International Journal of Applied Power Engineering (IJAPE)
Vol. 15, No. 1, March 2026, pp. 421~429
ISSN: 2252-8792, DOI: 10.11591/ijape.v15.i1.pp421-429

Enhancing power grid reliability: a hybrid blockchain and machine learning approach

Ravi V. Angadi[1], Suresh Kumar[2], A. K. Vijayalakshmi[3], G. N. Vidya Shree[1]
[1]Department of Electrical and Electronics Engineering, Presidency University, Bengaluru, India
[2]Department of Computer Science and Engineering, Presidency University, Bengaluru, India
[3]Sir M Visvesvaraya Institute of Technology, Bengaluru, Karnataka, India

Article Info

Article history:

Received May 13, 2025
Revised Dec 14, 2025
Accepted Jan 9, 2026

Keywords:

Blockchain
Contingency analysis
Machine learning
Power grid security
Smart contracts

ABSTRACT

As contemporary power grids are becoming more complex with the integration of renewable energy sources, distributed generation, and smart grid technologies. Conventional contingency analysis techniques, based on centralized architectures and static rule-based evaluations, tend to be inadequate in real-time fault detection, automated response, and cybersecurity. This paper suggests a hybrid approach that combines machine learning algorithms with blockchain technology to improve both predictive intelligence and security of contingency analysis. For the IEEE 30-bus test case, different line outage and generator failure cases were simulated. Different machine learning models, such as random forest (RF), support vector machine (SVM), and gradient boosting (GB), were trained to classify and predict these contingencies. In parallel, cryptographic primitives like advanced encryption standard (AES), Rivest–Shamir–Adleman (RSA), and elliptic curve cryptography (ECC) were tested in a blockchain setting to provide security for event data and enable automatic recovery steps through smart contracts. Outcomes illustrate that the GB showed the maximum fault classification rate (93.4%), and ECC ensured light yet robust data protection for blockchain activities. Against the conventional system, the designed model enhanced the response time in case of faults, accuracy, and system fault tolerance. This two-layer mechanism presents a scalable, proactive, and cyber-safe mechanism for the power grid in the future.

Corresponding Author:

Ravi V. Angadi
Department of Electrical and Electronics Engineering, Presidency University
Bengaluru, Karnataka 560064, India
Email: raviangadi4045@gmail.com or raviangadi@presidencyuniversity.in

1. INTRODUCTION

The contemporary power grids are becoming highly decentralized and data-driven cyber-physical systems. The traditional centralized designs of generation, transmission, and distribution cannot cope with renewable sources, electric vehicles, smart meters, and distributed generation that introduce intermittency, bidirectional flows, and fast fluctuations in demand variability [1], [2]. To overcome these, predictive analytics, real-time monitoring, and automations are part of smart grid programs. Maching learning (ML) involves historical and real-time data, which it analyzes to detect anomalies, forecast demand, and predict faults [3]. Similarly, blockchain technology is actively researched on safe, decentralized incentivation of energy, which offers immutable communication and automatic transactions by using smart contracts [4].

Most recent studies have talked about blockchain and machine learning togetherness in the future energy systems. Mololoth *et al.* [5] showed that they can facilitate safe trading of energy as well as smart grid control, and Venkatesan and Rahayu [6] introduced hybrid consensus and ML models to enhance the security

of blockchains. Nevertheless, most methods separate these technologies in the sense that they apply ML exclusively to analytics or blockchain exclusively to security without achieving these systems in a single contingency management system.

Contingency analysis is still necessary when analyzing the behavior of grids under contingencies such as line outages, major rises in generator failures, or transformer faults. Traditional rule-based or statically simulated models are barely able to adjust to dynamical grid conditions and are incapable of assisting real-time decision-making. The further increased monitoring through internet of things (IoT) also introduces new points of vulnerability to more severe cyber threats associated with the data manipulation and a denial-of-service attack (DoS) [7]. Moreover, centralized systems are single point of failure and cannot therefore be deemed reliable when dealing with high-frequency and low-latency environments.

To mitigate such shortcomings, this paper outlines a hybrid system, which is the integration of machine learning-infused predictive analytics and blockchain-enabled automation. Random forest (RF), support vector machine (SVM), and gradient boosting (GB) models will be trained using a grid parameter-based data set such as voltages, active/reactive power, and phase angles that classify fault situations using the IEEE 30-bus system. Meanwhile, cryptographic algorithms such as advanced encryption standard (AES), Rivest–Shamir–Adleman (RSA), and elliptic curve cryptography (ECC) are also being examined in the context of permissioned blockchain to protect the data and initiate the smart contract-based automatic response. The originality of this work is that it has a two-tier architecture, where ML models will predict early faults, and blockchain will ensure that mitigation measures are implemented safely and autonomously. Together, the intelligence and trust layer can decrease response time, improve classification accuracy, and improve resiliency. The paper is structured as follows: section 2 will present related work, section 3 will include all the information about the methodology of data simulation, training of the ML model, and the use of blockchain, section 4 will discuss the results, and the conclusion will be given in section 5 based on the main findings and some suggestions on the further directions.

2. LITERATURE REVIEW AND PROPOSED APPROACH

To manage the growing complexity, smart grids require smart control, real-time analytics, and automated protection. Machine learning (ML) has turned out to be valuable in detecting predictive faults, which allows large scales of data analysis regarding operations. The weaknesses of conventional fault analysis were mentioned by Liang [1] and Chandran *et al*. [2], who pointed out the problem of renewable integration and the necessity of adaptive fault response.

Blockchain has proved to be a solution to secure and decentralized energy management. As demonstrated by studies by Song *et al.* [3] and Choobineh *et al*. [4], it can improve transparency, authentication, and resistance to cyber-attacks. Smart contracts also automate activities including fault isolation and load management without the need of centralized manipulation.

There is little literature on combining ML-based prediction and blockchain-secured automation. Theoretical advantages of integration were discussed by Mololoth *et al.* [5], and hybrid consensus that is improved with the help of ML is discussed by Venkatesan and Rahayu [6]. Nevertheless, most methodologies address analytics and security independently, which leaves an opportunity to develop single frameworks with the ability to provide real-time fault prediction and preventive mitigation with sufficient security. The given work fills that gap and presents a hybrid ML-blockchain infrastructure implemented on the IEEE 30-bus system and providing predictive intelligence and automation based on cyber-security. Table 1 explains the associated terms and acronyms.

Table 1. Terminology and acronyms

Abbreviation	Description	Abbreviation	Description
AES	Advanced encryption standard (symmetric encryption)	GB	Gradient boosting
IoT	Internet of things	ECC	Elliptic curve cryptography (lightweight asymmetric encryption)
RF	Random forest	ML	Machine learning
RSA	Rivest–Shamir–Adleman	SVM	Support vector machine

The suggested architecture combines the ML-based prediction of faults with the secure automation based on blockchain technology. Live grid measurements of voltages, power flows, transformer/load condition are input to ML models trained on faults in the IEEE 30-bus condition on random forest, SVM, and gradient boosting. A permissioned blockchain guarantees the secure transfer of data and automatic operations

with smart contracts to isolate faults, shedding the load, and reassigning generators. Cryptographic algorithms (AES, RSA, ECC) are compared based on confidentiality and integrity, and ECC has the best performance-security trade-off. The architecture offers a predictive, decentralized, and cyber-secure method of contingency management that offers a better response time, accuracy, and resilience.

3. METHOD

The suggested methodology is a combination of machine learning to predict faults with blockchain-based secure automation: a three-tier structure is data simulation, ML-based prediction, and blockchain with cryptographic protection and smart contracts. The general process flow, as depicted in Figure 1, entails generation of the dataset, contingency simulation, development of the ML, and integration with the blockchain. It was tested on the IEEE 30-bus system, which contains 30 buses, 6 generators, and 41 lines of transmission, because it is balanced and can be used as a testbed in contingency studies [8], [9]. The MiPower was used to simulate fault scenarios such as transmission line outages, generator failures and transformer disturbances. Parameters of bus voltages, active/reactive power, and phase angles were measured during each run [10]. Each row of the dataset holds a fault type, location, and severity as a labeled grid state. Extracting features that were compatible with the latest power-system ML research [11], [12], the final training dataset was built with them. This systematic pipework guarantees reproducible and all-inclusive emulation of varied fault conditions [13].

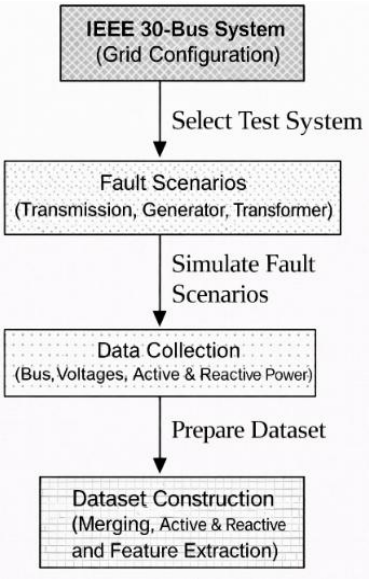


Figure 1. Process flow for building datasets and simulating fault scenarios with the IEEE 30-bus power system

Three trained ML models, including random forest, SVM, and gradient boosting, were created to categorize grid faults. RF, which is a group of decision trees, minimizes overfitting and the results may be interpreted through feature importance, making it resistant to noise and unbalanced data [14], [15]. SVM finds the best separating hyperplanes and classifies nonlinear patterns using RBF kernels, and thus classifies the complex grid behavior [16]. Gradient boosting, a progressive ensemble, collaborates with the previous learners and grabs grid search to optimize depth and learning rate, improving the recall of the minority fault classes [17]. Formally, given a dataset as in (1).

$$\mathcal{D} = \{(x_i, y_i)\}_{i=1}^{n} \quad (1)$$

Where $x_i \in R^d$ represents the feature vector of grid state parameters (e.g., voltages, power angles), and $y_i \in \{1,2,3\}$ is the corresponding fault class (e.g., line, transformer, generator fault). Each model learns a mapping function, as in (2).

$$f: R^d \rightarrow \{1,2,3\} \quad (2)$$

That minimizes the empirical risk, calculated in (3).

$$\min_{f \in \mathcal{H}} \left(\frac{1}{n} \sum_{i=1}^{n} \mathcal{L}(f(x_i), y_i) \right) \quad (3)$$

Where L denotes a classification loss function such as cross-entropy or hinge loss, depending on the model architecture.

The training of models was done with the help of the 10-fold cross-validation, and their performance was determined through accuracy, precision, recall, and F1-score. RF and GB are already been proven to be good tools in smart-grid fault analytics [18], [19]. The cryptographic evaluation framework is provided in Figures 2(a) and 2(b), where the AES, RSA, and ECC are compared in terms of resource efficiency, level of security, and speed of encryption. Symmetric cipher is called AES, and it is fast with low latency but has difficulties in key management decentralization [20]. RSA is an asymmetric algorithm, which means that it is very secure and requires a high level of computation overhead, which restricts its practical use in real-time [21]. ECC is an asymmetric scheme, being lightweight and offering the same level of RSA security using smaller keys, hence it is suitable in the case of IoT-based power systems. ECC encryption as in (4):

$$C = (kG, P + kQ) \quad (4)$$

is effective and safe because the elliptic curve discrete logarithm problem is tough [22], [23]. ECC became an optimal compromise between performance and security when it came to the blockchain-based data exchange. The smart contract layer makes the operations secure and auditable because it automates the operations, including fault isolation, load shedding, and re-dispatching of generators once the ML models predict the faults. Every operation is stored on the authorized blockchain, which removes the delay during the manual processing and increases the resilience [24]-[27].

The blockchain and machine learning components of the proposed structure complement each other as demonstrated in Figure 3 to develop an automated, secure, and dynamic system of power grid management. Predictive fault detection: machine learning models, specifically, the random forest, SVM, and gradient boosting classifiers, process real-time grid data streams continuously. These models predict potential malfunctions such as these through the previous system trends and patterns.

Lastly, the ML and blockchain layers work together to provide predictive and secure grid management. ML models do real-time inference on sensor data continuously and identify early warning signs of line outages, generator failures, and load imbalance. The blockchain will activate smart contracts to take remedial measures when outstanding patterns are observed. This unified pipeline can guarantee tamper-resistant logs, safe operation, full traceability, and malicious resistance to reorganization- timely, correct, and dependable contingency response through the synthesis of data-based forecasting and decentralized automation.

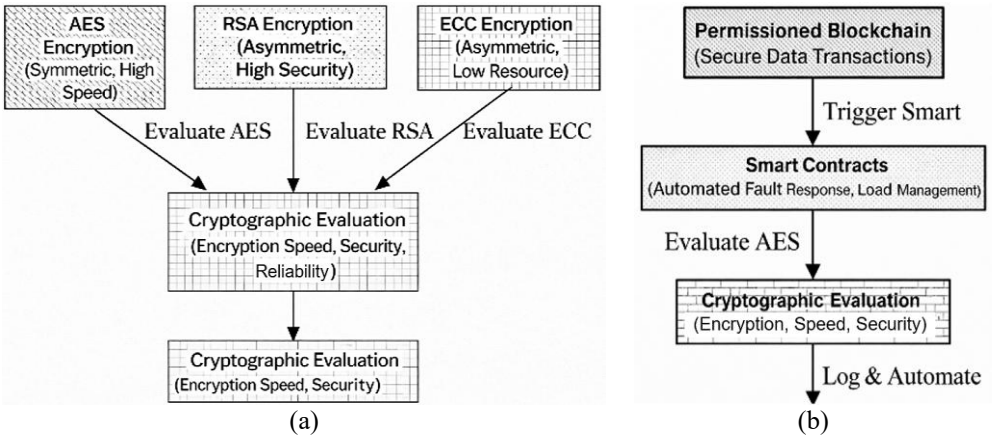


Figure 2. Framework for secure power grid operations using cryptography and smart contracts: (a) comparison of AES, RSA, and ECC based on security and efficiency for smart grids and (b) smart contract–based automated fault handling for secure and auditable grid operation

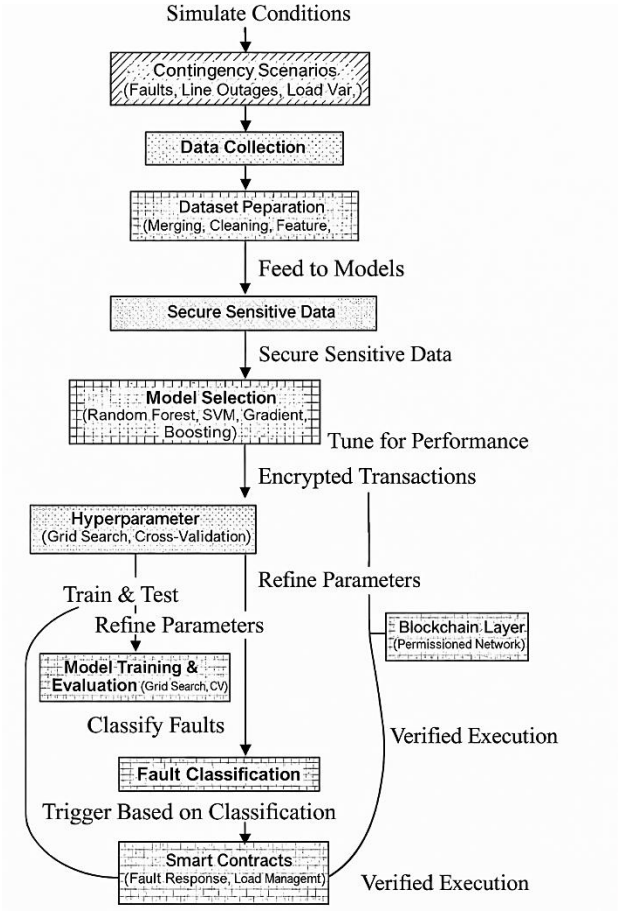


Figure 3. Complete architecture of the proposed hybrid machine learning and blockchain model for predictive and secure power grid management

4. RESULTS AND DISCUSSION

The section implies the results of the machine learning models, analysis of the cryptographic algorithms, and comparisons of the suggested hybrid framework and the traditional contingency management methods. Figure 4 and Table 2 demonstrate the overall comparison case of machine learning model and cryptographic algorithm evaluation [18]-[23]. GB had the best predictive accuracy of 93.4 percent and an F1-score of 0.92; thus is the most trustworthy when it comes to predicting faults within dynamic smart grids. RF with 91.5% accuracy and F1-score of 0.90, as well as SVM with 86.1% accuracy and F1-score of 0.84, are robust to noisy and imbalanced data, but the former achieved higher accuracy and larger F1-score at the cost of increased training time. Simultaneously, ECC has become the most optimal cryptography option, which has a high level of security and low weight baking when contrasted to AES and RSA, which presents it as an ideal cryptography option in the context of blockchain-based automation.

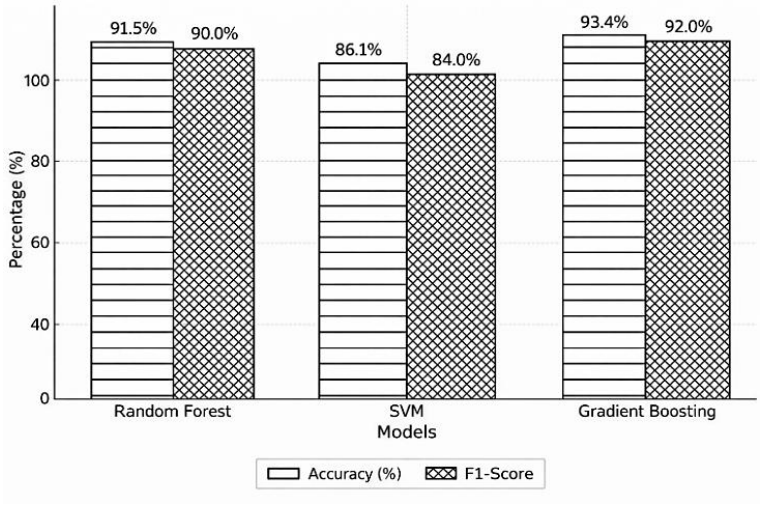
Table 3 can be used to sum up the comparative features of AES, RSA, and ECC. The encryption and decryption rate is the highest in AES, so it is appropriate in high-frequency streams of data, but decentralized key management is difficult. RSA is a secure algorithm, but with high computational costs, it is not applicable in real-time sensor data. The combination of low computation with high security along with smaller key sizes, ECC is the most suitable in blockchain-based smart grids. The level of security that ECC provides is quite high, with a relatively low level of computational burden, which justifies its use in the proposed hybrid system.

Figure 5 shows the relative enhancement of the proposed hybrid model compared to the traditional methods. Traditional contingency management is based on predetermined regulations and manual control, which provoke delays and lack of flexibility. As compared to the hybrid ML-blockchain framework, it reached:

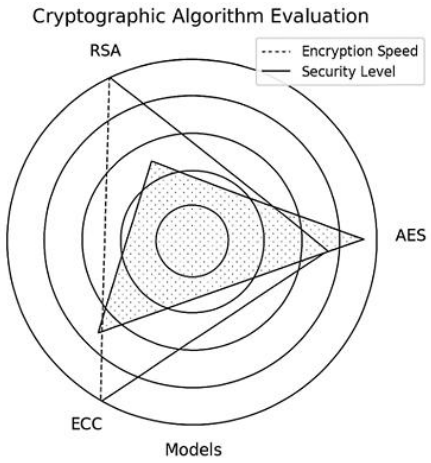
- Accurate prediction of faults is increased by 40 percent, which is due to prediction using ML.
- The response time is cut in half by 60% (because of automated smart contract execution).
- Improved data security since the blockchain register cannot be tampered with.

- Better cybersecurity, with built-in encryption tools.
- Decentralized architecture that enables better scalability.

These findings validate the claim that integrating predictive intelligence with secure autonomous execution is a much more effective means at increasing grid resilience and reliability than traditional methods.



(a)



(b)

Figure 4. Comparative performance of the proposed hybrid framework: (a) ML models compared for fault prediction accuracy and F1-score and (b) cryptographic algorithms compared for security and computational efficiency in blockchain-based smart grids

Table 2. Machine learning model performance comparison

Model	Accuracy	F1-score	Training time	Qualitative insight
Random forest	91.5%	0.90	Moderate	Balanced, interpretable, robust to noise
Support vector machine (SVM)	86.1%	0.84	High	High precision, slow training
Gradient boosting (GB)	93.4%	0.92	High	Best accuracy, robust model

Table 3. Cryptographic algorithm comparison

Algorithm	Key type	Encryption speed	Security level	Suitability for blockchain
AES	Symmetric	Very high	Medium	Best for fast encryption
RSA	Asymmetric	Low	High	High security, less efficient
ECC	Asymmetric	High	High	Best for lightweight security

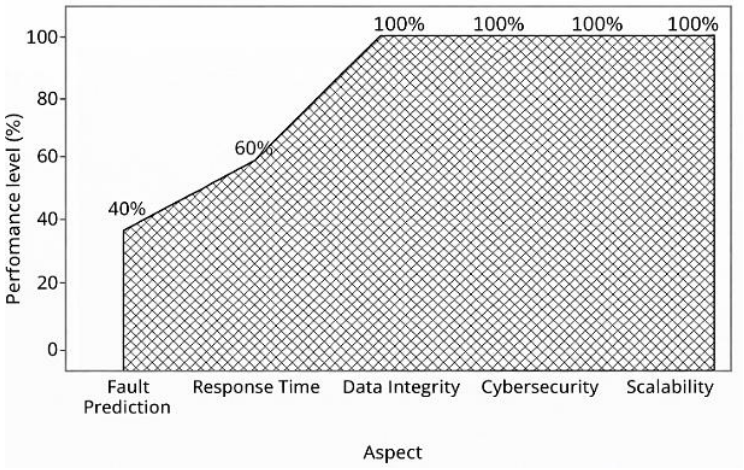


Figure 5. Stacked area chart illustrates the comparative improvement achieved by the proposed model over traditional methods in fault prediction, response time, data integrity, cybersecurity, and scalability

5. CONCLUSION

The research paper suggests a hybrid architecture of machine learning-assisted fault prediction and blockchain-based secure automation of smart grid contingency management. Gradient boosting model reached 93.4% accuracy and made predictions 40 percent more accurate than the old methods and smart contract-based automation lowered response time by 60 percent. ECC turned out to be the most effective cryptography solution, which provided good security and low calculation requirements.

The framework can overcome the main challenges, which are lack of predictive capabilities, manual interventions, and cyber threats by providing a scalable architecture, reliable architecture, and architecture that is tamperproof. The fact that it can identify, segregate, and overcome failures in an autonomous manner is a strong indication of viability in the real world. The future work will be concentrated on large-scale validation, low latency edge-AI, federated learning, distributed training, and advanced cybersecurity techniques to enhance blockchain-based smart grids.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ravi V. Angadi	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	
Suresh Kumar	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓			
A. K. Vijayalakshmi	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓	
G. N. Vidhya Shree		✓				✓		✓	✓					

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] X. Liang, "Emerging power quality challenges due to integration of renewable energy sources," *IEEE Transactions on Industry Applications*, vol. 53, no. 2, pp. 855–866, 2017, doi: 10.1109/TIA.2016.2626253.

[2] S. Chandran, R. Gokaraju, and K. Narendra, "An extended impedance-based fault location algorithm in power distribution system with distributed generation using synchrophasors," *IET Generation, Transmission and Distribution*, vol. 18, no. 3, pp. 479–490, 2024, doi: 10.1049/gtd2.13086.

[3] W. Song, Y. Li, and D. Yang, "Research on the application of blockchain in the energy power industry in China," *Journal of Physics: Conference Series*, vol. 1176, p. 042079, Mar. 2019, doi: 10.1088/1742-6596/1176/4/042079.

[4] M. Choobineh, A. Arabnya, B. Sohrabi, A. Khodaei, and A. Paaso, "Blockchain technology in energy systems: a state-of-the-art review," *IET Blockchain*, vol. 3, no. 1, pp. 35–59, Mar. 2023, doi: 10.1049/blc2.12020.

[5] V. K. Mololoth, S. Saguna, and C. Åhlund, "Blockchain and machine learning for future smart grids: a review," *Energies*, vol. 16, no. 1, p. 528, Jan. 2023, doi: 10.3390/en16010528.

[6] K. Venkatesan and S. B. Rahayu, "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques," *Scientific Reports*, vol. 14, no. 1, p. 1149, Jan. 2024, doi: 10.1038/s41598-024-51578-7.

[7] Y. T. Aklilu and J. Ding, "Survey on blockchain for smart grid management, control, and operation," *Energies*, vol. 15, no. 1, p. 193, Dec. 2021, doi: 10.3390/en15010193.

[8] R. V. Angadi, S. B. Daram, and P. S. Venkataramu, "Contingency analysis of power system using big data analytic techniques," in *2020 5th International Conference on Computing, Communication and Security (ICCCS)*, Oct. 2020, pp. 1–7, doi: 10.1109/ICCCS49678.2020.9276796.

[9] A. Adeyemi *et al.*, "Blockchain technology applications in power distribution systems," *The Electricity Journal*, vol. 33, no. 8, p. 106817, Oct. 2020, doi: 10.1016/j.tej.2020.106817.

[10] R. V. Angadi, J. A. Mangai, V. J. Manohar, S. B. Daram, and P. V. Rao, "An ensemble based data mining model for contingency analysis of power system under STLO," *International Journal of Applied Power Engineering (IJAPE)*, vol. 12, no. 4, pp. 349–358, 2023, doi: 10.11591/ijape.v12.i4.pp349-358.

[11] T. Hidayat and R. Mahardiko, "Data encryption algorithm AES by using blockchain technology: a review," *Baca: Jurnal Dokumentasi Dan Informasi*, vol. 42, no. 1, p. 19, 2021, doi: 10.14203/j.baca.v42i1.643.

[12] A. Farissi, A. Pradata, and K. Miraswan, "Securing messages using AES algorithm and blockchain technology on mobile devices," *SinkrOn*, vol. 8, no. 2, pp. 1166–1171, May 2023, doi: 10.33395/sinkron.v8i2.12381.

[13] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: classification by sources of threats," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 468–483, Dec. 2018, doi: 10.1016/j.jesit.2018.01.001.

[14] S. Beheshtaein, R. Cuzner, M. Savaghebi, and J. M. Guerrero, "Review on microgrids protection," *IET Generation, Transmission and Distribution*, vol. 13, no. 6, pp. 743–759, 2019, doi: 10.1049/iet-gtd.2018.5212.

[15] Z. Lu and H. Mohamed, "A complex encryption system design implemented by AES," *Journal of Information Security*, vol. 12, no. 02, pp. 177–187, 2021, doi: 10.4236/jis.2021.122009.

[16] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, "Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices," *Sensors*, vol. 24, no. 12, p. 4008, Jun. 2024, doi: 10.3390/s24124008.

[17] P. Biswas, A. Rashid, A. Biswas, M. A. Al Nasim, K. D. Gupta, and R. George, "AI-driven approaches for optimizing power consumption: a comprehensive survey," *Discover Artificial Intelligence*, vol. 4, p. 116, 2024, doi: 10.1007/s44163-024-00211-7.

[18] X. Wang, F. Yao, and F. Wen, "Applications of blockchain technology in modern power systems: a brief survey," *Energies*, vol. 15, no. 13, p. 4516, Jun. 2022, doi: 10.3390/en15134516.

[19] R. Qin, L. Zhao, D. Li, K. Yang, J. Xuan, and H. Wang, "Research on design and application of power dispatch based on blockchain," *ACM International Conference Proceeding Series*, pp. 155–162, 2021, doi: 10.1145/3460537.3460564.

[20] S. Cheng, B. Zeng, and Y. Z. Huang, "Research on application model of blockchain technology in distributed electricity market," *IOP Conference Series: Earth and Environmental Science*, vol. 93, no. 1, p. 012065, Nov. 2017, doi: 10.1088/1755-1315/93/1/012065.

[21] S. Ushkewar, S. Vispute, J. More, S. P. Deshmukh, and S. K. Bhil, "Blockchain and AI-powered intelligent power grid: analysis and implementation," *International Conference on Innovations in Cybersecurity and Data Science Proceedings of ICICDS*, 2024, pp. 227–236, doi: 10.1007/978-981-97-5791-6_18.

[22] D. Nallaperuma *et al.*, "Online incremental machine learning platform for big data-driven smart traffic management," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4679–4690, Dec. 2019, doi: 10.1109/TITS.2019.2924883.

[23] R. V. Angadi, S. B. Daram, and P. S. Venkataramu, "Analysis of power system security using big data and machine learning techniques," *2020 IEEE 17th India Council International Conference (INDICON)*, 2020, pp. 1–8, doi: 10.1109/INDICON49873.2020.9342458.

[24] J. Jithish, B. Alangot, N. Mahalingam, and K. S. Yeo, "Distributed anomaly detection in smart grids: a federated learning-based approach," *IEEE Access*, vol. 11, pp. 7157–7179, 2023, doi: 10.1109/ACCESS.2023.3237554.

[25] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efficient mutual authentication protocol for smart grid under blockchain," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2681–2693, Sep. 2021, doi: 10.1007/s12083-020-01020-2.

[26] S. B. Daram, N. Golla, R. V. Angadi, R. Bandam, K. A. Vijayalakshmi, and K. Sesiprabha, "Application of blockchain technology for power system security using condition number," *2023 Second International Conference on Trends in Electrical, Electronics, and Computer Engineering (TEECCON)*, 2023, pp. 46–50, doi: 10.1109/TEECCON59234.2023.10335805.

[27] I. Alhamrouni *et al.*, "A comprehensive review on the role of artificial intelligence in power system stability, control, and protection: insights and future directions," *Applied Sciences*, vol. 14, no. 14, p. 6214, Jul. 2024, doi: 10.3390/app14146214.

BIOGRAPHIES OF AUTHORS

Dr. Ravi V. Angadi received his B.E. in electrical and electronics engineering from VTU, Belagavi, Karnataka (India) in 2010, M.Tech. degree in power electronics from JNTUA, Anantapur (India) in 2014, and his Ph.D. from Presidency University, Bengaluru in 2023. He is currently working as an assistant professor in the Department of Electrical and Electronics Engineering at Presidency University, Bengaluru, Karnataka (India). He has guided UG students' projects sponsored by KSCST, DST, and VTU-RGS. He filed two project patents, one of which has been granted and the other published by the patent office. He has published numerous papers in national and international journals, conferences, and book chapters. He is a life member of IE (I) and ISTE, and a member of IEEE. He can be contacted at email: raviangadi4045@gmail.com.

Suresh Kumar is studying computer science and engineering (data science) in Presidency University, Bengaluru, India, pursuing a B.Tech. He is well-grounded in the field of machine learning, deep learning, artificial intelligence, data analytics, and blockchain technology. His skills are in predictive modelling, data preprocessing, feature engineering, and model optimization. He knows Python, C, C++, Java, JavaScript, and SQL, and has worked with frameworks, including TensorFlow, Scikit-Learn, PyTorch, and Pandas. Also, he is particularly interested in natural language processing, computer vision, and AI-based automation. He can be contacted at email: sureshkumard3140@gmail.com.

A. K. Vijayalakshmi received her B.E. in electrical and electronics engineering from U.B.D.T College of Engineering, Davangere, Karnataka (India) in 2011, M.Tech. degree in power system engineering from Visvesvaraya Technological University, Belagavi (India) in 2014, and she is pursuing Ph.D. from Visvesvaraya Technological University, Belagavi (India). She is currently working as an assistant professor in the Department of Electrical and Electronics Engineering at Sir M Visvesvaraya Institute of Technology (Sir MVIT), Bangalore, Karnataka (India). She has guided UG students' projects sponsored by KSCST. She has published numerous papers in national and international journals, conferences, and book chapters. She is a life member of ISTE and IAENG. She can be contacted at email: vijayalakshmiak9@gmail.com.

G. N. Vidya Shree is presently enrolled in a B.Tech. course in electronics and electrical engineering (EEE) at Presidency University, Bengaluru, India. She has solid background in power systems, embedded systems, control systems, and circuit design. Her specialization is electrical circuit analysis, signal processing, microcontrollers, and power electronics. Her languages and programming experience include C, C++, Python, MATLAB, and experience and expertise in work with Arduino, Raspberry Pi, and FPGA programming. She can be contacted at email: vidyashreevidyashree165@gmail.com.