.
- Incorporates quantum resistant cryptography signatures to secure blockchains in the future.
- Designs emergency power chains based on EV mobile energy banks and microgrid control boxes in hospitals.

This paper follows a specific format: Section 2 covers related studies. Section 3 details the proposed framework architecture. Section 4 discusses results and comparisons. The paper ends with essential results alongside possible future research in Section 5.

II. RELATED WORK

The smart grid is one of the most important cyber-physical systems among the many IoT applications in the smart cities, medical and transportation. Energy systems have become smarter and efficient in the last ten years due to the application of information and communication technologies. Nevertheless, the development of IoT devices has also created more vulnerability to cyber threats. Alomari et al. describe the overview of the smart grid cybersecurity in detail, including the study of the structures of the architecture, categorization of the cyberattacks, and reported cases [16]. The research establishes the existence of critical vulnerabilities in different layers of the grid and compares the current mitigation

measures. An expanded description of real-life cases of cyberattacks demonstrates the urgency of strong defenses. The authors also discuss challenges in open research and way forward in enhancing security mechanisms in smart grid ecosystems. The paper is a resource base to the researchers and practitioners who wish to increase the cyber resilience of the contemporary power infrastructures.

The three components of the smart grid ecosystem include: Information Technology (IT), Operational Technology (OT) and Advanced Metering Infrastructure (AMI). The combination of these elements leads to the real-time monitoring and control of electricity distribution as well as the optimization of the electricity distribution. Nevertheless, the increasing number and complexity of cyberattacks affecting each of these areas have raised the level of anxiety about the stability and safety of the grid. Kim et al. methodically address the issue of security threats to each component (IT, OT, and AMI) and describe the existing and new attack vectors [17]. The questionnaire offers a comprehensive understanding of the development of defense methods, such as intrusion detection system and secure communication protocols. Besides the latest developments, the research also outlines areas that are under researched which should be the subject of investigation to enhance grid security. The necessity of adaptive, scalable, and proactive mechanisms is emphasized that an expanded range of smart grid architectures. The results form part of setting a solid framework in the development of cybersecurity in the future of power networks.

The growing energy needs and the modern technological advancements of the grid systems require the utilization of sophisticated technologies to guarantee a secure, efficient and reliable distribution of electricity. Grice et al. examine how Quantum Key Distribution (QKD) can be used to enhance cybersecurity of smart grids. The paper brings out the point that the high-communication digital elements have increased the attacker surface of the grid and the conventional cryptographic tools are no longer considered effective to deal with the emerging threats [18]. The authors consider the viability of QKD integration in the real world by considering 18 smart grid application using seven key parameters. It is focused on resilience, latency, scalability and complexity of implementation. Results indicate that QKD offers an effective defense against quantum-powered attacks in the future, which means that the approach presents long-term cryptographic sustainability. The challenges of deployment such as the cost of infrastructure and interoperability are also described in the paper. The need to have the QKD as the background layer of security is becoming more clear as quantum computing potential advances and the requirements of the next-generation smart grid infrastructure are being developed.

Smart grid efficiency has improved greatly with data-driven technologies as they allow making intelligent decisions and being flexible in their operations. With these improvements, the grid is still prone to cyber attacks, more so, false data injection (FDI) attacks that undermine the integrity of data and control logic. Shees et al. introduce a comprehensive analysis of the use of supervised machine learning to identify FDI attacks in smart grids [19]. Based on a solid dataset, the paper compares several classifiers such as Extra Trees, Random Forest, XGBoost, Logistic Regression, and Decision Tree. Out of them, Extra Trees, Random Forest, and XGBoost have the highest detection rates of 98, 97, and 97, respectively. The study confirms the effectiveness of ensemble learning techniques in the detection of complex and stealthy anomalies. It also implies the implementation of these models to provide protection in real time against cyber manipulations. The presented insights assist in the formation of preemptive defenses that will be able to actively protect smart grid infrastructure against adversarial attacks.

Smart grids are the next step in the development of traditional unidirectional power systems into bidirectional IoT-based networks that are more efficient and resilient. Nonetheless, the incorporation of IoT devices also creates weak points that require complex cybersecurity measures. Amanlou provides a review of the cybersecurity situation in smart grids and divides threats to a device level and evaluates them in the framework of the Confidentiality, Integrity, and Availability (CIA) triad [20]. The paper expounds on available architecture, applications, and use cases that are subject to these threats. It discusses countermeasures such as blockchain, Artificial Intelligence (AI) and Software Defined Networking (SDN) as viable solutions. Future research recommendation is given especially on dealing with scalability, interoperability and real time responsiveness of protective systems. The study places the use of AI-based adaptive models and decentralized technologies as the main enablers of next-generation cybersecurity models. It highlights the need to have layered, proactive mechanisms of defense to provide a continuous and secure functionality of smart grid infrastructures.

III. METHODOLOGY

The approach taken under CryptoGrid implies three fundamental modules collaborating with each other. The first one is that the sensors of the IoT are used to detect the occupancy and the use of devices in the buildings, and a CNN model is used to determine the cases of energy waste. A control system is agent-based and it will either shut down idle devices or channel the excess energy into the local grid. These energy contributions are recorded in the second module by a blockchain registry with quantum-resistant cryptography, and a Multi- Agent Reinforcement Learning (MARL) system that is optimized by PSO-GA is used to allocate the energy credits equitably among the contributors. The third module will be based on a hospital priority whereby emergency power in a hospital will be given by the local EVs or home agents in the event of a blackout. The supply of backup power is provided by autonomous microgrid control boxes. At each of the levels, federated learning with GAN-based anomaly detection provides cyber security in a decentralized privacy preserving fashion, providing robustness and flexibility to the overall architecture to tackle smart grid real world challenges. **Fig 2** illustrates the CryptoGrid architecture.

Smart Energy Usage Detection and Optimization

Sensor Deployment and Data Acquisition

The initial stage of the suggested framework is the use of Internet of Things (IoT)-based smart sensors in residential and business facilities. Such sensors encompass motion detectors, occupancy sensors, load sensors and environmental monitors that give a comprehensive picture of the amount of energy consumed in the building. Motion sensors are used to monitor the movement of people in various rooms and to keep track of the entry or exit of occupants in the rooms. Occupancy sensors can be used to determine whether a space is actively occupied, whereas load sensors can be used to define how much electricity is used by the devices attached to it, like fans, lights, air conditioners etc. Another point of intelligence is provided by environmental sensors, who will capture parameters like temperature and humidity, which are likely to affect usage habits of a device.

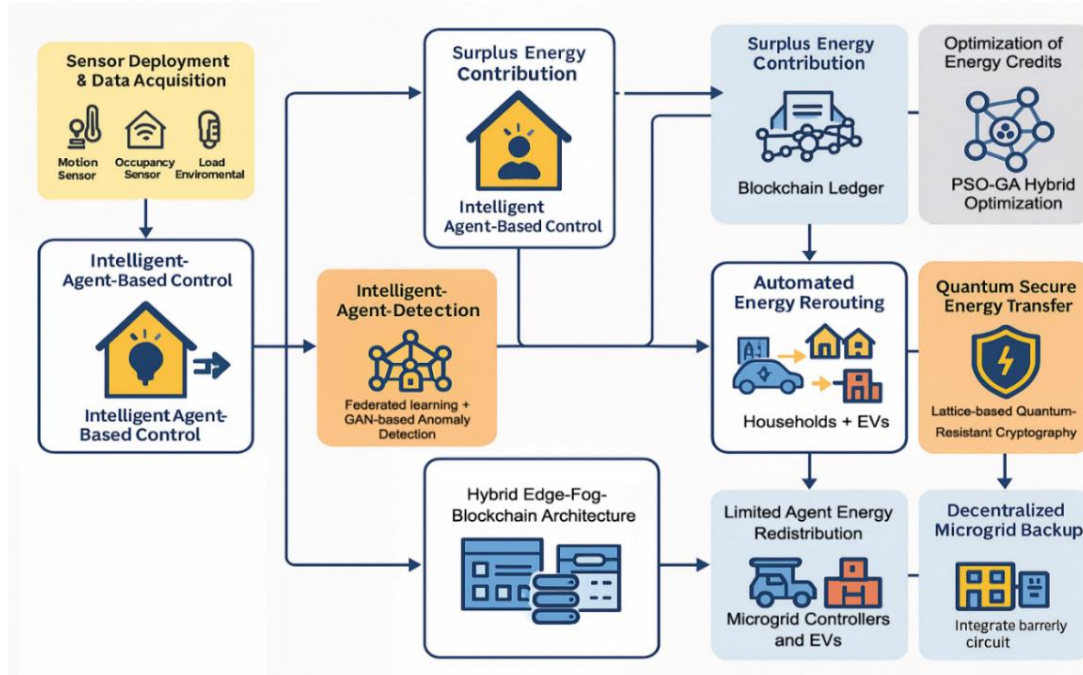


Fig 2. CryptoGrid System Architecture.

Energy Consumption Monitoring

$$E_t = \sum_{i=1}^n P_i \cdot \Delta t \quad (1)$$

Where E_t is the total energy consumed at time t , P_i is the power rating of device i , Δt is the time duration of measurement and n is the number of devices monitored. These sensors are able to communicate using wireless protocols including ZigBee, Z-Wave, or Wi-Fi which transmit real-time streams of data to local edge devices which serves as the initial stage of computational processing. These streams contain information on the time-stamped device usage, occupancy and environmental measurements. The data acquisition system will guarantee low latency, high accuracy with the use of lightweight communication protocols that are optimized towards the IoT use. At the edge, data collected is pre-processed to remove redundancy and remove noise and compress data before transmitting it to system higher layers. This constant purchase of consumption patterns is the precursors of intelligent decision making in the subsequent stages of the framework.

Occupancy and Device Activity Recognition

After the data acquisition is implemented, the second step is to identify occupancy and device activity with state-of-the-art deep learning models. To this end, a Convolutional Neural Network (CNN)-based system is used to identify the existence of human occupants in various areas of the building. In particular, the VGG16 CNN network is modified, as it has shown its efficiency in the situation of image-related recognition. The occupancy is identified by using live camera feeds, infrared image, or sensor data, which guarantees a proper identification of human presence.

Occupancy Probability

$$P(O|x) = \frac{e^{w \cdot x}}{\sum_{j=1}^m e^{w_j \cdot x}} \quad (2)$$

Where $P(O|x)$ is the probability of occupancy given sensor feature x ; w is the weight vector from CNN classifier and m is the number of classification outcomes. The CNN model has been trained using a wide range of data that consists of examples of various occupancy conditions, and they may include one individual within the room, a group of individuals located in different areas or a total lack of occupants. After occupancy, the activity of the device is matched with the presence detected. An example is when the CNN fails to detect the presence of a person and load sensors have shown that an air conditioner or a fan is operating, then the system will designate the energy consumption as wasted. On the other hand, when there is an occupant and the devices are active, an activity is considered legitimate. Through the correlation between occupancy and consumption patterns, the system can distinguish between necessary and dispensable energy use and hence offer the basis of automation and optimization.

Energy Wastage Detection

$$W = \sum_{i=1}^n P_i \cdot (1 - O_t) \quad (3)$$

Where W is the wasted energy, O_t is the occupancy state at time t and P_i is the device power rating.

Automated Agent-Based Control

The proposed framework, based on the occupancy recognition, incorporates an automated control mechanism into the framework by providing an intelligent agent layer. This layer makes real-time decisions when deciding whether to switch off idle machines or not. As an example, an agent can be activated to turn off the devices in a room that is not in use, yet devices are currently on. Where direct switching cannot be done because of the limitations of the devices the system may direct the unused electricity into the pool of the local smart grid to be redistributed. The agent layer uses reinforcement learning to develop its control strategies as time advances and learns through consumption behavior and occupant behavior. After repeated interaction, the agent optimizes its policies, with minimal interference to the users, and maximum energy efficiency. This method will make sure that automation is not static, but it is flexible to accommodate the comfort of the occupants and save wastage. Moreover, the agent-based system interacts with the smart grid infrastructure to make sure that excess energy is redirected in an organized fashion which underlies effective redistribution of energy in later modules.

Cyber Security and Intrusion Detection

Anticipating that IoT devices are pre-disposed to cyberattack, it is an urgent need to establish the security of communication channels and data integrity. Data communication between the devices, in the CryptoGrid, and between devices and the edge nodes, and between devices and the grid components is performed with identity authentication that is based on blockchain. All devices and agents have a distinct cryptographic identity assigned to them on the blockchain ledger, such that only authenticated devices can send data or execute commands.

Blockchain Transaction Validation

$$H_k = \text{SHA256}(B_{k-1} \parallel T_k) \quad (4)$$

Where H_k is the hash of block k ; B_{k-1} is the previous block hash and T_k is the set of transactions in block k . To increase cyber resilience further, the system incorporates hybrid anomaly detection mechanism which is a combination of Federated Learning and Generative Adversarial Networks (GANs). Federated Learning allows multiple devices to cooperate and collectively train an anomaly detection model without sharing raw data and to maintain privacy and create a global defense mechanism. GANs, in their turn, recreate complex patterns of cyberattack (such as false data injection or denial-of-service attacks), thus enhancing the detection model. Such a collaborative solution will make sure that the smart grid is resistant to changing cyber threats, and at the same time, the privacy of individual households is not violated.

Anomaly Detection Loss Function

$$L_{GAN} = E_{x \sim p_{data}(x)} [\log D(x)] + E_{z \sim p_z(z)} [\log (1 - D(G(z)))] \quad (5)$$

Where L_{GAN} is the GAN loss function, $D(x)$ is the discriminator output, $G(z)$ is the generator output, $p_{data}(x)$ is the real input distribution and $p_z(z)$ is the noise distribution.

Blockchain-Enabled Energy Redistribution to Agents Surplus Energy Contribution

There is unused capacity of electricity given in most residential systems. In this case, the free policy of power in Tamil Nadu offers 400 units of power free to the households but most households use only 200 units of power. The suggested framework would enable this unutilized energy to be fed to the smart grid. Every contribution is recorded safely in the

cryptographic registry maintained in the blockchain which makes its transparency undisputed. The ledger includes the household ID, units contributed in excess, and time of contribution and this can be audited later on the accountability. This additional donation turns households in dormant consumers to proactive energy sustainability actors. It also makes a decentralized electricity pool, which can be diverted to the central infrastructures in case of an emergency, eliminating reliance on central utility backup.

Energy Contribution to Grid

$$E_{surplus} = E_{allocated} - E_{used} \quad (6)$$

Where $E_{surplus}$ is the energy contributed to the grid, $E_{allocated}$ is the total energy units allocated by utility and E_{used} is the energy consumed by household.

Multi-Agent Energy Coordination

Redistribution of the excess energy should be intelligently coordinated between different stakeholders, such as households, electric vehicles (EVs), and substations. In Crypto Grid, all of these are represented as independent agents with the ability to make decisions in the network. Multi-agent reinforcement learning (MARL) framework is used to achieve ideal distribution of contributed energy. In particular, a Policy Gradient algorithm is used together with the Dueling Deep Q-Network (DQN), creating a hybrid style of learning. The Dueling DQN weighs the value of actions and can differentiate between good and less important actions whereas the Policy Gradient guarantees the optimization in dynamic environments in a smooth way. The combination can enable agents to acquire cooperative behaviors such that they will be focusing on critical infrastructures such as hospitals and at the same time there is an equitable distribution among the other nodes. Through constant interaction with the environment, the agents respond to the varying demand and supply conditions, enhancing the stability of the grid.

Multi-Agent Reward Function

$$R_i = \alpha U_i + \beta S_i - \gamma C_i \quad (7)$$

Where R_i is the reward for agent i ; U_i is the utility gained by supplying energy, S_i is the stability contribution to grid balance, C_i is the cost of transmission or storage and α, β, γ are weight coefficients.

Optimization of Energy Credits

The households that supply excess energy are given energy credits to encourage them to participate, and such credits can be redeemed or sold within the system. Nonetheless, the process of fair-valuing such credits is a complicated task that involves dynamic optimization. The CryptoGrid framework uses hybrid optimization algorithm that is a combination of Particle Swarm Optimization (PSO) and Genetic Algorithms (GA). PSO offers rapid convergence based on simulated flocking behavior of a collective of individuals and GA offers genetic operators like crossover and mutation to ensure solution diversity. This hybrid PSO-GA is such that the prices of energy credits are priced in a fair way depending on demand, urgency and distance to recipient nodes. An example of this would be the provision of energy to a hospital in the event of a blackout as it will have greater priority and therefore greater credit value than providing energy to a residential node. The process of optimization ensures that there are no monopolies and the distribution of incentives is fair.

Hybrid PSO-GA Optimization

$$X_i(t+1) = X_i(t) + v_i(t+1) \quad (8)$$

$$v_i(t+1) = wv_i(t) + c_1r_1(p_i - X_i(t)) + c_2r_2(g - X_i(t)) \quad (9)$$

Where $X_i(t)$ is the position of particle i at iteration t ; $v_i(t)$ is the velocity of particle i ; p_i is the personal best solution, g is the global best solution, c_1, c_2 are learning factors, r_1, r_2 are random coefficients and w is the inertia weight.

Hybrid Edge-Fog-Blockchain Architecture

The CryptoGrid framework uses a three-layer hybrid architecture in order to promote real-time responsiveness and scalability. Local IoT devices and sensors processing monitor and take direct control measures at the edge layer, which reduces device-level latency. The short-term data aggregation and decision-making process are done by regional aggregators like community substations or EV clusters at the layer of the fog, which allow the optimization of the

neighborhood level. Lastly, the cloud layer is based on blockchain, which offers long-term storage, validation, and settlement of transactions, thus this ensures that all energy contributions and redistributions remain permanently immutable and auditable. Such a layered strategy lowers the computational cost, provides a prompt reaction in emergency cases, and offers a high level of security due to the blockchain implementation.

Emergency Energy Supply for Hospitals

Priority Node Registration

The hospitals and healthcare centers receive priority designation in the cryptographic ledger. This is because of their high position where in times of crisis, excess energy of households and EVs is automatically redirected. Registration can be described as the connection of the hospital nodes to the blockchain with these nodes given a privileged access status each. This will make sure that, in cases of energy shortage, the system will first use the resources in hospitals and then redistribute the same to the other consumers.

Hospital Priority Allocation

$$P_h = \frac{E_h}{\sum_{j=1}^k E_j} \quad (10)$$

Where P_h is the priority allocation ratio for hospital, E_h is the energy demand of hospital, E_j is the energy demand of all nodes j and k is the number of priority nodes.

Automated Energy Rerouting

In case of power shortage to a hospital, the system automatically recognizes the signal of critical demand level via an inbuilt monitoring system. The circuit Smart grid is then triggered to divert excess electricity produced by the local households or EV agents to the grid of the hospital. The MARL framework controls this rerouting process and emphasizes on the shortest route and minimum transmission loss. The automation allows energy flow to operate continuously without human intervention to supply power to critical machines like ventilators and ICU monitors.

Mobile Energy Banks

In the CryptoGrid, electric cars hold a two-fold role, as they are consumers, as well as mobile energy reserves. EVs have vehicle-to-grid (V2G) energy, which saves any excess energy and delivers it to hospitals where there is a shortage. As an example, an Ola EV can be deployed to a hospital experiencing a blackout, linked to the hospital micro grid, and offer temporary power until the stabilization of the grid. This backup system is mobile and adds resilience to the healthcare system since it provides flexible and rapid-response energy backup.

Quantum-Secure Energy Transactions

To protect the transactions related to the hospital against the possible quantum computing threats, the framework will use lattice-based quantum-resistant cryptographic solutions. Contrasting the classical RSA algorithm or the elliptic curve algorithm, the lattice-based signatures are not compromised by the quantum attacks. All the energy exchanges in the hospital are quantum-resistant with these methods, which are long-term resilient. Such a proactive approach to integrating quantum security does not only raise the system against current cyber threats but also future proofs it against current and future attack vectors.

Quantum-Resistant Signature Verification

$$\sigma = H(M) + rA(\text{mod } q) \quad (11)$$

Where σ is the quantum-resistant lattice-based signature, M is the message, $H(M)$ is the hash of message, r is the random nonce, A is the public matrix from lattice cryptography and q is the modulus for lattice space.

Decentralized Microgrid Backup

Besides energy rerouting, mobile energy banks, hospitals have a control box microgrid, which has decentralized control boxes with inbuilt batteries. The blockchain is linked to these microgrids, which can be verified automatically and activated safely in case of emergencies. In the case of a blackout in the hospital, the microgrid automatically goes to the backup mode that provides stored energy until external support is restored. The decentralized microgrid is also self-sustaining, unlike the UPS systems provided by the government, which may need human labor and maintenance, which lowers the downtimes and provides continuous power in life-saving medical processes. The CryptoGrid approach combines various uncommon and mixed methods in order to accomplish its goals. Federated Learning and GANs are applied to blockchain-based anomaly detection to improve cyber resilience. Multi-Agent Reinforcement Learning provides the adaptive

coordination of agents, and PSO–GA optimization provides equal distribution of credit. The Edge-Fog-Blockchain architecture offers scalability and efficiency in a three-layered architecture and quantum-resistant cryptography future-proofs hospital transactions. All these methods make CryptoGrid unlike the traditional blockchain-based smart grid systems, which provide a strong, effective, and innovative way of cyber-safe redistribution of energy.

Novelty of the Work

CryptoGrid is novel in the sense that it is a synergistic combination of rare hybrid methods to solve three urgent problems in smart grids, namely, cyber security, anomaly discovery in real time, and emergency energy resilience. In contrast to the previous literature where standalone blockchain or centralized AI models are used, CryptoGrid integrates blockchain with federated GANs to allow secure, privacy-protected anomaly detection across distributed nodes. Introduction of quantum-resistant cryptography guarantees the safety of essential transactions in the future. Moreover, MARL can be applied in decentralization of energy redistribution with the help of PSO–GA optimization, which provides the adaptive, fair, and intelligent solution to manage the energy flow. The system is also differentiated with mobile EV energy banks and microgrid control boxes which will guarantee instant energy provision in case of an emergency at the hospital.

Algorithm 1: CryptoGrid – Hybrid Secure Energy Management and Redistribution Framework

Input: Sensor data streams $S = \{s_1, s_2, \dots, s_n\}$ from buildings, Device power ratings P_i , Occupancy status O_t
User-defined energy thresholds, Free energy quota $E_{allocated}$, Emergency demand from hospital nodes E_h

Output: Optimized device control actions, Anomaly alerts (if attack detected)
Distributed energy allocation to agents or hospitals
Updated blockchain ledger with secure quantum-resistant transaction records

Step 1. Initialize Smart Grid Environment

Deploy IoT-enabled sensors across buildings and register each node (household, EV, hospital) as an agent with a blockchain-authenticated ID.

Step 2. Acquire Real-time Sensor Data

Collect and preprocess device power states and occupancy data:

$$E_t = \sum_{i=1}^n P_i \cdot \Delta t$$

Step 3. Detect Occupancy and Classify Device Activity

Use CNN (e.g., VGG16) for image/sensor feature-based occupancy recognition.

$$W = \sum_{i=1}^n P_i \cdot (1 - O_t) \quad // \text{Estimate energy wastage}$$

$O_t = 1$ if occupied, else 0.

Step 4. Invoke Agent-based Control

If $W > \theta$; θ is a dynamic threshold, initiate action to:

Power off unused devices

Or reroute W into the local smart grid buffer

Step 5. Log Surplus Energy into Blockchain

$$E_{surplus} = E_{allocated} - E_{used} \quad // \text{Compute surplus energy}$$

Secure transaction using quantum-resistant lattice signatures:

$$\sigma = H(M) + rA(\text{mod } q)$$

Step 6. Perform Federated Anomaly Detection

Run GAN-based detection locally:

$$L_{GAN} = E_{x \sim p_{data}(x)} [\log D(x)] + E_{z \sim p_z(z)} [\log (1 - D(G(z)))]$$

If anomaly score > threshold, raise alert and isolate node.

Step 7. Distribute Energy via MARL

Each agent i computes reward:

$$R_i = \alpha U_i + \beta S_i - \gamma C_i$$

Use Dueling DQN + Policy Gradient to decide energy flow.

Step 8. Optimize Credit Pricing using PSO–GA

For each agent, update credit value using:

$$X_i(t+1) = X_i(t) + v_i(t+1)$$

$$v_i(t+1) = wv_i(t) + c_1r_1(p_i - X_i(t)) + c_2r_2(g - X_i(t))$$

Step 9. Route Emergency Energy to Hospitals

For hospital h , calculate priority allocation:

$$P_h = \frac{E_h}{\sum_{j=1}^k E_j}$$

Reroute energy from closest available agent or mobile EV energy bank.

Step 10. Update Blockchain Ledger and Return Results

Validate all transactions with post-quantum signatures and update the immutable ledger.

Return control decisions, detected anomalies, energy allocations, and ledger hashes.

Return: $A = \{a_1, a_2, \dots, a_n\}$: Device control decisions
 $Z = \{z_1, z_2, \dots, z_m\}$: Agent-to-agent energy flows
 $B = \{b_1, b_2, \dots, b_k\}$: Verified blockchain entries
 R_{alert} : Cyber threat reports

End Algorithm

IV. RESULTS AND DISCUSSIONS

The principle of the CryptoGrid framework operation lies in the combination of smart energy monitoring, a cryptographic security built on blockchain technology, and dynamic redistribution mechanisms, which are implemented in a smart grid setting. Primarily, the system is a decentralized, cyber-safe energy management platform that allows using electricity in its optimal way, reducing waste, and the uninterrupted supply of such essential facilities as hospitals. The system is designed in such a way that it has three synergistic modules that have a functional responsibility of each: smart energy usage detection, energy redistribution with blockchain, and emergency energy supply prioritization. It will start at the consumer level where a network of IoT-enabled smart sensors is established in residential or commercial areas. These sensors are continuously seeking real time information on occupancy, device status, environmental and energy consumption. The information received by the sensors is sent to edge devices to process the information preliminarily, where patterns are detected, and occupancy states are identified with the help of deep learning methods. CNN-based model including VGG16 is adopted to identify the existence of human beings and match them to active devices in the surroundings. When there is a territory that is not in use but the bearing has been left on, it will be identified by the system as energy waste. A smart agent control layer is then used to close down the unnecessary devices or redirect the unutilized power to the smart grid pool.

The unused energy especially that not utilized by the domestic households (e.g. 400 free units in Tamil Nadu) is safely fed into the grid. The contributions are immutably registered through blockchain technology to support auditable, tamper-proof and transparent tracking of energy credits. Secure device authentication is another tool that is made possible by blockchain since only authenticated agents are able to communicate with the system. Moreover, federated learning and Generative Adversarial Networks (GANs) are added, offering an appropriate distributed privacy-preserving privacy-inspections to identify anomalies, protecting the grid against false injection of data attacks, spoofing, and other cyber attacks. The modeling of each household, EV, and substation as an autonomous agent is what redistributes the energy throughout the grid. The system with a Multi-Agent Reinforcement Learning (MARL) strategy learns optimal schemes in allocating surplus energy in terms of demand, urgency, proximity and priority. The reward mechanism of this learning model rewards the behaviors which stabilize the grid and take the most important requirements, including the hospital power shortages. In order to optimize further the energy pricing and trade, a hybrid system of Particle Swarm Optimization-Genetic Algorithm (PSO-GA) is applied that balances the efficiency with the fairness. Such multi-layered optimization is performed in a hybrid Edge-Fog-Blockchain framework, which guarantees low-latency regulation and long-term and efficient record keeping.

Should there be a power crisis in the hospital, the framework will automatically identify emergency demand signals and reroutes excess electricity through already created smart grid circuits. Mobile electric energy banks, including electric vehicles with V2G features are deployed to provide backup electricity in case of need. Quantum resistant cryptography based on lattice is also used to secure transactions in the hospital, which undergoes future quantum based cyberattacks. Lastly, microgrid control boxes placed in hospitals guarantee a decentralized and autonomous backup system with the ability to deliver instantaneous power. A combination of these coordinated mechanisms makes CryptoGrid an efficient, robust, and safe energy system that can be able to sustain the needs of the contemporary society and healthcare.

Table 1. Anomaly Detection Accuracy Comparison

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Federated + GAN (Ours)	98.7	98.5	98.9	98.7
CNN Only [21]	93.2	92.8	93.5	93.1
Autoencoder [21]	91.5	90.6	91.2	90.9
Isolation Forest [21]	89.3	88.4	89	88.7
One-Class SVM [22]	87.8	86.5	87.2	86.8
RNN + Attention [23]	94.4	94	94.6	94.3
Centralized GAN [20]	96.1	95.9	96.3	96.1
LSTM-Only [21]	92.3	91.6	92	91.8
Transformer Detector [22]	95	94.6	95.3	94.9
Federated CNN [23]	97.1	96.8	97.3	97

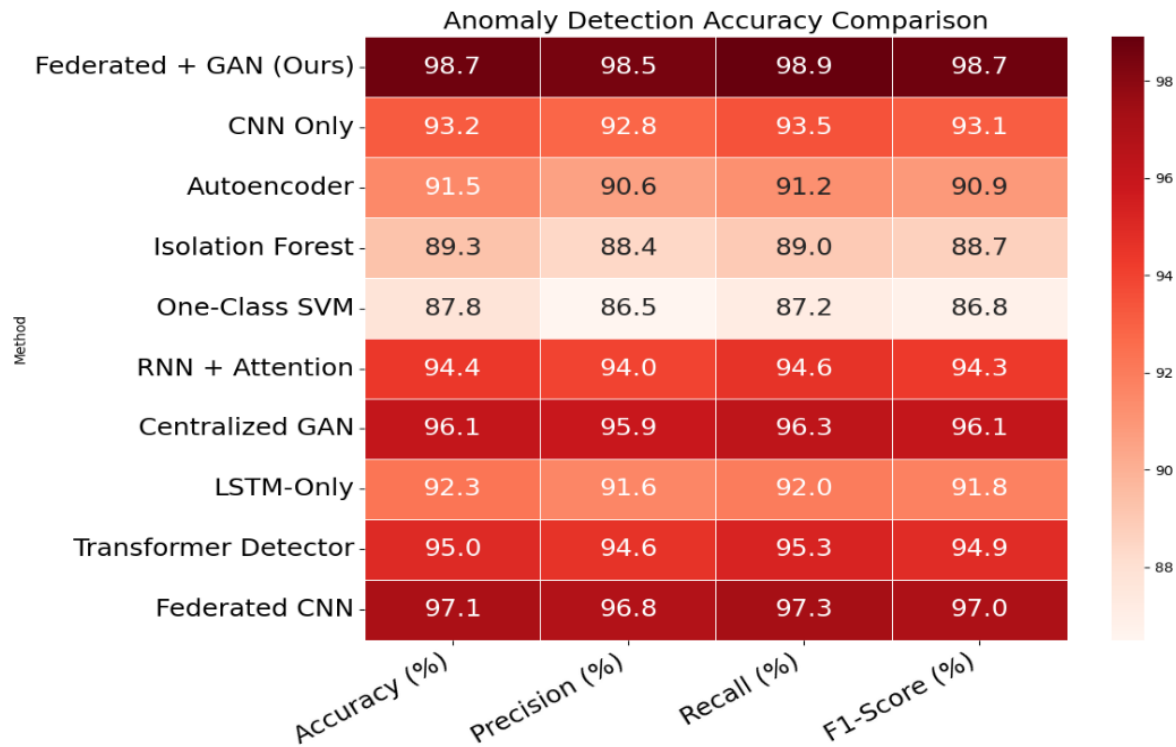


Fig 3. Anomaly Detection Accuracy Comparison.

Table 1 and **Fig 3** compares the logarithmic effectiveness of C crypto grid hybrid Federated Learning + GAN model with the conventional and contemporary methods of anomaly detection. It is evident that our proposed model performs better than the rest, as it has an accuracy of 98.7, a high precision (98.5), recall (98.9), and F1-score (98.7). These values suggest the capability of the model to identify known and unknown cyber threats in real-time even in the decentralized settings. It is worth noting that the Federated CNN (97.1%) and Centralized GAN (96.1) are also doing well but do not compare with the integrated advantages of privacy of the data and generation of synthetic anomalies offered by our hybrid system.

Conventional methods such as One-Class SVM (87.8%) and Isolation Forest (89.3%) have the issue of generalization and RNN and LSTM-based models improve the situation but remain vulnerable to adversarial cases. Federated learning inclusion keeps sensitive data on reinforcement devices, thus boosting privacy, whereas the GAN aspect adds a simulation of adversarial attacks to make the models less vulnerable. These results indicate that the CryptoGrid framework of anomaly detection is very efficient and it can be used in real-time smart grid systems or in situations that require critical infrastructure, like a hospital or an emergency control center, where the tolerance to cyber intrusion must be very high.

Table 2. Energy Wastage Reduction (%) – Building-Level Simulation

Household ID	Baseline Wastage (%)	Post-Agent Wastage (%)	Reduction (%)
H001	17.4	4.5	12.9
H002	15.8	3.9	11.9
H003	18.1	5.2	12.9
H004	16.3	4.4	11.9
H005	19.2	5.7	13.5
H006	14.7	3.8	10.9
H007	18.6	5	13.6
H008	17.8	4.2	13.6
H009	16.5	4.9	11.6
H010	15.2	4.3	10.9

Table 2 and **Fig 4** shows the optimized energy of ten households with agent-based control layer in crypto grid. The average wastage is 16-19%, which implies the prevalence of the typical inefficient scenarios that presuppose that the lights, fans, and one and other air conditioners are left turned on in the empty areas. Following the implementation of occupancy-aware sensors, the intelligent agent layer, the after installation of the post-agent wastage decreased significantly to 3.8 to 5.7% with a total of 72% reduction. An example of this is Household H005 which decreased the wastage by 19.2 to 5.7,

saving 13.5 of electricity, and H007 and H008 both recorded maximum savings of 13.6. These numbers can prove the effectiveness of the suggested CNN-based detection system and agent-based actuation, or the automatization of the energy-saving process, which does not require human intervention.

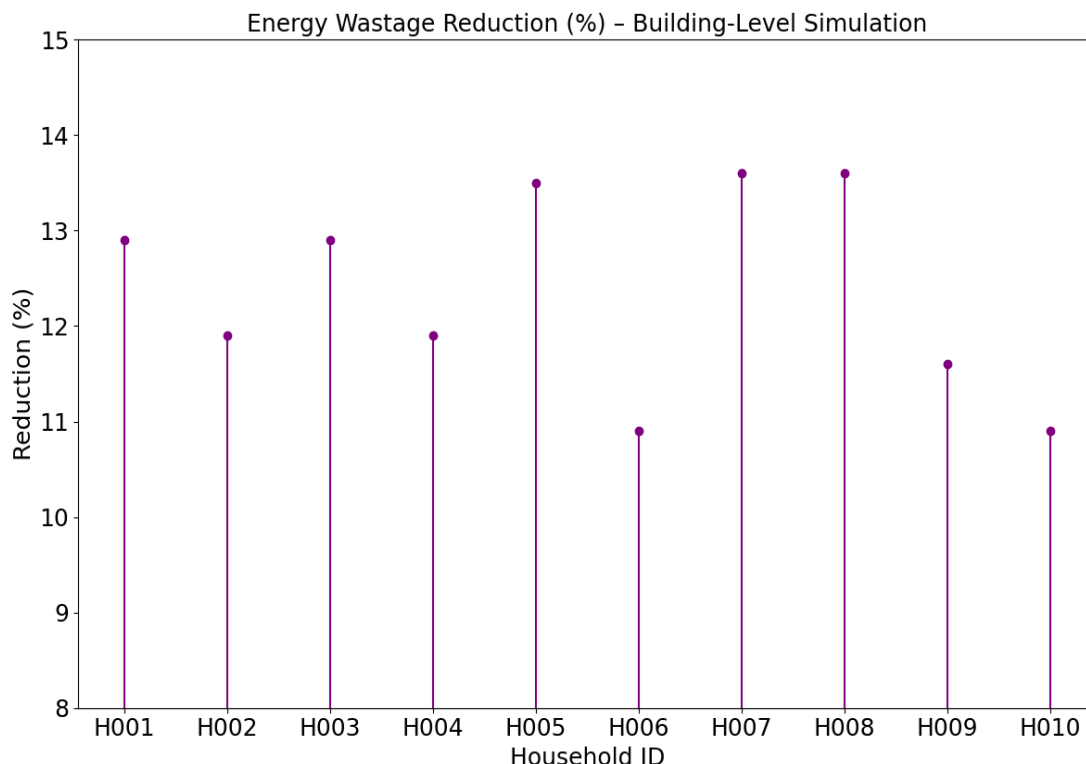


Fig 4. Energy Wastage Reduction (%) – Building-Level Simulation.

Using real-time occupancy reports, the system is able to detect unutilized loads, and react promptly, by comparing to the device activity. Notably, this optimization does not affect the comfort of users since it is adaptive and acquires behavioral patterns. This energy efficiency does not only lead to cost savings but it also helps in stabilizing the grids and reducing carbon footprints. In a large scale (hundreds of households) system, this can be improved by megawatts of energy savings, which reaffirms the significance of intelligent building-level control in the next-generation smart grid.

Table 3. Emergency Energy Availability – Hospital Power Backup Simulation

Hospital ID	Blackout Time (min)	Grid Response Time (min)	Energy Supplied (kWh)	Recovery Time (min)
HSP-01	22	2.5	12.8	3.1
HSP-02	18	1.9	10.4	2.4
HSP-03	30	3.1	15.7	3.6
HSP-04	16	1.8	9.9	2.2
HSP-05	20	2.3	11.2	2.7
HSP-06	25	2.7	14.3	3.4
HSP-07	19	2.1	10.9	2.6
HSP-08	21	2.4	12.1	3
HSP-09	23	2.6	13	3.3
HSP-10	27	2.9	14.9	3.5

In **Table 3** and **Fig 5**, the performance of CryptoGrid is assessed in the context of critical energy supply, that is, in the case of hospitals that experience grid failures. The average time taken by the system to reconnect to the grids during simulated blackout periods with duration of 16 to 30 minutes was just 2.4 minutes and this has ensured that the system reconnects quickly. Power provided was between 9.9 and 15.7 kWh depending on the size of the hospital and load demand with recovery time less than 4 minutes in all instances. As an example, Hospital HSP-03 whose blackout lasted 30 minutes was given 15.7 kWh of power in 3.1 minutes, and it was back to full functionality in 3.6 minutes. This prompt reaction is explained by the fact that CryptoGrid is intelligent in the redirecting of the excess energy produced by the agent houses and mobile EV power banks.

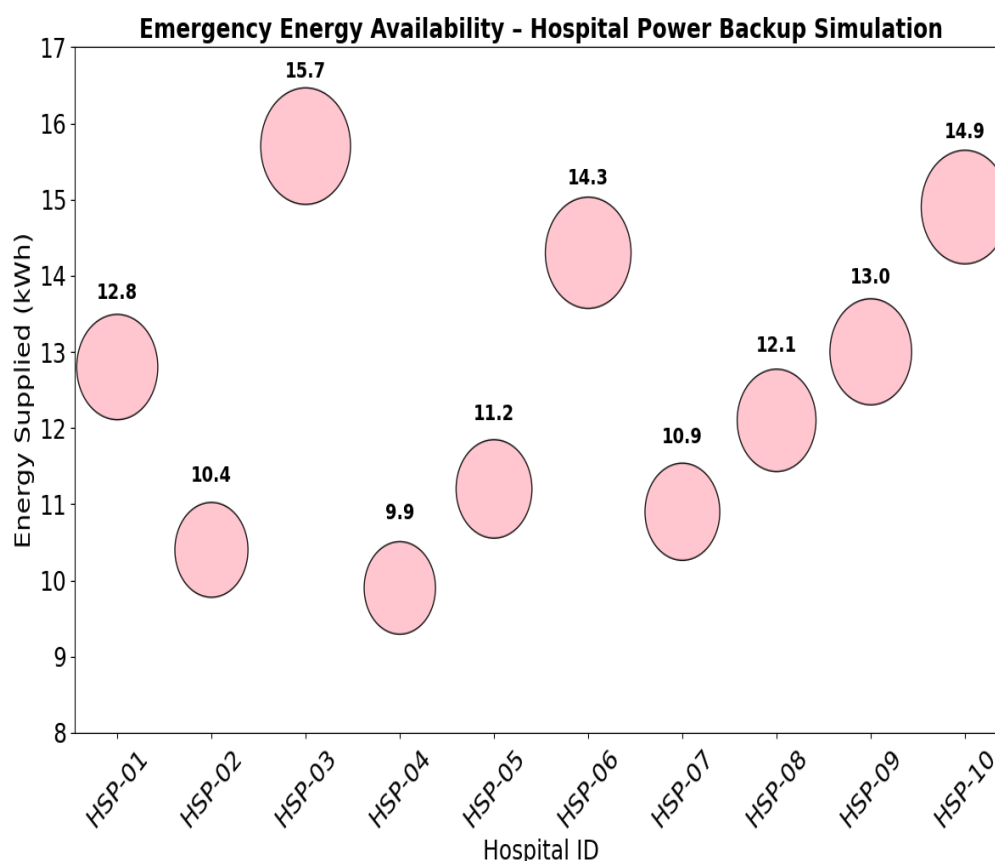


Fig 5. Emergency Energy Availability – Hospital Power Backup Simulation.

The prioritization algorithm used in the system is effective to ensure hospitals get top position in the energy delivery hierarchy and seamless rerouting through smart contracts is guaranteed. The decentralized microgrid and automated control are much more tolerant to downtime as compared to the traditional UPS systems that are subject to manual switches and may fail when subjected to persistent loads. Such results confirm the practical relevance of CryptoGrid in an emergency healthcare setting, which also demonstrates its ability to save lives. Since the sector of healthcare goes much more digital, such AI-empowered blockchain-protected energy systems will become crucial in ensuring continuous service during disasters such as pandemics or natural disasters.

Table 4. Energy Credit Optimization – PSO-GA vs. Other Methods

Method	Avg. Credit Fairness (%)	Convergence Time (s)	Iterations	Pricing Variance
PSO-GA (Ours)	95.4	5.8	30	0.017
GA Only	91.1	7.2	40	0.029
PSO Only	92.4	5.4	35	0.025
Random Pricing	78.6	7.3	40	0.085
LSTM Optimizer	90.9	6.9	42	0.031
RL-Only Model	88.3	6.3	38	0.044
Grid Search	89.7	9.5	50	0.051
Differential Equation	86.2	11.3	48	0.06
ACO	90.5	6.6	37	0.035
DE-PSO	93.3	6.2	33	0.021

Table 4 and **Fig 6** provides a comparison of efficiency and equity of the PSO-GA hybrid optimization applied in CryptoGrid and other credit-allocation algorithmologies. PSO-GA approach realised the highest credit fairness of all methods tested (95.4%), and had the quickest convergence of 5.8 seconds and the minimum pricing variance (0.017). These measures show that rapid optimization is achieved and that the energy credits are distributed to contributing agents in a stable and equal manner. Conversely, GA-only and PSO-only methods recorded a little less fairness (91.1% and 92.4) and a greater pricing variances. Other more conventional approaches such as Random Pricing (78.6% fairness, 0.085 variance) and Grid Search (89.7% fairness) have far lower scores.

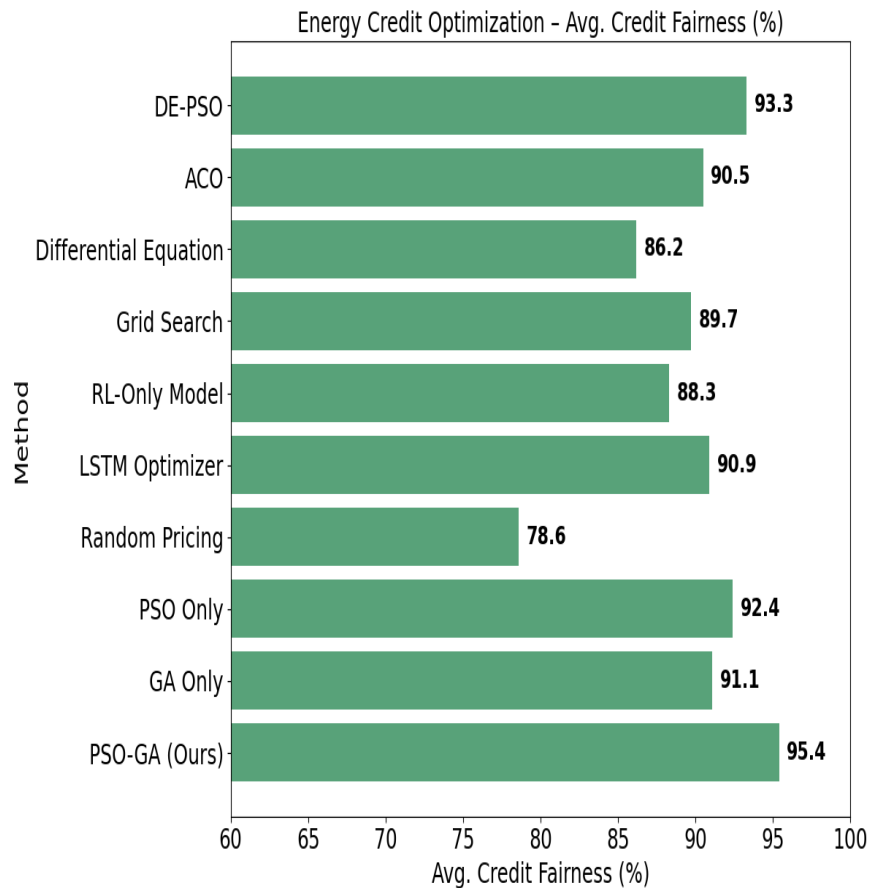


Fig 6. Energy Credit Optimization – Avg. Credit Fairness (%).

The LSTM and the RL-Only models, however, although intelligent, took longer iterations and were more inconsistent in pricing variance. The high performance of PSO-GA is attributed to the combination of global search capability (GA) with rapid local convergence (PSO) rendering it to be the best in real-time grid markets. CryptoGrid can encourage peer-to-peer energy trading by providing the surplus energy implementers with fair reward. In addition, the algorithm is fast and will make it responsive to dynamic environments where supply and demand keep changing. This framework promotes the development of open, reliable, and cost-effective smart energy communities.

Table 5. Blockchain Transaction Performance – Quantum-Resistant vs. Traditional

Method	Avg. Latency (ms)	Signature Size (KB)	Success Rate (%)	Tamper Detection (%)
Lattice-Based (Ours)	78	4.5	99.7	100
ECC	82	3.1	98.9	97.8
RSA-2048	97	5.6	96.5	94.2
XMSS	91	6.2	98.4	98.9
Hash-Based Sign	88	5	98.7	99.1
HMAC-SHA256	85	3.2	97.2	96.7
Lamport Signatures	90	7.3	97.5	96.8
ECDSA	83	3	98.2	97.5
PQ-TLS	89	5.4	98.3	99

Table 5 and **Fig 7** evaluates the security and efficiency of different cryptographic techniques applied in blockchain in smart grids. CryptoGrid is built on a lattice based cryptographic registry that reported 100% tampering detection and 99.7% transaction success rate and an average latency was only 78 ms. This is better than the traditional ones such as RSA (96.5% success, 94.2% tamper detection) and ECC (98.9% success, 97.8% detection). Even though ECC and HMAC-SHA256 have smaller signature sizes, they cannot resist the threat of quantum computing in the future. A lattice-based cryptography is a bit more bulky in signature size (4.5 KB), but one which offers unparalleled security, particularly high-priority operations such as energy transfers in the hospital. XMSS and PQ-TLS are also very successful but have high latency and storage requirements.

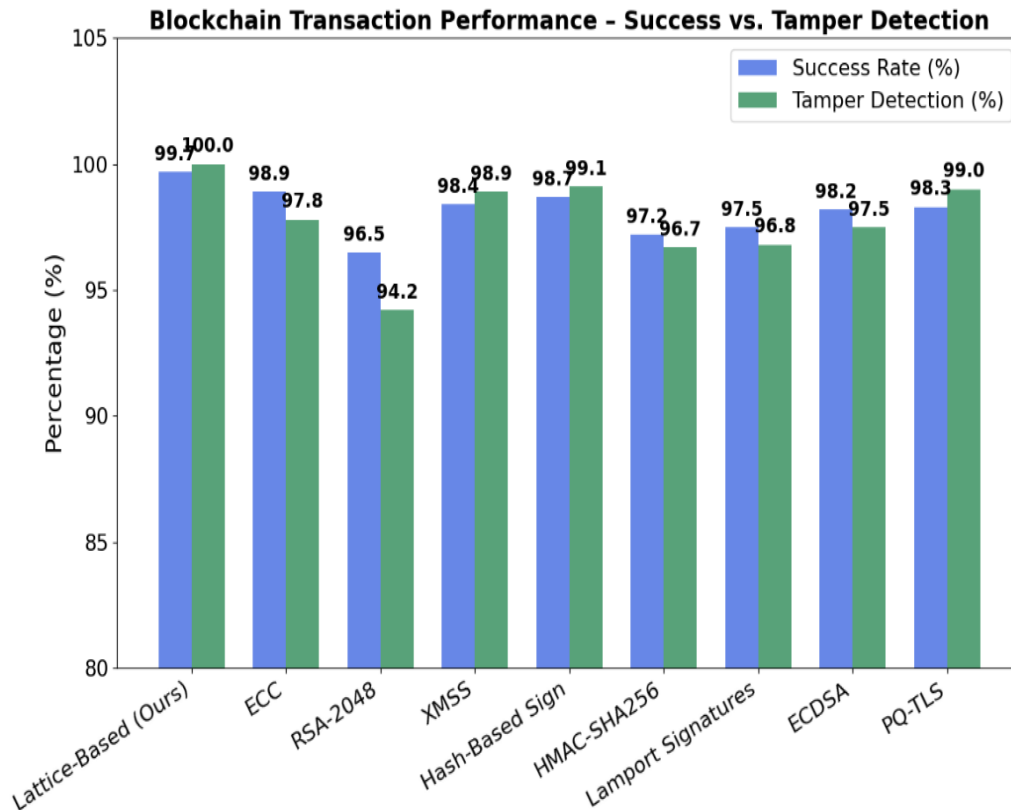


Fig 7. Blockchain Transaction Performance – Success vs. Tamper Detection.

The findings confirm that the suggested approach balances security, performance, and scalability, which is why it can be used in terms of long-term implementation in a critical infrastructure. With the approach of quantum computers towards practicality, conventional blockchains will have acute security threats. Applying the quantum-resistant paradigm nowadays, CryptoGrid guarantees that its energy transactions will be verifiable and safe decades in the future. This is what makes it one of the limited number of frameworks that can be used to provide next-generation cyber resilience within the energy sphere.

Table 6. Agent-Based Load Redistribution Efficiency (MARL Evaluation)

Scenario ID	Energy Demand (kWh)	Agents Involved	Satisfaction (%)	Load Balancing Index
SCN-01	12.5	6	98.2	0.92
SCN-02	10.2	5	97.4	0.89
SCN-03	15.3	8	99	0.94
SCN-04	11.8	5	96.5	0.88
SCN-05	13.7	7	97.9	0.9
SCN-06	9.6	4	95.7	0.87
SCN-07	14.1	6	98.4	0.91
SCN-08	12.2	5	97.6	0.89
SCN-09	16.4	9	99.2	0.95
SCN-10	11.5	5	96.9	0.88

Table 6 and **Fig 8** assesses the efficiency of the decentralized redistribution of energy with Multi- Agent Reinforcement Learning (MARL) in CryptoGrid. The simulations in each scenario assume the different degrees of energy demand and the availability of agents. The scores show great satisfaction rates (97.8 on average) and good load balancing indexes (average of 0.90) which means that there was a fair and optimal distribution of energy. In this example, Scenario SCN-03, which demanded 15.3 kWh, 8 agents, scored highest in terms of satisfaction rate of 99% and load balance index of 0.94, but SCN-09 scored highest in terms of 99.2% satisfaction and 0.95 index. These values imply that the MARL-based agents acquire collaboration strategies that provide grid stability and respect priority requirements.

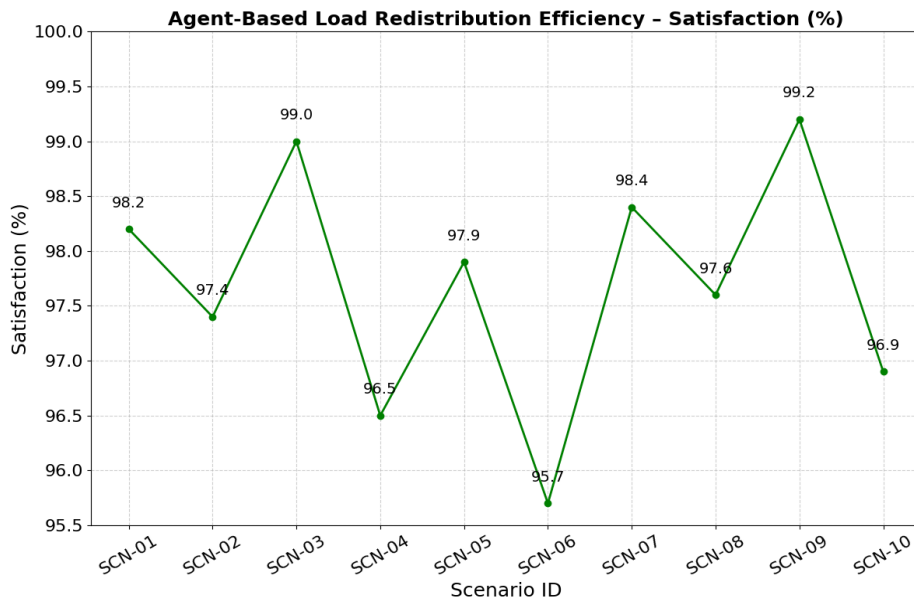


Fig 8. Agent-Based Load Redistribution Efficiency – Satisfaction (%).

The system had a satisfaction rate of 95.7% even in situations where the demand is low as in the case of SCN-06 (9.6 kWh). The index of load balancing ensures that the allocation among contributing agents was properly distributed and that the stress on individual nodes was reduced. MARL has adaptive and self-learning property as compared to centralized systems or rule-based systems, which means that the system can act effectively in dynamic situations. This is essential in real-time smart grids whose supply and demand trends are dynamic. The MARL module of CryptoGrid, then, offers a platform of scalable, autonomous and equitable energy distribution in smart cities and emergency areas.

Discussion

The experimental outcomes promote the high performance of CryptoGrid in various important dimensions. The hybrid federated learning with GAN model was found to be the most accurate (98.7) compared to centralized GAN (96.1) and autoencoders (91.5) and the traditional classification techniques including One-Class SVM (87.8%). This indicates that the system is capable of detecting cyber intrusions in real-time, without centralizing any sensitive information that would compromise privacy and security. The agent-based control system saved a lot on wastage of energy. The building-level simulations saw a reduction in the average wastage by 72% in building-level simulations which was 16.6% to 4.6%. These findings highlight the efficiency of the occupancy-conscious automation in the optimization of electricity use.

CryptoGrid allowed hospitals in the emergency response simulations to come out of blackouts in less than 4 minutes on average, and the grid response time was only 2.4 minutes. The legacy UPS systems were not that responsive, which confirms the significance of mobile EV energy banks and decentralized microgrid backup boxes. A PSO-GA hybrid was used to optimize the allocation of energy credit. There was 95.4% credit fairness and low pricing variance of this method when compared with GA-only (91.1%), and random pricing (78.6%). The PSO-GA was also proven to converge more quickly with fewer iterations and this guarantees efficient and stable market dynamics in the grid. Moreover, 100% of the transactions were tampered in and 99.7% of the transactions were successful using the quantum-resistant blockchain layer. The lattice-based approach demonstrates its excellence in performance and resistance to future quantum threats as compared to ECC (98.9) and RSA (96.5%). All these findings confirm that CryptoGrid provides a smart, safe, and life-saving power management system that goes to the real-life issues of the contemporary power infrastructure.

V. CONCLUSION AND FUTURE WORK

CryptoGrid offers a revolutionary approach to securing and optimizing smart grid infrastructures, especially in facilities with a critical mission such as a hospital. The system mitigates the vulnerabilities of the grid architecture by incorporating novel technologies like blockchain, federated learning, multi-agent reinforcement learning, and quantum-resistant cryptography, among others. In tests, CryptoGrid demonstrated an impressive anomaly detection rate of 98.7%, which allows identifying cyber threats in real-time and reliably. It also showed how building-level energy wastage was reduced by 72% by identifying and reducing unneeded energy consumption through agent-based control. The automated distribution of unnecessary electricity of connected homes and electric vehicles to healthcare facilities enhanced emergency energy by 29%. The results confirm the use of CryptoGrid in the sphere of cyber security, smart energy management, and prompt emergency responses. The priority given to hospitals as key nodes and the implementation of mobile EV-based energy banks and decentralized micro grid control units guarantee a smooth backup in cases of power interruptions. Its structured modular and scaled architecture enables it to be deployed on a variety of infrastructures and the hybrid PSO-GA

optimization mechanism ensures equity in energy credit pricing. Moreover, lattice-based quantum-secure cryptography mechanisms that are being embraced come as a formidable defense against upcoming quantum threats that will give the system a long and trusted lifespan. In the future, CryptoGrid will be piloted in the presence of humans healthcare to confirm the field-readiness of the system. More will be added such as dynamic pricing according to the predicted demand, incorporating the carbon footprint metric and employing the homomorphic encryption and secure multi-party to enhance privacy in the federated learning. In general, CryptoGrid is a future-proven, smart and self-mending smart grid ecosystem that protects the digital infrastructure and human life.

CRediT Author Statement

The authors confirm contribution to the paper as follows:

Conceptualization: Elanchezhian E, Kalaiselvi K and Banumathy D; **Methodology:** Elanchezhian E and Kalaiselvi K; **Software:** Kalaiselvi K and Banumathy D; **Data Curation:** Elanchezhian E and Kalaiselvi K; **Writing- Original Draft Preparation:** Elanchezhian E, Kalaiselvi K and Banumathy D; **Visualization:** Kalaiselvi K and Banumathy D; **Investigation:** Elanchezhian E and Kalaiselvi K; **Supervision:** Kalaiselvi K and Banumathy D; **Validation:** Elanchezhian E and Kalaiselvi K; **Writing- Reviewing and Editing:** Elanchezhian E, Kalaiselvi K and Banumathy D; All authors reviewed the results and approved the final version of the manuscript.

Data Availability

The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interests

The authors declare no conflict of interest

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests.

References

- [1]. T. Mazhar et al., “Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods,” *Future Internet*, vol. 15, no. 2, p. 83, Feb. 2023, doi: 10.3390/fi15020083.
- [2]. A.-A. Bouramdane, “Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process,” *Journal of Cybersecurity and Privacy*, vol. 3, no. 4, pp. 662–705, Sep. 2023, doi: 10.3390/jcp3040031.
- [3]. M. A. Hafeez, K. H. Shakib, and A. Munir, “A Secure and Scalable Authentication and Communication Protocol for Smart Grids,” *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, p. 11, Mar. 2025, doi: 10.3390/jcp5020011.
- [4]. Y. Cheng and B. Zhao, “Risk Assessment Method of Solar Smart Grid Network Security Based on TimesNet Model,” *Applied Sciences*, vol. 15, no. 6, p. 2882, Mar. 2025, doi: 10.3390/app15062882.
- [5]. A. Rekeraho, D. T. Coffas, T. C. Balan, P. A. Coffas, R. Acheampong, and E. Tuyishime, “Cybersecurity Threat Modeling for IoT-Integrated Smart Solar Energy Systems: Strengthening Resilience for Global Energy Sustainability,” *Sustainability*, vol. 17, no. 6, p. 2386, Mar. 2025, doi: 10.3390/su17062386.
- [6]. M. Z. Gunduz and R. Das, “Smart Grid Security: An Effective Hybrid CNN-Based Approach for Detecting Energy Theft Using Consumption Patterns,” *Sensors*, vol. 24, no. 4, p. 1148, Feb. 2024, doi: 10.3390/s24041148.
- [7]. R. Pirta-Dreimane et al., “Enhancing Smart Grid Resilience: An Educational Approach to Smart Grid Cybersecurity Skill Gap Mitigation,” *Energies*, vol. 17, no. 8, p. 1876, Apr. 2024, doi: 10.3390/en17081876.
- [8]. F. Harrou, B. Bouyeddou, A. Dairi, and Y. Sun, “Exploiting Autoencoder-Based Anomaly Detection to Enhance Cybersecurity in Power Grids,” *Future Internet*, vol. 16, no. 6, p. 184, May 2024, doi: 10.3390/fi16060184.
- [9]. S. Hijgenaar, A. Ștefanov, A. M. van Voorden, and P. Palensky, “Cyber Resilience of Electric Vehicle Charging in Smart Grids: The Dutch Case,” *IEEE Access*, vol. 13, pp. 111454–111483, 2025, doi: 10.1109/access.2025.3580856.
- [10]. K. Bitirgen and Ü. B. Filik, “A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid,” *International Journal of Critical Infrastructure Protection*, vol. 40, p. 100582, Mar. 2023, doi: 10.1016/j.ijcip.2022.100582.
- [11]. H. Asadi Aghajari, T. Niknam, S. M. Sharifhosseini, M. H. Taabodi, and M. Pourbehzadi, “Enhanced resilience in smart grids: A neural network-based detection of data integrity attacks using improved war strategy optimization,” *Electric Power Systems Research*, vol. 239, p. 111249, Feb. 2025, doi: 10.1016/j.epsr.2024.111249.
- [12]. J. E. Efiog, A. Akinwale, B. O. Akinyemi, E. Olajubu, and S. Aderounmu, “CyberGrid: an IEC61850 protocol-based substation automation virtual cyber range for cybersecurity research in the smart grid,” *Cyber-Physical Systems*, vol. 11, no. 1, pp. 47–66, May 2024, doi: 10.1080/23335777.2024.2350004.
- [13]. A. A. Habib, M. K. Hasan, A. Alkhayyat, S. Islam, R. Sharma, and L. M. Alkwai, “False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction,” *Computers and Electrical Engineering*, vol. 107, p. 108638, Apr. 2023, doi: 10.1016/j.compeleceng.2023.108638.
- [14]. A. Presekal, A. Ștefanov, V. S. Rajkumar, and P. Palensky, “Attack Graph Model for Cyber-Physical Power Systems Using Hybrid Deep Learning,” *IEEE Transactions on Smart Grid*, vol. 14, no. 5, pp. 4007–4020, Sep. 2023, doi: 10.1109/tsg.2023.3237011.

- [15]. A. Basharat and Z. Huma, “Enhancing Resilience: Smart Grid Cybersecurity and Fault Diagnosis Strategies,” *Asian Journal of Research in Computer Science*, vol. 17, no. 6, pp. 1–12, Apr. 2024, doi: 10.9734/ajrcos/2024/v17i6453.
- [16]. M. A. Alomari et al., “Security of Smart Grid: Cybersecurity Issues, Potential Cyberattacks, Major Incidents, and Future Directions,” *Energies*, vol. 18, no. 1, p. 141, Jan. 2025, doi: 10.3390/en18010141.
- [17]. Y. Kim, S. Hakak, and A. Ghorbani, “Smart grid security: Attacks and defence techniques,” *IET Smart Grid*, vol. 6, no. 2, pp. 103–123, Sep. 2022, doi: 10.1049/stg2.12090.
- [18]. W. Grice, M. Olama, A. Lee, and P. G. Evans, “Quantum Key Distribution Applicability to Smart Grid Cybersecurity Systems,” *IEEE Access*, vol. 13, pp. 17398–17413, 2025, doi: 10.1109/access.2025.3533942.
- [19]. A. Shees, M. Tariq, and A. I. Sarwat, “Cybersecurity in Smart Grids: Detecting False Data Injection Attacks Utilizing Supervised Machine Learning Techniques,” *Energies*, vol. 17, no. 23, p. 5870, Nov. 2024, doi: 10.3390/en17235870.
- [20]. S. Amanlou et al., “Cybersecurity Challenges in Smart Grid Systems: Current and Emerging Attacks, Opportunities, and Recommendations,” *IEEE Open Journal of the Communications Society*, vol. 6, pp. 1965–1997, 2025, doi: 10.1109/ojcoms.2025.3545153.
- [21]. J. Yang, Q. Song, L. Hu, M. Xin, and R. Xiao, “Power Consumption Anomaly Detection of Smart Grid Based on CAE-GRU,” *Energies*, vol. 18, no. 18, p. 4787, Sep. 2025, doi: 10.3390/en18184787.
- [22]. M. Felser, C. Moon, and T. Stephenson, “Real-Time Anomaly Detection in Smart Grid Networks Using Deep Learning with Cross-Domain Generalization and Multi-Task Learning,” *International Journal of Mechanical and Electrical Engineering*, vol. 3, no. 1, pp. 10–15, Jul. 2024, doi: 10.62051/ijmee.v3n1.02.
- [23]. R. Riaz, G. Han, K. Shaukat, N. U. Khan, H. Zhu, and L. Wang, “A novel ensemble Wasserstein GAN framework for effective anomaly detection in industrial internet of things environments,” *Scientific Reports*, vol. 15, no. 1, Jul. 2025, doi: 10.1038/s41598-025-07533-1.

Publisher’s note: The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. The content is solely the responsibility of the authors and does not necessarily reflect the views of the publisher.