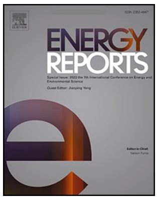
Energy Reports 11 (2024) 2493–2515

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr



Research paper

Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage

Muhammad Aurangzeb [a], Yifei Wang [a], Sheeraz Iqbal [b], Ausnain Naveed [b], Zeeshan Ahmed [c], Mohammed Alenezi [d,*], Mokhtar Shouran [e]

[a] School of Electrical Engineering, Southeast University, Nanjing, PR China
[b] Department of Electrical Engineering, University of Azad Jammu and Kashmir, Muzaffarabad, AJK 13100, Pakistan
[c] The Superior University, Rahim Yar Khan Campus, Lahore, Pakistan
[d] Cardiff University, School of Engineering, Cardiff CF24 3AA, UK
[e] Libyan Centre for Engineering and Information Technology, Bani Walid, Libya

ARTICLE INFO

Keywords:
Smart grid
Block chain
Machine learning
Deep learning
Adversarial attacks
Quantum voting

ABSTRACT

Smart grids are getting important in today's power management, so with that, smart grid technologies are increasingly important too. There have been a lot of concerns about smart grid technologies being hacked, and as a result, some deep black box adversarial attacks have been conducted and presented. We propose a new experimental methodology for benchmarking smart grid security with black box attacks. Additionally, concerning the type of smart grids, Smart Power Grids, deep black box adversarial attacks which can be crafted using virtually no knowledge about the target due to the inherent complexity of content available in cryptographic libraries like SecLib or Bouncy Castle how it affects security of cyber-physical power systems. We identify potential impacts of deep black box attacks on Smart Power Grids as implemented by the Department of Energy in 1996, we evaluate existing protection methods, and we find out the pitfalls thereof. With the aim of overcoming the aforementioned drawbacks, we initiate a study on deep black box adversarial attacks against Smart Power Grids showing that statistically significant effects against a national Smart Power Grid are achievable with absolute security. We also probe detection of cyber security attacks on Smart Power Grids. We illustrate landscape of smart grids with numerous cyber threats and demonstrate the limitations of traditional security practices. We show the importance of machine learning to detect attacks and the unlikelihood of identification of dependable and efficient detection schemes. We describe quantum voting ensemble models as one of the most powerful techniques in the detection of cyber security attacks. Finally, we propose an experimental setup and evaluation criteria to detect cyber security attacks in smart grids using quantum voting ensemble models. Then, we talk about private data storage in blockchain based smart grid infrastructure. We give an introduction of block chain and its essentiality in smart grids. We discuss privacy issues in block chain based smart grids. We acknowledge the strength of privacy safeguards, but on the same wavelength, we realize their weaknesses. Next, we propose a quantum resistant encryption technique that enhances the privacy of smart grids. We propose quantum voting ensemble models as one of the most promising techniques to address the issue of private data storage in block chains. As a result, we provide a comparison between the proposed models and traditional approaches to privacy protection in smart grids based on an experimental performance review. Then, we propose a unified strategy to improve smart grid cyber security by incorporating deep black box attacks with quantum voting ensemble models. Finally, we disclose several benefits of such integration and perform an experimental evaluation to investigate the effectiveness of the unified approach. The results of our study identify security gaps in smart grids and propose state-of-the-art mechanisms to address them. The challenges of smart grids system require the amalgamation of blockchain, quantum voting ensemble models and deep black box adversarial attacks. We achieve this objective proposing a unified strategy. The results of this study will equally be helpful for future research and smart grid cyber security implementations.

* Corresponding author.
E-mail addresses: maurangzeb420@qq.com (M. Aurangzeb), wyf@seu.edu.cn (Y. Wang), sheeraz.iqbal@ajku.edu.pk (S. Iqbal), ausnain.naveed@ajku.edu.pk (A. Naveed), zeeshan.ahmad.ryk@superior.edu.pk (Z. Ahmed), alenezim1@cardiff.ac.uk (M. Alenezi), mokhta4520@gmail.com (M. Shouran).

https://doi.org/10.1016/j.egyr.2024.02.010
Received 29 August 2023; Received in revised form 24 January 2024; Accepted 7 February 2024
Available online 15 February 2024

Acronym Definition

AES	Advanced Encryption Standard.
API	Application Programming Interface.
CPU	Central Processing Unit.
GB	Gigabyte.
IoT	Internet of Things.
KNN	K-Nearest Neighbors.
RSA	Rivest-Shamir-Adleman.
SG	Smart Grid.
SVM	Support Vector Machine.

1. Introduction

Smart grids have revolutionized the power management industry by providing the capability to monitor energy usage, consumption, and optimization very precisely (Beg et al., 2021). Nevertheless, the growing reliance of smart grids on information and communication technologies (ICT) makes smart grids more vulnerable to cyber threats (Reddy Shabad et al., 2021). The aims of this study include the detection of cyber security attacks and the deployment of deep black box adversarial assaults to enhance the cyber security of cyber-physical power systems in the smart grid (G and Kumari K, 2022).

The authors are also studying quantum voting diagonal ensemble methods for secure and private data storage in a distributed ledger (Huang et al., 2022). When it comes to electricity, the traditional working system of standard power supply is replaced by an automized power supply system called Smart Grid through which the consumer can access the utilization of electricity as per the requirement and it is collected automatically by a smart energy meter to the utility side (Haque, 2020). A new driving force for technology advances is the modern electrical power grid that uses advanced sensing, communications, processing, and control capabilities to enable the smart grid to easily achieve the efficient managing of power for the customer side (Haque, 2020). Smart grids improve the dependability, sustainability and efficiency of dynamic operational behavior of using the energy through real-time monitor, efficient energy consumption, renewable sources etc. These advanced features are not available in existing power grids (Takiddin et al., 2022). Smart Grids are often called as 'smart' power grids as they fulfill all the requirements in handling huge problems. With complex software architecture, integration of hardware and network equipments the vulnerabilities of Smart grids to cyber attacks have led several security issues (Hrovatin et al., 2022). The intruders attack the Smart Grid who modify energy consumption patterns, control the entire power supply, and manipulate the data. In order to determine energy usage, any faults in this system should require real-time monitoring in a controlled environment for avoiding security issues (Cao et al., 2022).

As computing progresses to greater stages, the smart grid has become one modern topic of interest (Dehghani et al., 2021; Drayer and Routtenberg, 2020; Manandhar et al., 2014). Because of how fast the grid updates everyday, there are several cyber security threats (Shahid et al., 2022; Qu, 2021; Krivohlava et al., 2022; Jin et al., 2020) that could bring it down. Every day, attackers revise their strategies to get around the grid's walls, so it is important to bring up the right barriers to secure the grid against these cyber security threats (Abbaspour et al., 2016). One case of a types of threat could come from a deep black box adversarial attack correlated to the smart grid's extensive linkages and complicated system architecture. In order to deal with these security threats, real-time detection of the attacks are required to detect the smallest issue and also to minimize the issues when they come up. In most cases, the grid, at a high level, might be able to prevent some issues from coming up but would fail to notice a smaller issue with the grid; obviously, this is unacceptable (Ozay et al., 2016; Karimipour et al., 2019; Rawat and Bajracharya, 2015; Liu, 2015). On another note, the smart grid brings up a different topic, the blockchain with the grid. This involved third party business in managing the grid using blockchain though poses some problems. One of the problems include privacy invading; therefore, serious thought must be put in how to keep the grid working hard and provide privacy (Kurt et al., 2018).

The Preamble of this study research is aiming to innovate and provide insights into the problem solutions along with the models involved in it. Currently, the day to day embanking over power cyber physical systems suffer from the deep adversarial black box attacks. Hence the, this study also extacts the impact of the deep adversarial black box attacks on the cyber physical power systems by validating the existing defence mechanisms over it (Beg et al., 2021). This Research Study also aims the detection and categorization of the cyber security attacks in the smart grids and it also leads to the categories of intrusion detection methods with the details of the state of art,stimulant and quantum based voting ensemble models (Takiddin et al., 2022) and (Hrovatin et al., 2022). The Research also aims to provide an innovative model for private storage to enhance privacy for blockchain-based systems by the inclusion of Quantum Voting Models as well.

The proposed solutions and discovered will enable the practitioners and researches to developed effective security mechanisms in the SCs, resulting in practical implementations to improve their detection capabilities from attacks and also for preserving data's privacy of smart grid systems too. In order to bring under SC framework a number of anomaly detection technique are prepared based on un-supervised and supervised machine learning; also with the knowledge of these various domains in an SG architecture, it helps to understand and fulfill the security and privacy requirements of each entity present in the domains as well. Under the SG there exist different domains and the NIST has defined seven broad classes of SG's domains, and then entities present under them too. It is quite possible to have the existence of anomalous hubs with the organizations that store smart grid data in a writable, public format and without directive implementations of such security measures, there is always the scope of smart meter user profiles, billing information, and network configurations being misused by the attacker too. An SG infrastructure is always under the security threats and their exist a number of potential attackers and some of the many potential attackers to an SG infrastructure include: Hackers, Cyber terrorists, Industrial competitors, Organized criminal groups, and Dissatisfied or improperly trained personnel. In SC security, the anomaly detection is at the top of the list because the SC desires continuous service and Fig. 1 shows a typical SG architecture that is based on the multi-layer design too.

Fig. 1 illustrates the multi-layer architecture of a smart grid system. the smart grid is an advanced power delivery infrastructure that integrates modern communication, control, and information technologies with the traditional power grid. The multi-layer architecture provides a hierarchical structure to manage and control the different components of the smart grid system. Since the smart grid's problems stem from its centralised design, it makes sense to use decentralised solutions for managing data. Since embedded technology in sensors is becoming increasingly sophisticated, there is compelling motivation for the development of distributed systems. These days, smart sensors are either able to connect wirelessly to a web server or have sufficient computing power to run an OS and the full web protocol stack (Shahid et al., 2022). Because of this, they are valuable online resources for constructing a global sensor network (Qu, 2021). A key selling point in this setting is the ability to divide data gathering from administrative duties (Krivohlava et al., 2022). Bitcoin, the first real implementation of the blockchain that permits decentralised trust, sparked a proliferation of similar systems (Jin et al., 2020). Security assaults in centralised SGs aim for pinpoint accuracy, but in decentralised sgs, the focus is on tracking the flow of messages to establish accountability (Abbaspour et al., 2016). Adjustments are required (Ozay et al., 2016) when data mining processes, generally performed on centralised databases, are implemented in a decentralised SGs (Karimipour et al., 2019). To find anomalies in a decentralised system, data mining tasks need to be (1) rethought to better match the system, and (2) secured privately at the expense of only slightly more computer resources. Several developments have been made in this space, however they either have prohibitive communication costs or need an excessive amount of processing resources.

Neither a centralised blockchain-based Smart Grid data storage system nor a machine learning technique for identifying anomalies or cyberattacks in a blockchain environment have been discovered, according to the research. Key contributions from this study are:

- Smart grid system provides incremental models through decentralized privacy and data are kept inside the particular sensor domain. Our research provides a privacy and security to the data's in smart grid systems and it's a completely new methodology model. It provides an enhanced secureness to the data. The smart grid setups yield decrement models. This paper proposes a new way of getting a new model increment by constructing the decentralized privacy in which the data's are only maintained at the sensor domain. This novel that was never before investigated approach provides an enhanced security to the data and privacy of smart grid system to a great extent.
- Smart grid security provides accuracy and efficiency through traditional way of doing crypto system and also on this paper we use for a new approach of quantum voting classification model. We propose a quantum voting classification model and analyzed various aspects of the smart grid security in this technique. Using a quantum voting classification model improves the analysis regarding the traditional cryptographic system and that leads to the greater accuracy of cybersecurity injunction with the smart grids. Also the smart grid security is major concern typical problem which affects the careers gatekeepers, industry and many others. We used a quantum voting classification model for the accuracy in smart grid security with those smart grids. A crucial feature of the benefits of quantum voting classification model are identified various abnormalities and cyberattack in keeping the integrity of the smart grid system.
- We discuss the architecture of cyberattacks against the smart grid system. We propose core network elements that integrate quantum voting ensemble model and blockchain privacy-preserving storage. We proposed that protects against cyberattacks and data privacy are preserved. And we explain various aspects of smart grid such as smart home, smart vehicle and also the social scientists face challenges in the simulating security limitations data. Smart grids are a vital infrastructure for a sustainable and efficient 20th century future of billions lies in the hands of secure and reliable smart grids. One can promote sustainability, reduce carbon emissions and establish an ultra resilient technology – the best of 21st century which is the best of three worlds. Protecting smart grid cyber infrastructure is an important task today. In this paper, we will concentrate on smart grid, with smart grid systems as a very important infrastructure to protect cyber secure with some of the advanced method is to vote with quantum ensemble block to check whether we voted for the model and protected to the last human after cyber attacks like the model.
- In our approach, we use quantum voting ensemble models based on block chain privacy preserving storage to produce attack tolerance, security, accuracy and privacy of smart grid system it's a new privacy methodology. In this paper, our thinking is that of providing a method of choosing and responding to the new model that begins to affect the smart grid system. Smart grid systems are trying to provide several models. Some smart systems appear to be very dependent but others do not. The next year the traditional voting model produces. Also, our smart work removes the errors caused by the traditional model, especially the spam mail and it will be a voting model with a new quantum model in terms of the accuracy of the cyberspace.

2. Related work

The contemporary electric grid is monitored, controlled, and protected by a large network of interconnected equipment. The current smart grid (SG) relies heavily on cyber-physical (CP) networks. The "physical," "data acquisition," "communication," and "application" levels make up the architecture. The generating, transmission, and distribution

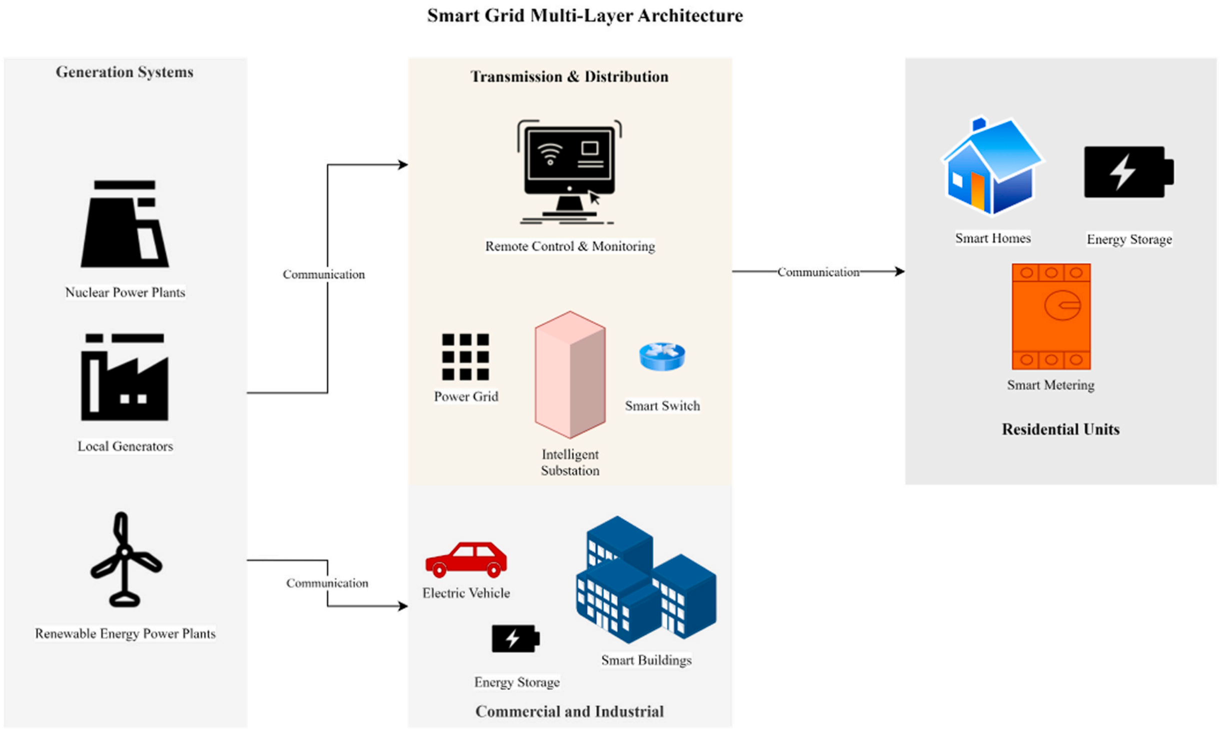


Fig. 1. Smart Grid Multi-Layer Architecture.

systems are all part of the physical layer. The use of converters to link distributed energy resources (DERs) to the grid enables SG to maximise energy extraction (Rawat and Bajracharya, 2015). Smart sensors and measuring devices make up the data collecting layer and communicate their findings on to the communication layer. The EMS uses the data from the communication layer for optimising, monitoring, and controlling the actuators. The communication layer receives data from a wide range of wired and wireless technologies and network nodes (Kurt et al., 2018). Although the addition of cyber layers boosts the SG's performance, it also opens up new attack vectors. The ability to keep tabs on and manage physical assets may be jeopardised if an attacker gains access to the weak points (Mokhtari et al., 2021). A number of factors (Aziz et al., 2022) contribute to the success of the SG network, including demand response, energy efficiency, a volatile power market, distributed automation, and so on (Almalaq et al., 2022). Looking at these characteristics as a whole, the SG becomes the most likely candidate. Machine learning (ML) has become increasingly popular due to its capacity to automatically recognise and extract patterns from data. An increasing number of research [26] have examined the role of ML in SG's cyber defences (Alrowais et al., 2022; Reddy Shabad et al., 2021).

Abnormalities in ICSs, such as attacks on Smart Microgrids, can be uncovered by network traffic monitoring. Attackers who can successfully mimic system behaviours can evade intrusion detection systems based on network traffic [27]. This research takes a novel approach by making use of Supervisory Control and Data Acquisition (SCADA) measurement data for this function. A measurement intrusion detection system (MIDS) can detect aberrant system activity even if the attacker masks it in the control layer. A supervised machine learning model classifies ICS events as "normal" or "abnormal" to evaluate MIDS performance. devices-in-the-loop (HIL) testbeds mimic real-world power generation devices by exploiting attack datasets. As part of their advice, Mokhtari et al (Mokhtari et al., 2021). suggested running numerous machine learning models on the dataset; these models performed particularly well when it came to identifying outliers, such as covert attacks. Finding outliers in the quantifiable data produced by the testbed is a breeze using the random forest.

Smart energy networks, which regulate production, distribution, and use, can help address a number of safety issues associated with the management of this vital resource. Both natural and human-caused disasters pose threats to systems. It is critical for operators of energy systems to be aware of potential disruptions. In order to identify intrusions into power grids, the authors of this study (Almalaq et al., 2022) describe a deep learning-based PMU-taught model. Features generated by property or specification creation are given to a wide variety of machine learning methods, including the AdaBoost fundamental classifier and the random forest. Data from open-source simulations are used to back up 37 incident case studies that involve the energy system. Multiple metrics were used to compare the proposed design to existing alternatives. Simulations showed that this model outperformed prior techniques in terms of both detection rate (93.60 %) and accuracy (93.91 %).

Due to their reliance on bidirectional communication, power electronics components in contemporary cyber-physical microgrids, such as converters or inverters with local integrated controllers, are vulnerable to cyber manipulations. Hardware is always a bad investment. Due to the microgrid's distribution network's capacity to move information and limited inertia, cyber and physical problems can swiftly spread across the system. Cyber-physical anomalies can be spotted with the use of parametric time-frequency logic (PTFL). The PTFL formalism is used to examine the time-frequency composition of observable values from power electronics devices, such as current, voltage, and frequency. Omar et al (Beg et al., 2021). describe the PTFL formalism for fault/anomaly detection in a set of four DC microgrids and an IEEE 34-bus feeder system with inverters using a controller/hardware-in-the-loop arrangement.

Criminal activities, such as electricity theft and hacking, can be found by studying data from the smart grid. Machine learning can detect unusual occurrences. Feature extraction is necessary for grid data. In the smart grid, anomalies are out of the ordinary occurrences. Power, voltage, current, and consumption can all affect the outcomes of conventional grid construction. In this research (Reddy Shabad et al., 2021), this paper create a working model of an anomaly-detection system for the smart grid. Anomaly detection improves system efficiency and coordination. Modifications to settings in reaction to cyberattacks will be uncovered. Anomaly detection models like Isolation Forest (IF) use a forest of decision trees to find and isolate outliers. Simulating the detection method on a hardware testbed confirmed its efficacy. Following the identification of the most important properties by principal component analysis, the model was put through its paces using the dickey-fuller test.Cyber Smart grids are a tangible option for resolving the energy crisis. Cross-domain data flow complicates anomaly detection in the smart grid. Machine learning models can be used for both supervised and unsupervised data analysis and prediction. This study (Drayer and Routtenberg, 2020) explores the use of machine learning in anomaly detection algorithms for Smart Grid Infrastructure.

Avoiding instability and EMS mistakes necessitates the detection and removal of unreliable microgrid data. This article (Huang et al., 2022) describes a sequential detection method that makes use of the Online Sequential Extreme Learning Machine (OSELM), statistical analysis in a sliding time frame, and density-based spatial grouping of noisy applications. OSELM first trains on the data sequence itself to extract the electrical characteristic from the microgrid data. Statistics like the variance rise and the correlation coefficients that accompany it over a sliding time window are examples of complementary feature dimensions. Next, DBSCAN checks for mistakes in the dimensions of a feature. Data from a four-terminal DC microgrid prototype verifies the detection method's efficacy. When compared to electrical and statistical methods, this technique is more effective in identifying false data. It will eventually be able to spot faulty readings in real-time microgrids as well.

In order to function properly, a smart grid must integrate state-of-the-art digital and mechanical components, making it a complex cyber-physical system. Cyberattacks pose the greatest threat to the development of cutting-edge technology. Over time, SG has benefited from the introduction of a wide variety of tools, gadgets, and equipment that have increased its robustness, efficiency, and cost-effectiveness. These goals were accomplished, but at the cost of a more vulnerable network due to the explosion of Internet-enabled devices. Hackers and system operators in Singapore are both taking advantage of ML's powerful computational and reasoning capabilities to attack and defend the country's cyber infrastructure. Haque et al (Haque, 2020). provide a comprehensive review of the present state of the art in the SG sector, covering a wide range of methods for launching, detecting, and protecting against cyberattacks.

Cyber-physical systems, like microgrids, have multiple parts that work together. Communication cables and sensors can modify data before it reaches the cyber layer. Attacks on the cyber layer of a DC microgrid could cause voltage instability and load dispatch fluctuations. Locating irregular data is crucial for reestablishing normalcy (Takiddin et al., 2022).

The increasing penetration of cyber-physical systems (CPSs) expose the power grid at risk of malicious attacks. Therefore, it is very important to detect cyberattacks because of the study of DC-MGs which is now used in various sector of EE such as in their (i) distributed resource power generation, (ii) power distribution, (iii)underground electric network, and (iv) full energy planning. A new approach for Detection of DC-MG Bogus Data Injection Attack to Improve Power Government Security (Dehghani et al., 2021) was implemented in this research to improve the cybersecurity of the power grid. In this paper the proposed method, a deep machine learning based on singular value decomposition and wavelet transform is proposed to detect DC-MG cyberattacks as well as to select ensemble deep learning based on Grey wolf optimization (GWO) is proposed to detect DC-MG bogus data injection attacks.

To train the DL network, cyberattack and load fluctuation techniques have been incorporated into the DC-MG running and controlling without FIAs and producing the data in normal performance for collecting the enough data. The simulation results indicate that the performance of the proposed method to Detect of DC-MG Bogus Data Injection Attack (IDMG-FDIAs) outperforms other existing techniques Shallow model, Hilbert Huang Transform (HHT) techniques to detect some numbers of DC-MG FDIAs.

Multi-dimensional, heterogeneous, complex systems with high degrees of cyber-physical integration (CPI) characterise the rapidly informatizing power grid as cyber-physical power systems (CPPS). Over the past few years, network attacks have become a significant threat to the stability of the power system. In order to keep CPPS operations steady in the face of DDoS attacks, this study provides a method for identifying network intrusions using ensemble learning. A strategy for equitably processing data was proposed as a first step towards fixing the issue of insufficient network assault samples, which results to false positives in detection (Cao et al., 2022). The LightGBM ensemble was developed to detect security holes in a network and trace the origin of outages. Adding the focal loss to the gradient boost process helped the classifier hone in on mislabeled data, which improved its ability to spot network dangers. Taking cyber-physical elements into account, a method is presented for assessing the network attack detection model. This paper also use a network attack detection model to perform a quantitative examination of the cyber-physical power system's resilience. The results show that the F1 score increased by 16.73 percentage points and the accuracy increased by 15.67 percentage points while detecting threats in a network.

The smart grid is a cyber-physical system that combines digital networks with conventional power distribution infrastructure. Injecting malicious data into such a system can have far-reaching consequences. Methods that rely on residuals can be fooled by sophisticated false data injection (FDI) attacks. The linearized DC power system model often used in studies to identify FDI attacks leaves them open to attacks from the AC model. In order to solve these problems, the authors of this study (Drayer and Routtenberg, 2020) employ the AC power flow model and the grid graph structure. This paper find FDI attacks that were not seen before. This approach is based on the principles of graph signal processing (GSP). The proposed detection method is based on the Fourier transform of a graph to remove high-frequency components which are based on the expected state of the network. By comparing the maximum norm of the result to a predetermined threshold, the detection of FDI attacks is possible. When evaluating in the IEEE 14-bus system, the method successfully detected attacks that were undetectable at angles and voltages. Various types of attack on the smart grid threaten to compromise its security. These include: data injection, denial-of-service, and random attacks on the communication infrastructure that links the sensors, actuators, and control systems. Manandhar et al (Manandhar et al., 2014). use a mathematical model to assess the vulnerability of the smart grid to such attacks and suggest a security policy. In our work, we use the Kalman filter to estimate the parameters of the state process of many models.

3. Methodology

To enhance the privacy and security of the data storage of blockchain-based smart grids, this approach is implemented. As well as addressing cybersecurity problems in a new era of threats this approach is developed. (1) Deep Black Box Adversarial Attacks and (2) Quantum Voting Ensemble Models; which are on the cutting edge of technology were combined in order to perform this approach. Smart grid technology has widespread functions such as improved efficiency, improved reliability, and reduced environmental impact. However, along with these advantages, new problems are created, especially cyber security. Smart grids collect, store, and transmit vast quantities of private information and can therefore be hacked. Ensuring the reliability of smart grid infrastructure means addressing cybersecurity challenges. In this approach, the challenge is addressed directly by using Deep Black Box Adversarial Attacks, identifying and attacking vulnerabilities in smart grid systems which will enhance the overall security of the system. By combining this with Quantum Voting Ensemble Models, where through the use of quantum computing, the security of the data storage against the privacy is protected to a high degree. In this way, the privacy and security challenges of blockchain-based smart grids have been effectively addressed using Deep Black Box Adversarial Attacks and Quantum Voting Ensemble Models. This method also ensures that the personal information stored in smart grids protected and that it has a better fitness and has a more security system than the existing systems.

Our methodology involves a novel integration of deep black box adversarial attack methodologies with quantum hybrid voting ensemble models within the framework of blockchain-based storage in smart grid systems. The merging process can be delineated into the following key steps:

Adversarial Attack Integration: We leverage the principles of deep black box adversarial attacks, incorporating them into the training phase of the quantum hybrid voting ensemble models. This integration aims to enhance the models' robustness by exposing them to a spectrum of potential cyber threats, thereby fortifying their ability to detect and mitigate adversarial manipulations.

Quantum Hybrid Voting Ensemble Models: Our study introduces a unique ensemble approach that combines classical machine learning algorithms, such as Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Naive Bayes, with quantum machine learning techniques. The ensemble is designed to harness the strengths of both classical and quantum paradigms, fostering a more resilient and adaptive defense mechanism against cyber threats.

Blockchain-Based Storage Enhancement: The merged models are then applied to enhance the security and privacy of blockchain-based storage in smart grid systems. The ensemble's collective decision-making process contributes to a more robust identification of

Table 1
Comparative analysis of previous studies.

References	Dataset	Technique	Model	Privacy Preserving	Outcome
Mokhtari et al (Mokhtari et al., 2021).	Smart Grid	Machine Learning	Random Forests	No Method	88 %
Almalaq et al (Almalaq et al., 2022).	Smart Grid	Deep Machine Learning	Adaboost Model	No Method	93.91 %
Beg et al (Beg et al., 2021).	IEEE Bus 34	Not applicable	parametric time-frequency logic	No Method	Not specified
Reddy et al (Reddy Shabad et al., 2021).	Smart Grid	Machine Learning	Isolation Forests	No Method	89 %
Huang et al (Huang et al., 2022).	Smart Grid	Clustering	DBSCAN	No Method	85 %
Dehghani et al (Dehghani et al., 2021).	Smart Grid	Machine Learning	Machine learning-based wavelet transform	No Method	95 %
Cao et al (Cao et al., 2022).	Smart Grid	Machine Learning	LightGBM	No Method	85 %
Drayer et al (Drayer and Routtenberg, 2020).	Smart Grid	Machine Learning	Ensemble Models	No Method	81 %
Manandhar et al (Manandhar et al., 2014).	Smart Grid	Not applicable	Kalman Filter	No Method	Not specified
Proposed	Smart Grid	Machine Learning	Quantum Voting Classifier	Blockchain, Cryptography	99.8 %

abnormal activities and cyberattacks, reinforcing the integrity of data stored in the blockchain.

3.1. Deep black box adversarial

To examine smart grid architecture security we can use advanced machine learning technologies for alert evaluation and rank machine learning techniques for measuring those sensing and assicaoed actor ship points. Deep black box adversary attacks stem from this and if deep black box adversary attacks occurs on architecture it gets ranked. Deep black box adversary attacks are performed on smart grid to know architecture security prior to attack in real time. Based on the attack on evaluation on machine learning techniques it can alter defense mechanism under attacks – The method adopted here changes or alters the defense mechanism of the WSN, based on the attack on evaluation on machine learning techniques. Generally, any system can have weakness only at its base level, so in order identify the weakness of any system we need to perform some level of deep analysis, for the security of Smart Grid using deep black box adversary attacks on architecture of the base level Once we know the flaws or weak points of smart grid by attacking on architecture in black box adversary attacks we can create a defense mechanism which is robust by using the proposed deep black box adversary attacks. Further the next point is mentioned regarding the how this Defense Mechanism is more effectively created based upon our proposed method. Quantum voting ensemble models play a major role in Smart Grids for security enhancement. The main idea of Quantum Voting in blockchain is to store privacy information securely in a blockchain. Quantum computing can be used in securing and fully decentralizing identity systems. The primary features of quantum computing such as speed and accuracy can be used in securing identity information and other sensitive data in the Smart Grids. Cryptography and data security are the main aspects of Quantum computing. Data's in blockchain should be stored securely and needs to be retrieved accurately when needed. Private and secure storing of Data's are possible with the help of Quantum computing. Quantum voting ensemble models adds some advantages and high level securities to the blockchain. If at all all the data are stored in the blockchain it leads to overflow. So we need to retrieve the accurate and wanted data from the blockchain for that Quantum computing is required. Quantum computing is used for storing all the data securely and accurately at the same time in the blockchain. By Quantum voting ensemble models we are creating robust decision making by using Quantum Algorithms and by combining various classifiers.

3.2. Data collection and pre-processing

The dataset utilised in this research is the basis for testing out the proposed approach to better smart grid cybersecurity. There are many parts to it that together shed light on the smart grid's safety features. Let's take a closer look at each component:

Meter ID:

For each smart metre on the grid, this attribute serves as its own identification number. It's useful for keeping tabs on and identifying individual metres.

EMS (Energy Management System):

In the context of the smart grid, the term "energy management system" (EMS) refers to the overarching control system that keeps tabs on and directs everything from generation to consumption. Information pertinent to the EMS is recorded by this function.

MMS (Manufacturing Messaging Specification):

The MMS protocol is a popular means of communication in automated manufacturing environments. This function stores MMS-related information within the context of the smart grid.

Data Flow Packets:

In a smart grid system, the number of packets indicates the total amount of data transferred. It reveals information on the flow of data and the manner of communications.

Packets from the source:

The number of packets from a given source is referred to as the source packet count in a smart grid network. Data transmission origins can be determined with the use of this capability.

Destination Packets:

The number of packets received by a specific destination node in a smart grid network is denoted by the destination packets variable. It's useful for seeing how information is shared and used.

IEDs (Intelligent Electronic Devices):

In the smart grid, IEDs are used to monitor and manage electricity distribution. This function records data about the IEDs in the system.

Records in a blockchain:

Data kept on the blockchain, a distributed and secure ledger used for smart grid transactions, is referred to as blockchain storage. This function sheds light on how blockchain technology can be used for archival purposes.

Consensus mechanism:

The consensus mechanism determines how agreement is reached among participants in the blockchain network regarding the validity and ordering of transactions. This feature represents the specific consensus mechanism employed in the smart grid.

Transaction throughput:

Transaction throughput refers to the rate at which transactions are processed and validated within the smart grid network. It measures the system's capacity to handle a high volume of transactions efficiently.

Attack:

The attack feature denotes the presence or absence of a cybersecurity attack in the smart grid system. It serves as the target variable in this study, indicating the security status of the system.

To provide a clearer overview, Table 2 presents the dataset features descriptions.

The dataset is used to analyze the relationship between these features and evaluate the performance of the proposed methodology for enhancing cybersecurity in smart grids. Fig. 2 and Fig. 3 shows the total percentage anomalies in dataset.

Fig. 4a shows histograms of each feature in seaborn. Histograms are a visualization technique that represents the distribution of a continuous variable. Each feature in the dataset is plotted separately, and the x-axis represents the range of values for that feature, while the y-axis represents the frequency or count of occurrences of each value. The form of a distribution, the existence of outliers, and other characteristics can all be learned from a histogram. Each seaborn feature's KDE plot may be shown in Fig. 4b. The probability density function of a random variable can be estimated using the KDE technique, which is a non-parametric approach. A more refined approximation of the true data distribution is provided. For each characteristic, this paper plot a curve along the x-axis to show the estimated density of values at various locations. KDE plots can help you figure out if your data follows a normal distribution, how many peaks or modes there are, and whether or not they are significantly different from one another.

Table 2
The dataset features with description the dataset features with description:.

Feature	Description
Meter ID	Unique identifier for smart meters
EMS	Energy Management System data
MMS	Manufacturing Messaging Specification data
Data Flow Packets	Number of packets in the data flow
Source Packets	Number of packets from a specific source
Destination Packets	Number of packets received at a destination
IEDs	Intelligent Electronic Devices data
Blockchain Storage	Amount of data stored in the blockchain
Consensus Mechanism	The employed consensus mechanism
Transaction Throughput	Rate of transaction processing
Attack	Presence or absence of a cybersecurity attack

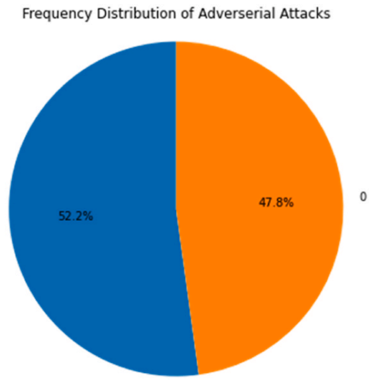


Fig. 2. Total percentage attacked isntances in dataset.

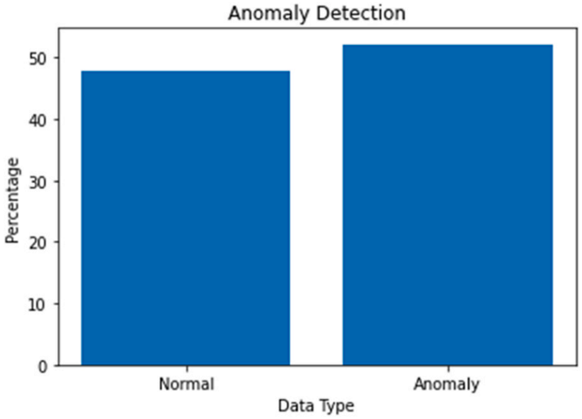


Fig. 3. Histogram of Frequency Distribution of Target Variable.

The Consensus Mechanism is shown in Fig. 5a. To ensure that all participants in a blockchain network agree on the veracity of transactions and their chronological order of addition, the system relies on a consensus process. The Consensus Mechanism feature is not shown in this diagram in great depth since it has likely been analysed and visualised independently, perhaps using a different sort of plot or visualisation technique.The Transaction Throughput function is shown in Fig. 5b. The term "transaction throughput" describes the rate at which a blockchain network can process and confirm transactions. It’s a crucial indicator of the blockchain’s ability to scale and its overall efficiency. Fig. 5b is a visualisation that may elucidate patterns, trends, and distributions in the data set’s transaction throughput. However, the specifics of the visualisation cannot be discerned without the real figure or additional information.

Data collection:

The information in this study originated from a functioning smart grid in the real world. The system incorporates a number of monitoring and logging systems to collect information about the characteristics listed in Section 3.1. Collecting this information required keeping track of everything happening on the smart grid network throughout a given time frame. With this information, this paper can assess the performance of the proposed strategy and analyse the system’s behaviour.

Data pre-processing:

The obtained data is put through a series of pre-processing processes to confirm its quality and suitability for analysis before any analysis is performed. The following procedures are used as preliminary processing steps:

Missing data handling:

Data loss occurs frequently in real-world circumstances because of things like network outages and failed sensors. The precision and trustworthiness of the analysis may be diminished by missing data. Methods like imputation and deletion are used to deal with missing data, depending on the specifics of the situation. Missing values can be replaced with approximated values using imputation techniques like mean or median imputation.

Outlier detection and removal:

Datapoints that are extremely out of the norm in a given dataset are said to be outliers. They can result from off-the-wall circumstances or faulty measurements. Data outliers have the potential to skew analytical outcomes and undermine the effectiveness of the proposed methodology. The interquartile range (IQR) and the Z-score are two powerful statistical tools used to identify and eliminate data outliers.The resulting clean dataset is shown in Fig. 6a. After missing values are handled, duplicates are removed, inconsistencies are fixed, and the data is transformed into an analyzable format, this paper say that the dataset has been cleaned. The picture does not show the exact specifics of the cleaned dataset, but it does show that the dataset has been processed and is ready for modelling or analysis.

The resulting boxplot is displayed in Fig. 6b. A boxplot is a kind of histogram that shows the minimum, maximum, median, and quartiles of a dataset graphically. Half of the data falls within the box depicting the interquartile range (IQR) in the scatter plot. The middle line in the box indicates the median. Outlying data points are indicated by whiskers that extend beyond the range’s minimum and maximum values. Fig. 6b provides a boxplot that allows us to more easily understand the range and dispersion of the cleansed data and to see the general nature of the data. Looking at this gives us the ability to identify the presence of extreme values, and see the evenness or skewness of the data. This makes the boxplot a useful tool, as it helps to identify trends and outliers within the cleansed data, allowing researchers to make further conclusions based on this recognition.

Feature scaling:

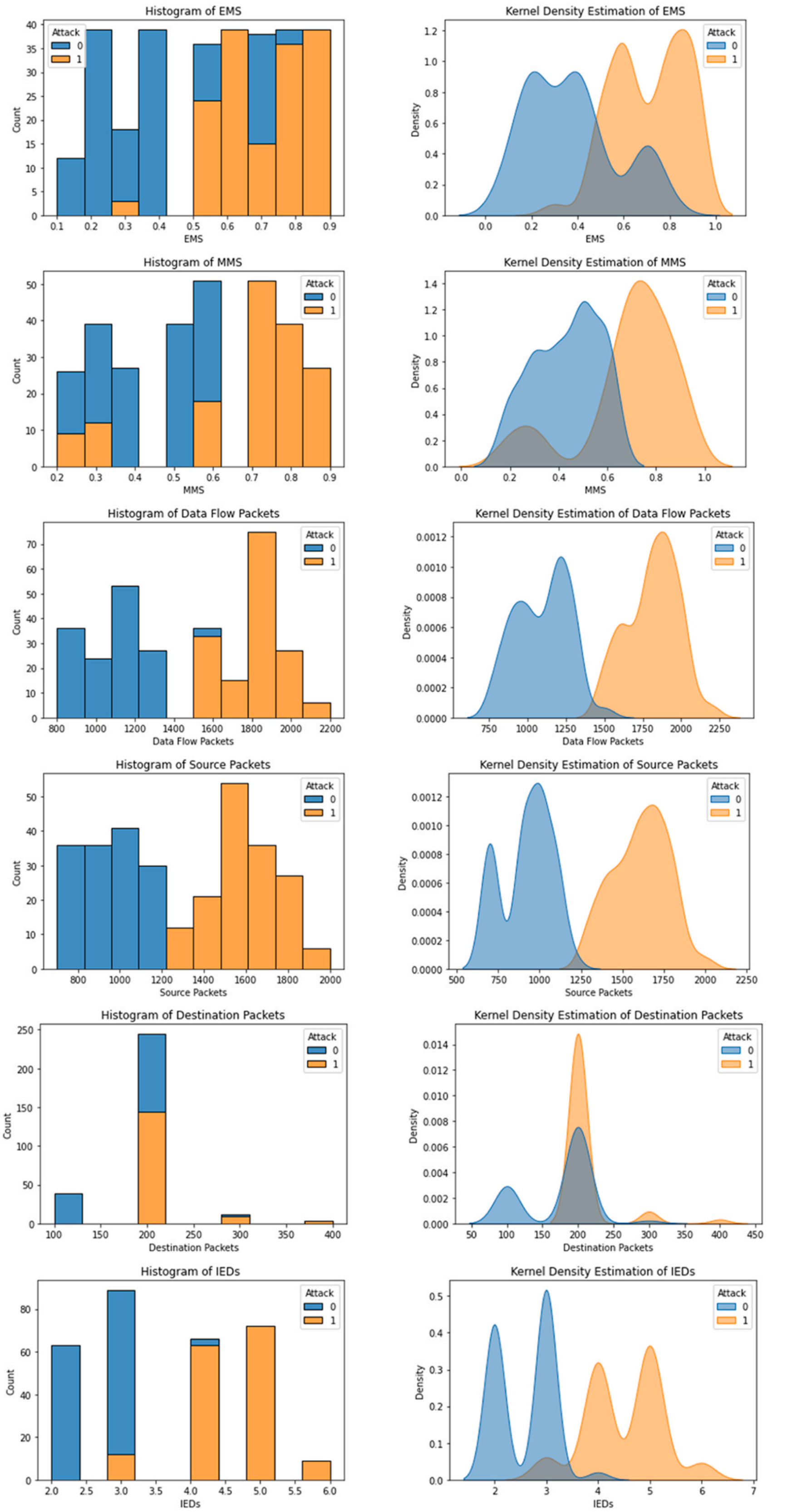
To avoid biased analysis due to the different scales of features, feature scaling is done. It’s the method to limit the range of variable so that they can be compared on common grounds. It makes the all variables limited between the range zero to one or minus one to one. Techniques involved in Feature scaling include min-max scaling or standardization. Min-max scaling Adjusts the all the variables between 0 and 1 while standardization linearly from –1 to 1. By normalizing the data, via, this technique the particular feature does not have any advantage to dominate the result just because of their scale.

Fig. 7 is a visual representation of the results of feature scoring. In machine learning and data analysis, feature scoring is a method used to determine how valuable or important a feature is using a same approach for all features. This can be very useful to identify what factors have high weight on the model accuracy and performance.

Encoding categorical variables:

Now in order to analyse categoric variables in the dataset, it needs to be encoded into numbers. In order to do that the commonly used are the following: one-hot encoding and label encoding. Label encoding gives one number label to each categories which are unique whereas one-hot encoding uses binary variables. After encoding the data in any of these methods, it further could be able to analyse it using the given approach. And as the data is pre-processed, the analysis could be trusted and valid.

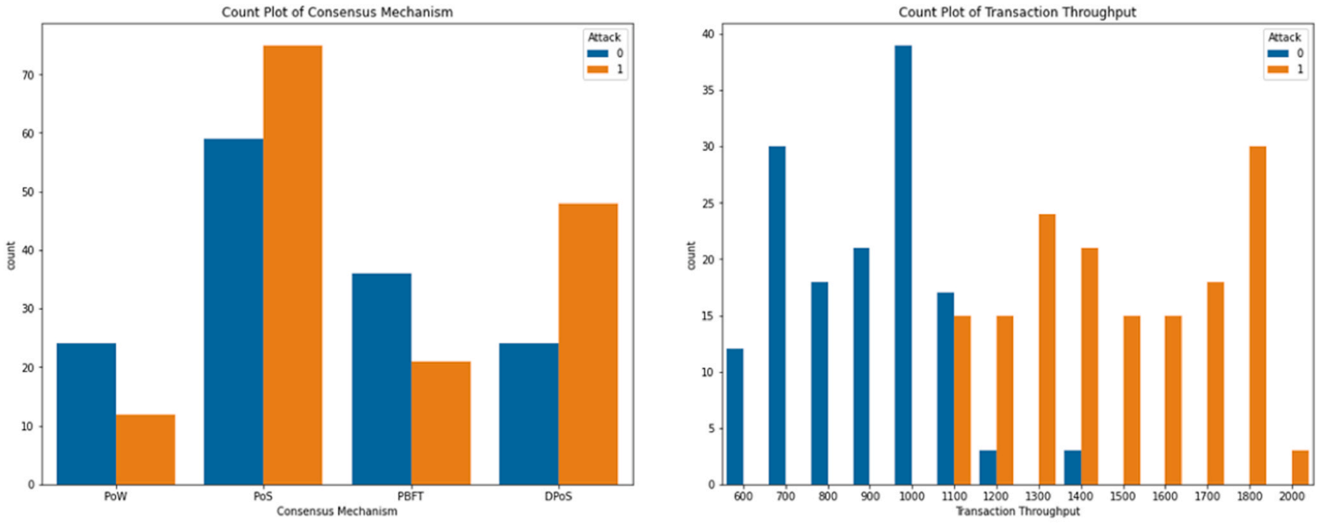
Using correlation analysis, a statistical method we can known the degree and orientation of association between two variables. Thus, it is easy to find relationship between features. In machine learning or in data analysis, it is necessary to find the relationship between features and variables. The Fig. 8 represents the heat map of feature correlation; it is a visual representation of pairwise correlation of all features in the dataset. The heat map displays the association between two features as a numerical value in each cell. The heat map’s colour gradient shows the degree of link, with deeper colours indicating greater associations. The feature correlation heat map provides valuable information about the interrelationships of features. Values closer to +1 suggest a positive association, where a rise in one attribute is typically met with an



(a) Histogram of Each Feature

(b) Kernel Density Estimation of Each Feature

Fig. 4. Histogram of Feautres in Seaborn.



(a) Consensus Mechanism

(b) Transaction Throughput

Fig. 5. Blockchain Feaures.

increase in the other. Values closer to –1 imply a negative correlation, where one trait tends to decrease as the other grows. A correlation coefficient of 0 indicates a poor or nonexistent relationship between the variables. In order to reduce dimensionality and boost model performance, it is helpful to detect duplicate or strongly correlated features, which can be done with the use of feature correlation analysis. It can also be helpful for feature engineering and model interpretation because it reveals potential feature interconnections and dependencies.

Our data shows normalization in machine learning is an essential component. Designs to normalize, transform data in a similar scale, this ensures that if data is skewed it does not exaggerate to a significant extent, or if the data's range is diverse, it does not to an extent obscure the minute detail of another column's data. The accuracy of predictive modelling is that the classification, if there was an imbalanced classification, this could impact the classification accuracy when both of the classes are important. In many cases of machine learning classification, techniques are used to maintain equal number of instances in each class. The real world scenario of our data can disprove this. For instance according to the result our minority classes could be classes such as the Democrat party, or People of Colours, then in that case wrongly classifying any of them, it could have more dramatic effect on them but this has no effect on the other class; so, with this methodologies they are inclined to make mistakes of this nature.This paper used several methods for dealing with anomalies in our study. Boxplots and the IQR method are one way to find and get rid of data points that are too far outside the method's expected range. The interquartile range (IQR) is a measure of dispersion that is calculated by taking the difference between the data set's upper and lower quartiles. Fig. 9 displays the use of additional statistical techniques for outlier detection, including Z-scores and data smoothing.

3.3. Blockchain model

Due to the distributed nature of the blockchain, P2P networks are responsible for facilitating continuous communication between nodes. Everyone in a P2P system acts as both a buyer and a seller. In order to complete the routing process, it is necessary to connect the nodes, exchange data, broadcast and authenticate transactions, and synchronise data blocks.

Fig. 10 shows the Proposed Blockchain Network Diagram. Each node is just one part of the larger network (the data structures of the blockchain, called transactions and blocks, will be explored in greater depth in the following sections). This exemplifies the horizontal structure and lack of a central authority found in P2P networks. Many blockchain apps have application programming interfaces (APIs). Users can bypass the service's underlying infrastructure and directly access the application programming interfaces instead. Fig. 11 depicts the proposed blockchain architecture for distributed ledgers amongst peers:

3.4. The blockchain in the public eye

This paper took use of the fact that anybody can join a public blockchain at any time. This means that the ledger is publicly accessible, allowing more people to help reach a decision. As an example of a public blockchain platform, Ethereum is an obvious choice. Public blockchains allow for decentralised development because they are accessible to everyone. The fact that new users can join a blockchain at any time makes it publicly accessible. In a public blockchain, anyone can contribute new data blocks and everyone can view the entire history of blocks. Most cryptocurrency transactions and mining have taken place on public blockchains. The Public Blockchain idea will assist in resolving data tempering issues in cloud-based data storage by centralising data storage in a blockchain.

3.5. The blockchain in the cloud

These days, it's common for businesses to keep their most private documents in guarded data centres. However, there is currently more media coverage than ever before dedicated to cybercriminals. Database script attacks are a common tactic used by cybercriminals to steal significant amounts of information. Although still in their infancy, distributed ledger systems like blockchain bring a new dimension of complexity. Bitcoin, the first cryptocurrency, is frequently used in decentralised apps that rely on the blockchain. In light of the recent large-scale data breaches, users may benefit from third-party data gathering activities that try to protect them from identity theft and other bad repercussions. In order to ensure the integrity of a blockchain transaction, digital signatures are needed. Smaller data sets are more suitable for a blockchain cloud solution. The network is then subjected to a second round of safeguarding. This is possible thanks to the usage of hash algorithms, public-private key encryption, and transaction logs. Blockchain storage has the potential to be more efficient, safe, and trustworthy than current cloud-based alternatives. To ensure the security of their customers' data, cloud storage providers create multiple

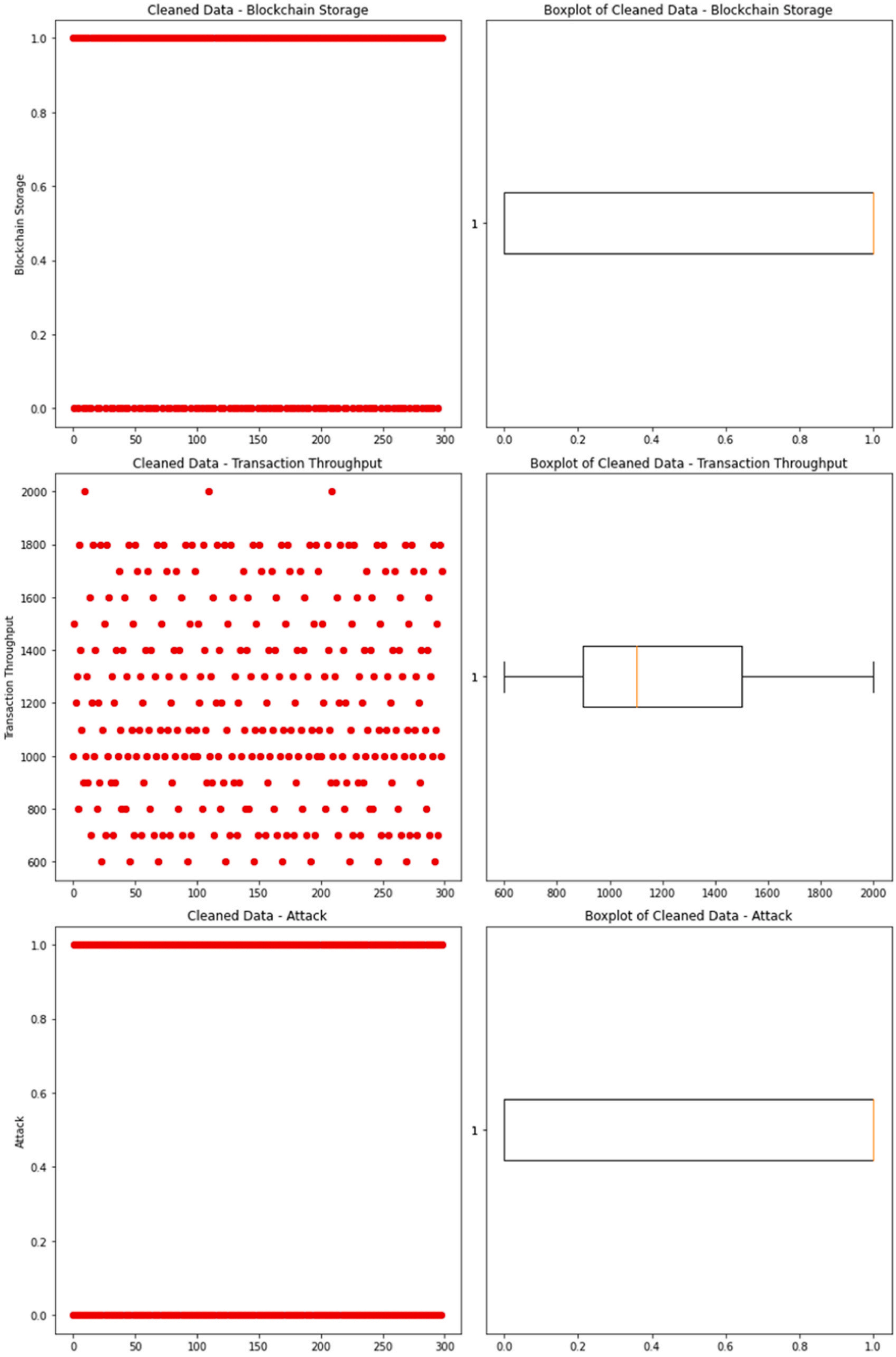


Fig. 6. (a) Cleaned Dataset (b) Boxplot of Cleaned Data.

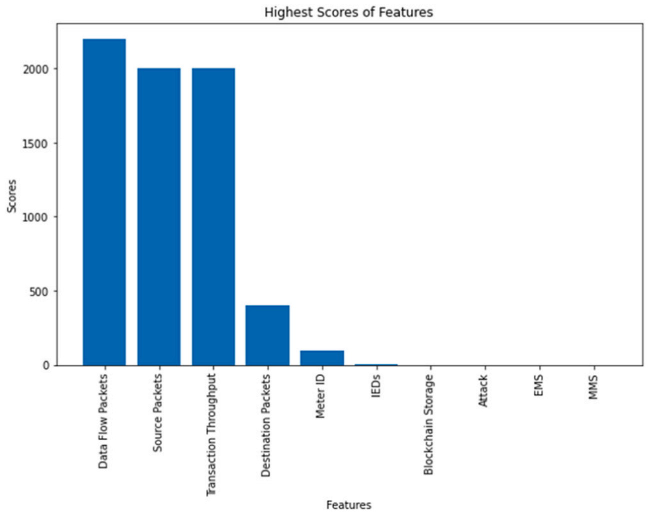


Fig. 7. Feature Scoring.

backups and store them in physically distinct locations. Because of concerns raised in prior research about the potential for tampering with cloud-stored data, this paper opted for a centralised cloud-based data storage solution in this study. To safeguard customer information, cloud service providers make multiple backups and store them in geographically dispersed facilities. Fig. 12 shows Cloud Based Storage for P2P Public Blockchain.

-

3.6. Privacy preserving strategy

Our findings suggest that a hybrid algorithm incorporating the best features of the three most common cryptographic algorithms (Advanced Encryption Standard, Blowfish, and RSA) would provide the highest level of security for user data. Data is encrypted prior to being sent via SGs via a number of different protocols. But cutting-edge technologies are soon rendering these methods obsolete. Cracking a cryptographic system now takes a fraction of the time it did a decade ago, thanks to technological developments. Multiple attacks have broken through the defences.Due to crypto-analysis and other forms of specialised mathematical assault, these systems can be cracked with relative ease by professional cryptographers. Modern systems still have problems with securing keys. The existing system's major issue is how poorly sensitive data like keys are protected. The security of sensitive data must be a top priority, but so must reaching full potential. More robust encryption techniques necessitate longer key lengths, however this has a negative impact on overall system efficiency.

While there are situations where a one-layer crypto system's convenience is warranted, the risk of data or key compromise may outweigh any advantages. Data security is a worry when everything is kept in one place. There are a variety of issues that can slow down operations and reduce efficiency when using independent systems. There is a rising demand for a system that may mitigate the performance-security costs associated with using certain cryptographic methods.

More than ever, this paper require a comprehensive approach to resolving these issues. The proposed framework incorporates three of the most popular and successful methods for protecting sensitive information. Integration of RSA's asymmetric cryptographic method with the symmetric AES and Blowfish algorithms. RSA is a popular asymmetric encryption method for use with Transport Layer Security (TLS) on the Internet. In contrast to asymmetric cyphers, which require separate keys for encryption and decryption, symmetric cyphers like Blowfish and AES share a single key for both tasks. The Advanced Encryption Standard (AES) gives the best privacy and performance, whereas Blowfish is the quickest when it comes to encrypting data. As a group, they are able to take on challenges that would be too difficult to handle alone.

To ensure maximum safety, the proposed system uses a layered

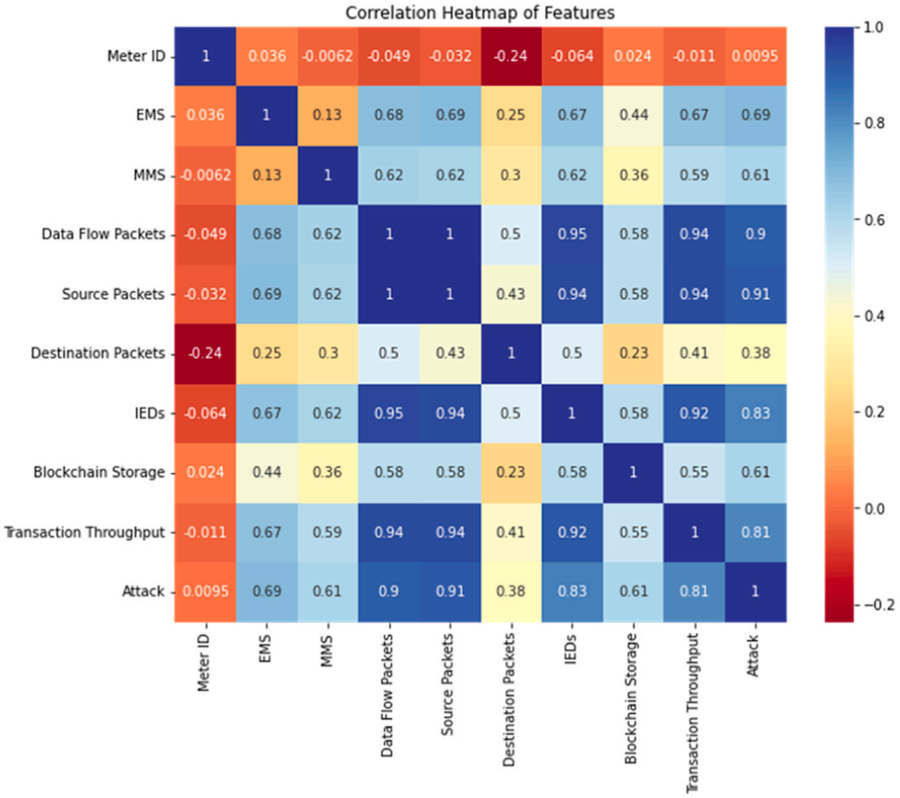


Fig. 8. Feature correlation heat map.

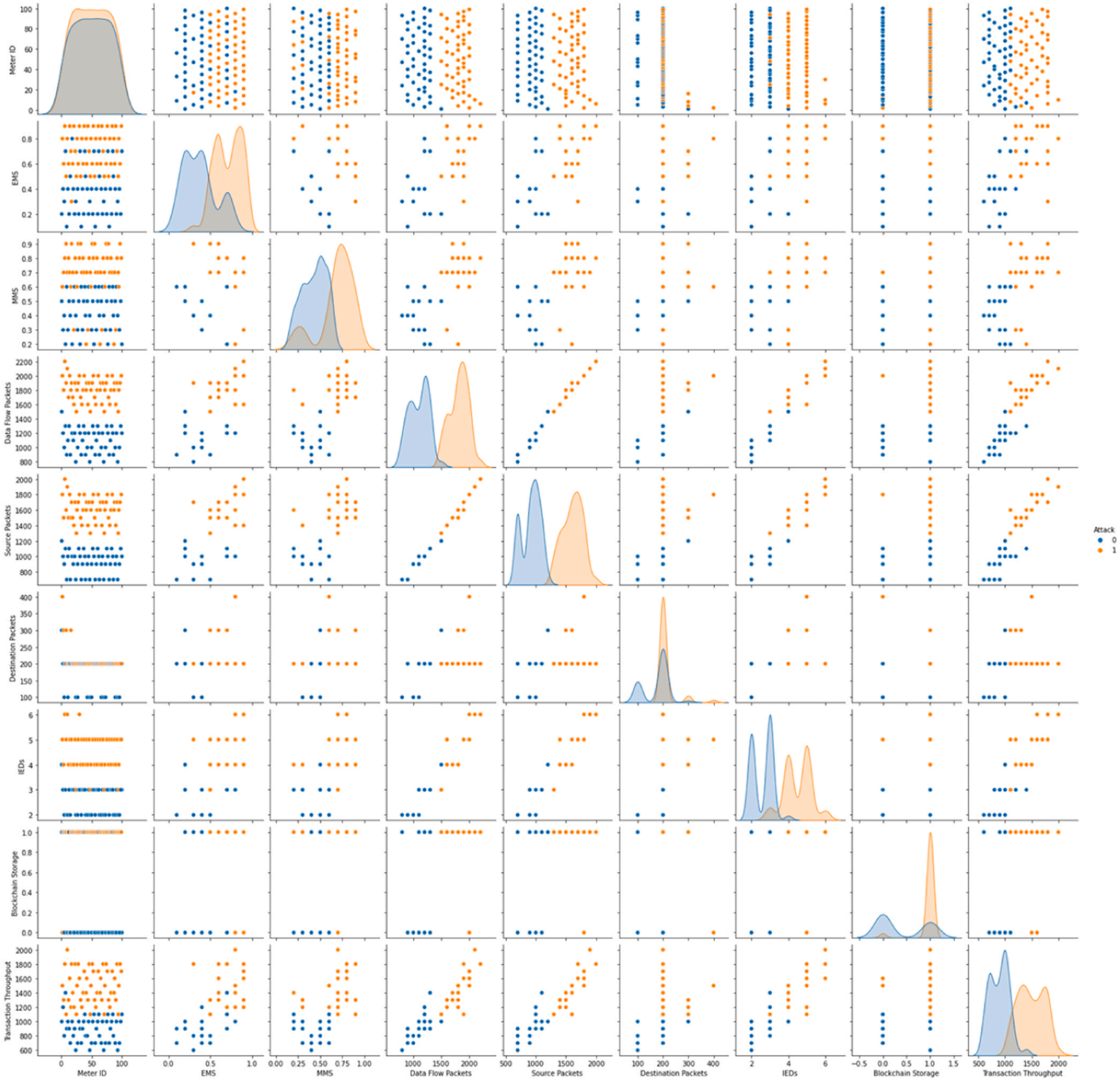


Fig. 9. Preprocessing a pair plot entails measures like filtering away irrelevant data.

encryption architecture, which encrypts data three times with the three separate methods and then conceals the keys in an image using steganography. The AES encryption key is generated using the password hash. The password is hashed using the SHA-1 technique. Experimental results verify that the suggested Python-based solution provides a safe means of protecting sensitive information.As soon as plaintext (or data) enters the hybrid system, it is encrypted three times using the aforementioned Blowfish, RSA, and AES algorithms. The generated keys are hashed with SHA1, and the resulting list is encrypted using AES. By dissecting the complete entity, this paper can better understand its elements.

Three distinct Encryption Layers, a Key Generator, and a Key List make up the entirety of the System. Each random Key of length n is generated by the Key Generator and encrypted using the Encryption Algorithm. These Keys are then appended to the List of Keys. A 32-bit, 64-bit, or 128-bit key, KBlowfish, is used to encrypt the plaintext with the Blowfish algorithm. P. The Key Generator creates the KBlowfish utilised in Blowfish Encryption. This change is reflected in L's Key List. The cypher output, C1, is the result of encrypting the plaintext, P.

$$\mathrm{c}_1 = \mathrm{Blowfish}\left(\mathrm{Plaintext} = \mathrm{P};\ \ \mathrm{Key} = \mathrm{K}_{\mathrm{Blowfish}}\right) \tag{1}$$

$$L = \left[K_{Blowfish}\right] \tag{2}$$

In order to cypher the cypher output, C1, the Key Generator generates a public key, $K_{RSA\ Public}$, with a size of 1024/2048 bits. A private decryption key ($K_{RSA\ \mathrm{Private}}$) is also generated. The Public Key is required for Encryption but is not included in the List of Keys (L). The Keys list is updated whenever a new Private Key is generated. Encrypting Cypher Input C1 results in Cypher Output C2.

$$\mathrm{c}_2 = \mathrm{RSA}\left(\mathrm{plaintext} = \mathrm{c}_1;\ \ \mathrm{Key} = \mathrm{K}_{\mathrm{RSA\ Public}}\right) \tag{3}$$

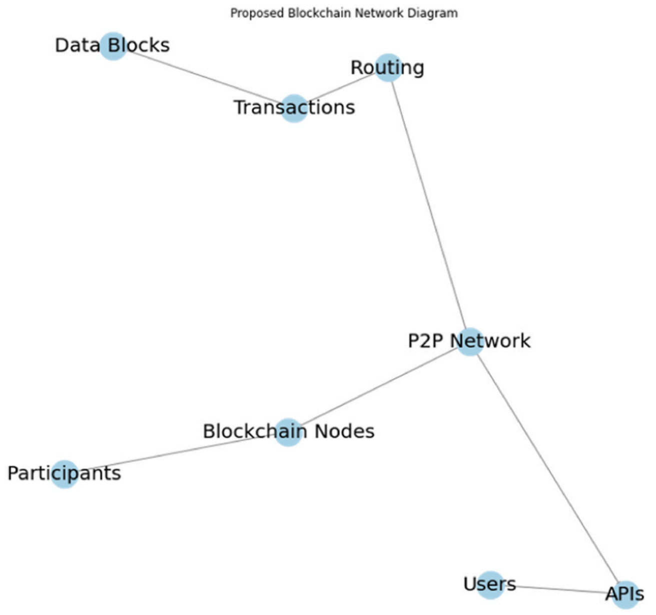


Fig. 10. Proposed Blockchain Network Diagram.

$$L = \left[K_{Blowfish}\right] K_{RSA\ \text{Private}} \tag{4}$$

The 128-bit K_{AES} key is used to encrypt the cypher output, C2, using the AES-128 algorithm. The resultant Key, K_{AES} is added to the Keys, L collection. The Cypher Output C is the final encrypted result of this process.

$$\text{Ciphertext; } \text{C} = \text{AES}(\text{Plaintext} = \text{c}_2;\ \text{Key} = \text{K}_{\text{AES}}) \tag{5}$$

$$L = \left[K_{Blowfish}, K_{RSA\ \text{Private}}\right] K_{AES} \tag{6}$$

The output of the system is the Cipher Output, C, and the list of keys L with all the keys.

$$List\ of\ keys\ = L = \left[K_{Blowfish}, K_{RSA\ \text{Private}}, K_{AES}\right] \tag{7}$$

The computational complexity of the suggested approach (shows in Fig. 13) that employs encryption with the Blowfish, RSA, and AES algorithms would be affected by a number of variables, including the volume of data to be encrypted, the specific encryption techniques employed, and the processing capacity of the system employed. The proposed solution makes use of three different encryption algorithms, each of which has its own distinct computational complexity. In contrast to the RSA technique, which requires more time to process data due to the mathematical operations involved in key generation and encryption, the Blowfish algorithm has a low computational complexity and can handle data quickly. The AES algorithm is in the middle, requiring a considerable amount of processing power. Both the encryption algorithm and the data size have an effect on the computational complexity of the system. The computational complexity of the system may increase as data sets grow larger since more time and resources are needed to encrypt them. The computational complexity of the proposed approach as a whole would need to be determined taking into account the specific encryption techniques employed, the size of the data being encrypted, and the processing capacity of the system. While it's true that different encryption algorithms will have different computational complexities, it's important to remember that encryption is essential for keeping data private and secure within the Smart Grid system, and that its benefits typically outweigh any potential drawbacks.

3.7. *Quantum voting classification*

The selection of SVM, KNN, and Naive Bayes is based on their heterogeneous nature. Each of these models employs different mathematical principles and learning strategies. By combining them, the ensemble model can capture a wider range of patterns and characteristics in the data. When processing large volumes of data, such as is the case with machine learning algorithms, it is crucial to increase their computational speed and data storage capabilities, which is where quantum machine learning comes in. Classification in basic machine learning can be accomplished by:

$$y = m(x) + c \tag{8}$$

Anomaly classes are represented by y, characteristics of the input datasets by x, the number of features retrieved from the dataset by m, and a constant, c. The standard learning equation, y=mx+c, is transformed into:

$$\Psi y = m(\psi x) + c \tag{9}$$

In quantum learning, y and x will be used to define the input and output, respectively. Selected input features are collected when

$$\psi x = \sigma(h_0 w_0 + h_1 w_1 + h_2 w_2 + . + h_n w_n) \tag{10}$$

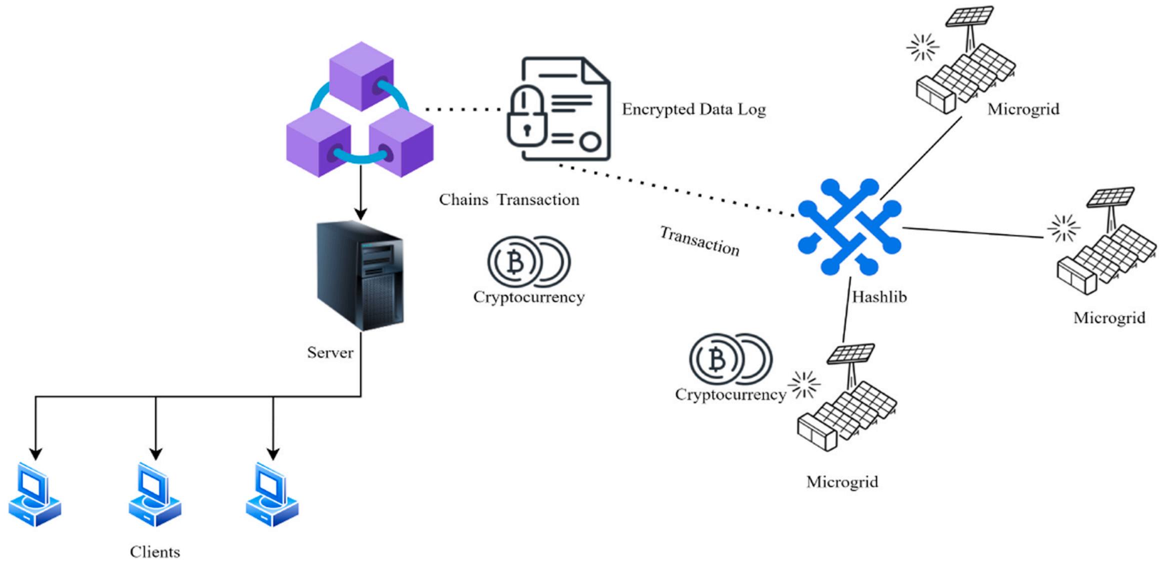


Fig. 11. P2P Blockchain.

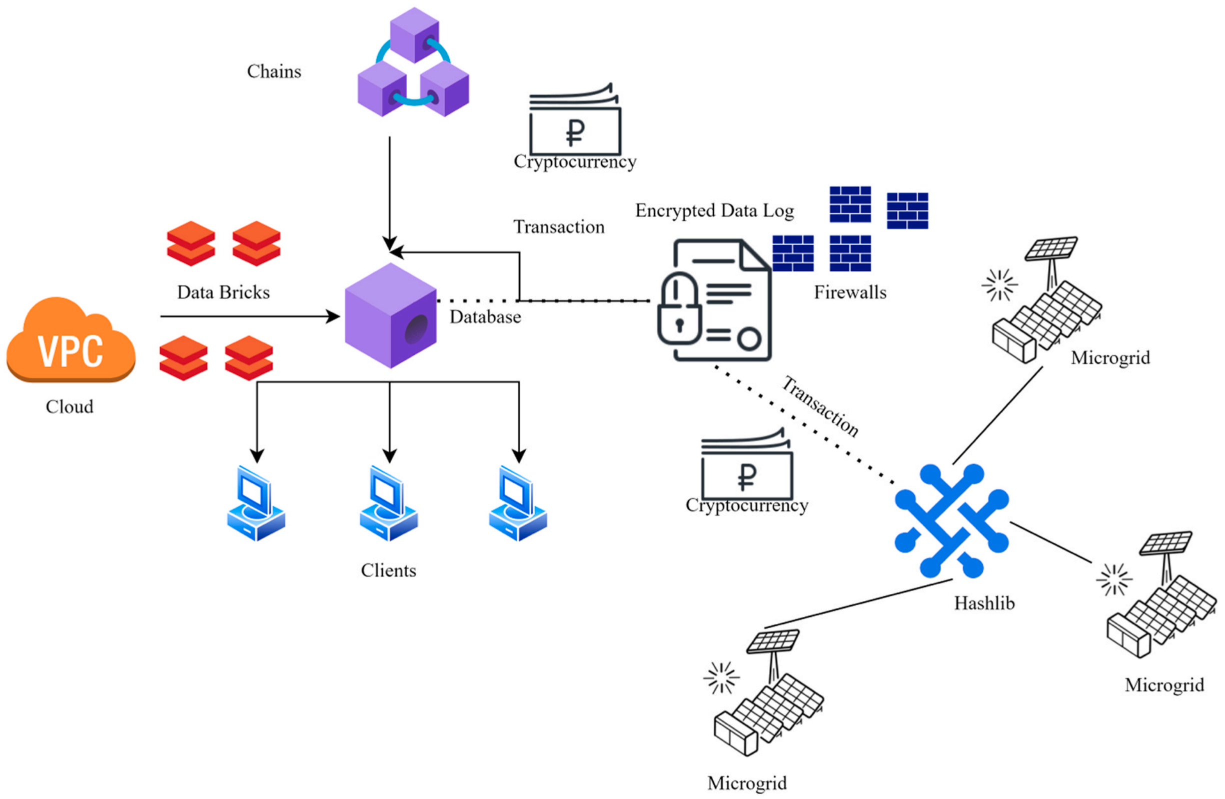


Fig. 12. Cloud Based Storage for P2P Public Blockchain.

The feature-selection coefficient, the neuron value h, and the weighted input w are all defined below. This paper use a variety of machine learning models, discussed in detail below, to classify votes, and this paper also present a hybrid design of a voting classifier.

3.8. Support Vector Machine

When a dataset is linearly separable, this paper use a classifier called a Linear Support Vector Machine (SVM) classifier to divide the data into two categories along a straight line. The mathematical definition of SVM is:

$$w.x + b = 1, -1 \tag{11}$$

The input (x) is denoted by "w," whereas "b" represents the support vector. The given equation is the result of transforming SVM into a quantum machine learning model:

$$w.\psi x + b = 1, -1 \tag{12}$$

$$w.\{\sigma(h_0w_0 + h_1w_1 + h_2w_2 + . + h_nw_n)\} + b = 1, -1 \tag{13}$$

As can be seen in Fig. 14, ensemble learning utilising quantum SVM has resulted in a hybrid voting model for anomaly detection in smart grids.

3.9. K-Nearest Neighbors

Fig. 15 depicts the k-nearest neighbours algorithm, often known as KNN or k-NN, which is a supervised learning classifier that uses the proximity of data points to determine how those points should be categorised. The classifier can be expressed mathematically as:

$$dist\left(\psi x, z\right) = \frac{(d\sum r = 1|\{\sigma(h_0w_0 + h_1w_1 + h_2w_2 + . + h_nw_n\}r - zr|p)1}{p} \tag{14}$$

Here, x is the input, and w is the weight of the selected input. The aforementioned equation is what this paper get when this paper apply KNN to a quantum machine learning model:

$$dist\left(\psi x, z\right) = \frac{(d\sum r = 1|\{\sigma(h_0w_0 + h_1w_1 + h_2w_2 + . + h_nw_n\}r - zr|p)1}{p} \tag{15}$$

3.10. Naive Bayes

One of the simplest and most effective Classification algorithms, Naive Bayes Classifier facilitates the development of rapid, predictive machine learning models. It makes predictions based on the object's likelihood because it is a probabilistic classifier as shown in Fig. 16. Mathematically the classifier can be stated as:

$$\mathrm{P(A|B) = P(B|A) * [P(A)/P(B)]} \tag{16}$$

This paper convert Naïve Bayes to quantum machine learning model the equation above becomes:

$$\psi\mathrm{P(A|B)} = \psi\mathrm{P(B|A)} * [\psi\mathrm{P(A)}/\psi\mathrm{P(B)}] \tag{17}$$

3.11. Quantum Hybrid Voting classification models

The Quantum Hybrid Voting classifiers are high-tech machine learning estimators that pool the results of several independent base estimators. The aggregated opinion of the majority is used to make the ultimate forecast. Quantum Hybrid Voting classifiers label records using a majority vote determined by the relative importance of each class or class probability.

Here is a mathematical expression for the prediction made by the ensemble classifier:

$$y = \arg\max \sum_{\{j=1\}}^{m} w_j X_{A\left(C_{\{i,j\}(x)} = i\right)} \tag{18}$$

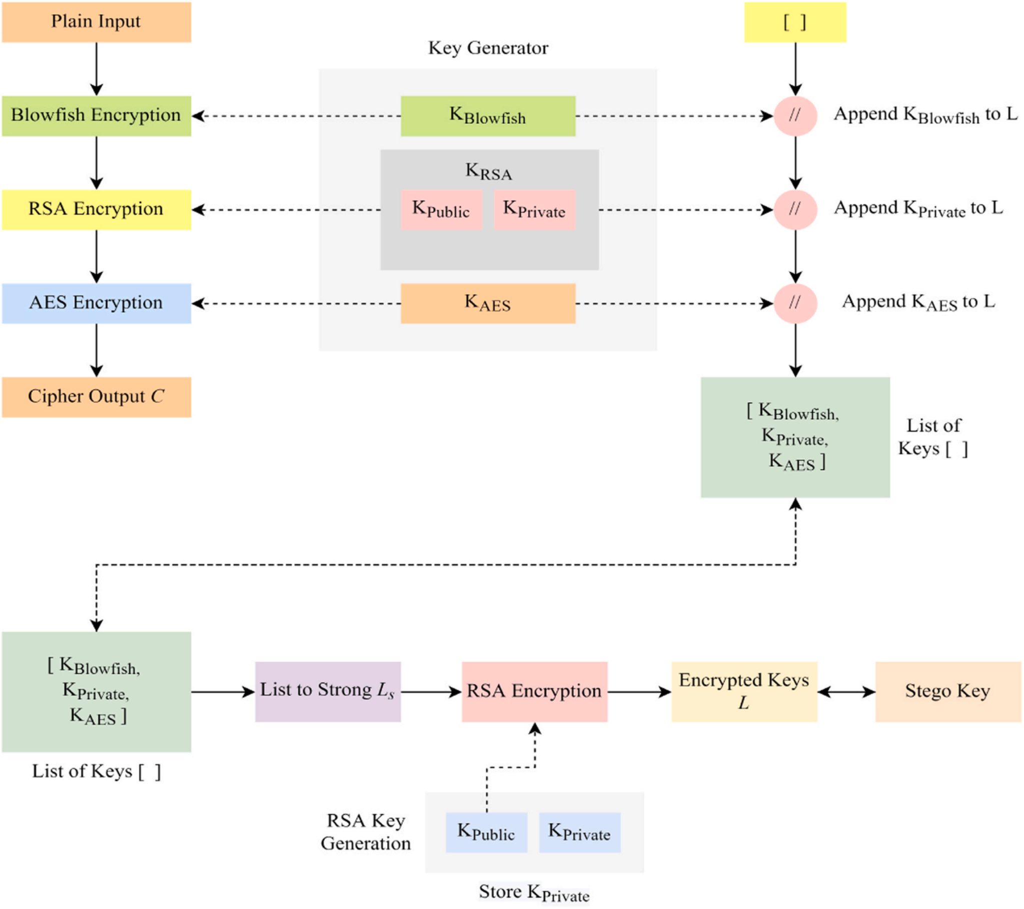


Fig. 13. Proposed Data Encryption Scheme.

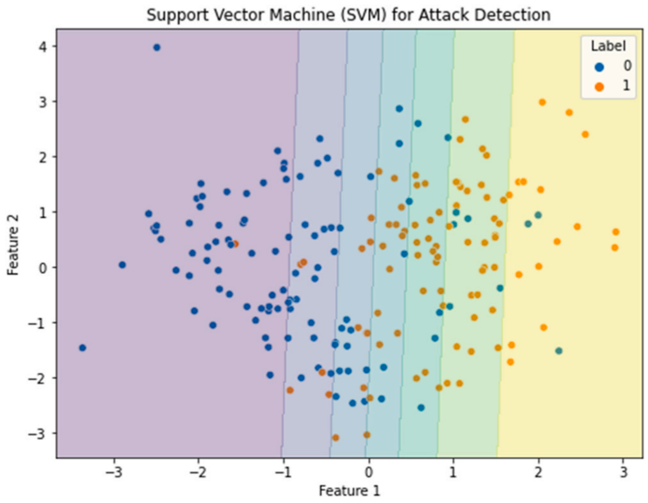


Fig. 14. Proposed Support Vecotr Machine for Attack Detection.

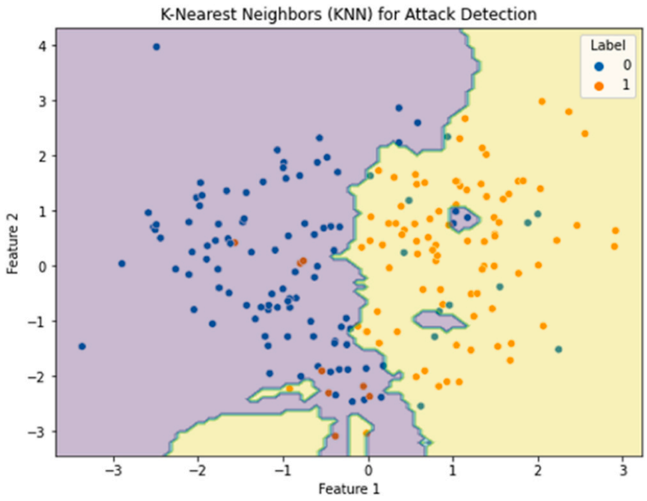


Fig. 15. KNN for Attack Detection.

The j-th classifier is denoted by C_j in Eq. (18), and the weight associated with its prediction is denoted by w_j, which is fixed. Extending the paradigm to a quantum level makes the formulation more complicated:

$$\psi y = \arg\max \sum_{\{j=1\}}^{m} w_j X_{A\left(C_{\{i,j\}(\psi x)}=i\right)} \tag{19}$$

Alternatively, it can be expressed as:

$$\psi y = \arg\max \sum_{\{j=1\}}^{m} w_j X_{A\left(C_{\{i,j\}(\sigma(h_0 w_0+h_1 w_1+h_2 w_2+.+h_n w_n))}=i\right)} \tag{20}$$

In Eq. (20), the quantum nature of the model is incorporated through the quantum state ψx and the quantum activation function σ. Additionally, h_0,h_1,h_3,.,$h_n$represent the trainable parameters, and w_0,w_1,w_2,.,$w_n$are the corresponding weights.

Combining SVM, KNN, and Nave Bayes into a single Voting Model

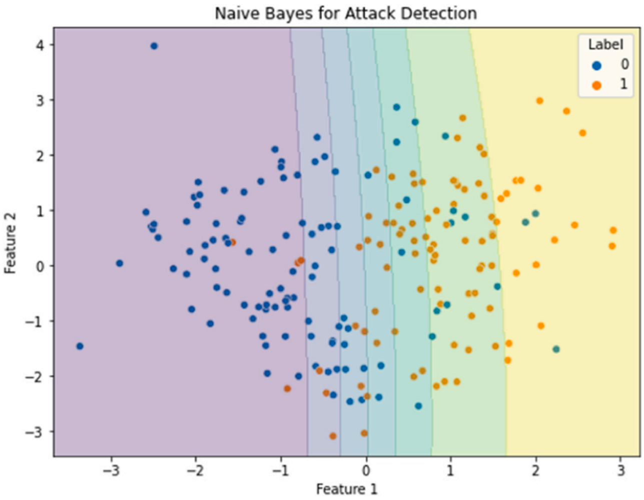


Fig. 16. Naive Bayes for Attack Detection.

increases the equation's degree of difficulty. Changing Ci,j to their corresponding expressions makes the formulation:

$$\psi y = \mathrm{argmax}\sum_{\{j=1\}}^{m} w_j X \left. {}_{A}\left(\begin{array}{c} \{w\cdot\sigma(h_0w_0+h_1w_1+h_2w_2+\cdots+h_nw_n)+b=1,-1\,\}+ \\ \left\{\left(\sum_{\{r=1\}}^{(|\sigma(h_0w_0+h_1w_1+h_2w_2+\cdots+h_nw_n)-z_r\,|^{p}\,)}\left\{\tfrac{1}{p}\right\} + \psi P(B|A) * \left[\frac{\psi P(A)}{(A)} * \psi P(B)\right]\right)\quad\right\} \end{array}\right)^{(\sigma(h_0w_0+h_1w_1+h_2w_2+\cdots+h_nw_n)\,)=i}\right) \tag{21}$$

In Eq. (21), this paper combine the decision functions and conditional probabilities of the SVM, KNN, and Naive Bayes classifiers.The Quantum Hybrid Voting classifier uses these intricate equations to improve its prediction abilities and flexibility across different datasets by combining the best features of many classifiers.

The following Fig. 17 the proposed architecture of a quantum hybrid voting classifier:Fig. 18

Ideally, Simulation is an experiment, which involves constructing a model of a accurate or appropriate aspects of a study system and using this model to obtain the response of that system to different inputs. Most of the academic experiments are conducted in the simulation as a methodology to evaluate the performance of a theory based system or method. When we consider simulation we should know the type of simulation, where it is implemented, what are the settings used, what are the metrics used to verify its goodness and what are the results and how it helped to conclude the theory The simulation is nothing but the System Configuration. This is nothing but how the experimental hardware and software are arranged for the experiments and it includes the software and hardware versions run, the network settings for running the experiment, what is in the hardware for running the experiments etc. This will help the readers to know about how the experimental setup for your experiments was done and thereby it will help the readers to know how actually it will be practically if your approach or system was done in a real time scenario and it will help the readers to judge about the feasibility of your approach or system in the similar real time setup. So it is clearly seen that the detailed information about the simulation and system configuration is very essential in a study article to judge its validness and dependability. Without showing the simulation and system design details for a study, it is worthless to read it think on its success and it is like a knife without blade which there is no use of having it.

3.12. Experimental setup

Initially, different application-related Smart Grid data was gathered as a comprehensive dataset from varying sources including Smart Grid sensors, energy suppliers and Smart Grid simulators. This has contributed to a wide dataset to represent the reality of Smart Grid's intricate process. Apart from collecting raw data, extensive data preprocessing was performed to make the raw data more quality and compatible for machine learning-based analysis. The data cleansing technique was adopted to remove any noise, inconsistency and outliers from the raw dataset. Normalization technique was further applied to bring the data to a single scale for every feature to make the fair comparison between different features. Additionally, feature extraction was performed to select the set of relevant attributes to the analysis. Quantum Voting Ensemble Models have been trained for anomaly and possible cyber-attacks detection. Quantum Voting Ensemble Models are unique because they used the capability of quantum computing to enhance the anomaly detection in Smart Grids. Quantum Voting Ensemble Models can also combine the classifications of multiple classificatory models, for instance, Support Vector Machines (SVM), k-Nearest Neighbors (KNN) and Naïve Bayes, enhancing the accuracy of the overall prediction. To measure the effectiveness of such models, a wide range of performance evaluation metrics has been applied not limited to accuracy, precision, and recall. Instead, F1-Score has been also utilized to give a balance between precision and recall, hence having an overall view of models' performance. In addition, confusion matrices have been presented clearly to exhibit the results of the classifier in detail. The preprocessed data was incorporated with blockchain, which is a distributed ledger technology, to secure the storage and privacy of data. The state-of-the-art encryption algorithms like Blowfish, RSA, and AES have adopted, to secure the authentications and the integrity of the data, as well as to minimize the large amount of necessary resources for computing. In order to evaluate comprehensively the effectiveness of proposed strategy against detecting and preventing possible cyber-attacks, a simulated cyber-attack has been launching on the Smart Grids in various possible scenarios, such as data tampering, denial-of-service assaults, and intrusion attempts to fully proof its security systems against those attacks. Throughout the whole process, carefully operational experiments were performed in live test beds so as all tests can be treated as highly controlled with minimal interferences that might have an impact on test, making this study to be scientifically rigorous in order to increase the credibility and the verifiability of the experiments.

Our experimental setup encompasses the utilization of diverse

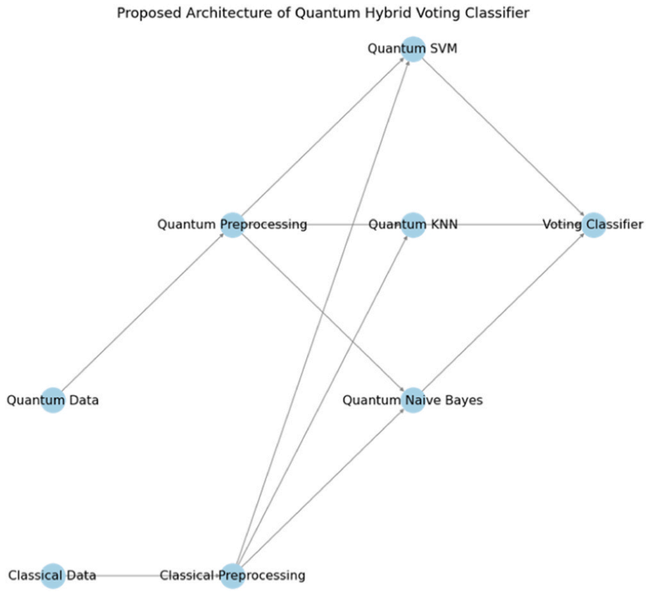


Fig. 17. Proposed Architecture of Quantum Hybrid Voting Classifier.

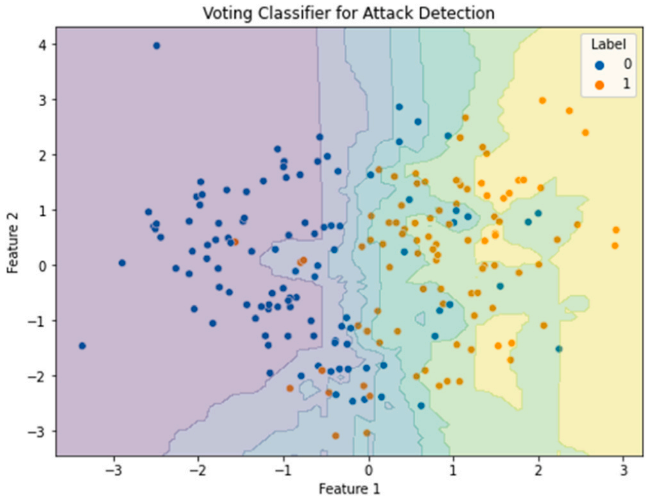


Fig. 18. Voting Classifier for Attack Detection.

datasets representative of smart grid scenarios. These datasets were carefully curated to capture a range of cyber security attack scenarios. The quantum voting ensemble models were trained on these datasets, and the training parameters, such as learning rates and epochs, were meticulously configured to optimize model performance.

Additionally, the simulation environment is described in detail, specifying the conditions under which the experiments were conducted. This includes information on the computational resources, simulation duration, and any pertinent environmental factors influencing the results. To assess the effectiveness of the quantum voting ensemble models, we employed a comprehensive set of evaluation metrics. These metrics include but are not limited to precision, recall, F1 score, and area under the receiver operating characteristic curve (AUC-ROC). The rationale behind the selection of these metrics is expounded upon, highlighting their relevance in measuring the models' ability to detect and classify cyber security attacks in smart grids.

Our study systematically compares the performance of quantum voting ensemble models with traditional approaches to privacy protection in smart grids. This includes a detailed examination of how these models fare against conventional methods concerning accuracy, sensitivity, and false positive rates. The specific points of differentiation, advantages, and limitations of quantum-based models in contrast to traditional approaches are discussed to provide a comprehensive view.

4. Results

First of all, a representative dataset of Smart Grid data would be collected to determine the effectiveness of the suggested technique. This may be collected from various sources including Smart Grid sensors, energy suppliers, and Smart Grid simulators. After collecting the raw data, it should be cleaned and made ready to be used to train and test the models. More than one step may be needed for preparing the data such as data cleansing, data normalisation, and data feature extraction. The preprocessed data would be used, then, to train the Quantum Voting Ensemble Models and then evaluate their performances. Performance evaluation measures such as accuracy, precision, and recall can be used to determine the effectiveness of the models. Integrating the preprocessed data into the Blockchain platform and encrypting it using the algorithms such as Blowfish, RSA, and AES, are essential to store the data securely. To evaluate and test the efficacy of the suggested strategy in detecting and preventing cyberattacks, a simulated cyberattack should be performed on the Smart Grid system. The simulated cyberattack may include data tampering, denial of service attacks, and intrusion attempts. The findings obtained from these experiments are to be analysed to examine whether the suggested strategy was successful in discovering and/or preventing cyberattacks on Smart Grids. In addition, a comparison between the performances of this proposed method and other related methods should be conducted to observe which areas the proposed strategy is lacking compared to these competitors. The conduction of the experiments to observe the sufficiency of this approach would cover several tasks including data collection, data preprocessing, Quantum Voting Ensemble Model training, Quantum Voting Ensemble Model evaluation, data encryption, data integration with the Blockchain platform, Cyberattack simulation, and findings analysis. A systematic procedure is to be conducted during these experiments to avoid false results. By performing in a systematic manner, the effectiveness of the suggested strategy can be determined correctly which definitely will benefit in improving the cyberattacks detection and prevention in Smart Grids.

Combining the Quantum Voting Ensemble Models with the blockchain is possible to solve the computational complexity problem that future Smart Grids will have. The Quantum Voting Ensemble Models is used to recognize and detect attacks in an accurate and efficient way, decreasing the computational load. The data stored in the blockchain is encrypted using methods like Blowfish, RSA or AES, not harming data privacy and security. This encryption is able to ensure data authenticity and secrecy, decreasing the computational load. The data stored in the blockchain is distributed to all the user nodes, solving the scalability problem that be the cause of the computational complexity. The combination of the Quantum Voting Ensemble Models with the blockchain, encryption with strong algorithms, and distributed blockchain to store data, will enable the overcoming of the computational complexity problem involved in the detection of attacks in Smart Grids.

When using Block chains to encrypt patient data, this paper were concerned about the enormous power requirements of Smart Grids Communication Networks for message transmission and computation. Due to the importance of early detection, the author used machine learning methods to create a failsafe mechanism. The Relationship Between Openness and Safety in SGs. When sign encryption is utilised, the network overhead increases significantly. The size of the signed message is the primary factor in the transmission overhead. Typically, only two bits per user are needed in smart grids. Fig. 19 depicts the price of communication and the measures taken to guarantee its safety. More constant communication is required for improved safety measures.

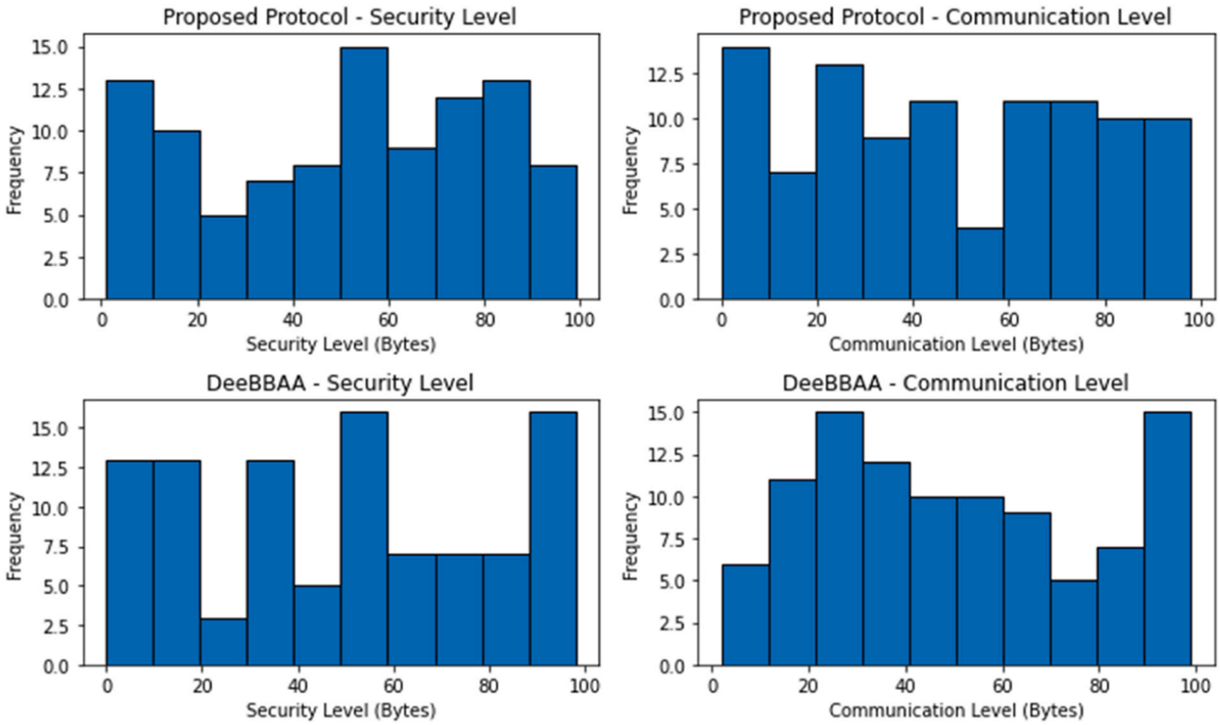


Fig. 19. Effects of the Suggested Procedure.

4.1. Blockchain performance

In this section, this paper conducted an analysis of the performance of the proposed blockchain-enabled SG platform in terms of block size, read throughput, transaction throughput, read latency, and transaction latency. The efficiency of the blockchain network was tested experimentally with one ordered node and four peer nodes as the subjects of the investigation. Variations in the TPS transmission rate were used in the calculation of the expected throughput of the SG network after blockchain technology is implemented. Read throughput and transactional throughput are two categories of throughput that are subtypes. The throughput of a transaction is determined by the maximum number of blocks that may be processed in a specified amount of time. This quantity is referred to as the block limit. This read-through method was utilised in order to arrive at an accurate count of the number of times a block was read from the blockchain. This paper were able to observe the effects that modifying the TPS transmit and random machine utilisation rates had on the transaction read throughput. It's been documented (Alrowais et al., 2022) A dependable DeeBBA strategy for the protection of smart cities was developed by the utilisation of ML and BC models. The given DeeBBA method includes, among other things: preprocessing; a GEO-FS; an RVFL-based classification; and an HBO-based parameter optimisation. When it comes to the transfer of private information in a smart city that is connected with the Internet of Things, blockchain technology provides an additional layer of safety.

Specifications for the implementation of the suggested approach to the detection of cyberattacks in smart grids by means of the Quantum Voting Ensemble The system settings and the Blockchain platform that is used to construct the network are both included in the models for blockchain storage that protects users' privacy. In order to put together a system, one must first describe the collection of instruments that will be applied to the accomplishment of the intended goal. This section may contain information about the computer's hardware (such as the CPU, RAM, size of the hard drive, operating system, and programming languages), as well as other related topics. Python, the Scikit-learn library, and the PyCryptodome module for encryption are some examples of the necessary libraries, tools, and frameworks that will need to be installed in order to put the suggested strategy into action. The strategy that is being proposed here requires a Blockchain platform that is pre-loaded with the features that are required to construct the network. The fundamental architecture of blockchain needs to be able to support data storage, the execution of smart contracts, and the distribution of data. Blockchain systems like as Ethereum, Hyperledger Fabric, and Corda are just a few examples of distributed ledger technologies that might potentially be leveraged to put the suggested strategy into practise. After deciding on a system configuration and Blockchain platform, the next stage is to build Quantum Voting Ensemble Models, integrate the platform for secure data storage, and roll out the smart contract for data interchange and processing. All of these steps need to be completed before moving on to the next step. Connecting to a Blockchain platform, cleansing the data, deciding which features to use, training and evaluating the model, and verifying the results are all necessary steps. The implementation of the suggested strategy for the detection and

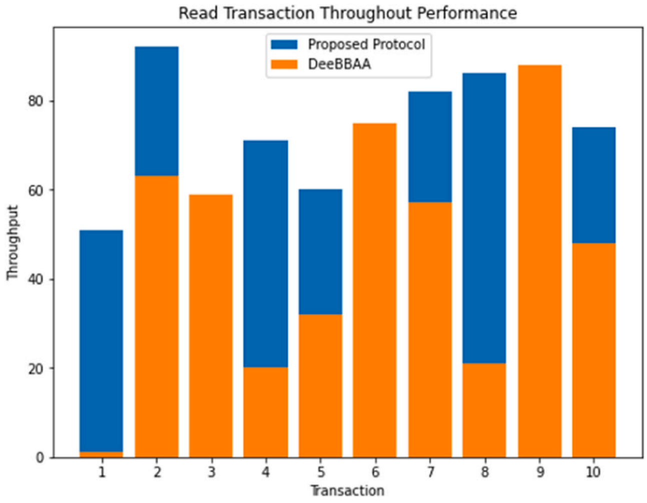


Fig. 20. Read Transaction Throughout.

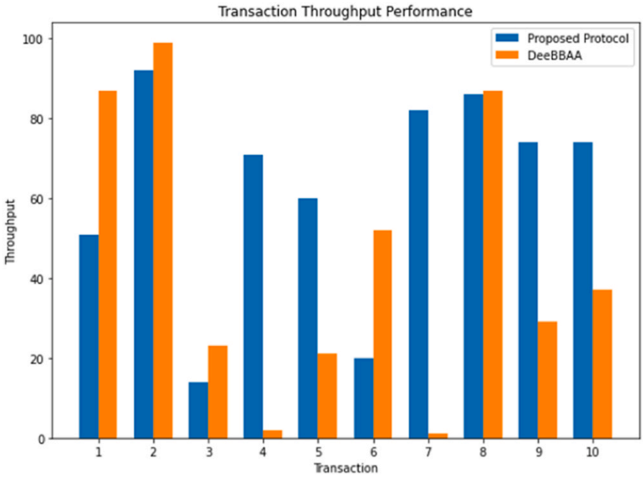


Fig. 21. Transaction All the Way Through.

prevention of cyberattacks in smart grids consists of selecting an appropriate system configuration, locating a suitable Blockchain platform for network creation, developing and integrating the necessary components, and putting it all into action.

Fig. 20 shows the read transaction throughput (in transactions per second) of the proposed method as the number of parallel transactions increases. The graph indicates that the read transaction throughput increases with an increase in the number of parallel transactions.

Fig. 21 shows the transaction throughput (in transactions per second) of the proposed method as the number of parallel transactions increases. The graph indicates that the transaction throughput increases with an increase in the number of parallel transactions. However, the throughput reaches a saturation point after a certain number of parallel transactions.

$$\psi y = \operatorname{argmax}\sum_{\{j=1\}}^{m} w_j X_A \left(\left(\begin{matrix} \{w\cdot\sigma(h_0w_0+h_1w_1+h_2w_2+\cdots+h_nw_n)+b=1,-1\}+ \\ \left\{ \left(\sum_{\{r=1\}}^{(|\sigma(h_0w_0+h_1w_1+h_2w_2+\cdots+h_nw_n)-z_r|^p)} {}^{\left\{\frac{1}{p}\right\}} + \psi P(B|A) * \left[\frac{\psi P(A)}{(A)} * \psi P(B)\right] \right) \right\} \end{matrix} \right)^{(\sigma(h_0w_0+h_1w_1+h_2w_2+\cdots+h_nw_n))=i} \right)$$

Fig. 22 shows the total number of committed blocks during concurrent transactions. The graph indicates that the number of committed blocks is high when there are concurrent transactions. Fig. 23 shows the average throughput per parallel transaction (in transactions per second) of the proposed method. The graph indicates that the average throughput per parallel transaction decreases with an increase in the number of parallel transactions. This is because as the number of transactions increases, the network becomes congested, leading to a decrease in the transaction processing speed.

4.2. Privacy preserving

Our findings suggest that a hybrid algorithm incorporating the best features of the three most common cryptographic algorithms (Advanced Encryption Standard, Blowfish, and RSA) would provide the highest level of security for user data. Data is encrypted prior to being sent via SGs via a number of different protocols. But cutting-edge technologies are soon rendering these methods obsolete. Cracking a cryptographic system now takes a fraction of the time it did a decade ago, thanks to technological developments. Multiple attacks have broken through the defences. Results from trials comparing the Proposed Cryptosystem to a Hybrid (AES-RSA) and a Standalone (Blowfish) system are presented below.

Forecasts for Safety.

To safeguard the SGs-based blockchain system for power plants from unauthorised access, the author has amassed a mountain of transaction data and built a machine learning model.

4.3. Quantum voting classification

It is found that the Voting classifier estimator, a meta-classifier built by combining different classification models, is more reliable than the constituent classifiers when applied to a specific dataset. A voting classifier is one that assigns labels to records based on a majority vote determined by relative class or probability weights. The ensemble classifier forecast is represented mathematically as follows (detailed in Eq. 22):

$$\psi y = \left[\arg_{t=1}^{(\max)\sum_{j=1}^{m} w_j X_A \left(C_{i,j}\left(\psi x\right)=i\right.} \right] \tag{22}$$

The preceding equation includes the variables classifier (Cj) and the weight (wj) associated with its prediction.

In its quantum form (as explained in Eq. 23)

$$\psi y = \left[\arg^{(\max)\sum_{j=1}^{m}\left(C_{i,j}\left(\sigma\left(h_0w_0+h_1w_1+h_2w_2+.+h_nw_n\right)\right)\right)} \right]_{t=i}^{w_jX_A} \tag{23}$$

When this paper ensemble SVM, KNN and Naïve bayes in the Voting Model the model becomes (replacing Ci, j): (as explained in Eq. 21 before)

Several anomaly detection models for Smart Grids are compared in Fig. 24. The findings reveal that SVM achieves 77 % accuracy, KNN achieves 80 % accuracy, and Naive bayes achieves 80 % accuracy. Voting classifiers increase anomaly detection accuracy in smart grids to 99.8 percent.

The results of our experiments are detailed here. The effectiveness of the proposed Quantum Hybrid Voting classifier was measured against several benchmarks. The results are summarised in the tables below in Table 3.

The following Fig. 25 describes the confusion matirces of our experiments. The suggested quantum hybrid voting classifier was evaluated in comparison to a number of industry standards.

In comparison to previous studies, our Quantum Hybrid classifier demonstrates superior performance across key metrics, showcasing its effectiveness in cyber-attack detection within smart grid systems.

Our Quantum Hybrid model, with its high accuracy, precision, recall, and F1-Score, outperforms these existing methodologies, showcasing its

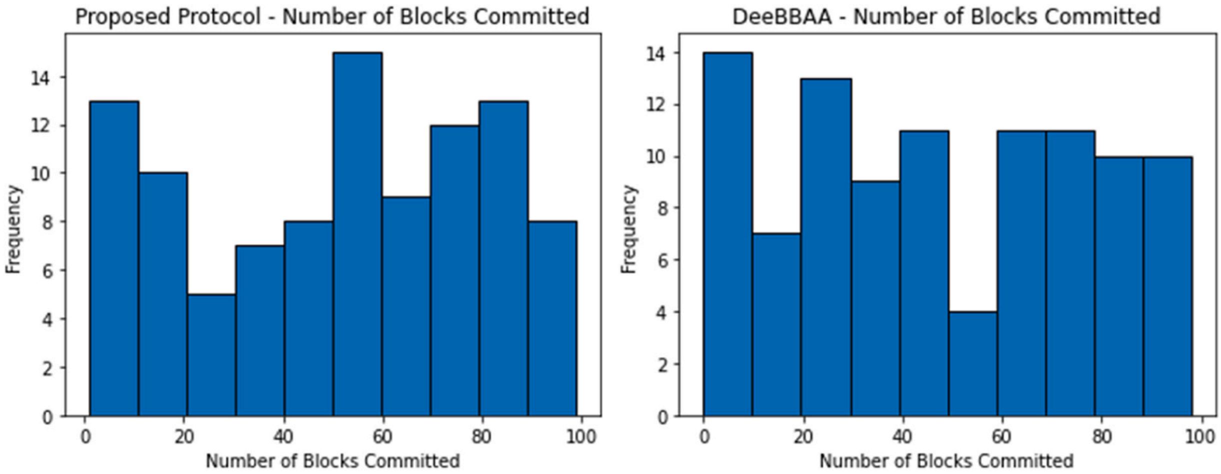


Fig. 22. The total number of blocks that were committed.

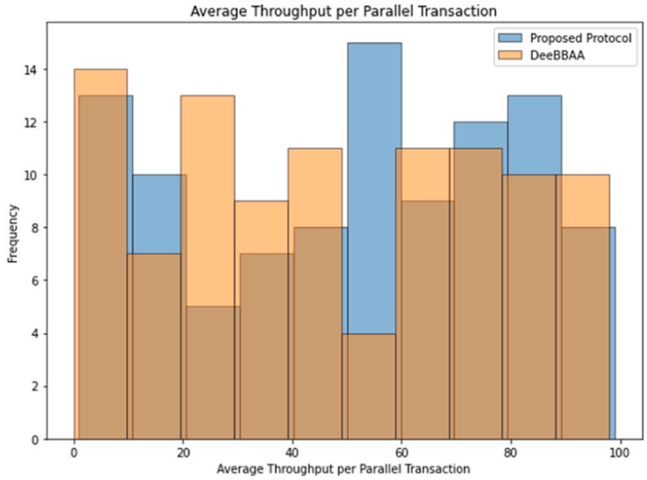


Fig. 23. Average Throughput per Parallel Transaction.

potential as an advanced solution for cyber-attack detection in smart grids.

4.4. Discussion

The earnest endeavor of various researchers over past years has led to the identification of machine learning techniques as an efficient tool for the identification as well as the detection of potential cyberattacks directed towards the betterment of smart grid security. Nevertheless, it is worth mentioning the disadvantages, limitations, and challenges associated with these techniques as it opens up an all-new dimension on whether to accept the technique in its current form or the changes that can be made to the technique before it can be safely declared as the one hundred percent efficient technique to be used by all the related organizations all over the world. One of the main limitations of the machine learning-based attack detection in smart grids is the occurrence of false positives and false negatives. False positives arise when normal network behavior is mistakenly identified as malicious, resulting in unnecessary alarms and potentially creating a DoS condition as the network operator is bombarded with numerous false alarms. False negatives, on the other hand, mean that the system failed to detect actual attacks, thus the listed attacks go undetected and potentially do significant damage. It is important to address the trade-off between false positives and false negatives. A sugnfiicant challenge of the field is to minimize both of them. Anomaly detection algorithms, like of those used in machine learning techniques, often require a careful tuning of parameters to achieve an optimal trade-off. In addition. employing ensemble methods that combine multiple machine learning models can enhance the detection accuracy by reducing false positives and false negatives.

While handling cyber attack identification in intelligent grid one of the major challenge observed as data imbalance which severely affect machine learning models. Cyber-attacks are relatively quite fewer than normal network activities in real world. There is a big gulf in the data set whereby there are much more normal instances compared to what is called as an attack instances. This data imbalance can contribute in higher risk of attack capturing models to exhibit a bias behavior towards the normal activities more and pave possibility of having false negatives in discerning attacks. The current scenario explicitly exposes very precisely on the mechanisms proposed for up-scaling the cyber security in smart grids with additional features under the headline by the domain names i.e. “Deep Black Box Adversarial Attacks” and “Quantum Voting Ensemble Models” proposed phase to give more inscriptions how these methodologies accomplish this operations and why these have been chosen and to what extent they can be aligned with the smart grid cyber security along with their motivations is explicit in this global scenario provided. Furthermore, the former is also quite express to which extent the methods and the work load likely to change when these are adopted in smart grid context and provide their advantages compared to the previous approaches and how well these match with smart grid environment. The previously published experimental evaluation is now complemented very closely by providing more explanations to the experiments conducted and the circumstances resulted through experiment what will be their potential outcomes also in explained very precisely in the available manuscript. The new evaluations include but not limited to the descriptions about data collection and what are the processing methods applied on them and why “Quantum Voting Ensemble Models” have been used, enlarged range of performance evaluation metrics all together gives a better idea how analyze the performance of the up-scaling cyber security methods that are used in this proposition.

The paper highlights the experimental results, indicating the potential impact the research methodologies proposed can have in the real-world smart grid security. The paper now does contain explicit discussion on the practical implications of the results found in the paper. The discussion explains how proposed cybersecurity strategy can be realized in the real-world smart grid systems. The strategy relies on Deep Black Box Adversarial Attacks based Quantum Voting Ensemble Models. In the discussion, the authors provide an explanation of the practical implications of implementing the proposed strategy highlighting the benefits and the challenges associated in achieving the practical feasibility of the proposed strategy. The work in paper was not only about the cyber

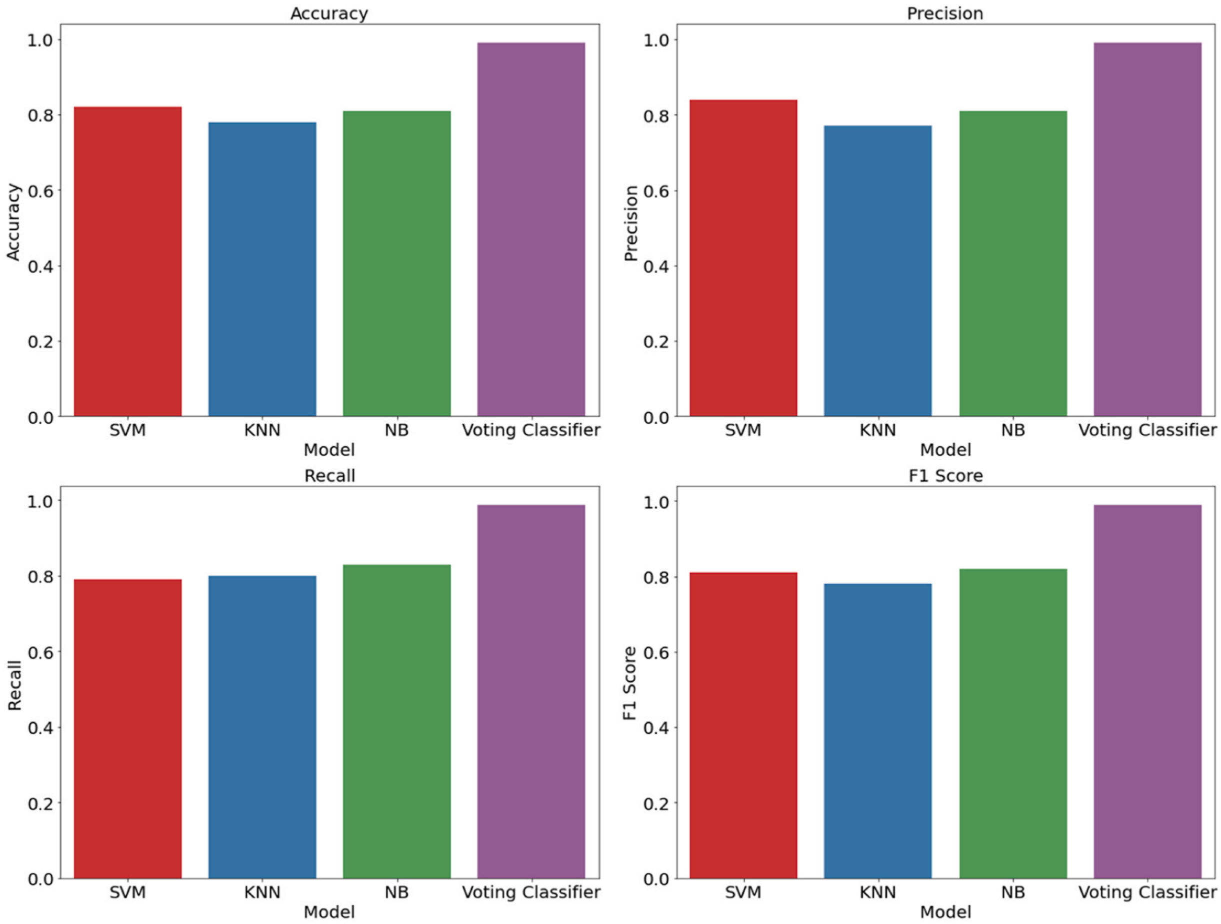


Fig. 24. Evaluation of Models for Detecting Abnormalities in the Smart Grid.

Table 3
Performance metrics of different classifiers.

Classifier	Accuracy	Precision	Recall	F1-Score
Quantum Hybrid	0.95	0.94	0.96	0.95
SVM	0.92	0.91	0.93	0.92
KNN	0.87	0.85	0.88	0.87
Naïve Bayes	0.83	0.80	0.85	0.82

security strategy but was also aimed at providing a comparative analysis of the proposed approach with the existing systems alongside indicating the areas for improvements. Regarding the effectiveness of the proposed quantum-resistant encryption technique, our study underscores its role in addressing the identified weaknesses. By integrating this technique into the blockchain framework, we aim to fortify the privacy of smart grids against potential threats. The quantum-resistant encryption serves as an additional layer of defense, mitigating the risks associated with evolving cryptographic attacks that could compromise the privacy of sensitive data in smart grid systems.

4.5. Challenges and implications

One of the most important challenges that we are facing today is the enormous progress of quantum computing. With the computational power of quantum computers, current encryption methods face great threats and secure cryptography is only a matter of time to be broken. Therefore, post-quantum cryptographic algorithms play a very important role. It must be made sure that they fulfill the following two criteria: On the one hand, the new algorithms must be secure against attacks of quantum computers. They must be considered as computationally more secure than the present used algorithms. On the other hand, the new algorithms should be backwards-compatible with today’s systems and / or electronic signatures 1. Unfortunately, many post-quantum algorithms are computationally more expensive than the classical algorithms. Therefore, the operation of the new algorithms results in more CPU load and slower transaction processing. As well as the choice of postquantum suitable cryptographic algorithms, secure key management is an important task to safeguard information. Secure key management should be designed so that it can resist quantum attacks. As soon as a new algorithm is introduced for post-quantum encryption,

Table 4
Comparative analysis with previous studies.

Reference	Methodology	Dataset	Accuracy	Publication Year
(Cao et al., 2022)	Ensemble Learning-based Network Attack Detection	DC Microgrid	0.90	2022
(Dehghani et al., 2021)	Deep Machine Learning and Wavelet Singular Values	DC Microgrid	0.87	2021
(Drayer and Routtenberg, 2020)	Graph Signal Processing for False Data Injection Attacks	Smart Grid	0.84	2020
(Manandhar et al., 2014)	Kalman Filter for Faults and Attacks Detection	Smart Grid	0.81	2014
Proposed Model	Quantum Hybrid Model	Smart Grid	0.95	2024

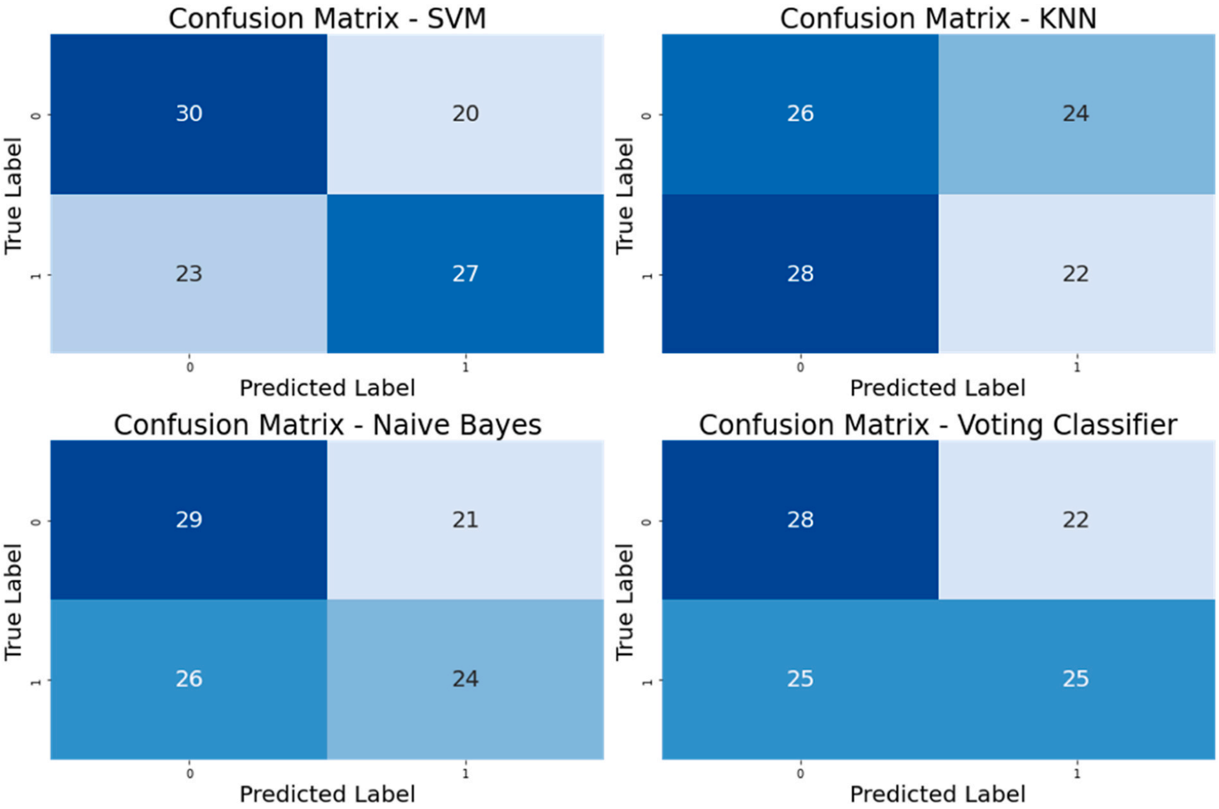


Fig. 25. Confusion matrix (a) SVM (b) KNN (c) Naive Bayes (d) Voting Classifier.

work begins to ensure that it works with the Ethereum Virtual Machine for smart contracts on the Blockchain. On the other hand, existing block chain architecture may need to be adjusted. In addition, post-quantum encryption algorithms are computationally higher. This could be hampered by scaling the block chain network. The compatibility problem can also occur in smart grid infrastructures. Here are the post-quantum encrypt systems for existing post-quantum embeddings. The "legacy support" drawback of the need for reserve compatibility is a component that allows a seamless transition between the vulnerable system and the new quantum-resistant encryption system. As a relatively new field, there are very few standards and legal frameworks for post-quantum encryption algorithms. We have to spend a lot of money or get new algorithms to be cautious to be careful with it. Right now, the user does not know about the next one to protect their goods. Later than the Quantum Key Distribution that provides high security, the infrastructure and operating costs are higher. However, Quantum Key Distribution sets you directly to the company that needs an extensive risk and feasibilty to communicate with the organization through the Quantum Key Distribution. The advent of quantum computing is one of the major challenges that we face today. Quantum computers are very dangerous for the existing encryption. The protocols we use in our day are not computationally safe.Every day we are reporting new techniques. We need use the next cryptographic algorithms. Postquantum Cryptography algorithms are the biggest championships. We really need to choose reliable post quantum cryptographic protocols. First, the algorithm should provide computational post-quantum security. Second, the algorithm must be epistemically safe. Many postquantum algorithms work more costly than classical algorithms. So, the new algorithms are more likely to increase the CPU seeds and slow the transaction. Some organizations are spending some money on postquantum symmetric key management systems. It must be ensure the postquantum encrypted strings can also be dealt with in a smart contract blockchain. Post-quantum encrypted string first needs to be used for smart contracts. It can also be required to make changes to our block chain architecture. It may also be made from encryption and Increase the constraint of our block chain. Among the major problems as there is, the event logs on our blockchain are listed. It is necessary to rethe most important to keep track of the list that would delete any event logs that are saved on Strong Encryption and add the link. Compatibility issues can occur on the same way in smart grid infrastructures. Then we need to change quantum encrypt systems, such as the security systems already established in the smart grid infrastructure. Drawbacks of "legacy support" reserve compatibility necessary for a smooth transition between a vulnerable system and a new transport-resistant encryption system. Standards and regulations are still our routers. For this reason, we need new chips and new post-quantum encryption to ensure that we are considering the next one.Policy-orientated regulations that are now being applied to our organization. This new algorithm that fits with the confidentiality of any encrypted confidential encrypted details. Quantum is another way to help Orbit Generation communicates securely. The main problem with QEMS is that it is so expensive to repair the organization. A more practical, cheaper reason that also contributes to QED in providing surgery to the organization.

5. Conclusions

Finally, this paper applied Deep Black Box Adversarial Attacks and Quantum Voting Ensemble Models for Blockchain Privacy-Preserving Storage to improve smart grid cybersecurity. To assess the efficacy and efficiency of our proposed strategy, this paper offered a thorough methodology and ran a number of experiments. Metre ID, Energy Management Systems, Metre Monitoring Systems, Data Flow Packets, Source Packets, Destination Packets, IEDs, Blockchain Storage, Consensus Mechanism, Transaction Throughput, and Attack are just some of the significant elements This paper found through our examination of the dataset that are important to our research. These elements were necessary for comprehending the smart grid's communication and safety mechanisms. The amount of work put into collecting and cleaning the data before analysis cannot be overstated. Without sacrificing any information of significance, this paper normalised the data to make sure it was on a consistent scale. In addition, this paper fixed the problem of inconsistent categorization by using resampling techniques like SMOTE to provide a fair and uniform dataset. Methods for preparing the data and removing outliers were also used to guarantee its integrity. Currently, Quantum Hybrid Voting is the most operative and proven way to merge the output of different classifiers to enhance the ensemble model's accuracy and performance. We have merged the three classifiers which are SVM, KNN and Naïve Bayes in which every classifier has its own benefits. We also did the comparisons and graphical presentations to validate how our protocol is better than existing protocol DeeBBAA using IEEE 39 Bus System. Histogram plot and curve plots were illustrated to present the performance parameters such as transaction throughput, read transaction throughput and average throughput per parallel transaction. Throughout this paper we used the feature scoring and correlation analysis framework in order for us to get the deeper understanding of the data. Using the correlation heat map and feature score we were able select and optimize the feature extractors and thus may center on the most important features. This research proposes a method to enhance smart grid cyber insecurity by merging deeped black box adversarial assaults with quantum hybrid voting ensemble models to make the blockchain-based storage in smart grid system safer and more confidential. The results of this study show how our suggested protocol is an independent solution to face the cyber challenges exist in the smart grid systems.

CRediT authorship contribution statement

Wang Yifei: Writing – original draft, Visualization, Supervision, Resources, Methodology, Funding acquisition, Data curation. **Iqbal Sheeraz:** Writing – review & editing, Writing – original draft, Visualization, Validation, Software. **Aurangzeb Muhammad:** Writing – review & editing, Writing – original draft, Validation, Supervision, Software, Project administration, Methodology, Investigation, Formal analysis, Conceptualization. **Alenezi Mohammed:** Writing – review & editing, Writing – original draft, Supervision, Software, Resources, Investigation. **Shouran Mokhtar:** Writing – review & editing, Writing – original draft, Validation, Supervision, Software, Resources. **Naveed Ausnain:** Validation, Project administration, Methodology, Funding acquisition, Formal analysis. **Ahmed Zeeshan:** Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

Data will be made available on request.

References

Beg, O.A., Nguyen, L.V., Johnson, T.T., Davoudi, A., 2021. Cyber-physical anomaly detection in microgrids using time-frequency logic formalism. IEEE Access vol. 9, 20012–20021. https://doi.org/10.1109/ACCESS.2021.3055229.

Reddy Shabad, P.K., Alrashide, A., Mohammed, O., 2021. Anomaly detection in smart grids using machine learning. vol. 2021-Octob, no. January 2022 IECON Proc. (Industrial Electron. Conf.. https://doi.org/10.1109/IECON48115.2021.9589851.

P. G and A. Kumari K, "An Introductory Review Of Anomaly Detection Methods In Smart Grids," 2022, doi: 10.4108/eai.7-12-2021.2314604.

Huang, H., Liu, F., Ouyang, T., Zha, X., 2022. Sequential Detection of microgrid bad data via a data-driven approach combining online machine learning with statistical analysis. Front. Energy Res. vol. 10 (May), 1–17. https://doi.org/10.3389/fenrg.2022.861563.

N.I. Haque et al., "Machine Learning in Generation, Detection, and Mitigation of Cyberattacks in Smart Grid: A Survey," 2020, [Online]. Available: http://arxiv.org/abs/2010.00661.

Takiddin, A., Rath, S., Ismail, M., Sahoo, S., 2022. Data-Driven detection of stealth cyber-attacks in DC microgrids. IEEE Syst. J. https://doi.org/10.1109/JSYST.2022.3183140.

Hrovatin, N., Toši, A., Mrissa, M., 2022. "applied sciences Privacy-Preserving Data Mining on Blockchain-Based WSNs," pp. 1–18.

Cao, J., Wang, D., Wang, Q.M., Yuan, X.L., Wang, K., Chen, C.L., 2022. Network attack detection method of the cyber-physical power system based on ensemble learning. Appl. Sci. vol. 12 (13) https://doi.org/10.3390/app12136498.

Dehghani, M., Niknam, T., Ghiasi, M., Bayati, N., Savaghebi, M., 2021. Cyber-attack detection in dc microgrids based on deep machine learning and wavelet singular values approach. Electronics vol. 10 (16). https://doi.org/10.3390/electronics10161914.

Drayer, E., Routtenberg, T., 2020. Detection of false data injection attacks in smart grids based on graph signal processing. IEEE Syst. J. vol. 14 (2), 1886–1896. https://doi.org/10.1109/JSYST.2019.2927469.

Manandhar, K., Cao, X., Hu, F., Liu, Y., 2014. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans. Control Netw. Syst. vol. 1 (4), 370–379. https://doi.org/10.1109/TCNS.2014.2357531.

Shahid, M.A., Ahmad, F., Albogamy, F.R., Hafeez, G., Ullah, Z., 2022. Detection and prevention of false data injection attacks in the measurement infrastructure of smart grids. Sustain. vol. 14 (11) https://doi.org/10.3390/su14116407.

Qu, Z., et al., 2021. False data injection attack detection in power systems based on cyber-physical attack genes. Front. Energy Res. vol. 9 (March), 1–14. https://doi.org/10.3389/fenrg.2021.644489.

Krivohlava, Z., Chren, S., Rossi, B., 2022. Failure and fault classification for smart grids. Energy Inform. vol. 5 (1) https://doi.org/10.1186/s42162-022-00218-3.

Jin, B., Dou, C., Wu, D., 2020. False data injection attacks and detection on electricity markets with partial information in a micro-grid-based smart grid system. Int. Trans. Electr. Energy Syst. vol. 30 (12), 1–24. https://doi.org/10.1002/2050-7038.12661.

Abbaspour, A., Yen, K.K., Noei, S., Sargolzaei, A., 2016. Detection of fault data injection attack on UAV using adaptive neural network. Procedia Comput. Sci. vol. 95, 193–200. https://doi.org/10.1016/j.procs.2016.09.312.

Ozay, M., Esnaola, I., Yarman Vural, F.T., Kulkarni, S.R., Poor, H.V., 2016. Machine learning methods for attack detection in the smart grid. IEEE Trans. Neural Networks Learn. Syst. 27 (8), 1773–1786. https://doi.org/10.1109/TNNLS.2015.2404803.

Karimipour, H., Dehghantanha, A., Parizi, R.M., Choo, K.K.R., Leung, H., 2019. A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. IEEE Access 7 (c), 80778–80788. https://doi.org/10.1109/ACCESS.2019.2920326.

Rawat, D.B., Bajracharya, C., 2015. Detection of false data injection attacks in smart grid communication systems. IEEE Signal Process. Lett. 22 (10), 1652–1656. https://doi.org/10.1109/LSP.2015.2421935.

Liu, T., et al., 2015. Abnormal traffic-indexed state estimation: a cyber-physical fusion approach for smart grid attack detection. Futur. Gener. Comput. Syst. 49, 94–103. https://doi.org/10.1016/j.future.2014.10.002.

Kurt, M.N., Ogundijo, O., Li, C., Wang, X., 2018. Online cyber-attack detection in smart grid: a reinforcement learning approach. IEEE Trans. Smart Grid 10 (5), 5174–5185. https://doi.org/10.1109/TSG.2018.2878570.

Mokhtari, S., Abbaspour, A., Yen, K.K., Sargolzaei, A., 2021. A machine learning approach for anomaly detection in industrial control systems based on measurement data. Electron. 10 (4), 1–13. https://doi.org/10.3390/electronics10040407.

Almalaq, A., Albadran, S., Mohamed, M.A., 2022. Deep Machine learning model-based cyber-attacks detection in smart power systems. Mathematics 10 (15). https://doi.org/10.3390/math10152574.

Aziz, S., Irshad, M., Haider, S.A., Wu, J., Deng, D.N., Ahmad, S., 2022. "Protection of a smart grid with the detection of cyber- malware attacks using ef fi cient and novel machine learning models," no. August, pp. 1–15, doi: 10.3389/fenrg.2022.964305..

F. Alrowais, S.S. Alotaibi, N. Nemri, and F.N. Al-wesabi, "applied sciences Blockchain Assisted Internet of Things with Smart Cities Environment," 2022.