IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 November 2023, accepted 28 January 2024, date of publication 1 February 2024, date of current version 7 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3361039

TOPICAL REVIEW

A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security

NAVEEN TATIPATRI AND S. L. ARUN
School of Electrical Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India
Corresponding author: S. L. Arun (arun.sl@vit.ac.in)

This work was supported by the Office of Dean, Academic Research Velllore Institute of Technology (VIT), Vellore.

ABSTRACT Continuous communication and information technology advancements facilitate the modernization of the conventional energy grid into an integrated platform. Internet-of-Things (IoT) incorporates power systems, particularly smart grid features and the delivery of new services from the utility side to the end user over a two-way communication channel. However, severe security vulnerabilities have been created due to over-dependency on IoT based communication systems. In addition, critical information exchange between any two entities or devices is always an appealing target for cyber-attackers, especially with financial interest motive by damaging integrity, confidentiality and authenticity in a communication channel. Maintaining data security and preserving privacy in between two entities during the transmission or any data distribution are essential. The potential attacks and impacts of those attacks need to be investigated to develop an effective cyber security infrastructure. Thus, considerable researchers focused on detection and mitigation of these vulnerable cyber-attacks using advanced computation tools. This review article thoroughly investigated possible ways to address cyber security challenges such as smart meter security, end-users privacy, electricity theft cyber-attacks using blockchain and cryptography against communication attacks in smart grid. The operational impacts of cyber-attacks on power system security, as well as the economic impact on deregulated energy markets, have been extensively explored. In addition, the robustness of security features and cryptographic methods against various cyber-attacks is investigated to suggest unexplored cyber-attacks for future scope. Specially, the study of real-world cyber security events, case studies, new findings and new scopes in diverse power industries are carried out. More than 135 research articles has been examined for this review article. This paper mainly concentrates on distribution-side cyber-attacks with impact analysis, detection and protection techniques.

INDEX TERMS Cyber attacks, cyber security, cryptography, Internet of Things, power systems, smart grid.

I. INTRODUCTION

In recent accomplishments, integration based on Machine-to-Machine (M2M) communication and widespread application of IoT communication technology played a vital role in smart grid. Incorporating IoT into a smart grid enables seamless interactions throughout all energy sectors such as generation, transmission and distribution, [1]. A traditional grid has a mechanized one-way communication infrastructure with fewer sensors. In contrast, a smart grid has digital two-way communication with more sensors. While adopting a future power system incorporating IoT provides effective billing, improved corrective capabilities during failures and enhanced operational efficiency [2].

Using a two-way communication channel, consumers and service providers communicate via smart meters, sensors, Advanced Metering Infrastructure (AMI), meter data management systems, and utility servers [4]. A smart grid includes an intelligent monitoring system that monitors all electricity flowing through the system which can more

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaosong Hu.

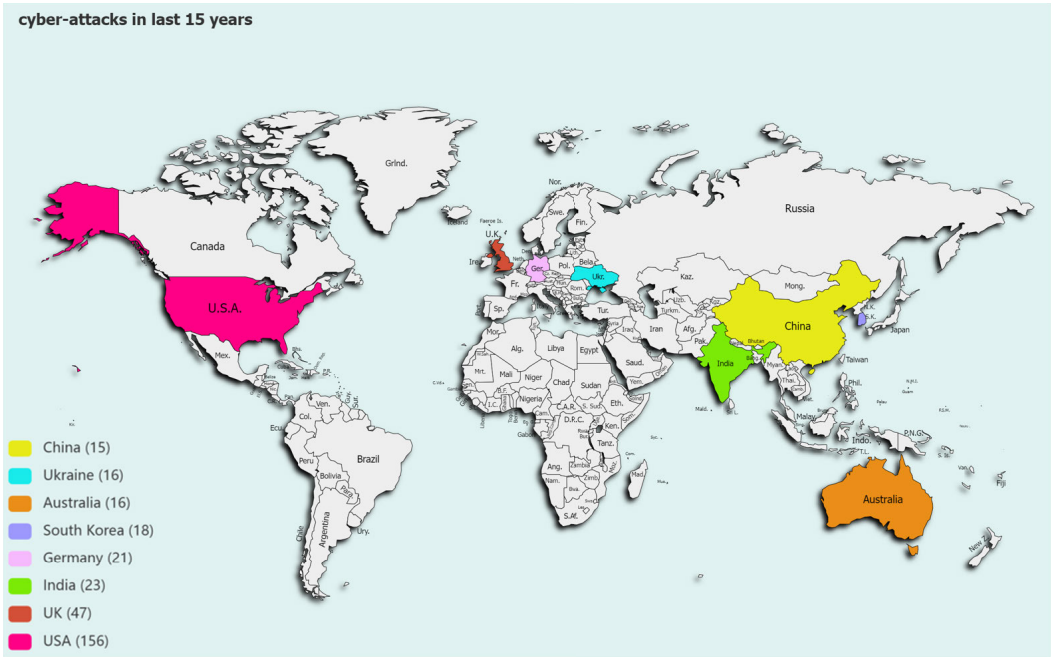

FIGURE 1. Reported cyber-attack incidence in last 15 years around the world [3].

efficiently balance the power flow, detect surges, outages and technical energy losses. In addition, smart grid technology also reduces operational costs, saves energy by using demand side management, demand response and Transactive Energy Management (TEM) technologies.

Through internet-based communications, public solutions on control and monitor the smart grid and high dependency could cause disaster due to vulnerabilities. Further, attackers could find infrastructure desirable [5]. Hence, increased connectivity and digitalisation pose new security challenges. For instance, an attacker can attack electronic devices by corrupting state estimation readings to maintain im-balance in between demand, supply in real time due to device data falsification [6]. Then, the smart grid's sensitivity could make it a cyber-terrorism target [7]. As a result, it is crucial to examine smart grid components and identify past flaws and cyber security problems. It can even cause plant failure and subsequent physical damage. Virtual networks of the power sector are essential, and attacks on them can impact a country's prosperity, public safety, and national defense. According to a survey by United Nations, most of the world's population already lives in cities (55 % in 2018), and by 2050, that figure will be closer to 68% [8]. These people rely heavily on reliable electricity distribution. Brownouts or blackouts can significantly impact safety and security in such urban settings. Since the last few decades, cyber security attacks have been the most serious concern. According to specops sources [3], the USA has witnessed the most cyber-attacks in the recent decade, followed by the United Kingdom, India, Germany, and South Korea as shown in Fig. 1. The simple fact is that most urban electric infrastructures are ageing and pushed to their breaking points. As mentioned earlier, the urban population data highlights the critical need to secure the utility operations. Deploying an Intrusion Detection System (IDS) and firewalls to secure power grid data, account management, non-segregated networks are necessary.

In recent years, cryptographic primitives are becoming essential solution to provide security for critical information transfer in communication channel by using message authentication codes, hash functions for authentication and Authenticated Key Agreement (AKA) schemes to encrypt messages while maintaining privacy and confidentiality in smart meters to the divisional network [9]. Therefore, this review paper aims to analyze the cyber-attack vulnerabilities and suggests research aspects to meet smart grid security requirements and fulfil security objectives by using detection and mitigation techniques such as cryptography, artificial intelligence, and blockchain. Meanwhile, study how security criteria affect data security, privacy, and cyber threats during data transmission. In [10], researchers have discussed deep learning and machine learning with different network operations, algorithms, and datasets to create a functional IDS which provides cyber security to the system. Arezoo Hasankhani et al., identified the following primary areas for blockchain technology applications in smart grids: demand response, EVs, IoT technology, decentralized energy balance, energy marketing [11]. In addition, a realistic aspect of the main advantages and disadvantages of using blockchain technology in smart grids have been discussed. In [12] authors reviewed about different cyber-attacks, strategies, and approaches for providing cyber security in energy systems. In [13], authors discussed cryptographic approaches as well

as key management techniques. In addition, discussed the security and integrity verification tools for communication protocols.

IoT incorporated power systems, particularly smart grid features posing cyber security vulnerabilities due to over dependency on communication systems. Therefore, the ideal approach for protecting smart grids and energy systems from cyber attacks is to provide accurate, up-to-date, and efficient overviews and details regarding identifying and dealing to cyber-attacks. As of now, researchers have put together several review articles in the literature on block chain, machine learning and deep learning based techniques for cyber security in power systems. However, prior work has not been done in power systems on communication attacks such as Denial of Service (DoS), Man-In-The-Middle (MITM), replay attacks, and so on. This review article assesses the feasibility of identifying the primary fields for cryptographic technology applications in smart grid sectors such as energy marketing systems, M2M and substation communications.

A. ABBREVIATIONS AND ACRONYMS

AMI -	Advanced Metering Infrastructure
AKA -	Authenticated Key Agreement
AVISPA -	Automated Validation of Internet Security Protocols and Application
BAN logic -	Burrows-Abadi-Needham logic
CK -	Canetti and Krawczyk
CPS -	Cyber Physical Security
DoS -	Denial of Service
DER -	Distributed Energy Resources
ECC -	Elliptic Curve Cryptography
ECQV -	Elliptic Curve Qu-Vanstone
FDIA -	False Data Injection Attack
GNY -	Gong, Needham and Yahalom logic
GOOSE -	Generic Object-Oriented Substation Event
IoT -	Internet of Things
IDS -	Intrusion Detection System
MITM -	Man-In-The-Middle
M2M -	Machine-To-Machine
NPP -	Nuclear Power Plant
PMU -	Phasor Measurement Unit
PLC -	Programmable Logic Controller
PMAKE -	Privacy-preserving Multi-factor Authenticated Key Establishment
PF-DA -	Pairing Free-Data Aggregation
PUF -	Physical Unclonable Function
PIDMS -	Proactive Intrusion Detection and Mitigation System
RES -	Renewable Energy Sources
ROM -	Random Oracle Model
SCADA -	Supervisory Control And Data Acquisition
SVM -	Support Vector Machine
TEM -	Transactive Energy Management
TES -	Transactive Energy System
TESP -	Transactive Energy Simulation Platform

II. TAXONOMY OF CYBER ATTACKS IN POWER SYSTEMS

Taxonomy is the structured classification of things or concepts. Our proposed taxonomies aim to classify various types of vulnerabilities or cyber attacks across the generation, transmission, and distribution sectors. The damages incurred through cyber attacks and the vulnerabilities of attacks on power grids will vary based on the field and strategies employed by the attackers. The majority of cyber-attack exploitation is directly or inversely associated with grid instability. While cyber attacks on the generation sector have primarily relied on False Data Injection Attacks (FDIA) [20], the transmission sector has become a victim of physical access-based attack vectors such as time delay attacks [21], load redistribution attacks, time synchronisation attacks [22], load altering attacks [23], false command injection attacks,and cyber-physical attacks [24]. Most cyber attack vulnerabilities in the distribution sector are network access-based, including MITM attacks [25], DoS attacks [26], Replay attacks [27],and malware attacks. In addition, taxonomy of cyber attacks to power grid with impacts on power systems is presented in fig. 2.

III. RESEARCH MOTIVATION AND CONTRIBUTIONS

The motivation for this survey arises from the quote, ''wherever IoTs are present, cyber-attack vulnerabilities are also present''. IoT applications include intelligent information transfer, monitoring of pollution, green infrastructure, smart homes, and connected healthcare. Smart grid is the major IoT application, which provides the structure sensing, communication and processing methods necessary for a smart energy systems. The rapid improvements in IoT technology give the new potential for the seamless operation of the smart grid systems. On the other hand, IoTs are becoming cyber-attack vulnerabilities like critical information leakage, and infrastructure damage.

Furthermore, IoT vulnerabilities may leads to grid blackouts like Ukraine's electricity grid attacks in 2015 and 2016 where attackers try to open circuit breakers to stop the electricity supply by using malicious bad firmware injection. In addition to that attackers implemented DoS attack on telecommunication system to block the communication in between consumers and grid. This study describes a public network-based smart grid defensive mechanism, opened possibilities of cyber attacks on smart grids and assists potential researchers and participants in this field in understanding the structure of an IoT-enabled smart grid system, as well as security breaches, prevention, and detection of those security breaches in smart energy systems. The significant contributions of the article are as follows:

1) A thorough examination of random cyber risks across various power sectors such as generation, transmission, distribution, and consumption have been conducted.
2) Detection techniques for various cyber-attacks such as impersonation, replay, privileged insider, man-in-the-middle, denial of service, ephemeral secret leakage,

TABLE 1. Comparison of proposed work with Existing Literature.

Ref.no	Year	A	B	C	D	E	F	G	H	I	J	K	L
[14]	2023	✔	✘	✔	✘	✘	✘	✘	✘	✘	✘	✘	✘
[15]	2023	✔	✘	✔	✔	✘	✘	✘	✘	✘	✘	✘	✘
[13]	2023	✔	✘	✔	✔	✘	✘	✔	✔	✘	✘	✘	✘
[16]	2023	✔	✔	✔	✔	✘	✘	✔	✘	✘	✘	✔	✘
[17]	2023	✔	✔	✔	✘	✔	✘	✘	✘	✘	✘	✔	✘
[18]	2023	✔	✘	✔	✘	✔	✔	✔	✘	✘	✘	✘	✔
[19]	2023	✔	✘	✔	✘	✘	✘	✔	✘	✘	✘	✔	✘
Proposed Work	-	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

✔ - Assessment existing literature provided ;
✘ - Assessment existing literature didn't provided
A - Cyber-attacks in Power Grid ; **B** - Energy Marketing System ; **C** - AI based Detection and Protection scheme; **D** - Smart Meters Security ; **E** - Case study ; **F** - Real-world Cyber-attacks ; **G** - Cryptography Algorithms in Power Grid ; **H** - Verification Tool ; **I** - Cyber-attack Robustness Assessment ; **J** - Security features Assessment ; **K** - Block chain ; **L** - Cyber-attack impact Assessment

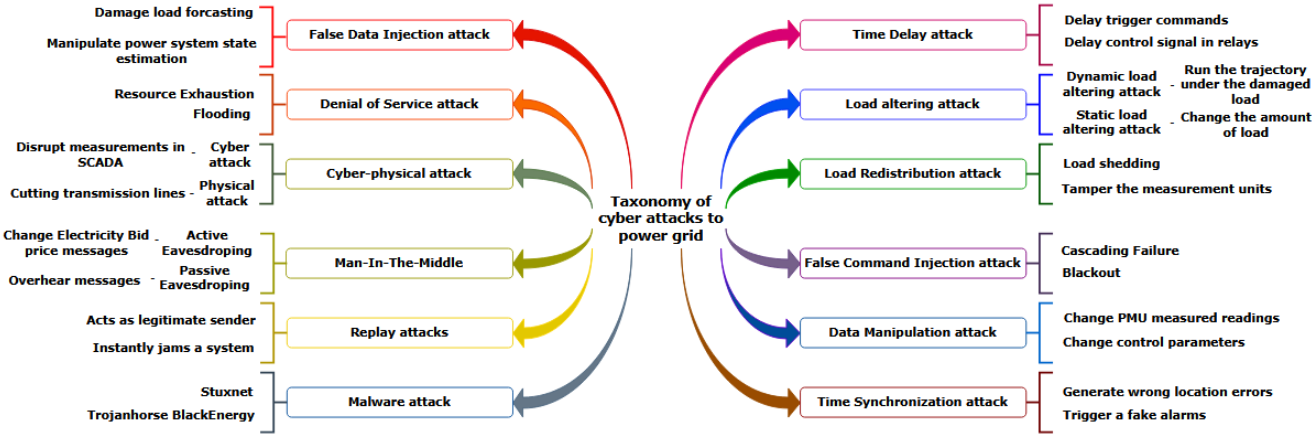

FIGURE 2. Possible Cyber attacks Impact on Power systems.

resending, masquerade and device stolen have been investigated. Furthermore, cyber security strategies against these threats have been examined.

3) The significance of different cryptographic algorithms in data privacy and protection while sharing data between two entities has been analyzed.
4) The study of real-world cyber security events and case studies in diverse power industries are carried out. Further, research gaps in smart grid cyber security are identified and highlighted.

The organization of this paper is as follows: section IV provides a review of cyber-attacks in power generation systems. Section V addresses a review of cyber-attacks in power transmission systems. Section VI presents a review of cyber-attacks in power distribution systems consists impact analysis, detection and security using various advanced methods. Section VII provides case studies and addresses real-world cyber-attack incidences on power systems. Finally, section VIII concludes, highlighting the findings, future directions and suggesting possible future research perspectives.

IV. REVIEW ON CYBER-ATTACKS IN POWER GENERATION SYSTEM

Electricity generation mainly depends upon Nuclear Power Plant's (NPP), hydroelectric, and thermal power plants. Based on the present literature survey, power sectors are changing their approaches to sustainable energy by increasing the integration of renewables even though they have meteorological origins of variability in energy generation [28]. In addition, Renewable Energy Sources (RES) locations are decentralized, which may require fewer employees to report updates in person, which can become a time-consuming process for grid operators and leads to the installation of remote operation tools and IoT devices in power generation systems. In [29], researchers have reviewed wind farm threats, security, unauthorized wind turbine control, disruption and mitigation techniques used to improve confidentiality in the system. In addition, the researchers highlighted future work focused on understanding and combating persistent threats which will increasingly target wind farm assets. The authors of [30] provided a comprehensive review of Cyber Physical Security (CPS), particularly FDIA, in power generation

systems based on the national institute of standards and technology security framework. In [31], the authors have discussed the CPS of photo-voltaic systems and vulnerabilities under various cyber-attacks, such as replay attacks, FDIA, and infrastructure tampering attacks. Furthermore, challenges and opportunities in creating cyber-secure power electronics systems for the next generation have been addressed to assist readers with future research paths. In [32], using real network data and energy generation measurements collected by a wind turbine at Lancaster University, the researchers investigated the amount of malicious scans carried out by Mirai-infected bots in order to penetrate the wind turbine. Furthermore, ping to death with big ICMP packets was investigated.

A. CYBER-ATTACKS DETECTION IN POWER GENERATION SYSTEM

Cyber-attacks, such as FDIA and MITM, are becoming significant threats in power systems, intending to modify the power system condition, which may lead to improper control actions. Fayha almutairy et al., have developed deep learning models such as Wavelet and Temporal convolutional network to detect FDIA in power systems with high RES penetration. In addition, the performance of the developed models has been evaluated on IEEE 14 bus system with an detection rate of more than 99% and 118-bus system with an detection rate of 97% [33]. In [34], researchers have developed a hybrid deep convolution–recurrent neural network to detect electricity theft in renewable energy-based distributed generation-units with detection rate of 99.3% and low false alarm rate of 0.22%. In [35], the authors have implemented a novel distribution algorithm for detecting cyber-attacks such as adversary manipulation of wind farms turbine-specific control logic parameters. In addition, the implemented algorithm has been tested at the Horns Rev wind farm in Denmark. The presented work shows that the implemented algorithm can also provide cyber security for wind farms. In [36], Huang et al. have developed an online platform to detect cyber-attacks in automated generation control using dynamic watermarking techniques without hardware upgrades on generation units. In addition, the developed technique can also be used for large-scale power systems.

B. CYBER-SECURITY IN POWER GENERATION SYSTEM

Cyber security is an essential countermeasure to mitigate cyber-attacks and protect critical infrastructure in power generation systems. In [37], researchers have presented a protection approach using a digital frequency relay to protect equipment from large power fluctuations for longer duration in wind energy systems. In [38], authors have implemented an operating reliability evaluation mechanism for multi-state power systems to achieve dynamic system reliability by considering cyber malfunctions. In [39], researchers have implemented a comprehensive algorithm with the help of the proportional fairness index to coordinate defence countermeasures of microgrids during any cyber-attack. Furthermore, it analyzed cyber defence based on coalitional game theory.

In [40], Lee and Huh have presented the system information and event management analysis method to prevent the leakage of peak information and hackings through insecure web services in NPPs. In [41], researchers have developed a framework using knowledge-based hidden makrove modelling to analyze the integrative cyber-attack reaction in NPPs. In addition, researchers have developed a security state estimation method utilizing online updated hidden Markov models to analyze the functional impact. Poong Hyun Seong et al., have designed a cyber-attack reaction planning approach based on Markov decision process model and the Monte-Carlo tree search algorithm to develop optimal reaction plans that improve response margin time and conserve time essential to secure NPPs safety [42].

FDIAs are becoming a primary threat to the generation system, causing disruptions in control logic parameters and state estimation readings to damage the electricity generation quantity, power market by maintaining imbalance in power generation. It is necessary for power plants to provide security for equipment and critical information with improved marginal time and a low false alarm rate against FDIA.

V. REVIEW ON CYBER-ATTACKS IN POWER TRANSMISSION SYSTEM

Because of its size and the need for high system availability, the energy sector has adapted to digital technology, leading to cyber-attack or cyber-physical attack vulnerabilities to the transmission system. Attackers can use various attack vectors, such as malicious activities, malware injections, and viruses, to compromise the networks, measurements and also changes power flow of the transmission system which can cause a blackout or significant disruption in the power grid [43]. In addition, several sensors have been deployed to analyse the real-time operation of a power system by monitoring bus injection powers, bus voltages, and line currents. The control center assesses the stability of the grid based on redundant measures transmitted through the Supervisory Control And Data Acquisition (SCADA) system. Transferring measured data can also lead to cyber-attacks vulnerabilities. Power systems security threats have been classified into three types:

1) Physical attacks on networks can be considered as terrorist attacks, which may cause disrupting substation operations, cutting transmission lines, or generator units to fail.
2) Cyber-attacks that disrupt measurements or data transmission in SCADA systems.
3) Cyber-physical or coordinated attacks, such as the tripping of transmission lines are the consequence of FDIA's capabilities [24].

In [44], Hossein Rahimpour et al., presented a potential cyber attack vulnerabilities and their risks pertaining to power transformers in power networks. In [45], researchers have considered timing attacks, replay attacks and FDIA to analyze the impact of cyber-attacks on High Voltage Direct Current transmission-based oscillation damping control. In addition, the implementation of cyber-attack preventive measures for Alternative Current-High Voltage Direct Current systems, which have strong, robust control schemes and accurate detection algorithms considered for future scope. Habib Rajabi Mashhadi et al., have proposed an analytical method to analyse the influence of renewable energy power plants on transmission network congestion [46]. In [24], researchers have developed mixed integer linear program model to implement load transmission attacks via FDIAs, which may cause many transmission lines to overflow. The developed model established a standard to analyze realistic cyber-attacks that may disrupt transmissions and cause a blackout. In addition, developing a detection strategy for cyber-attacks aimed at transmission line congestions in Direct Current state estimation is considered for future studies. In [47], Yury Dvorkin et al., have implemented a bi-level optimization model to analyze the impact of distributed cyber-attacks on the distribution and transmission electrical grid. In addition, future research is projected into how attackers can use publicly available grid sources to create more harmful attack strategies.

A. CYBER-ATTACKS DETECTION IN POWER TRANSMISSION SYSTEM

Mohsen ghafouri et al., have implemented a new detection scheme based on thevenin equivalent system parameters, which performs fast and accurate detection of possible cyber-physical attacks on the voltage stability monitoring of transmission system [48]. In addition, the implemented scheme has been utilized to calculate an indicator that detects Phasor Measurement Unit (PMU) data attacks. In [49], Wilson et al. proposed a deep-learning based stacked autoencoder framework for developing machine-learning features against transmission SCADA attacks. Also, presented unsupervised learning framework to detect automatic and adaptive attacks in the transmission SCADA system. Furthermore, the framework can also be improved so that it not only detects but also locates the event on each line planned. In [50], researchers have presented a cyber-physical data analysis using a deep-autoencoder to monitor transmission protection systems. A ridge regression-based classifier has been deployed to identify cyber anomalies. In addition, the outcomes of the presented models can be investigated as the underlying cause of reported incidents with the aid of cyber log data from protection equipment.

Transformer taps have mostly been used in transmission networks to manage bus voltages. Therefore, tap change commands carried across the SCADA network are always appealing targets for attackers to disrupt system operation. To address the issue, the authors have developed an algorithm that detects the presence of a concealed misleading tap change command in the on-load tap changer [51]. In [22], the authors have proposed a detection technique for cyber-attacks against line current differential relay by using a learning-based framework which employs a multi-layer perceptron model to detect FDIAs, and time synchronization attacks and to divide them from faults. In [52], Pal et al. proposed a mechanism for detecting PMU data manipulation attacks by using that mechanism which continuously monitors the equivalent impedance of transmission lines and divides observed anomalies to detect the presence and location of attacks.

B. CYBER-SECURITY IN POWER TRANSMISSION SYSTEM

Security systems are one of the most crucial components for transmission system. With ongoing automation, they are becoming more digital and more efficient at delivering electricity which exposing them to cyber-attack vulnerabilities and generating many challenges. In [53], researchers have proposed an algorithm to detect the additional placement of PMUs for maximum security against FDIAs. The algorithm has been evaluated for a range of IEEE-30, 57 and 118 bus-based electric transmission network models. Future research analyze the impact of cyber-attacks on PMU placement strategies in realistic transmission networks. In [21], Lou et al. designed a time delay attack, which delays the delivery of system control commands and a recurrent neural network is used to predict delay values from input traces. The results demonstrated that long short-term memory-based deep learning approach could work well in power plant control systems based on data traces from three sensor measurements such as pressure, temperature, and power generation. In [54], Dehghani et al. launched an FDIA on the information exchange between independent system operator and under-operating agents in the power transmission system to evaluate system security levels. Blockchain has developed to increase the data confidentiality between independent system operator and under-operating agents.

The transmission system is more vulnerable to time delay and PMU data manipulation attacks. Due to a time delay attack, a delay in trigger commands can cause critical infrastructure damage or cascade failure, and PMU data manipulation may lead to load shedding or power overflow in a transmission system. Late detection of FDIA can cause power transmission lines tripping, change in power flow, and large-scale cascade failure [55], some defences against power transmission line attacks include maintaining PMU placement strategies, implementing fast key agreement protocols for secure communication and using blockchain to maintain confidentiality while sending commands.

VI. REVIEW ON CYBER-ATTACKS IN POWER DISTRIBUTION SYSTEM

Distribution networks are more susceptible to cyberattacks due to their vast size and decentralized nature. In addition,

IoT applications become integral part in distribution system components such as electricity marketing, substations, smart meters as shown in the Fig. 2. As a result, they are exposed to major cyber-security risks, such as attacks, vulnerabilities, and consequences. Due to their control and communication requirements, even Distributed Energy Resources (DER) and battery storage installation may pose negative impact on the grid. In [5], the authors have reviewed the threats and potential cyber-security vulnerabilities, attack countermeasures, and security requirements in IoT-based smart grids. The below mentioned literature evaluated impact analysis of cyber attacks in smart distribution system.

In [56], Ma explained the cyber security challenges in smart cities, such as critical information leakage and intentional cyber-attacks by considering four essential components in smart cities such as smart grid, the smart homes, the smart transmission system, and the smart healthcare system. Furthermore, future research focus on cyber security challenges, threats to user privacy, and relevant authorities and policymakers. Researchers utilized the observer-based method and the decomposition form of the system matrices to analyze the impact of DoS attacks on state estimation in [26]. In addition, the detection and estimation of distributed attacks have been considered for future study. Researchers have implemented a game theory model for power plants, transmission lines, and distribution networks to analyze cyber-attacks and defence probability [57]. In addition, it allows decentralized defence strategies to make defenders separate decision-makers planned for future studies.

In [58], researchers have analyzed the security and privacy of emerging peer-to-peer electricity trading markets. Further, designing privacy-preserving protocols for the defined scenarios using the specified requirements as a guideline is proposed for future studies. In [59], Marufu et al. proposed a strategy for determining how successful cheating attacks on power marketing schemes can be executed in resource-constrained smart microgrids. In addition, mitigation techniques are implemented to prevent cheating attacks. The authors have presented a systematic detection of possible cyber-attacks and examined the influence of attacks on power market operation in association with TEM–based power systems [60]. Furthermore, intend to examine and analyze the impact of additional attacks, such as DoS and replay attacks, on the microgrid's peer-to-peer markets, as well as deploy detection schemes in the microgrid considered for future work. In [61], researchers have presented an ensemble decision tree approach based on the bagging technique to find possible anomalies in the electricity market and physical measurements within the Transactive Energy System (TES), which can reduce the impact of outliers. In addition, the presented approach may be tested on advanced use scenarios to depict a few realistic TES behaviors. In [62], Zhang et al. implemented a deep-stacked autoencoder algorithm to identify possible anomalies in the electricity market and physical measurements with an accuracy rate of 96.9%. The proposed algorithm analyzed the main cause and provide appropriate control actions to protect utilities and prosumers from cyber intrusion. In [63], Wang et al. detected possible anomalies in TES by considering zero-mean FDIA and analyzed cyber-attacks impact on price, quantity and market clearing price. In [64], researchers build a electrical trading protocol in the java programming language to maintain privacy preserve in between prosumers and utility by using blockchain and Elliptic Curve Cryptography (ECC). Pal et al. analyzed the influence of data integrity attacks on electricity pricing exchange in between distribution system operator and price-responsive loads in TES [65]. The system performance is evaluated using four metrics such as operational, financial, comfort, and reliability metrics under data integrity attack by using a 240-bus western electric co-ordinating council transmission model with modeling of the distribution system at specific buses. In [66], researchers have analyzed the impact of manipulated malicious bid prices and quantity cyber-attacks in TEM. Moreover, the TEM operation has been studied through proxy attacks simulated on the TE30 test system. In [67], the authors have created a comprehensive simulation-based transactive energy valuation method to systematically assess the system value, process, object, and design. In addition, a co-simulation-based Transactive Energy Simulation Platform (TESP) has been developed based on the valuation method to perform marketing operations. The work remarks that can deploy agents and market mechanisms without reprogramming any simulators.

A. CYBER-ATTACKS THROUGH DEVICES

AMI is a catch-all word for whole infrastructure, from smart meters to control center equipments which establish communication between two-entities or devices. The purposes of AMI can include remote meter reading for error-free data, identifying network problems, load profiling, and energy audits by sending energy usage data in near real-time. Unfortunately, sophisticated cyber-attacks on AMI are an open and apparent vulnerability. Attackers typically target less secure system elements such as AMIs to manipulate energy and consumption reports based on financial motives. When the system is heavily loaded, the failure of a single critical component can cause a chain reaction of component failures, eventually leading to blackout. To safeguard the necessary infrastructure from cyber-attacks several researchers analyzed attack detection and protection techniques.

1) DETECTION OF DEVICES THROUGH CYBER-ATTACKS

Energy theft has become one of the most concerning attacks in electricity distribution system. In [68], researchers utilized support vector regression and impact difference to detect possible anomaly pricing cyber-attacks that influence the guidelines of smart meter electricity rates in smart home systems. Bhattacharjee and Das implemented a two-tier approach to detect the FDIA in data consumption without increasing the false alarms in smart meters by using

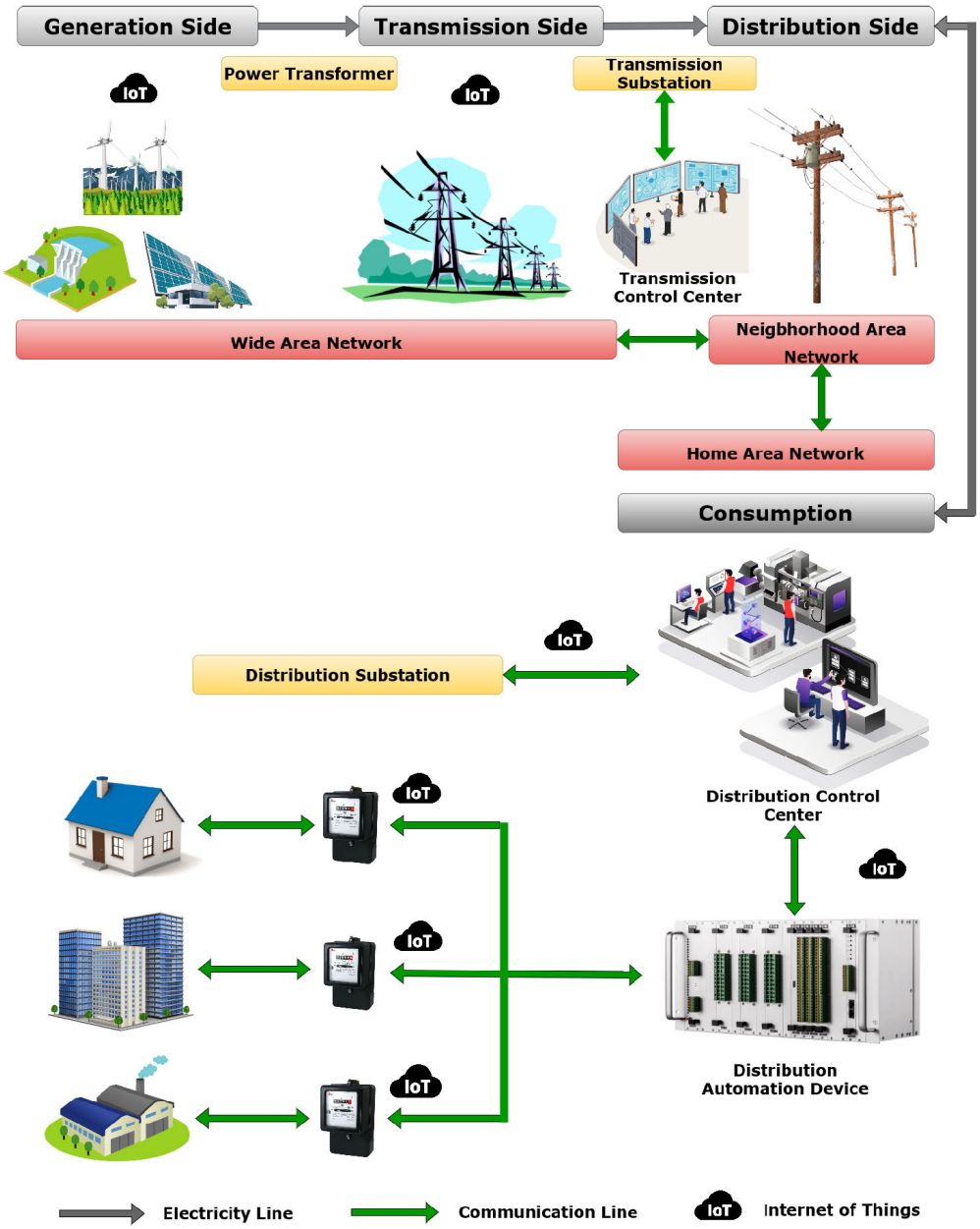

FIGURE 3. Advanced Communication Infrastructure for Power network.

harmonic - arithmetic mean ratio as tier-1 and residential under the curve as tier-2 [20]. The work highlights that the analysis on ON-OFF and data omission attacks with minor modifications to the tier-2 detection level approach can also be considered for future studies. In [69], researchers have developed an isolation forest-based detection method to detect FDIA without a pre-training procedure for detection labels in a power system with an fast detection accuracy rate 96.3% at time 1.944 sec. In [70], the authors have developed a highly randomized tree algorithm to detect FDIA, which jeopardizes power system state estimation by applying FDIA into smart meter measurements. The developed algorithm has achieved detection accuracy of 99.76% with IEEE-118 bus, 99.39% with IEEE-57 bus and 97.8% with IEEE-14 bus systems respectively. Furthermore, developed algorithm showed more accurate results than Support Vector Machine (SVM), k-nearest neighbor and random forest. Furthermore, a stacked autoencoder has been used in co-ordination with a highly randomized tree classifier to deal with dimensionality. In [71], researchers have developed multiple-stage IDS techniques, such as temporal failure propagation graph, SVM, for intrusion detection and generating attack pathways for recognizing attack events in smart meters.

2) CYBER-SECURITY FOR DEVICES THROUGH CYBER-ATTACKS

Yankson and Ghamkhari developed an attack-thwarting technique for preventing load-altering attacks, which can rectify

frequency disturbances in power grids [23]. Furthermore, the developed technique has given effective results when tested on IEEE 33-bus power distribution system. In [72], the authors presented a bi-level optimization strategy for determining the most compromised and effective attacks as well as independent system operators effective response. Besides that, a defense strategy has been developed to reduce network losses and maintain rated voltage and current values.

B. CYBER-ATTACKS THROUGH ADVERSAL USERS

Adversary users may act maliciously by tampering their meters to decrease the electricity consumption, resulting in financial losses to utility companies or service providers and grid instability. Researchers proposed various detection and mitigation techniques in the existing literature.

In [73], Ahmadian et al. incorporated FDIA into the measurement system, in which the attacker acts as a virtual bidder in the day-ahead and real-time markets to maximize its profit by trading and proposed the mathematical programming equilibrium constraint-based single-level optimization problem to determine the optimal cyber-attacks against state estimation. In [74], researchers designed a easy-to-implement detection algorithm based on a co-variance estimator to detect and identify coordinated electricity theft incidence by evaluating both dependent & independent smart meter data generation process.

In [75], Yang et al. described a resilience technique for defending Programmable Logic Controller's (PLC) from critical information tampering attacks. In addition, generated a data authentication mechanism with an accuracy of 97.4% for the message digest in PLC-to-PLC communication. In [76], researchers have developed a privacy-aware AKA scheme to provide secure communication in between smart meters and service providers. Moreover, the developed scheme ensures the physical security of smart meters by utilizing light-weight cryptographic primitives such as one-way hash functions and PUF. Gope, implemented an efficient Privacy-preserving Multi-factor Authenticated Key Establishment (PMAKE) scheme based on reverse fuzzy extractor, one-way hash function and PUF to achieve secure smart grid communication [77]. Furthermore, the implemented scheme can guarantee the physical security for smart meters. The Table 2 and 3, presented the simulation platforms used to evaluate the performance of proposed techniques or algorithms against cyber-attacks.

TABLE 2. Proposed schemes with analyzed IEEE-bus Networks.

Ref.no	IEEE Buses
[78]	IEEE 37 - Bus
[34]	IEEE 123 - Bus Test System
[38]	IEEE RTS (Reliability Test System)
[45]	IEEE New England 39 - Bus AC-HVDC
[24]	IEEE 118 - Bus
[47]	IEEE RTS & IEEE 13 - Bus Distribution feeder
[48]	IEEE New England 39 - Bus & IEEE 118 – Bus
[51]	IEEE 118 - Bus
[22]	IEEE 39 - Bus
[53]	IEEE 14 - Bus for impact analysis & IEEE - 14, 30, 57, 118
[54]	IEEE 14 - Bus Network
[79]	IEEE 14 - Bus
[69]	IEEE 118 - Bus
[70]	IEEE 14, 30, 57, 118 - Bus
[23]	IEEE 33 - Bus Power Distribution System
[72]	IEEE 94 - Bus
[80]	IEEE 57 & 118 - Bus
[81]	IEEE 9 - Bus
[82]	IEEE 57 - Bus
[83]	IEEE 33 - Bus
[33]	IEEE 14 & 118 - Bus

TABLE 3. Proposed schemes with analyzed Simulation Networks.

Ref.no	Different Simulation Scenarios
[65]	Western Electric Co-ordinating Council 240 - Bus model
[35]	High Fidelity Simulation Test - Bed
[36]	NPCC 140 - Bus System
[62]	TESP & IEEE 9 - Bus System
[66]	TESP & IEEE 9 - Bus System
[67]	TESP & IEEE 9 - Bus System
[61]	TESP & IEEE 9 - Bus System
[84]	OPNET Simulator
[85]	SUMO & OMNET ++
[86]	Speed Goat Real-Time Digital Simulator
[87]	Power World Transient Simulation Tool
[73]	5 - Bus PJM(Pennsylvania-Jersey-Maryland) System
[88]	Xilinx ISE 14.7

C. ATTACKS THROUGH COMMUNICATION CHANNELS

A smart grid is an IoT-based application that allows energy providers to exchange electricity information with their customers or devices. However, the distribution systems reliance on communication networks makes it highly vulnerable to cyber-attacks. Attackers exploit this by attempting to steal information transferring through communication lines via DoS attacks and MITM, which can result in service interruption, energy theft or critical data theft. In addition, an attacker may try to eavesdrop on crucial messages transmit to the market operator. As a result, the attacker could know the identities of users, smart meter readings, bidding-offer information, electricity supply and demand information from these critical messages. Any drawback happen while providing security may leads to grid instability, AMI damage, and blackouts. Many researchers published various analysis methods, detection, and protection techniques in the literature to control the communication attacks. In [89], researchers reviewed about cyber systems and cyber physical systems, as well as the communication standards and protocols utilized in smart grids. In [90], authors presented a trust-based multi-path routing protocol for secure communication in the Mobile ad hoc network by minimising packet losses and detecting malicious nodes. In addition, cryptography and block chain approaches for providing high security to Mobile ad hoc network are being considered for future scope.

1) DETECTION OF COMMUNICATION CHANNEL CYBER-ATTACKS

In [80], the researchers proposed a cyber-attack detection scheme based on kernel principal component analysis

and randomized trees algorithm for dimensional reduction between the sensor and gathered measurements in smart grid networks. The performance of proposed scheme has been evaluated using standard IEEE 57 and 118 bus systems. In [91], researchers have proposed an artificial feed-forward network using a true data integrity agent-based model to detect false data cyber-attacks in smart grid systems for security assessment. The proposed model has detection accuracy of 98.91% through replay cyber-attacks. The proposed model can also be used in intelligent transportation systems for cyber-security.

In [81], the authors have considered the cosine similarity matching and chi square detector approach for use to detect cyber-attack in smart grid. In addition, the Kalman filter estimation method has been utilized to measure the divergence between actual and estimated data in order to detect attacks. In [84], researchers have developed supervised machine learning algorithms such as tree classification, naive bayes, multilayered perceptron, and multinomial logistic regression algorithms for classification tasks between network abnormality effects such as cyber-attacks and faults on energy-aware smart home systems. In [92], the authors have presented an IoT micro-security add-on that leverages a convolution neural network model to identify phishing attacks on IoT devices. In addition, the recurrent neural network-long short-term memory model has been hosted on back-end services to identify botnet attacks on IoT devices. In [93], researchers have developed an attack detection technique based on a deep belief network and interval state estimator to detect malicious attacks and electrical load forecasting. Moreover, the proposed mechanisms been evaluated on IEEE 14 and 118-bus systems. In [94], the authors have presented an adaptive and resilient N-IDS model using deep learning architectures to monitor network traffic, detect and classify network attacks such as jamming attacks, DoS attacks, and MITM attacks.

In [95], the authors have proposed a data integrity-based effective IDS with two phases: data sampling and selecting features to protect the network with accurate detection rate of 0.936 sec and false alarm rates of 0.33%. Even though the proposed system performs better in unstable conditions, it only detects data integrity-based attacks. In [79], researchers have developed an IDS architecture to monitor and detect lethal attacks such as price manipulation attacks, DoS attacks with detection rate of more than 95% and false positive rate is below 5% using a cumulative sum algorithm in smart grid. In [96], the authors have proposed an SVM algorithm to detect active eavesdropping attacks with detection probability of 95% using artificial training data in the wireless communication channel. From the presented work, adding more hidden features to the proposed algorithms can improve detection performance.

In [97], Sahoo et al. presented a cooperative mechanism based on the cooperative vulnerability factor to detect potential deceptive cyber-attacks in cyber-physical Direct Current microgrids. Furthermore, the proposed mechanism performance has been examined in MATLAB environment. In [85], authors developed a cross-layer IDS based on random forest and k-nearest neighbor to detect spoofing attacks in inter-vehicle communications. Based on the results of the IDS, attackers have been barred from using the wireless charging mechanism.

2) COMMUNICATION CHANNEL CYBER-ATTACKS DETECTION AND CYBER-SECURITY

The use of the internet for data communication between building controllers, such as smart meters and the electric grid, renders the system susceptible to cyber-attacks. A skilled adversary may be able to manipulate the exchanged data which will harm the system. In [98], researchers designed, implemented, and evaluated a monitoring system for open-flow networks and injected proxy attack in between open-flow controller and open-flow switches to capture messages and monitor traffic data. From the presented work, it is to be noted that they can deploy multiple monitoring systems for load balancing and upgrade open-flow versions from 1.0 to 1.1. The authors of [99] created a singular value decomposition technique and private pilot to identify active attacks by authenticating the sender based on the wireless channel. Furthermore, passive eavesdropping and active attacks have been defended using the concept of one-time pad by encrypting wireless channels with a private plot. In [100], researchers have proposed an authentication method to overcome false data flow and improve false data detection with less detection time 4.67 sec without increasing end-user overload in smart grid communication. In [82], the authors have proposed a deep learning-based dual denoising auto-encoder and unified scheme to protect the cyber physical system from eavesdropping attacks and to detect typical cyber-attacks, such as FDIA, DoS, and relay attacks. The proposed scheme performance has been evaluated on IEEE-57 bus system. In [86], researchers have presented a dynamic state estimation technique based on an unknown input observer to estimate the presence of unknown inputs in the microgrid communication channel for stable operation. In addition, a residual function has been generated that detects the presence of FDIA and triggers a detection alarm for attack isolation and mitigation.

3) CYBER-SECURITY FOR COMMUNICATION CHANNEL ATTACKS

A smart meter is an essential component of the smart grid and transmits real-time data to a utility centre. According to the united nation-national institute of standards and technology, bi-directional communication between the two parties opens doors for cyber-attack vulnerabilities. Implementing security for that kind of attack is one of the challenging tasks. Cryptography is one of the efficient technique to provide security against communication channel attacks such as DoS, MITM, jamming attacks, replay attacks, impersonation attacks not only in smart grid but also in health care purpose. In [101], authors proposed a logistic map based

key generation for secure communication by maintaining confidentiality and authenticity in Mobile ad hoc based health care network. Fig. 4. express the structure of cryptography primitive.

In [102], researchers presented an AKA scheme with privacy preservation for smart grid communication. When an adversary compromises a smart meter device, this scheme considers reducing the possibility of a critical leakage attack. In addition, the work highlights that blockchain technology can be used to better authentication schemes for privacy protection in smart grid.

In [103] and [104], Abbasinezhad-Mood and Nikooghadam proposed an ECC-based self-certified key distribution mechanism to address the issue of public key infrastructure maintenance in between smart meters and service providers in smart grid. However, Khan et al. discovered security problems such as the inability to provide security against DoS attacks, insider attacks, anonymity and failure to update the identity and keys from Mood and Nikooohadam's work. Therefore, the design of an authentication scheme to mitigate the flaws mentioned above has been considered for future work. In [105], Ashok Kumar Das et al., proposed a new anonymous signature-based authenticated key exchange scheme for IoT-enabled smart grid, called AAS-IoTSG which allows a smart meter to establish a session key for encrypted communication by mutually authenticating with a service provider. From the presented work, the proposed method can be tested on a Raspberry Pi to demonstrate its viability for IoT-enabled devices with limited resources such as smart meters. In [106], researchers proposed identity-based signature to demonstrate an anonymous key agreement methodology for smart grid system. Moreover, the proposed protocol not only provides authentication but also provides smart meter anonymity. In [107], the authors have presented a novel symmetric homo-morphic scheme to achieve lightweight aggregation for encryption which can provide secure and efficient authentication in smart grids. In [108], Braeken et al. presented a Elliptic Curve Qu-Vanstone (ECQV) certificate-based key agreement paradigm for smart metering communications, which does not require a secure network during entity registration and is resistant to key escrow. Furthermore, the proposed scheme can also be secure under Random Oracle Model (ROM). In [109], researchers have developed a key management scheme based on ECC to mitigate MITM and re-transmission attacks between smart meters and power companies (outside the HAN). The results revealed that the false factor is directly proportional to detection time. For example, the identification time increases by 1.4 seconds as the false factor rises from 0.1 to 0.3.

Cryptographic algorithms have been used to mitigate communication attacks between devices like smart meters and service providers in the power distribution system, which typically uses cryptographic keys to maintain perfect secrecy. Whenever cryptographic algorithms need to be strengthened, it is often possible to use larger keys or hybrid with two algorithms. In [110], researchers presented a defence strategy using event-based cryptography to keep attackers away from obtaining critical information in the sensor communication channel between the plant and the cyber physical system supervisor. In [111], the authors have developed a secure communication methodology using recursive inter-networking architecture, which addresses almost all communication attacks in a closed environment like LAN. Besides, recursive inter-networking architecture capabilities and features can replace existing communication technology while providing increased security. Furthermore, the work highlights that the developed method can be extended to open environments such as wide area networks and neighbourhood area networks. In [112], researchers have designed an Advanced Encryption Standard-512 bit algorithm for faster processing speed with a stable surface environment in web-based applications with more secure communication.

Elakrat and Jung developed a field-programmable gate array security mechanism to minimize information-gathering attacks based on a cryptographic approach to secure data confidentiality and prevent the injection of malware into the vital digital assets data communication system of NPP [113]. In [114], researchers have developed a secure access control scheme based on certificate-less signcryption with a proxy re-encryption scheme which can secure in ROM. The work remarks that the presented scheme can also be extended to merge attribute-based signcryption with proxy re-encryption schemes. In [115], the authors have implemented a lightweight privacy-preserving Q-learning (LiPSG) framework for smart grid energy monitoring. Moreover, four additive secret-sharing-based sub-protocols such as secure action selection, SMAX, SEle and SGry were developed to perform the atomic operations efficiently and securely. Kumar et al. developed a hardware chip integrated S-box advanced encryption standard algorithm to secure the smart grid SCADA system and chip performance is evaluated using field programmable gate array with different key sizes and grid sizes [88]. In [116], the authors present a lightweight fault-tolerant privacy-preserving data aggregation strategy using modified Paillier cryptosystem, ECC, Chinese-remainder theorem, and hash function technique. Furthermore, the proposed scheme robust against all security features. In [117], researchers have developed a novel Pairing Free-Data Aggregation (PF-DA) scheme based on certificate-based cryptography to reduce the impact of certificate pre-checking problems in the energy internet-based smart grid communication networks. Furthermore, designing the decentralised data aggregation scheme can be provided more security for smart grid communication.

In [25], the authors have presented single and multi-antenna models by applying the Stackelberg game with renewed intelligent simulated annealing algorithm and the stochastic algorithm with feedback to provide security

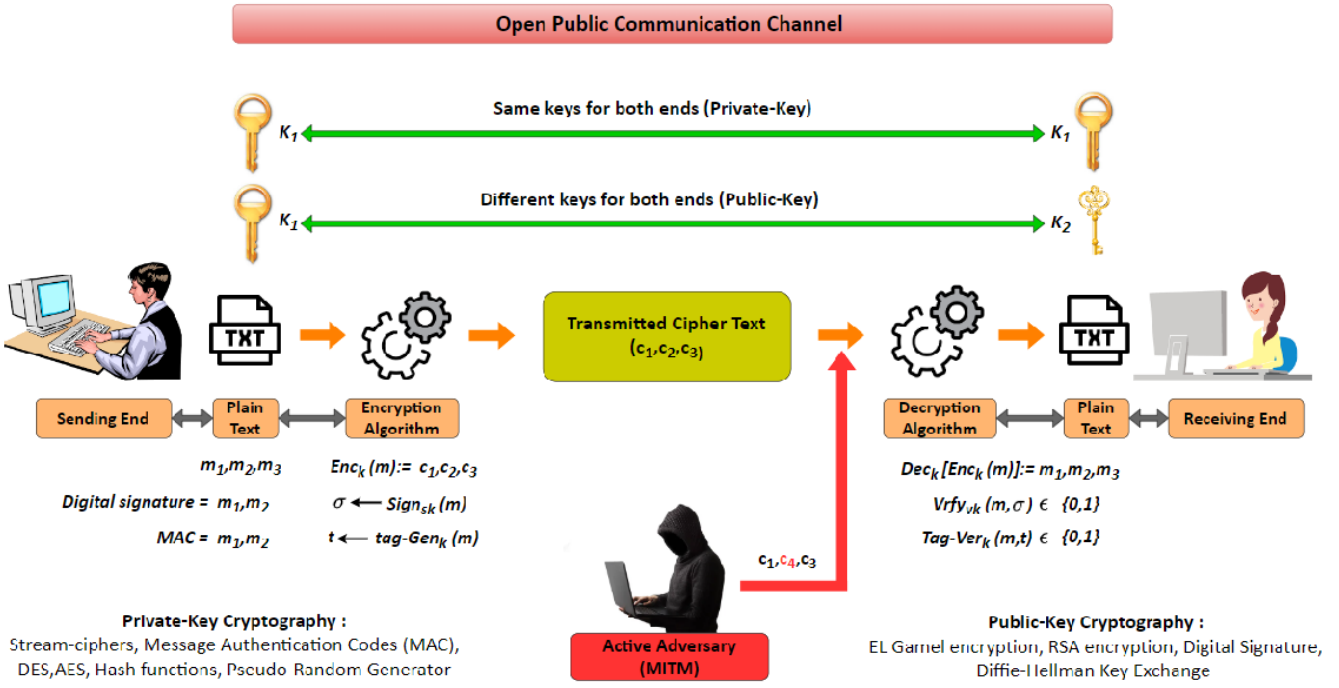

FIGURE 4. A Detailed Overview of Cryptographic Primitives in Communication Channel.

against jamming and MITM attacks in green cyber-physical communication systems. In [118], researchers have proposed a cyber-security architecture that integrates identity-based security mechanism and intelligent security system for energy management to provide appropriate security and privacy for components, data, and actions in the energy internet. The evaluated results of the proposed architecture expressed safety and efficiency for energy internet. Marcos Vicente Moreira et al., presented a security module to prevent MITM attacks between controller and sensor communication channel in cyber-physical systems. Furthermore, the extension of the security module offered NA-safe controllability [119]. In [120], researchers have developed a super-lightweight security protocol using a logical XOR and one-way hash function to secure the smart grid neighbourhood area network communications. The work highlights the implementation of a lightweight scalable blockchain-based multi-party computational protocol that can be employed for resource constraint networks. In [121], the authors have proposed a resilient scheduling strategy that uses additional metrics based on the difference between forecasted and actual bills to detect FDIA in interconnected multiple smart buildings. Besides, the support vector regression method has been used to calculate predicted bills.

Moghadam et al. developed a lightweight protocol based on hash and private key to mitigate IEC62351 security flaws while facilitating key agreement in smart grid [27]. The developed protocol can agree the session key within 0.057ms. Furthermore, it explored privacy, authentication, and private data transfer security between two entities and tested several sorts of cyber-attacks such as impersonation, replay, and MITM attacks. In [122], researchers have presented the timing performance of the RSASSA-probabilistic signature scheme digital signature algorithm to secure the Generic Object-Oriented Substation Event (GOOSE) messages in power system control operations. The work highlights the requirement of cyber-security and time domains that an authentication scheme can achieve.

In [123], [124], and [125], researchers have developed multiple techniques such as PUF- based AKA scheme and reconfigurable authenticated key exchange scheme to secure communication channels by mitigating energy theft attacks, such as ephemeral leakage attacks in between service providers and smart meters. In [126], researchers have developed a lightweight mutual authentication scheme based on PUF to encrypt communications in between smart meters and neighbourhood gateways. In [127], the authors have presented a novel authentication key exchange approach based on low-cost memristor-PUF to investigate security between the head-end system and smart meters. Furthermore, the work highlights that the presented scheme for analysing various other attack scenarios, such as replay attack, MITM,

and impersonation attack, has been considered as future scope.

In [128], researchers developed an anonymous authentication approach based on a group signature scheme with configurable linkability with tokens to reduce double spending and billing scam in the smart grid. In [129], the authors developed a hash function, ECC, and symmetric encryption-based anonymous and reliable authentication scheme for the smart grid to ensure the integrity of information transmitted between the smart meter and central service provider. Limbasiya and Arya have discussed various attacks, authentication schemes, and security parameters for secure communication in the smart grid system [130]. Researchers have presented a Diffie-hellman-based message authentication protocol for smart grid communications between the HAN-gateways and BAN-gate ways [131]. In [132], researchers have developed a lightweight ECC-based mutual authentication scheme with trifling operations to secure communication between consumers and substations for smart-grid environments. The presented work shows that the developed scheme can also analyze real-time data communications in smart grid. In [133], researchers have introduced a new AKA protocol using an ECQV implicit certificate to access data securely by providing mutual authentication in smart meters for smart grid environments. Aziz et al. implemented a lightweight authentication protocol based on the hash function with masked identity to secure information exchange between the control centre and smart breakers in a smart grid [83]. The work highlights that the proposed scheme injecting into the REF542plus controller using manufacturing software such as CAN open digital field bus can provide low computation and communication costs for real-time smart grid applications. Gope, proposed a lightweight authentication scheme, while ensuring strong user anonymity support to satisfy all the security features of M2M based home network services [134]. In [135], the authors have introduced mutually authenticated key establishment scheme to provide secure communication between the multiple smart meters and service providers in a cloud-enabled smart grid system. The work remarks the necessity to design two protocols to mitigate: one to store the gathered data in the cloud server and the other to obtain the processed data from the cloud server. In [136], [137], and [138], researchers have developed an ECC-based authentication protocol to mitigate considered communication attacks between smart grid devices and utility centres. Besides, another researcher proposed a privacy-preserving lightweight authentication scheme based on pseudo-identity and secret parameters to address the shortcomings of the ECC authentication protocol. Such shortcomings are the protocol insecurity against masquerade, smart grid device theft, and failure to ensure robust mutual authentication.

In [139], the authors have proposed a blockchain and homo-morphic encryption-based privacy-preserving data aggregate model to prevent internal and external attacks such as MITM, privileged-insider attacks, and impersonation attacks with low computational cost in a cloud computing-based smart grid system. In [140], the researchers have developed a blockchain-based secure and lightweight authentication protocol with centralized register authority to mitigate the majority of common attacks, such as replay attacks, jamming attacks, and DoS attacks in practical smart grid environments. In addition, the work highlights that the developed protocol can be used for batch verification and to evaluate dynamic issues. The Table 4. gives detailed view about the vital characteristics for cyber security against cyber attacks.

As discussed earlier, the proposed schemes can withstand a wide range of attacks, which is critical for communication networks. The security of proposed schemes is evaluated both formally and informally depending on their robustness against major cyber-attacks. From the mentioned literature, the effectiveness of proposed schemes against all possible cyber-attacks are examined in Table 5. Furthermore, the proposed schemes are primarily focused on providing security against well-known attacks such as the replay attack, MITM, impersonation attack, and failing to provide security against insider attacks, which is very difficult to detect, as shown in Fig. 5.

The proposed schemes needs to meet common security requirements such as data integrity, privacy, confidentiality and availability in order to develop good security. Table 6 presented how well the proposed schemes are defended against all potential security vulnerabilities. From the discussed literature, un-tracebility is one of the important security feature, schemes are failing to provide strong security which will become a biggest concern as shown in Fig. 6.

VII. CYBER-ATTACK INCIDENCE IN POWER SYSTEMS

A. CASE-STUDIES

Based on 2015 Ukraine cyber-attack, the authors have implemented the cascading outage analysis to analyze the impact of various cyber-attacks by opening all devices, generators, and loads connected to the lines of every transmission and distribution system provider in the North American regional interconnection system [87]. In [141], the authors have implemented electrical power system analysis software in a petrochemical plant to analyze the influence of electrical parameters on modified remote data transmitted cyber-attacks in SCADA systems. Furthermore, the designed cyber-attacks can be mitigated by using cryptography. The authors looked into cyber terrorism in NPPs after the 2014 cyber-attack on the South Korean NPP [142]. In addition, GEN-4, radiation control, and secure information management have been explored as potential solutions to the problem of cyber terrorism in NPPs. In [143], the authors developed a multi-state markov model to analyse the impact of integrity attacks such as command messages for circuit breakers and modifying IED parameter. In [144], researchers analysed IoT-related vulnerabilities, potential mitigation, and prevention techniques for real-world cyber security incidents

TABLE 4. Vital characteristics to provide cyber-security against cyber-attacks.

Ref.no	Year	Platform	Cryptographic Library	Verification Tool	Cryptographic Algorithm
[128]	2017	gcc Apple LLVM Version 8.0.0	TEPLA 2.0	-	Group Signature
[134]	2017	-	Crypto++ library	-	Light weight anonymous authentication & key agreement protocol
[131]	2017	-	-	proverif	Diffie-hellman based message authentication
[103]	2018	STM32 F4 DISCOVERY & Nano pi M3 board for to ends	Stm32 & open SSL	Proverif, ROM	ECC- based self-certified key distribution scheme
[83]	2018	MATLAB R2014a	Java class cryptosystem	-	Crypto hash function, SKA, SGMA
[106]	2018	-	-	Proverif, ROM	Identity based AKE protocol
[108]	2018	-	-	AVISPA	Secure key agreement model based on ECQV certificates
[27]	2019	LAN employed the switched Ethernet network	-	AVISPA	ECC based authentication
[76]	2019	Ubuntu 12.04 virtual machine	JPBC library Pbc 05.14 & JCE library	-	Privacy - preserving authentication protocol using PUF
[122]	2019	python	-	-	RSASSA-Probabilistic Signature Scheme
[138]	2019	Grid smart home hardware testbed, Pentium IV, Hiper smart card	-	AVISPA	ECC based authentication
[126]	2020	AT91SAM3X8E micro controller board	Arduino Libs as a cryptographic library	Mao, Boyd's logic	Light-weight mutual authentication protocol based on PUF
[137]	2020	Pentium IV, Hiper smart card	-	AVISPA, BAN logic, ROR	Light weight authentication using pseudo-identity and secret parameters
[125]	2020	-	-	Scythe, AVISPA	End-to-end PUF based AKE
[77]	2020	Ubuntu 12.04 virtual machine	JPBC library Pbc-05.14	-	PMAKE scheme based on PUF
[102]	2021	NS-3 version 3.28	C/C++ open SSL library	-	Authenticated Key Agreement
[109]	2021	Communication inside the network on IEEE 802-15-4 & network outside the building on IEEE 802-16 WiMAX	-	-	ECC based authentication
[132]	2021	NS – 2.35	PBC library version 05.12	AVISPA	ECC based authentication
[105]	2021	Philips Hiper smart card	-	AVISPA, ROR	ECC-based schnorr's signature based AKE
[136]	2021	Pentium IV, Hiper smart card	-	Proverif, BAN logic	Light weight authentication using pseudo-identity and secret parameters
[129]	2021	Pycrypto, Rasberry pi-3	-	ROM, scythe based security	ECC-based AKE protocol (ARAP-SG)
[120]	2021	AT91SAM3X8E for smart meter & Intel® core™ i7- 3612QM CPU @ 2.10 GHz and 6GB-RAM for NG	Arduino Libs as a cryptographic library	Mao, Boyd's logic	Super light-weight secure protocol based on one-way hash function and logical XOR
[135]	2021	-	-	GNY logic, Proverif	Mutually authenticated key establishment protocol
[133]	2021	-	-	CK security model	Authenticated key agreement protocol based on ECQV implicit certificate
[117]	2022	Ubuntu 12.04 virtual machine	JPBC library Pbc-05.14 & JCE library	ROM	PF-DA designed by using certificate-based cryptography
[127]	2022	MATLAB (Mathworks) using okamoto protocol	-	NIST 800-22 statistical tests	Memristor based - PUF

TABLE 5. Robustness of proposed schemes against Cyber-attacks.

Ref.no	A	B	C	D	E	F	G	H	I
[105]	✔	✔	✔	✔	✘	✔	✘	✘	✔
[102]	✔	✔	✔	✔	✘	✘	✘	✘	✘
[131]	✔	✔	✘	✔	✘	✘	✘	✘	✘
[27]	✔	✔	✘	✔	✘	✘	✘	✘	✘
[109]	✘	✘	✘	✔	✘	✘	✔	✘	✘
[132]	✔	✔	✔	✔	✘	✘	✘	✘	✔
[76]	✔	✔	✔	✔	✔	✘	✘	✘	✔
[136]	✔	✔	✔	✘	✔	✘	✘	✘	✔
[137]	✘	✔	✔	✔	✘	✘	✘	✔	✔
[138]	✔	✔	✘	✔	✘	✘	✘	✘	✔
[129]	✔	✔	✔	✔	✔	✔	✘	✘	✔
[125]	✔	✔	✔	✔	✘	✔	✘	✘	✔
[103]	✔	✔	✔	✘	✘	✔	✘	✘	✘
[106]	✔	✔	✘	✔	✘	✘	✘	✘	✘
[83]	✔	✔	✘	✘	✘	✘	✘	✘	✘
[77]	✘	✘	✔	✔	✘	✘	✘	✘	✔
[117]	✔	✔	✔	✔	✘	✘	✘	✘	✘
[134]	✘	✔	✘	✘	✔	✘	✘	✔	✘
[120]	✔	✔	✘	✔	✔	✘	✘	✘	✘
[126]	✔	✔	✔	✔	✘	✘	✘	✘	✔
[135]	✔	✔	✔	✔	✘	✔	✘	✘	✘
[133]	✔	✔	✘	✔	✔	✘	✘	✘	✘
[108]	✔	✔	✘	✔	✔	✘	✘	✘	✘

✔ - proposed scheme is strong against specified attack ;
✘ - proposed scheme is not strong against specified attack
A - Impersonation Attack ; **B** - Replay attack ; **C** - Privileged insider attack ; **D** - MITM ; **E** - DoS attack ; **F** - Ephemeral secret leakage attack ; **G** - Resending attack ; **H** - Masquerade attack ; **I** - Device stolen attack

TABLE 6. Robustness of proposed schemes against security features.

Ref.no	A	B	C	D
[103]	✔	✔	✔	✘
[106]	✔	✔	✘	✔
[83]	✔	✘	✔	✘
[125]	✔	✔	✔	✔
[105]	✔	✘	✔	✔
[102]	✘	✔	✔	✔
[131]	✘	✔	✔	✘
[27]	✔	✔	✔	✘
[109]	✘	✘	✘	✘
[132]	✔	✔	✔	✘
[76]	✔	✔	✘	✘
[136]	✔	✘	✔	✔
[137]	✔	✘	✔	✘
[138]	✔	✔	✘	✔
[129]	✔	✘	✘	✔
[77]	✔	✔	✔	✔
[117]	✘	✘	✘	✘
[134]	✔	✔	✔	✔
[120]	✘	✔	✔	✘
[126]	✘	✘	✔	✘
[135]	✔	✔	✔	✔
[133]	✔	✔	✔	✔
[108]	✔	✘	✔	✘

✔ - proposed scheme is strong against security feature ;
✘ - proposed scheme is not strong against security feature
A - Anonymity; **B** - Perfect Forward Secrecy; **C** - Mutual Authentication; **D** - Untracebility

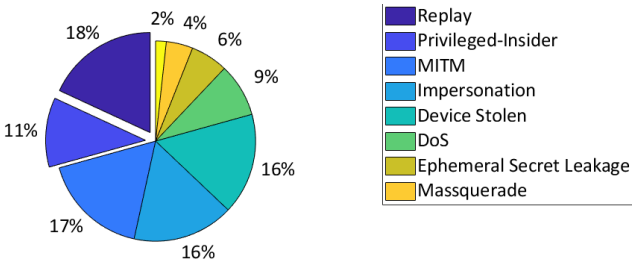

FIGURE 5. Percentage of cyber-attacks strong against proposed schemes.

affecting electricity consumers. In [145], researchers have proposed a generalized stochastic petri net to investigate the impact of integrating multi-level preventive, responsible measures on security indicators like mean-time-to-disrupt and system availability against cyber-attacks in NPPs. Furthermore, the proposed approach can also be extended to examine system dependability. In [146], the authors have provided a case study demonstration on the Proactive Intrusion Detection and Mitigation System (PIDMS) to examine the packet replay attack scenario in photo voltaic inverter communication. Moreover, PIDMS is extensible to other smart grid devices to send and receive cyber-physical data streams. In [78], researchers have presented tandem stability and machine learning-based classifiers to analyze the influence of time delay attacks on automatic generation control in the power grid. The presented approach has been evaluated and verified on the IEEE 37-bus system model.

B. REAL-WORLD CYBER-ATTACK INCIDENCES ON POWER SYSTEMS

1) ZERO-DAY ATTACK ON DAVIS-BESSE NPP, 2003

By injecting a zero-day attack into a micro-soft SQL server, attackers gained access to the secret and control

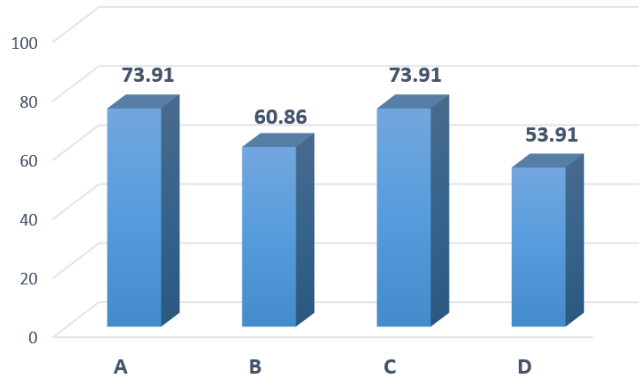

FIGURE 6. Percentage of proposed schemes strong against specified security features.

networks of Davis-Besse NPP in Ohio. The injected malware generated a massive amount of traffic in order to disrupt communication networks between corporate and control networks. In addition, the worm had left a safety monitoring system inoperable for more than five hours. Employees were unable to monitor the core temperature sensors at the plant.

2) STUXNET ATTACK ON NUCLEAR PROGRAM OF IRAN, 2010

On November 29, 2010, the Iranian president stated that the stuxnet virus had destroyed hundreds of centrifuges used to enrich uranium at Natanz nuclear enrichment. According to estimates, the stuxnet worm destroyed Nine Eighty-four uranium enrichment centrifuges and destroyed enrichment efficiency by thirty percent. Another virus corrupted government computers at nuclear plants and stolen data in 2012.

3) CYBER-ATTACK ON KOREA HYDRO AND NUCLEAR POWER, 2014

On December 23, 2014, Korea Hydro and Nuclear Power announced that their computer systems had been hacked. ''Unless you stop operating the nuclear power plants until Christmas and give us $1 billion, we will continue to release the facility's secret data'', the hackers posted on their twitter page. Furthermore, two nuclear reactor manuals from Korea Hydro and Nuclear Power were posted online, exposed ten thousand employee's personal data.

4) SANDWORM ATTACK ON UKRAINE ELECTRICITY COMPANY, 2015

On December 23, 2015, remote cyber intrusions at three electric power distribution companies caused a blackout that left over 2,25,000 customers without power for 16 hours in Prykarpattyaoblenergo, Ukraine. The attackers injected malware through spear phishing emails with malicious attachments, gaining access to the SCADA control and then opened breakers at over 30 substations. Furthermore, serial-to-ethernet servers, backup power was disabled with bad firmware, and a DoS attack on the utility telephone system was also carried out.

5) INDUSTROYER ATTACK ON UKRAINE ELECTRICITY COMPANY, 2016

On December 17, 2016, a remote cyber intrusion occurred at a local substation that supplies power to the capital city of Kyiv. Attackers opened breakers at a substation again. However, this time they attempted to compromise the relays.

6) DTRACK ATTACK ON KUDANKULAM NPP, 2019

On September 4, 2019, malware was discovered on a personal computer belonging to a user who was connected to an administrative internet network. The nuclear power corporation of India limited issued an official statement confirming the incident. ''This PC has been disconnected from the critical internal network and networks are constantly monitored.''

7) REVIL RANDSOMWARE ATTACK ON UK ELECTRICITY MARKET, 2020

On May 12, 2020, hackers attacked internal IT systems at Elexon, which is center of balancing and settlement system, works for the energy system operators of Great Britain's national grid. Elexon's official response to this incident was as follows: ''the attack is to our internal IT systems and ELEXON's laptops only. Electricity supply is not affected.''

8) CYBER-ATTACK ON LADAKH ELECTRICITY DISTRIBUTION CENTER, 2022

On March 2022, unknown hackers attempted but failed to hack into an electricity distribution center. ''two attempts by the hackers to target electricity distribution centers near Ladakh were unsuccessful. We have already strengthened our defenses to counter such attacks,'' said India's minister of power and renewable energy.

VIII. CONCLUSION

This paper reviewed various approaches for cyber-attacks detection, protection and impact analysis in multiple areas such as wind farms, PV systems, transmission systems, smart meters and communication channels. A need of cyber security for IoT-based smart grid systems has been examined. This review article analyzed the literature to provide an overview of the need and potential methods for detecting and mitigating cyber attacks, particularly communication attacks, using artificial intelligence, block chain and cryptographic primitives. When it comes to the analysis of proposed literature, it suggested vital characteristics, simulation platform, libraries to do practical design, simulation and verification of cryptographic primitives for secure communication between two endpoints in a smart grid system. and Furthermore, the robustness of security properties, cryptographic algorithms against various cyber attacks was analyzed to suggest an unexplored attack.

A. FINDINGS

Based to the literature, FDIA is the most serious concern in the power system. The authors presented unique detection strategies for FDIA by employing thevenins equivalent parameters [48], an extremely randomised tree algorithm [70], and auto regressive models such as wavelet and TCN instead of the recurrent family model [33]. Not only FDIA, eavesdropping attack also one of the cyber security vulnerable attacks in smart communication system. Researchers developed a deep learning architecture [94], SVM [96], decomposition form of the system matrices [26], dual denoising auto-encoder based encryptor [82] and a certificate-less signcryption [114] to analyse impact and detect DoS, eavesdropping attacks. Furthermore, researchers utilised a zero-knowledge proofs & the pailiers crypto system [102], as well as a blockchain & homomorphic encryption based aggregation architecture [139], to minimise smart meter data manipulation attacks.

Based on presented literature, the following new findings are highlighted in the field of power systems cyber-attacks:

- FDIA's is one of the concerned attacks in power systems. Machine learning-based techniques such as extremely randomized tree and isolation forest could deliver accurate and fast detection of FDIAs with an accuracy of more than 99.75% and a detection time of less than 1.944 seconds, respectively. Because, false factor increases then detection time also increases.
- Cryptographic algorithms such as elliptic curve-based encryption incorporated with block chain, will facilitate electricity trading without the mediator as well as provide low computation cost for data aggregation. In addition, the kind of approach will provide authenticated security for deregulation energy markets such as TEMS, Demand Response.
- To satisfy the IEC 61850 protocols in the standard of IEC 62351, the control commands must transmit within 4ms between substation to circuit breakers. Hash function and private key based protocol can agree on the session key within 0.057ms, which satisfies the time restrictions of GOOSE and sampled value protocols and will provide private key privacy and session key security against communication attacks such as MITM, replay attack and DoS attack. Furthermore, RSASSA-PKCS-V1_5 fails to meet the timing standards of GOOSE messages, which may leads to revisit the IEC 62351-6 standard with new considerations for better cyber security.

B. FUTURE DIRECTIONS

The comprehensive review has opened up new scopes in power systems cyber securities.

- Establishment of a detection approach based on dynamic watermarking to detect sophisticated adversaries that can be scaled up to large-scale power systems [36].
- A deep stacking auto-encoder technique can also be used to identify the root cause and implement appropriate control measures to prevent cyber intrusion between utilities and consumers in smart grid [62].
- Despite FDIA detection in smart grid, artificial feed-forward networks based on a true-data integrity agent model can be employed for cyber security in intelligent transportation systems [91].
- Merging of attributed-based signcryption with proxy re-encryption scheme to secure data from communication attacks in smart grid [114].
- A lightweight multiparty computation protocol based on blockchain that can also be suitable for resource-constrained networks like the smart grid [120].
- Blockchain technology can also provide better authentication protocols for the smart grid privacy protection [102].

The following research areas are suggested in the field of cyber-attacks in power systems based on existing research:

1) Development of decentralized defense system to identify and mitigate threats in renewable energies such as wind and photo-voltaic systems, based control networks using artificial intelligent control techniques that can be extend to large-scale power systems. Furthermore, evaluation of the impact of renewable energy power plants temporal characteristics and participation in power markets.
2) Development of effective strategies for analyzing the impact, detecting and protecting against cyber-attacks on state estimation (PMU, Direct Current, Alternative Current -High Voltage Direct Current) in transmission lines, as well as improving a framework for locating the events at each line.
3) Implementation of a framework to analyze a few realistic behaviours of agents, operators and electricity market mechanisms and the development of cyber security actions for data manipulation attacks and energy theft attacks using intelligent transportation in TES.
4) There is a need to analyze the impact of cyber-attacks such as DoS and MITM in various environments like peer-to-peer energy trading, M2M communication, TES, demand side management, and distribution side, as well as design the detection schemes and monitoring systems to identify meters that inject false power consumption data and to handle zero-day sort of attacks.
5) The scope of IoT- based smart grid projects is limited to closed environments (LAN, recursive internet working architecture). There is a need to extend the real-world smart grid infrastructures, such as the implementation and evaluation of a prototype in collaboration with smart grid operators or service providers, to analyze real-world data communication in smart grids.
6) Establishment of a lightweight authentication scheme to address specific cyber security challenges such as privacy of users and policy makers, reducing the protocol message size, lowering the computational cost

and shortening the time domains for a distributed secret-key management scheme. To enhance the privacy protection in smart grid communication channels blockchain technology shall be adopted.

IX. CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

REFERENCES

[1] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[2] S. Garg, K. Kaur, G. Kaddoum, J. J. P. C. Rodrigues, and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3548–3557, May 2020.

[3] C. Ang. (2021). *The Most Cyber Attsignificant Acks From 2006-2020, by Country*. [Online]. Available: https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/

[4] M. Benmalek and Y. Challal, "MK-AMI: Efficient multi-group key management scheme for secure communications in AMI systems," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–6.

[5] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094.

[6] R. E. Pérez-Guzmán, Y. Salgueiro-Sicilia, and M. Rivera, "Communication systems and security issues in smart microgrids," in *Proc. IEEE Southern Power Electron. Conf. (SPEC)*, Dec. 2017, pp. 1–6.

[7] M. Z. Gunduz and R. Das, "Analysis of cyber-attacks on smart grid applications," in *Proc. Int. Conf. Artif. Intell. Data Process. (IDAP)*, Sep. 2018, pp. 1–5.

[8] H. Ritchie and M. Roser. (2018). *Two-Thirds of Global Population Will Live in Cities By 2050, Our World in Data*. [Online]. Available: https://ourworldindata.org/urbanization

[9] M. Benmalek, Y. Challal, and A. Derhab, "Authentication for smart grid AMI systems: Threat models, solutions, and challenges," in *Proc. IEEE 28th Int. Conf. Enabling Technologies: Infrastructure Collaborative Enterprises (WETICE)*, Jun. 2019, pp. 208–213.

[10] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "Machine learning and deep learning approaches for cybersecuriy: A review," *IEEE Access*, vol. 10, pp. 19572–19585, 2022.

[11] A. Hasankhani, S. M. Hakimi, M. Bisheh-Niasar, M. Shafie-khah, and H. Asadolahi, "Blockchain technology in the future smart grids: A comprehensive review and frameworks," *Int. J. Electr. Power Energy Syst.*, vol. 129, Jul. 2021, Art. no. 106811.

[12] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electr. Power Syst. Res.*, vol. 215, Feb. 2023, Art. no. 108975.

[13] M. Abdalzaher, M. Fouda, A. Emran, Z. Fadlullah, and M. Ibrahem, "A survey on key management and authentication approaches in smart metering systems," *Energies*, vol. 16, no. 5, p. 2355, Mar. 2023.

[14] M. Sewak, S. K. Sahay, and H. Rathore, "Deep reinforcement learning in the advanced cybersecurity threat detection and protection," *Inf. Syst. Frontiers*, vol. 25, pp. 589–611, Aug. 2022.

[15] S. Banik, S. K. Saha, T. Banik, and S. M. M. Hossain, "Anomaly detection techniques in smart grid systems: A review," in *Proc. IEEE World AI IoT Congr. (AIIoT)*, Jun. 2023, pp. 331–337.

[16] J. Kua, M. B. Hossain, I. Natgunanathan, and Y. Xiang, "Privacy preservation in smart meters: Current status, challenges and future directions," *Sensors*, vol. 23, no. 7, p. 3697, Apr. 2023.

[17] K. Y. Yap, H. H. Chin, and J. J. Klemeš, "Blockchain technology for distributed generation: A review of current development, challenges and future prospect," *Renew. Sustain. Energy Rev.*, vol. 175, Apr. 2023, Art. no. 113170.

[18] S. S. Koduru, V. S. P. Machina, and S. Madichetty, "Cyber attacks in cyber-physical microgrid systems: A comprehensive review," *Energies*, vol. 16, no. 12, p. 4573, Jun. 2023.

[19] M. Lydia, G. E. P. Kumar, and A. I. Selvakumar, "Securing the cyber-physical system: A review," *Cyber-Phys. Syst.*, vol. 9, no. 3, pp. 193–223, Jul. 2023.

[20] S. Bhattacharjee and S. K. Das, "Detection and forensics against stealthy data falsification in smart metering infrastructure," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 1, pp. 356–371, Jan. 2021.

[21] X. Lou, "Learning-based time delay attack characterization for cyber-physical systems," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*, Oct. 2019, pp. 1–6.

[22] A. Ameli, A. Ayad, E. F. El-Saadany, M. M. A. Salama, and A. Youssef, "A learning-based framework for detecting cyber-attacks against line current differential relays," *IEEE Trans. Power Del.*, vol. 36, no. 4, pp. 2274–2286, Aug. 2021.

[23] S. Yankson and M. Ghamkhari, "Transactive energy to thwart load altering attacks on power distribution systems," *Future Internet*, vol. 12, no. 1, p. 4, Dec. 2019.

[24] J. Khazaei, "Cyberattacks with limited network information leading to transmission line overflow in cyber–physical power systems," *Sustain. Energy, Grids Netw.*, vol. 27, Sep. 2021, Art. no. 100505.

[25] K. Wang, L. Yuan, T. Miyazaki, Y. Chen, and Y. Zhang, "Jamming and eavesdropping defense in green cyber–physical transportation systems using a Stackelberg game," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4232–4242, Sep. 2018.

[26] R. Gao and G.-H. Yang, "Sampled-data distributed state estimation with multiple transmission channels under denial-of-service attacks," *Appl. Math. Comput.*, vol. 429, Sep. 2022, Art. no. 127229.

[27] M. F. Moghadam, M. Nikooghadam, A. H. Mohajerzadeh, and B. Movali, "A lightweight key management protocol for secure communication in smart grids," *Electr. Power Syst. Res.*, vol. 178, Jan. 2020, Art. no. 106024.

[28] I. Staffell and S. Pfenninger, "The increasing impact of weather on electricity supply and demand," *Energy*, vol. 145, pp. 65–78, Feb. 2018.

[29] J. Staggs, D. Ferlemann, and S. Shenoi, "Wind farm security: Attack surface, targets, scenarios and mitigation," *Int. J. Crit. Infrastructure Protection*, vol. 17, pp. 3–14, Jun. 2017.

[30] J. Y. Siu and S. K. Panda, "A review of cyber-physical security in the generation system of the grid," in *Proc. IECON 46th Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2020, pp. 1520–1525.

[31] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo, W. Song, M. D. R. Greidanus, S. Sahoo, F. Blaabjerg, J. Zhang, L. Guo, B. Ahn, M. B. Shadmand, N. R. Gajanur, and M. A. Abbaszada, "A review of cyber–physical security for photovoltaic systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 10, no. 4, pp. 4879–4901, Aug. 2022.

[32] A. Jindal, A. K. Marnerides, A. Scott, and D. Hutchison, "Identifying security challenges in renewable energy systems: A wind turbine case study," in *Proc. 10th ACM Int. Conf. Future Energy Syst.*, Jun. 2019, pp. 370–372.

[33] F. Almutairy, L. Scekic, R. Elmoudi, and S. Wshah, "Accurate detection of false data injection attacks in renewable power systems using deep learning," *IEEE Access*, vol. 9, pp. 135774–135789, 2021.

[34] M. Ismail, M. F. Shaaban, M. Naidu, and E. Serpedin, "Deep learning detection of electricity theft cyber-attacks in renewable distributed generation," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3428–3437, Jul. 2020.

[35] N. Trantham and A. Garcia, "Reputation dynamics in networks: Application to cyber security of wind farms," *Syst. Eng.*, vol. 18, no. 4, pp. 339–348, Jul. 2015.

[36] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6816–6827, Nov. 2018.

[37] I. Gandhi, L. Ravi, V. Vijayakumar, and V. Subramaniyaswamy, "Improving security for wind energy systems in smart grid applications using digital protection technique," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102265.

[38] H. Jia, C. Shao, D. Liu, C. Singh, Y. Ding, and Y. Li, "Operating reliability evaluation of power systems with demand-side resources considering cyber malfunctions," *IEEE Access*, vol. 8, pp. 87354–87366, 2020.

[39] N. Fardad, S. Soleymani, and F. Faghihi, "Cyber defense analysis of smart grid including renewable energy resources based on coalitional game theory," *J. Intell. Fuzzy Syst.*, vol. 35, no. 2, pp. 2063–2077, Aug. 2018.

[40] S. Lee and J.-H. Huh, "An effective security measures for nuclear power plant using big data analysis approach," *J. Supercomput.*, vol. 75, no. 8, pp. 4267–4294, 2019.

[41] C. Lee, Y. Ho Chae, and P. H. Seong, "Development of a method for estimating security state: Supporting integrated response to cyber-attacks in NPPs," *Ann. Nucl. Energy*, vol. 158, Aug. 2021, Art. no. 108287.

[42] C. Lee, S. M. Han, Y. H. Chae, and P. H. Seong, "Development of a cyberattack response planning method for nuclear power plants by using the Markov decision process model," *Ann. Nucl. Energy*, vol. 166, Feb. 2022, Art. no. 108725.

[43] T. Krause, R. Ernst, B. Klaer, I. Hacker, and M. Henze, "Cybersecurity in power grids: Challenges and opportunities," *Sensors*, vol. 21, no. 18, p. 6225, Sep. 2021.

[44] H. Rahimpour, J. Tusek, A. Abuadbba, A. Seneviratne, T. Phung, A. Musleh, and B. Liu, "Cybersecurity challenges of power transformers," 2023, *arXiv:2302.13161*.

[45] R. Fan, J. Lian, K. Kalsi, and M. Elizondo, "Impact of cyber attacks on high voltage DC transmission damping control," *Energies*, vol. 11, no. 5, p. 1046, Apr. 2018.

[46] M. J. P. Jaghargh and H. R. Mashhadi, "Structural and behavioural evaluation of renewable energy power plants' impacts on transmission network congestion using an analytical approach," *IET Renew. Power Gener.*, vol. 14, no. 7, pp. 1164–1173, May 2020.

[47] Y. Dvorkin and S. Garg, "IoT-enabled distributed cyber-attacks on transmission and distribution grids," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2017, pp. 1–6.

[48] M. Ghafouri, M. Au, M. Kassouf, M. Debbabi, C. Assi, and J. Yan, "Detection and mitigation of cyber attacks on voltage stability monitoring of smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5227–5238, Nov. 2020.

[49] D. Wilson, Y. Tang, J. Yan, and Z. Lu, "Deep learning-aided cyber-attack detection in power transmission systems," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[50] A. Ahmed, V. V. G. Krishnan, S. A. Foroutan, M. Touhiduzzaman, C. Rublein, A. Srivastava, Y. Wu, A. Hahn, and S. Suresh, "Cyber physical security analytics for anomalies in transmission protection systems," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 6313–6323, Nov. 2019.

[51] S. Chakrabarty and B. Sikdar, "Detection of hidden transformer tap change command attacks in transmission networks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5161–5173, Nov. 2020.

[52] S. Pal, B. Sikdar, and J. H. Chow, "Classification and detection of PMU data manipulation attacks using transmission line parameters," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 5057–5066, Sep. 2018.

[53] Q. Yang, L. Jiang, W. Hao, B. Zhou, P. Yang, and Z. Lv, "PMU placement in electric transmission networks for reliable state estimation against false data injection attacks," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1978–1986, Dec. 2017.

[54] M. Dehghani, M. Ghiasi, T. Niknam, A. Kavousi-Fard, M. Shasadeghi, N. Ghadimi, and F. Taghizadeh-Hesary, "Blockchain-based securing of data exchange in a power transmission system considering congestion management and social welfare," *Sustainability*, vol. 13, no. 1, p. 90, Dec. 2020.

[55] F. Mohammadi and R. Rashidzadeh, "Impact of stealthy false data injection attacks on power flow of power transmission lines—A mathematical verification," *Int. J. Electr. Power Energy Syst.*, vol. 142, Nov. 2022, Art. no. 108293.

[56] C. Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," *Energy Rep.*, vol. 7, pp. 7999–8012, Nov. 2021.

[57] X. G. Shan and J. Zhuang, "A game-theoretic approach to modeling attacks and defenses of smart grids at three levels," *Rel. Eng. Syst. Saf.*, vol. 195, Mar. 2020, Art. no. 106683.

[58] M. Montakhabi, A. Madhusudan, S. van der Graaf, A. Abidin, P. Ballon, and M. A. Mustafa, "Sharing economy in future peer-to-peer electricity trading markets: Security and privacy analysis," in *Proc. Workshop Decentralized IoT Syst. Secur. (DISS)*, San Diego, CA, USA, 2020, pp. 1–6.

[59] A. Marufu, A. V. Kayem, and S. D. Wolthusen, "The design and classification of cheating attacks on power marketing schemes in resource constrained smart micro-grids," in *Smart Micro-Grid Systems Security and Privacy*. Cham, Switzerland: Springer, 2018, pp. 103–144.

[60] R. Dasgupta, A. Sakzad, and C. Rudolph, "Cyber attacks in transactive energy market-based microgrid systems," *Energies*, vol. 14, no. 4, p. 1137, Feb. 2021.

[61] A. Arman, V. V. G. Krishnan, A. Srivastava, Y. Wu, and S. Sindhu, "Cyber physical security analytics for transactive energy systems using ensemble machine learning," in *Proc. North Amer. Power Symp. (NAPS)*, Sep. 2018, pp. 1–6.

[62] Y. Zhang, V. V. G. Krishnan, J. Pi, K. Kaur, A. Srivastava, A. Hahn, and S. Suresh, "Cyber physical security analytics for transactive energy systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 931–941, Mar. 2020.

[63] P. Wang, K. Ma, J. Lian, and D. J. Hammerstrom, "On anomaly detection for transactive energy systems with competitive market," *Int. J. Electr. Power Energy Syst.*, vol. 128, Jun. 2021, Art. no. 106662.

[64] S. Fkaier, M. Khalgui, G. Frey, Z. Li, and J. Yu, "Secure distributed power trading protocol for networked microgrids based on blockchain and elliptic curve cryptography," *IET Smart Grid*, vol. 6, no. 2, pp. 175–189, Apr. 2023.

[65] S. Pal, S. Biswas, S. Sridhar, A. Ashok, J. Hansen, and V. Amatya, "Understanding impacts of data integrity attacks on transactive control systems," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2020, pp. 1–5.

[66] V. V. G. Krishnan, Y. Zhang, K. Kaur, A. Hahn, A. Srivastava, and S. Sindhu, "Cyber-security analysis of transactive energy systems," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo. (T&D)*, Apr. 2018, pp. 1–9.

[67] Q. Huang, T. E. McDermott, Y. Tang, A. Makhmalbaf, D. J. Hammerstrom, A. R. Fisher, L. D. Marinovici, and T. Hardy, "Simulation-based valuation of transactive energy systems," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 4138–4147, Sep. 2019.

[68] Y. Liu, S. Hu, and T.-Y. Ho, "Leveraging strategic detection techniques for smart home pricing cyberattacks," *IEEE Trans. Depend. Secure Comput.*, vol. 13, no. 2, pp. 220–235, Mar. 2016.

[69] Y. Song, Z. Yu, X. Liu, J. Tian, and M. Chen, "Isolation forest based detection for false data attacks in power systems," in *Proc. IEEE Innov. Smart Grid Technol. Asia (ISGT Asia)*, May 2019, pp. 4170–4174.

[70] S. H. Majidi, S. Hadayeghparast, and H. Karimipour, "FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid," *Int. J. Crit. Infrastruct. Protection*, vol. 37, Jul. 2022, Art. no. 100508.

[71] C.-C. Sun, D. J. Sebastian Cardenas, A. Hahn, and C.-C. Liu, "Intrusion detection for cybersecurity of smart meters," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 612–622, Jan. 2021.

[72] P. A. Giglou and S. N. Ravadanegh, "Defending against false data injection attack on demand response program: A bi-level strategy," *Sustain. Energy, Grids Netw.*, vol. 27, Sep. 2021, Art. no. 100506.

[73] S. Ahmadian, X. Tang, H. A. Malki, and Z. Han, "Modelling cyber attacks on electricity market using mathematical programming with equilibrium constraints," *IEEE Access*, vol. 7, pp. 27376–27388, 2019.

[74] J. Tao and G. Michailidis, "A statistical framework for detecting electricity theft activities in smart grid distribution networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 205–216, Jan. 2020.

[75] K. Yang, H. Wang, H. Wang, and L. Sun, "An effective intrusion-resilient mechanism for programmable logic controllers against data tampering attacks," *Comput. Ind.*, vol. 138, Jun. 2022, Art. no. 103613.

[76] P. Gope and B. Sikdar, "Privacy-aware authenticated key agreement scheme for secure smart grid communication," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3953–3962, Jun. 2018.

[77] P. Gope, "PMAKE: Privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid," *Comput. Commun.*, vol. 152, pp. 338–344, Feb. 2020.

[78] X. Lou, C. Tran, R. Tan, D. K. Y. Yau, Z. T. Kalbarczyk, A. K. Banerjee, and P. Ganesh, "Assessing and mitigating impact of time delay attack: Case studies for power grid controls," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 141–155, Jan. 2020.

[79] M. Attia, S. M. Senouci, H. Sedjelmaci, E.-H. Aglzim, and D. Chrenko, "An efficient intrusion detection system against cyber-physical attacks in the smart grid," *Comput. Electr. Eng.*, vol. 68, pp. 499–512, May 2018.

[80] M. R. C. Acosta, S. Ahmed, C. E. Garcia, and I. Koo, "Extremely randomized trees-based scheme for stealthy cyber-attack detection in smart grid networks," *IEEE Access*, vol. 8, pp. 19921–19933, 2020.

[81] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[82] S. Wu, Y. Jiang, H. Luo, and X. Li, "Deep learning-based defense and detection scheme against eavesdropping and typical cyber-physical attacks," in *Proc. CAA Symp. Fault Detection, Supervision, Saf. Tech. Processes (SAFEPROCESS)*, Dec. 2021, pp. 1–6.

[83] I. Aziz, H. Jin, I. Abdulqadder, Z. Hussien, Z. Abduljabbar, and F. Flaih, "A lightweight scheme to authenticate and secure the communication in smart grids," *Appl. Sci.*, vol. 8, no. 9, p. 1508, Sep. 2018.

[84] G. Tertytchny, N. Nicolaou, and M. K. Michael, "Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103121.

[85] D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F. J. Aparicio-Navarro, A. Argyriou, and H. Janicke, "A novel intrusion detection system against spoofing attacks in connected electric vehicles," *Array*, vol. 5, Mar. 2020, Art. no. 100013.

[86] A. O. Aluko, R. P. Carpanen, D. G. Dorrell, and E. E. Ojo, "Real-time cyber attack detection scheme for standalone microgrids," *IEEE Internet Things J.*, vol. 9, no. 21, pp. 21481–21492, Nov. 2022.

[87] B. Huang, M. Majidi, and R. Baldick, "Case study of power system cyber attack using cascading outage analysis model," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2018, pp. 1–5.

[88] N. Kumar, V. M. Mishra, and A. Kumar, "Smart grid security by embedding S-Box advanced encryption standard," *Intell. Autom. Soft Comput.*, vol. 34, no. 1, pp. 623–638, 2022.

[89] M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *J. Netw. Comput. Appl.*, vol. 209, Jan. 2023, Art. no. 103540.

[90] M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba, "TBSMR: A trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network," *Secur. Commun. Netw.*, vol. 2021, pp. 1–9, Apr. 2021.

[91] S. Sengan, V. Subramaniyaswamy, V. Indragandhi, P. Velayutham, and L. Ravi, "Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning," *Comput. Electr. Eng.*, vol. 93, Jul. 2021, Art. no. 107211.

[92] G. D. L. T. Parra, P. Rad, K.-K.-R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *J. Netw. Comput. Appl.*, vol. 163, Aug. 2020, Art. no. 102662.

[93] H. Wang, J. Ruan, Z. Ma, B. Zhou, X. Fu, and G. Cao, "Deep learning aided interval state prediction for improving cyber security in energy internet," *Energy*, vol. 174, pp. 1292–1304, May 2019.

[94] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Proc. Comput. Sci.*, vol. 185, no. 1, pp. 239–247, 2021.

[95] R. B. Benisha and S. R. Ratna, "Detection of data integrity attacks by constructing an effective intrusion detection system," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 11, pp. 5233–5244, Nov. 2020.

[96] T. M. Hoang, T. Q. Duong, H. D. Tuan, S. Lambotharan, and L. Hanzo, "Physical layer security: Detection of active eavesdropping attacks by support vector machines," *IEEE Access*, vol. 9, pp. 31595–31607, 2021.

[97] S. Sahoo, S. Mishra, J. C. Peng, and T. Dragicevic, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[98] Y. Taniguchi, H. Tsutsumi, N. Iguchi, and K. Watanabe, "Design and evaluation of a proxy-based monitoring system for OpenFlow networks," *Sci. World J.*, vol. 2016, pp. 1–10, Jan. 2016.

[99] Y. Huang, L. Jin, Z. Zhong, Y. Lou, and S. Zhang, "Detection and defense of active attacks for generating secret key from wireless channels in static environment," *ISA Trans.*, vol. 99, pp. 231–239, Apr. 2020.

[100] A. Tolba and Z. Al-Makhadmeh, "A cybersecurity user authentication approach for securing smart grid communications," *Sustain. Energy Technol. Assessments*, vol. 46, Aug. 2021, Art. no. 101284.

[101] M. Sirajuddin, C. Rupa, S. Bhatia, R. N. Thakur, and A. Mashat, "Hybrid cryptographic scheme for secure communication in mobile ad hoc network-based E-healthcare system," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–8, Jun. 2022.

[102] X. Xiang and J. Cao, "An efficient authenticated key agreement scheme supporting privacy-preservation for smart grid communication," *Electric Power Syst. Res.*, vol. 203, Feb. 2022, Art. no. 107630.

[103] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.

[104] A. A. Khan, S. Itoo, V. Kumar, M. Ahmad, and S. Jangirala, "Cryptanalysis and design flaws of anonymous ECC based self-certified key distribution scheme for smart grid," *Mater. Today, Proc.*, vol. 57, pp. 2185–2189, Jan. 2022.

[105] J. Srinivas, A. K. Das, X. Li, M. K. Khan, and M. Jo, "Designing anonymous signature-based authenticated key exchange scheme for Internet of Things-enabled smart grid systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 4425–4436, Jul. 2021.

[106] K. Mahmood, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Gener. Comput. Syst.*, vol. 88, pp. 491–500, Nov. 2018.

[107] C. Guo, X. Jiang, K.-K. R. Choo, X. Tang, and J. Zhang, "Lightweight privacy preserving data aggregation with batch verification for smart grid," *Future Gener. Comput. Syst.*, vol. 112, pp. 512–523, Nov. 2020.

[108] A. Braeken, P. Kumar, and A. Martin, "Efficient and provably secure key agreement for modern smart metering communications," *Energies*, vol. 11, no. 10, p. 2662, 2018.

[109] T. Chen, X. Yin, and G. Wang, "Securing communications between smart grids and real users; providing a methodology based on user authentication," *Energy Rep.*, vol. 7, pp. 8042–8050, Nov. 2021.

[110] P. M. Lima, L. K. Carvalho, and M. V. Moreira, "Confidentiality of cyber-physical systems using event-based cryptography," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 1735–1740, 2020.

[111] N. B. Samyuel and B. A. Shimray, "Securing IoT device communication against network flow attacks with recursive internetworking architecture (RINA)," *ICT Exp.*, vol. 7, no. 1, pp. 110–114, Mar. 2021.

[112] A. N. Nazarov and A. N. A. Koupaei, "An architecture model for active cyber attacks on intelligence info-communication systems: Application based on advance system encryption (AES-512) using pre-encrypted search table and pseudo-random Functions(PRFs)," in *Proc. Int. Conf. Eng. Telecommun. (EnT)*, Nov. 2019, pp. 1–5.

[113] M. A. Elakrat and J. C. Jung, "Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network," *Nucl. Eng. Technol.*, vol. 50, no. 5, pp. 780–787, Jun. 2018.

[114] E. Ahene, Z. Qin, A. K. Adusei, and F. Li, "Efficient signcryption with proxy re-encryption and its application in smart grid," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9722–9737, Dec. 2019.

[115] Z. Wang, Y. Liu, Z. Ma, X. Liu, and J. Ma, "LiPSG: Lightweight privacy-preserving Q-learning-based energy management for the IoT-enabled smart grid," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3935–3947, May 2020.

[116] I. A. Kamil and S. O. Ogundoyin, "EPDAS: Efficient privacy-preserving data analysis scheme for smart grid network," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 33, no. 2, pp. 208–217, 2021.

[117] G. K. Verma, P. Gope, and N. Kumar, "PF-DA: Pairing free and secure data aggregation for energy internet-based smart meter-to-grid communication," *IEEE Trans. Smart Grid*, vol. 13, no. 3, pp. 2294–2304, May 2022.

[118] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, "Cyber security framework for Internet of Things-based energy Internet," *Future Gener. Comput. Syst.*, vol. 93, pp. 849–859, Apr. 2019.

[119] P. M. Lima, M. V. S. Alves, L. K. Carvalho, and M. V. Moreira, "Security against communication network attacks of cyber-physical systems," *J. Control, Autom. Electr. Syst.*, vol. 30, no. 1, pp. 125–135, Feb. 2019.

[120] S. Aghapour, M. Kaveh, M. R. Mosavi, and D. Martín, "An ultra-lightweight mutual authentication scheme for smart grid two-way communications," *IEEE Access*, vol. 9, pp. 74562–74573, 2021.

[121] B. K. Sethi, A. Singh, D. Singh, and R. Misra, "Optimal energy m anagement of s mart b uildings under cyber attack," *Int. J. Energy Res.*, vol. 45, no. 14, pp. 19895–19908, Nov. 2021.

[122] S. M. Farooq, S. M. S. Hussain, and T. S. Ustun, "Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages," *IEEE Access*, vol. 7, pp. 32343–32351, 2019.

[123] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 580–589, Feb. 2019.

[124] P. Gope and B. Sikdar, "A privacy-aware reconfigurable authenticated key exchange scheme for secure communication in smart grids," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5335–5348, Nov. 2021.

[125] M. Tahavori and F. Moazami, "Lightweight and secure PUF-based authenticated key agreement scheme for smart grid," *Peer Peer Netw. Appl.*, vol. 13, no. 5, pp. 1616–1628, Sep. 2020.
[126] M. Kaveh and M. R. Mosavi, "A lightweight mutual authentication for smart grid neighborhood area network communications based on physically unclonable function," *IEEE Syst. J.*, vol. 14, no. 3, pp. 4535–4544, Sep. 2020.
[127] H. M. Ibrahim, H. Abunahla, B. Mohammad, and H. AlKhzaimi, "Memristor-based PUF for lightweight cryptographic randomness," *Sci. Rep.*, vol. 12, no. 1, pp. 1–18, May 2022.
[128] H. Kishimoto, N. Yanai, and S. Okamura, "An anonymous authentication protocol for the smart grid," in *Smart Micro-Grid Systems Security and Privacy*. Cham, Switzerland: Springer, 2018, pp. 29–52.
[129] M. Tanveer, A. U. Khan, H. Shah, A. Alkhayyat, S. A. Chaudhry, and M. Ahmad, "ARAP-SG: Anonymous and reliable authentication protocol for smart grids," *IEEE Access*, vol. 9, pp. 143366–143377, 2021.
[130] T. Limbasiya and A. Arya, "Attacks on authentication and authorization models in smart grid," in *Smart Micro-Grid Systems Security and Privacy*. Cham, Switzerland: Springer, 2018, pp. 53–70.
[131] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K.-R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *J. Parallel Distrib. Comput.*, vol. 132, pp. 242–249, Oct. 2019.
[132] D. Sadhukhan, S. Ray, M. S. Obaidat, and M. Dasgupta, "A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography," *J. Syst. Archit.*, vol. 114, Mar. 2021, Art. no. 101938.
[133] M. Qi and J. Chen, "Two-pass privacy preserving authenticated key agreement scheme for smart grid," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3201–3207, Sep. 2021.
[134] P. Gope, "Anonymous mutual authentication with location privacy support for secure communication in M2M home network services," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 1, pp. 153–161, Jan. 2019.
[135] V. Sureshkumar, S. Anandhi, R. Amin, N. Selvarajan, and R. Madhumathi, "Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3565–3572, Sep. 2021.
[136] A. Irshad, S. A. Chaudhry, M. Alazab, A. Kanwal, M. S. Zia, and Y. B. Zikria, "A secure demand response management authentication scheme for smart grid," *Sustain. Energy Technol. Assessments*, vol. 48, Dec. 2021, Art. no. 101571.
[137] S. Yu, K. Park, J. Lee, Y. Park, Y. Park, S. Lee, and B. Chung, "Privacy-preserving lightweight authentication protocol for demand response management in smart grid environment," *Appl. Sci.*, vol. 10, no. 5, p. 1758, Mar. 2020.
[138] N. Kumar, G. S. Aujla, A. K. Das, and M. Conti, "ECCAuth: A secure authentication protocol for demand response management in a smart grid system," *IEEE Trans. Ind. Informat.*, vol. 15, no. 12, pp. 6572–6582, Dec. 2019.
[139] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Comput. Electr. Eng.*, vol. 93, Jul. 2021, Art. no. 107209.
[140] W. Wang, H. Huang, L. Zhang, Z. Han, C. Qiu, and C. Su, "BlockSLAP: Blockchain-based secure and lightweight authentication protocol for smart grid," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1332–1338.
[141] M. Stănculescu, S. Deleanu, P. C. Andrei, and H. Andrei, "A case study of an industrial power plant under cyberattack: Simulation and analysis," *Energies*, vol. 14, no. 9, p. 2568, Apr. 2021.
[142] H. S. Cho and T. H. Woo, "Cyber security in nuclear industry—Analytic study from the terror incident in nuclear power plants (NPPs)," *Ann. Nucl. Energy*, vol. 99, pp. 47–53, Jan. 2017.
[143] M. Bahrami, M. Fotuhi-Firuzabad, and H. Farzin, "Reliability evaluation of power grids considering integrity attacks against substation protective IEDs," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1035–1044, Feb. 2020.
[144] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, "Consumer, commercial, and industrial IoT (in) security: Attack taxonomy and case studies," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 199–221, Jan. 2021.
[145] D. Tripathi, A. K. Tripathi, L. K. Singh, and A. Chaturvedi, "Towards analyzing the impact of intrusion prevention and response on cyber-physical system availability: A case study of NPP," *Ann. Nucl. Energy*, vol. 168, Apr. 2022, Art. no. 108863.
[146] S. Hossain-McKenzie, A. Chavez, N. Jacobs, C. B. Jones, A. Summers, and B. Wright, "Proactive intrusion detection and mitigation system: Case study on packet replay attacks in distributed energy resource systems," in *Proc. IEEE Power Energy Conf. Illinois (PECI)*, Apr. 2021, pp. 1–6.

NAVEEN TATIPATRI received the B.Tech. degree in electrical and electronics engineering and the M.Tech. degree in power systems from Jawaharlal Nehru Technological University (JNTU), Anantapur, Andhra Pradesh, India, in 2017 and 2020, respectively. He is currently pursuing the Ph.D. degree with the School of Electrical Engineering, VIT, Vellore. His research interests include transactive energy management systems and cyber security for communication channel attacks in power systems.

S. L. ARUN received the B.E. degree in electrical and electronics engineering from the Institute of Road and Transport Technology, Erode, India, in 2010, the M.Tech. degree in power systems from NIT Calicut, Kerala, India, in 2013, and the Ph.D. degree in electrical engineering from NIT Tiruchirappalli, India, in 2019. He is currently an Assistant Professor with the School of Electrical Engineering, VIT, Vellore, India. He has published many research papers in reputed international journals and international and national conferences. His research and teaching interests include smart grid technology, demand response, P2P energy transactions, cyber security for smart grid, power system analysis, operation and control, distributed generation, and micro-grid.