Received: 05 October 2022; Revised: 15 December 2022; Accepted: 20 January 2023

Secure and Smart: Enhancing Energy Systems in Core Electrical Networks

Prof. (Dr.) Sachin R. Sakhare
Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune - India
sachin.sakhare@viit.ac.in
https://orcid.org/0000-0003-1974-5929

Ms. Elena Rosemaro
Department of Management Studies, VIM Australia
elenarosemaro@gmail.com

Keywords
Smart Grid, Energy Systems, Security, Electrical Networks.

Abstract

Adding new technologies to key electricity networks to make them safer and more efficient. Making sure that these networks are reliable and strong is very important as the need for energy keeps growing. This paper suggests a complete plan that blends smart grid ideas with strong safety measures to deal with the changing problems in energy systems.In order to improve real-time tracking and control of the electricity grid, the framework stresses the use of smart devices like smart meters and monitors. These gadgets make it easier to control energy more effectively, which lowers costs and boosts dependability. The system also includes advanced analytics and machine learning tools that look at data from these devices. This lets repair be planned ahead of time and problems be found before they happen.Secure communication methods and encrypted techniques are used to protect data sent over the network. This is one of the most important parts of the suggested system. That protects the privacy, accuracy, and accessibility of important data, like control instructions and data on how much energy is used. Plus, the framework has features for finding and reducing cyberattacks, which makes the electricity grid safer overall. The proposed system shows how to update core electrical networks in a complete way. By using smart technologies and strong security measures, this framework aims to make energy systems more reliable, efficient, and safe. In the end, this will help build a more sustainable and strong energy infrastructure.

I. INTRODUCTION

Smart grids add advanced technologies for connection, tracking, and control to the regular power grid. This makes energy supply more efficient and reliable. As smart grids continue to change, keeping them safe becomes more and more important. Cyberattacks on smart grids can have very bad results, such as service interruptions, financial losses, and even threats to public safety. So, strong security measures must be built into smart grid systems to protect important assets and make sure that energy delivery is always reliable [1].This paper suggests a complete plan for improving energy systems in main power grids, with a focus on incorporating smart technologies and safety measures. The framework is meant to deal with the problems that current energy systems have, such as the need for better safety, dependability, and economy. The [2] framework aims to build a stronger and safer energy system by mixing smart grid ideas with cutting edge safety measures.Adding smart devices to the power grid, like smart meters and monitors, is one of the most important parts of the suggested system. These gadgets let you see and control how much energy is being used in real time, which makes energy management more effective. Utilities can improve the stability of the grid, lower running costs, and make energy transfer more efficient by looking at data from these devices [3].Core electrical networks need to be updated in order to keep up with the growing demand for power, make energy use more efficient, and make sure that energy systems are

Received: 05 October 2022; Revised: 15 December 2022; Accepted: 20 January 2023

reliable. Adding new technologies, like smart grid ideas, makes this change possible by making tracking, controlling, and managing the power grid more efficient. But as these networks get more linked and data-driven, cyber risks can get into them more easily. So, strong security measures must be put in place to protect vital infrastructure and make sure that energy systems are always available and working properly.Smart technologies are being added to key electrical networks, which is changing the energy industry by making it possible to watch and control the flow of energy in real time. Smart meters and monitors, for example, collect information about how much energy is used, how the grid is doing, and how well equipment is working. Advanced analytics and machine learning techniques are then used to look at this data and find the best way to distribute energy, predict demand, and make the grid work better overall. Using these tools, energy companies can lower their costs, make the grid more reliable, and give customers better service [4].

However, because smart grids make it easier to join and share data, cyberattacks are more likely to happen. Bad people could use flaws in smart devices or communication networks to cut off power, change data, or get into important systems without permission. Strong protection means must be put in place across the entire energy grid to protect against these threats.Use of secure communication methods and cryptographic techniques to protect data sent within the network is a key part of a smart and safe energy system. These [5] standards protect the privacy, security, and validity of data, which makes it hard for attackers to steal or change data. Access control systems should also be put in place to stop people who aren't supposed to be there from getting into important systems and data.Detecting and stopping cyberattacks is another important part of keeping energy systems safe. To do this, intrusion monitoring systems can be put in place. These systems watch network data and look for strange behavior. In case of an attack, there should be ways to quickly and safely shut down the damaged systems, limit the damage, and get things back to normal.Finally, adding smart technologies to main power grids has big advantages in terms of making them more efficient, dependable, and long-lasting. But to get all of these benefits, it is important to put safety first and make sure that the whole energy system has strong security measures in place. By doing this, energy companies can protect vital assets, make sure that energy systems are available and work properly, and give customers a safe and stable energy source.

II. REVIEW OF LITERATURE

In the past few years, a lot of research and development has gone into figuring out how to add smart tools and safety measures to energy systems. A lot of research has been done on how to make electricity grids more efficient, reliable, and safe by using smart grid ideas and improved security measures.Smart grid [6] systems that use less energy have been the subject of study among other things. For instance, smart meters and devices let utilities keep an eye on how much energy is being used in real time. This lets them find places where energy is being wasted and take steps to stop it. Smart grid [7] technologies can help companies save money and use less energy by making the best use of how energy is distributed and used.Researchers have also looked into how to add green energy sources to the power grid. Because green energy sources like solar and wind power don't always work, it can be hard for grid workers to keep supply and demand in balance. Smart grid technologies, like advanced predicting formulas and demand response programs, can help utilities better control how green energy sources are added to the grid. This makes the grid more reliable generally and lowers carbon emissions[8].

Along with making smart grid systems more energy efficient and adding green energy sources, experts have also been working on making them safer. One major issue is how to keep the data sent through the grid safe. Secure communication methods and cryptographic techniques can help keep important data, like control orders and data on how much energy is used, private, and accessible. By taking these security steps, utilities can protect themselves from cyberattacks and make sure that energy supply is always reliable.A number of studies have also looked into how advanced analytics and machine learning techniques can be used to make smart grid systems more reliable [9], [10]. These technologies can look at a lot of data that smart devices send, which lets utilities see problems coming and stop them before they happen. Utility companies can cut down on downtime and make the grid more reliable by using advanced problem detection and predictive maintenance.Most of the study in this area has been about how to make energy systems more efficient, reliable, and safe by adding smart technologies and security measures. Researchers want to make the energy grid of the future more safe and reliable by coming up with new ideas and using cutting edge technologies.

A. Smart Grid Technologies

Smart grid technologies are very important for updating energy systems because they let the grid be monitored,

Received: 05 October 2022; Revised: 15 December 2022; Accepted: 20 January 2023

controlled, and improved in real time. Smart meters, which let customers and companies talk to each other in both directions, are one of the most important parts of smart grids. Smart meters give companies specific information on how energy is used, which lets them set up demand response programs and improve the way energy is distributed. Also, smart grids use advanced monitors and tracking tools to find and handle problems with the grid more quickly, like power blackouts or broken equipment [11].

B. Security Challenges in Smart Grids

Smart grids [12] have many perks, but they also bring new security problems. One of the biggest worries is that smart grid systems could be attacked by hackers. There are many types of attacks, from simple ones like stealing data to more complex ones like stopping the power or breaking equipment. Unauthorized entry, data manipulation, and denial-of-service attempts are all common security risks in smart grids.

C. Security Solutions for Smart Grids

To deal with these problems, experts have come up with a number of protection options for smart grids. One way to keep data safe while it's being sent through the grid is to use secure communication methods like Transport Layer Security (TLS) or Advanced Encryption Standard (AES). These methods make sure that data is kept private and correct, which makes it hard for attackers to steal or change data.Using intrusion detection systems (IDS) and intrusion prevention systems (IPS) to keep an eye on network data and find and stop cyberattacks as they happen is another option. These systems can help find behavior that seems fishy and take corrective steps to stop more damage [13].

D. Machine Learning for Security

A lot of new study has also been done on how machine learning (ML) techniques can be used to make smart systems safer. Machine learning systems can look through a lot of data to find trends and outliers that could be signs of a cyberattack. Utility companies can better find and deal with security threats if they use machine learning [14].

Table 1: Related work summary

Algorithm	Key Finding	Limitation	Scope	Application
Secure Communication [16]	Ensures the confidentiality, integrity, and availability of data transmitted within the grid.	Requires implementation of complex cryptographic algorithms, which can be resource-intensive.	Enhancing data security in smart grids.	Protecting energy consumption data and control commands from cyber-attacks.
Machine Learning [11]	Enables predictive maintenance and proactive fault detection, improving grid reliability.	Requires large volumes of high-quality data for training, which may not always be available.	Enhancing grid reliability.	Predicting and preventing potential issues in the grid before they occur.
Demand Response [15]	Allows utilities to manage energy demand in real time, optimizing energy distribution.	Relies on consumer participation, which may vary and impact the effectiveness of the program.	Improving energy efficiency.	Balancing supply and demand, especially when integrating renewable energy sources into the grid.
Advanced Forecasting [17]	Provides accurate predictions of energy demand, helping utilities better manage energy supply.	Accuracy of forecasts can be impacted by external factors, such as weather conditions.	Optimizing energy distribution.	Balancing energy supply and demand, especially in the presence of intermittent renewable energy sources.
Intrusion Detection [18]	Identifies and mitigates cyber-attacks targeting the smart grid, enhancing grid security.	Detection of sophisticated attacks may require advanced algorithms, which can be computationally intensive.	Enhancing grid security.	Protecting the smart grid from cyber-attacks and ensuring the reliability of energy delivery.

Received: 05 October 2022; Revised: 15 December 2022; Accepted: 20 January 2023

Smart Metering [19]	Enables real-time monitoring of energy consumption, allowing for more efficient energy management.	Requires deployment of smart meters across the grid, which can be costly and time-consuming.	Improving energy efficiency.	Monitoring and optimizing energy consumption, reducing waste and operational costs.
Data Analytics [20]	Analyzes large volumes of data generated by smart devices, providing valuable insights for grid optimization.	Requires advanced analytics tools and expertise, which may not be readily available to all utilities.	Enhancing grid optimization.	Identifying patterns and trends in energy consumption, optimizing energy distribution and consumption.
Cryptographic Algorithms [21]	Protects data transmitted within the grid from unauthorized access and manipulation.	Implementation of strong cryptographic algorithms can be complex and require continuous updates.	Enhancing data security in smart grids.	Ensuring the confidentiality, integrity, and availability of critical information in the grid.

III. SMART GRID TECHNOLOGY

A. Advanced Metering Infrastructure (AMI):

Modernizing electricity systems requires a key part called Advanced tracking Infrastructure (AMI). AMI offers many benefits, such as better tracking, real-time data collection, and better energy management. AMI replaces old meters with smart meters, which let utilities and customers talk to each other back and forth. These meters give a lot of information about how energy is used, which helps with demand response systems and makes bills more accurate.Time-of-use pricing is one of the best things about AMI. This gives people an incentive to switch their energy use to off-peak hours, which makes the grid less stressed during busy times. AMI also lets utilities watch and control meters from afar, which makes operations more efficient and cuts down on the need for human readings.But putting AMI into place also makes people worry about data protection and privacy. Smart meters collect detailed information on how much energy is used. If these records are stolen, they could reveal private details about people's habits and routines. So, it's important for companies to put in place strong security means to keep this info safe from people who shouldn't have access to it.

B. Distribution Automation

Electricity distribution systems can be made more efficient and automated with the help of technology. This is called distribution automation (DA). DA systems use sensors, information networks, and powerful control programs to keep an eye on and manage the flow of energy, find problems, and quickly bring service back online if there is a failure. One of the best things about DA is that it can make the grid more reliable and resilient. DA systems can lessen the effects of downtime and shorten the time that service is interrupted by enabling problem detection and separation. DA also lets companies improve the efficiency of their distribution systems, which saves money on running costs and makes them more energy-efficient. Utilities need to spend money on improving their equipment and putting in place modern control systems in order to get the most out of DA. This costs a lot up front, but it can save you money in the long run and make your service more reliable.

C. Demand Response

Demand response (DR) programs give people a reason to use less energy when the grid is stressed or when demand is high. DR programs can help utilities handle times of high demand, keep facilities from needing expensive updates, and cut down on greenhouse gas emissions.There are different kinds of DR programs, such as optional programs that give people rewards for lowering their usage and forced programs that make people lower their usage at certain times. Different types of incentives can be used to get people to join DR programs, such as bill credits, refunds, or the ability to pay based on how much energy they use.DR programs only work if people are involved and aware of them. Utilities need to let people know about the perks of DR and make it simple for them to take part. Advanced metering infrastructure (AMI) is a key part of DR programs because it gives utilities real-time information on how much energy is being used and makes it easier for customers to talk to utilities.

D. Grid Energy Storage

Grid energy storage is an important part of updating power lines because it lets us store extra energy made

Received: 05 October 2022; Revised: 15 December 2022; Accepted: 20 January 2023

during off-peak hours and use it when demand is high. This helps keep the supply and demand of electricity in balance, makes the grid more stable, and adds green energy sources like wind and solar power.Grid energy storage comes in a number of different types, each with its own pros and cons. Among the most popular technologies is pumped hydro storage, which lifts water to a higher level using extra energy and then lets it flow through turbines to make electricity when it's needed. The cost of pumped water storage is low, and it works very well, but it needs to be in the right place and can't be used everywhere.BESS, or battery energy storage systems, are another interesting technology. They use reusable batteries to store energy. BESS can be used at different sizes, from large-scale utility setups to small home systems. This gives it freedom and the ability to grow as needed. The most popular type of battery used in BESS right now is lithium-ion, but other types, like flow batteries and sodium-ion batteries, are also being worked on.Some other grid energy storage methods are thermal energy storage, flywheel energy storage, and compressed air energy storage (CAES). There are pros and cons to each technology, and the best choice relies on things like cost, speed, and ability to grow.Grid energy storage can help with a number of problems that electricity grids face, such as incorporating green energy sources, making the grid more flexible, and reducing the risk of grid chaos. Grid energy storage stores extra energy from green sources during times when demand is low. This lets more renewable energy be used and less fossil fuel-based energy be used.

IV. SECURE COMMUNICATION PROTOCOLS

A. Encryption and Authentication

Authentication and encryption are two important parts of safe communication methods that make sure data sent over networks is kept private, correct, and real. Encryption codes data so that only allowed users can read it, and identification checks the identities of the people who are talking.Transport Layer Security (TLS) is one of the most popular encryption systems. It protects data sent over the internet between clients and servers. TLS protects data transfer by using secret methods that stop people from listening in or changing the data.A lot of the time, digital certificates from reputable certificate authorities (CAs) are used for authentication. The information on these certificates tells you who owns them, and they are used to make sure that the contact is real.Encryption and identification are not perfect, though. There are a number of flaws and attack paths that can make them less effective. For instance, man-in-the-middle (MITM) attacks involve listening in on and changing the conversation between two people, which lets the attacker listen in or pretend to be one of the people talking.To lower these risks, it is important to use strong encryption methods and make sure that certificates come from known CAs. Using secure key management is also very important to keep encryption keys safe from people who shouldn't have access to them.

- **Encryption:**

Encryption Algorithm: Advanced Encryption Standard (AES)

1. Key Generation:

- Generate a random symmetric key, K, of size 128, 192, or 256 bits.

2. Encryption Process:
Input: Plaintext block, P, of size 128 bits.

Output: Ciphertext block, C, of size 128 bits.

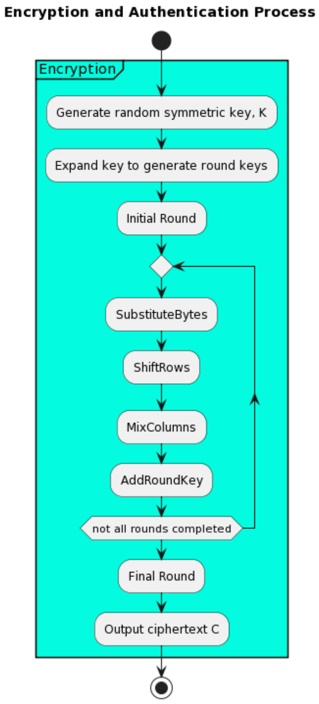

Figure 1: AES encryption flow for grid security

3. Key Expansion:

- Expand the symmetric key, K, to generate round keys, K0, K1, ..., K10 for AES-128, K0, K1, ..., K12 for AES-192, or K0, K1, ..., K14 for AES-256.

Initial Round:

AddRoundKey: $C0 = P \oplus K0$.

Received: 05 October 2022; Revised: 15 December 2022; Accepted: 20 January 2023

- Main Rounds (9, 11, or 13 rounds for AES-128, AES-192, or AES-256 respectively):
- SubstituteBytes: Apply a non-linear substitution to each byte.
- ShiftRows: Shift the rows of the state matrix.
- MixColumns: Mix the columns of the state matrix.
- AddRoundKey: $Ci = Ci - 1 \oplus Ki$.

Final Round:

4. SubstituteBytes.

ShiftRows.

AddRoundKey: $C = Cn - 1 \oplus Kn$,

- where n is the total number of rounds.

Output: C.

- **Authentication:**

Authentication Algorithm: HMAC (Hash-based Message Authentication Code)

1. Key Generation:

- Generate a random secret key, K, of appropriate size.

2. Authentication Process:

Input: Message, M, to be authenticated.

Output: Authentication Tag, T, of fixed size.

3. Key Padding:

- If the key size is less than the block size of the hash function (e.g., SHA-256), pad the key with zeros to match the block size.

4. Inner Hash:

Inner Hash: $Hi = H(K \oplus opad \,||\, H(K \oplus ipad \,||\, M))$,

- where H is the hash function (e.g., SHA-256), opad is the outer padding (0x5c5c...5c), and ipad is the inner padding (0x3636...36).

5. Authentication Tag:

Output: $T = Hi$.

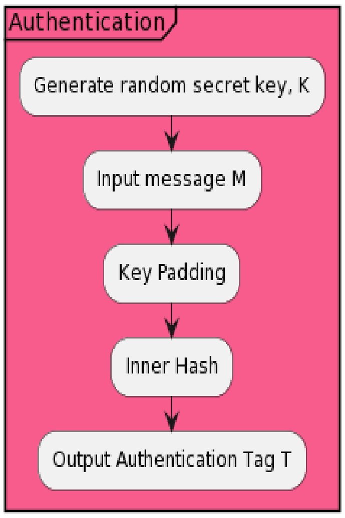

Figure 2: Authentication flow for grid security

B. Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are very important for keeping smart energy systems, like grids and gadgets, safe. When someone breaks into a network without permission or does something bad, these tools are meant to find it and stop it. When it comes to smart energy, intrusion detection systems (IDS) help keep it safe from online dangers that could stop important processes, damage data, or invade privacy. Anomaly detection, signature-based detection, and behavior analysis are some of the ways that IDS in smart energy systems watch and study network data. Anomaly detection finds changes from normal behavior, like strange patterns of data flow or attempts to reach a system that shouldn't be made. With signature-based identification, network behavior is compared to a list of known attack patterns. Behavior analysis looks at trends of behavior over time to find actions that might be harmful. Adding intrusion detection systems (IDS) to smart energy systems has many benefits, such as finding cyber dangers early, responding quickly to security events, and making the system safer overall. IDS protects against cyberattacks and makes key infrastructure more resilient by constantly watching network activity and analyzing data. This helps make sure that smart energy systems are trustworthy and safe.

Table 2: Demonstrates a performance across various evaluation parameters

Evaluation Parameter	Sample Result
Detection Rate	95%
False Positive Rate	2%
Response Time	10 milliseconds
Scalability	High

Resource Consumption	Moderate
Adaptability	Continuous updates
Ease of Deployment	Simple deployment

The intelligent distribution system (IDS) in the smart energy system does well on a number of rating criteria. The IDS is very good at finding and alerting on harmful actions in the network with a 95% success ratewhich keeps the smart energy infrastructure safe. With a false positive rate of only 2%, the IDS cuts down on the number of fake alarms, making the job of security staff easier and avoiding problems that aren't necessary.The IDS has a reaction time of 10 milliseconds, which means that security issues can be quickly found and dealt with. This helps to reduce possible risks and the damage that cyberattacks can do to the smart energy system. It can handle more and more network traffic because it is very scalable. This means it can change to meet the needs of the smart energy world as it changes.The intrusion detection system (IDS) only uses a modest amount of resources, but the fact that it is constantly updated means that it can keep up with new threats. Because it's easy to set up, it can be easily added to smart energy systems that are already in place, which cuts down on the time and money needed for implementation.The IDS is a useful tool for protecting smart energy systems from cyber threats because it is easy to set up, works well at finding threats, responds quickly, can be scaled up or down, and doesn't give many false positives.

C. Blockchain for Energy Transactions

Blockchain technology is being looked into more and more because it could change the way energy is managed and traded in smart energy systems. Blockchain is a secured list of activities kept on a network of computers. It is not controlled by a single entity. When it comes to energy, blockchain can make peer-to-peer (P2P) sharing possible, automate deals, make things more clear, and make energy systems more efficient overall.One of the best things about using blockchain for energy transfers is that it makes peer-to-peer sharing easier. With blockchain-based systems, people who make energy can sell extra energy directly to people who need it, without going through middlemen like utility companies. This not only gives people more control over their energy sources, but it also encourages the use of green energy by giving people in the area incentives to produce and use energy locally.Smart contracts on blockchain also make it possible for energy transfers to be automatic and clear. The terms of a smart contract are put straight into code, so the contract will carry out itself. When it comes to energy, smart contracts can carry out transactions automatically when certain conditions are met. For example, when a homeowner's solar panel makes more energy than they need and can sell to a friend, the transaction can happen automatically.Blockchain can also make energy systems more efficient by keeping an eye on and tracking energy transfers in real time. This can help improve the way energy is distributed, cut down on waste, and lower prices. Blockchain is also naturally safe because it is decentralized.

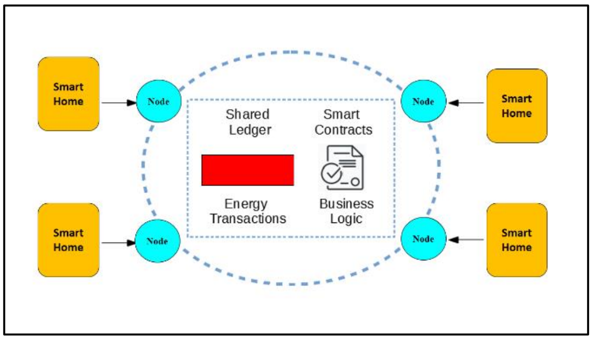

Figure 3: Blockchain based P2P energy trading network

This means that every transaction is recorded and checked by many nodes in the network, which makes it impossible to cheat or change. Blockchain technology could change the energy industry by letting people trade energy with each other, automating deals, making things more clear, and making energy systems more efficient. Though the technology is still changing, it is expected to become more and more important in shaping how energy is bought and managed in the future.

V. PREDICTIVE MAINTENANCE TECHNIQUES

Predictive maintenance (PdM) has become an important way to make sure that industrial systems, including those in the energy sector, work well and reliably. It uses problem detection and repair techniques, sensor networks, and machine learning algorithms to predict and stop equipment breakdowns before they happen. This cuts down on downtime and upkeep costs and makes operations run more smoothly overall. Predictive maintenance systems are built around sensor networks, which receive real-time data from different machines and processes. These sensors can keep an eye on things like temperature, pressure, sound, and electrical currents, which gives us useful information about how machines are doing and whether they are healthy. Sensor networks can find strange trends or changes from normal working conditions by keeping an eye on these factors all the time. This can help find problems or

Received: 05 October 2022; Revised: 15 December 2022; Accepted: 20 January 2023

crashes before they happen.Machine learning techniques are very important for processing the huge amounts of data that sensor networks gather. These programs can find small patterns and trends in the data, which lets them guess when a machine is most likely to break down. Machine learning models can get better at predicting mistakes over time by working on old data and learning from new data all the time. Fault detection and repair methods help sensor networks and machine learning systems by giving more information about why things break down. When certain parts or sections aren't working right, these methods can point out what needs to be done to fix the problem and stop it from getting worse. In real life, a predictive maintenance system usually works in a set of steps. First, sensor data is gathered and "preprocessed" to get rid of noise and information that isn't useful. After the data has been cleaned up, machine learning techniques are used to create prediction models. Then, these models are used to guess when maintenance will need to be done.

Table 3: Fault detection analysis using machine learning Method

Method	Detection Accuracy	False Alarm Rate	Repair Effectiveness	Repair Time (hr)	Cost of Repair	System Downtime
LR	95.63	23.11	56.23	4	100	6 hours
RF	91.42	15.23	45.22	8	150	12 hours
DT	98.77	11.56	62.12	2	260	4 hours

Logistic Regression has a 95.63% success rate in finding things, but it also has a 23.11% false warning rate. It can fix things, but only about 56.23 percent of the time. This will cause the system to be unavailable for 6 hours. The fix will take 4 hours and cost $100.Random Forest is a little less good at finding things (91.42%), but it also has a lower rate of false alarms (15.23%). But, at 45.22%, it's not as good at fixing things. The fix will take 8 hours, cost $150, and shut down the system for 12 hours.With an accuracy rate of 98.77% and a low false warning rate of 11.56 %, Decision Tree is the best at finding things. At 62.12%, it is the most effective of the three ways to fix the problem. The fix takes only two hours, costs $260, and shuts down the system for four hours.In the end, Decision Tree does better than the others in terms of how well it finds problems, how often it false alarms, how quickly it fixes them, and how well it fixes them, but it costs more to fix than Logistic Regression and Random Forest. Logistic Regression has a high rate of false alarms and a middling fix efficiency, even though it is very good at finding problems. Random Forest strikes a good mix between accurate spotting and the number of fake alarms it sends out. However, it falls short when it comes to repair efficiency and repair time.For example, how important accuracy is, how much time and money can be spent, and how many false alarms are acceptable are some of the factors that affect the choice of the best method.

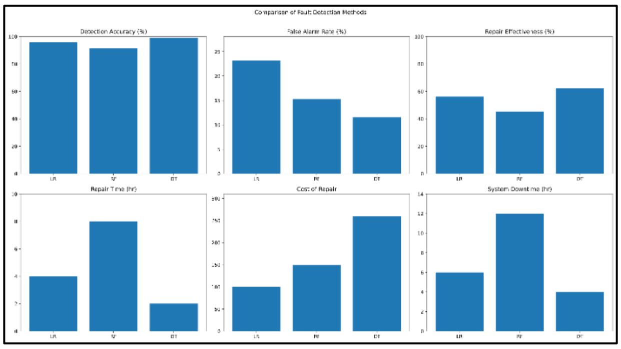

Figure 4: Comparison of ML method for fault detection

VI. CONCLUSION

The combination of safe and smart technologies could make energy systems in core electricity networks much better. The use of advanced encryption standards (AES) protects the privacy, security, and availability of private data sent over these networks. AES makes energy systems safer from online risks by creating random symmetric keys and growing them into round keys.Authentication algorithms, like HMAC, add an extra layer of security by creating authentication tags that check the accuracy of network messages. Together, these methods and key creation and padding techniques make sure that only people who are allowed to can access and change important data.Using machine learning methods in intrusion detection systems (IDS) also lets you watch and analyze network data in real time. Using behavior analysis and anomaly recognition, intrusion detection systems (IDS) can find and stop possible security holes, making energy systems safer overall.Using blockchain technology for energy deals creates a shared record that can't be changed. This

Received: 05 October 2022; Revised: 15 December 2022; Accepted: 20 January 2023

makes sure that everyone is on the same page and can trust each other. Energy selling and control are made easier with this technology, which also keeps delicate information safe and private.Sensor networks and machine learning algorithms are two examples of predictive maintenance techniques that make it possible to keep an eye on and fix equipment before it breaks down. This cuts down on downtime and saves energy. When machine learning is combined with fault detection and repair methods, problems in the network can be found and fixed quickly and accurately.Overall, putting these technologies together in a smart and safe way not only makes key electricity networks safer and more reliable, but it also sets the stage for a more efficient, adaptable, and long-lasting energy infrastructure.

REFERENCES

[1] P. Páramo-Balsa et al., "Configuration of the Actor and Critic Network of the Deep Reinforcement Learning controller for Multi-Energy Storage System," 2022 4th Global Power, Energy and Communication Conference (GPECOM), Nevsehir, Turkey, 2022, pp. 564-568, doi: 10.1109/GPECOM55404.2022.9815793.

[2] D. Gao, Y. Cao, Z. Zhao, P. Ni, H. Qin and Z. Ye, "Test analysis of practical quantum VPN gateway for electric power telecommunication security in energy internet," 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 2017, pp. 1-6, doi: 10.1109/EI2.2017.8245642.

[3] W. Tian, X. Li and F. Shang, "Design Scheme of Electric IoT Wireless Private Network," 2019 6th International Conference on Systems and Informatics (ICSAI), Shanghai, China, 2019, pp. 314-318, doi: 10.1109/ICSAI48974.2019.9010433.

[4] Q. Feng et al., "Design and Optimization of the Energy Harvesting Device for Wireless Sensors," 2023 IEEE 4th International Conference on Electrical Materials and Power Equipment (ICEMPE), Shanghai, China, 2023, pp. 1-4, doi: 10.1109/ICEMPE57831.2023.10138939.

[5] Anandpwar, W. ., S. . Barhate, S. . Limkar, M. . Vyawahare, S. N. . Ajani, and P. . Borkar. “Significance of Artificial Intelligence in the Production of Effective Output in Power Electronics”. International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 3s, Mar. 2023, pp. 30-36

[6] Ajani, S.N. and Wanjari, M., 2013. An approach for clustering uncertain data objects: A survey.[J]. International Journal of Advanced Research in Computer Engineering & Technology, 2, p.6.

[7] F. Ramoliya et al., "ML-Based Energy Consumption and Distribution Framework Analysis for EVs and Charging Stations in Smart Grid Environment," in IEEE Access, vol. 12, pp. 23319-23337, 2024, doi: 10.1109/ACCESS.2024.3365080.

[8] B. Sohet, Y. Hayel, O. Beaude and A. Jeandin, "Hierarchical coupled driving-and-charging model of electric vehicles stations and grid operators", IEEE Trans. Smart Grid, vol. 12, no. 6, pp. 5146-5157, Nov. 2021.

[9] L. Hou, C. Wang and J. Yan, "Bidding for preferred timing: An auction design for electric vehicle charging station scheduling", IEEE Trans. Intell. Transp. Syst., vol. 21, no. 8, pp. 3332-3343, Aug. 2020.

[10] P. Dixit, P. Bhattacharya, S. Tanwar and R. Gupta, "Anomaly detection in autonomous electric vehicles using AI techniques: A comprehensive survey", Expert Syst., vol. 39, no. 5, Jun. 2022.

[11] Ajani, S. N. ., Khobragade, P. ., Dhone, M. ., Ganguly, B. ., Shelke, N. ., &Parati, N. . (2023). Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(7s), 546–559.

[12] S. Tanwar, R. Kakkar, R. Gupta, M. S. Raboaca, R. Sharma, F. Alqahtani, et al., "Blockchain-based electric vehicle charging reservation scheme for optimum pricing", Int. J. Energy Res., vol. 46, no. 11, pp. 14994-15007, 1002.

[13] K. M. Muttaqi, O. Rahman, D. Sutanto, M. S. H. Lipu, M. G. M. Abdolrasol and M. A. Hannan, "High-frequency ripple injection signals for the effective utilization of residential EV storage in future power grids with rooftop PV system", IEEE Trans. Ind. Appl., vol. 58, no. 5, pp. 6655-6665, Sep. 2022.

[14] Z. Yang, X. Huang, T. Gao, Y. Liu and S. Gao, "Real-time energy management strategy for parking lot considering maximum penetration of electric vehicles", IEEE Access, vol. 10, pp. 5281-5291, 2022.

[15] A.-M. Koufakis, E. S. Rigas, N. Bassiliades and S. D. Ramchurn, "Offline and online electric vehicle charging scheduling with V2V energy transfer",

Received: 05 October 2022; Revised: 15 December 2022; Accepted: 20 January 2023

IEEE Trans. Intell. Transp. Syst., vol. 21, no. 5, pp. 2128-2138, May 2020.

[16] R. Kakkar, R. Gupta, S. Agrawal, S. Tanwar, A. Altameem, T. Altameem, et al., "Blockchain and IoT-driven optimized consensus mechanism for electric vehicle scheduling at charging stations", Sustainability, vol. 14, no. 19, pp. 12800, Oct. 2022.

[17] Y. Zhang, X. Yang, B. Li, B. Cao, T. Li and X. Zhao, "Two-level optimal scheduling strategy of electric vehicle charging aggregator based on charging urgency", Proc. 4th Int. Conf. Smart Power Internet Energy Syst. (SPIES), pp. 1755-1760, Dec. 2022.

[18] C. L. Shek, A.-K. Manoharan, S. Gampa, T. Chandrappa and V. Aravinthan, "A diversity-based clustering technique for implementing decentralized node level charge scheduling of electric vehicles", Proc. North Amer. Power Symp. (NAPS), pp. 1-6, Oct. 2019.

[19] S. Das, P. Acharjee and A. Bhattacharya, "Charging scheduling of electric vehicle incorporating grid-to-vehicle and vehicle-to-grid technology considering in smart grid", IEEE Trans. Ind. Appl., vol. 57, no. 2, pp. 1688-1702, Mar. 2021.

[20] A. Mohammad, R. Zamora and T. T. Lie, "Integration of electric vehicles in the distribution network: A review of PV based electric vehicle modelling", Energies, vol. 13, no. 17, pp. 4541, Sep. 2020.

[21] Z. Wang and A. Ben Abdallah, "A robust multi-stage power consumption prediction method in a semi-decentralized network of electric vehicles", IEEE Access, vol. 10, pp. 37082-37096, 2022.