FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 383-392 | e-ISSN: 2347-470X

IoT Security Framework Optimized Evaluation for Smart Grid

Ranjit Kumar[1], Rahul Gupta[2], Sunil Kumar[3] and Neha Gupta[4]

[1]*Assistant Professor, Department of CSE, Maharaja Agrasen University, Baddi, Himachal Pradesh, India; ranjitpes@gmail.com*
[2]*Associate Professor, Department of EEE, Maharaja Agrasen University, Baddi, Himachal Pradesh, India; rahul@mau.edu.in*
[3]*Assistant Professor, Department of CSE, Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India; sunilkumar27@gjust.org*
[4]*Associate Professor, Chitkara University Institute of Engineering & Technology, Chitkara University, Rajpura, Punjab, India; neha.gupta@chitkara.edu.in*

***Correspondence:** ranjitpes@gmail.com;

ABSTRACT- Modern systems' needs may be satisfied by smart grid technologies. Since we frequently struggle to effectively manage security, the smart grid's capacity is frequently underutilized. Despite the fact that a variety of solutions have been offered for securing the smart grid, the problem still exists that no single solution can entirely protect the environment. We provide a protection architecture for the IoT-connected smart grid. The proposed framework to secure IoT devices for the smart grid includes three complementary approaches. By conducting a rigorous comparative analysis of our proposed solution alongside four existing models, we contribute to the ongoing discourse on bolstering the security infrastructure of the smart grid IoT environment. Our optimized evaluation provides valuable insights into the strengths, weaknesses, and unique attributes of each model, offering a comprehensive understanding of their respective applicability and efficacy within the intricate realm of sensor-based applications. Two testing configurations were used to evaluate the Threat Mitigation Framework. It demonstrated superior performance in recognizing attacks like XSS across all testing configurations. In each of the two test sets, we also assessed the device management functions, and we found that they accurately recognized and presented IoT for the smart grid controller.

Keywords: Internet of Things, IoT, Security, Threat, Smart Grid.

ARTICLE INFORMATION

Author(s): Ranjit Kumar, Rahul Gupta, Sunil Kumar and Neha Gupta;
Received: 25/04/23; **Accepted**: 22/08/23; **Published**: 30/04/2024;
E- ISSN: 2347-470X;
Paper Id: IJEER230411;
Citation: 10.37391/IJEER.120208
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-12/ijeer-120208.html

Publisher's Note: FOREX Publication stays neutral with regard to jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

By 2023, businesses and consumers are projected to use more than 25 billion IoT devices [1]. Nearly all forms of human life-related activities currently leverage IoT architecture. Doctors and other medical personnel frequently employ IoT devices to remotely monitor patients. Other industries, including transportation, employ the IoT in things like smart cars [2]. The smart city will enable seamless interaction between people, systems, and devices, providing a practical and simple manner for people to carry out daily duties. A part of the smart city is the "smart grid." In actuality, it is a key element of the smart city. IoT devices used in homes are more prevalent than those in industries like manufacturing and healthcare. The goal of the smart grid IoT, like any other IoT, is to make consumer lives simple and comfortable. The following categories can be used to group smart grid IoT devices:

a) Communication components, *e.g.*, smart meter
b) Transmission lines, *e.g.*, actuators
c) Outage sensor, *e.g.*, motion detectors
d) Smart power generator, *e.g.*, solar panel
e) Lighting devices, *e.g.*, smart bulb

Most of the IoT devices that are frequently used by consumers are included in the list above. But given how unstable this market is and how frequently new devices are created or released, it is anticipated that this list will expand significantly. Security is a crucial issue that affects IoT devices generally and smart grid IoT devices particularly. The majority of vendors of smart grid IoT devices ship their products with little to no security. Smart grid IoT users are primarily impacted by this problem. While building IoT devices for the healthcare and manufacturing industries, manufacturers must frequently adhere to stringent specifications and apply quality control or safety precautions. As opposed to that, because the risks are less well known or less severe, sellers of IoT devices do not have as many criteria or specifications for home consumer products. Customers of smart grids rarely consider security since the majority of them lack the technical know-how needed to understand the hazards associated with IoT devices and how they work.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 383-392 | e-ISSN: 2347-470X

Despite the convenience and ease these devices offer, Smart grid IoT devices signify a vast threat to grid [3]. The grid and its user could suffer very catastrophic consequences from inadequate security. According to [4] the following are the top 10 IoT dangers or vulnerabilities for 2018:

1.1 Insecurely of Network Services

This issue applies to IoT services that permit remote access and are used on IoT devices. Simply said, it's best to disable any services that aren't being used because doing so compromises the availability and integrity of data. We must make sure that the device doesn't have any unnecessary open ports, like port 80 or 443, that can expose it to the Internet in order to protect against this vulnerability. The attack scenarios of buffer overrun, fuzzing, DDoS, and DoS are depicted in the four pictures below.

1.2 Absence of Update Mechanism in term of Security

This has to do with the absence of anti-rollback features and unsecure firmware updates for devices. When a device fails to update its firmware securely, an attacker may exploit this failure and fool the device into updating. All required features have been upgraded using the attacker's code.

1.3 Use of Obsolete Components

Third-party libraries that are out of date or deprecated should not be used. Third-party libraries are rarely regularly updated or maintained, especially when they are made available by small businesses or individuals. As a result, if they are utilized in the development of an IoT device, they eventually develop vulnerable to different attacks that may not have been possible when they were first developed. If a third library is necessary, it should be provided by a credible company that consistently updates its software

2. IOT SECURITY ISSUES

Smart Grid technology emerges with vulnerabilities and impediments especially for securing information which is the most vital concern. There are various issues of smart grid that comprises with the following IoT security.

2.1 Issues with Intrusion Detection Protection

To detect all harmful activity within the smart grid environment, it is necessary to set up an intrusion detection and prevention system. The solution must be effective and perform at a corporate level while still being simple and adaptable enough to work with a normal smart grid controller.

The following requirements apply to our IDS/IPS for the smart grid [5]:

a) Without the requirement for the smart grid controller to intervene or operate anything, the system should run continuously monitoring the smart grid environment.
b) A typical, non-technical smart grid controller should feel at ease utilizing the system's straightforward and user-friendly user interface.
c) The system must identify both recent and old threats.
d) The system must operate effectively without having a significant impact on network performance.

2.2 Issues with Device Management

In smart grid IoT, we are primarily attempting to address the following issues:

a) Verifying that each device is an actual, authentic device that the smart grid controller has linked.
b) A fake device generated by an attacker in the smart grid network should be flagged if it is not known to be a real device.

2.3 Issues with Privacy of Data

The privacy of the smart grid controller is at danger in a smart grid setting. Despite the user-friendliness and convenience that smart grid IoT devices offer, they gather a variety of data, some of which may contain sensitive data about the smart grid controller [6]. Here are a few instances of these situations:

a) Smart meter technology keeps track of a user's bill, electricity usage, and completed payments. The device constructer can receive the information and sell it to third parties who will use it to market products and services to the consumer.
b) Smart meter has a GPS sensor that always detects the smart grid connected device's location.

3. RELATED WORKS AND SOME INTRODUCED TECHNIQUES

IoT device security and privacy have recently become the subject of investigation. Sivaraman et al. (2015) predicted that the threat to user privacy would grow as more IoT devices were available, so they developed a network-level solution that keeps an eye on the network and records any suspicious activity. Using the network-defined security method will solve their problem. Based on characteristics like device activity and others like privacy, authorization, and authentication must be addressed [7].

The myriad security challenges in a smart grid system call for measures to protect it from attack. Providing data availability to ensure that authorized users may access the data at any time; maintaining confidentiality to ensure us. A smart network that lacks even one of these essential components is susceptible to cyberattacks [8] The following are a few attacks:

(a) eavesdropping attack;
(b) a ruse attack;
(c) A replay attack;
(d) A message modification attack;
(e) Denial of service attacks;
(f) Malicious code attacks [9].

For the IoT utilized area network, Enhanced Secure Device Authentication was created by Shen and Ma (2017). The utility server holds the public key, while the SM and gateway each retain their own private keys. The smart meter transmits to it when they initially communicate. After receiving both requests, the Utility Server generates the Pair-Wise Key (PWK), decrypts the messages using the senders' public keys, and then delivers it

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 383-392 | e-ISSN: 2347-470X

to both the SM and the Gateway. From there, a secured channel using the PWK can be used for direct communication between the SPBM and Gateway. Nevertheless, it appears that the solution only applies to SMs and not to other IoT devices. Furthermore, while network monitoring and privacy protection are issues that complement authentication, the solution exclusively solves authentication in the IoT network.

A framework for safeguarding smart meters from cyberattacks was introduced by Liu et al. (2016). Their research revealed two key attacks. To create a peak energy load that finally overloads transmission systems, the initial attack manipulates power prices through cloud data [10]. The second attack manipulates power pricing to raise frequency fluctuation, which triggers generator trips as a safety measure and results in a blackout for the affected area. According to the authors, the approach identified 98% of cyberattacks [11]. Despite these successful outcomes, our system only defends against a small portion of possible smart grid attacks since it primarily focuses cyberattack against smart meters. These exploits allowed them to get around authentication. They provided a list of suggestions for safeguarding smart plugs, which include the following: (a) implementing an encrypted communication protocol, (b) the use of data integrity mechanisms, (b) establishing mutual authentication between plugs and servers, (c) monitoring traffic with an intrusion detection system, (d) identifying brute force attacks with anti-bot measures [5]. Despite the fact that their paper provides in-depth analysis of the smart plug vulnerability, runs a no. of attacks to evaluate universal solution.

IoT Network Monitor is an IoT security solution created by Jonsdottir et al. (2018). To protect the Internet of Things network, it carries out three main tasks: (a) scanning; (b) performing deep packet inspection; and (c) monitoring botnet [12] Deep packet inspection raises the system performance's processing cost, raising concerns despite the fact that this solution addresses the entire IoT environment and does not focus on a single device like other solutions do.

An IoT security solution based on attack graph generation was proposed by Zhang et al. (2019). They investigated how the IoT network and the applications that use it interact, and they evaluated the weaknesses in the authentication process. The network's weak points that are targets for attacks are then displayed on the attack graph [13]. Although the concept sounds novel and intriguing, it appears that how well the model produces correct graphs will determine how accurately attacks are detected.

A blockchain-based IoT security technique was put out by Abunaser and Alkhatib (2019). Blockchain is widely employed in many various sectors of the economy, including finance, software development, and the Internet of Things, among others. With blockchain technology, blocks of transactions are continuously added to a public ledger. Blockchain has the ability to secure IoTs using a distributed method. The entire chain is not occupied by a single PC or gadget. Attacks like man-in-the-middle and malicious attacks can't change the blockchain because it is immutable. The immutable record of IoT device history is another benefit of blockchain technology [14].

Here's a comparative analysis table described in *table 1* summarizing the key concepts covered and concepts not covered in the existing articles related to the security of smart grid IoTs that we provided:

Table 1. Comparative Analysis of the Existing Articles Related to the Security of Smart grid IoTs

Article	Key Concepts Covered	Concepts Not Covered
[15]	- Types of threats	- Countermeasure methods
	- Security requirements	- Detection techniques
[16]	- Defense methods	- Impact analysis
	- Detection techniques	
[17]	- Security methods	- Detection techniques
	- Countermeasure approaches	
[18]	- DoS/DDoS threats	- Existing countermeasures
	- Smart grid components	
[19]	- Confidentiality, integrity	- Methods to defend/prevent threats
	- Specific countermeasures	
[20]	- Threats on energy companies, metering networks	- Security vulnerabilities in traditional energy network
	- Security and privacy requirements	- Privacy considerations

4. ML ALGORITHMS IN THREAT MITIGATION FRAMEWORK IN SMART GRID

Mitigation mechanisms comprise lightweight encryption, IDS, sensor authentication, antijamming, and behavior analysis.

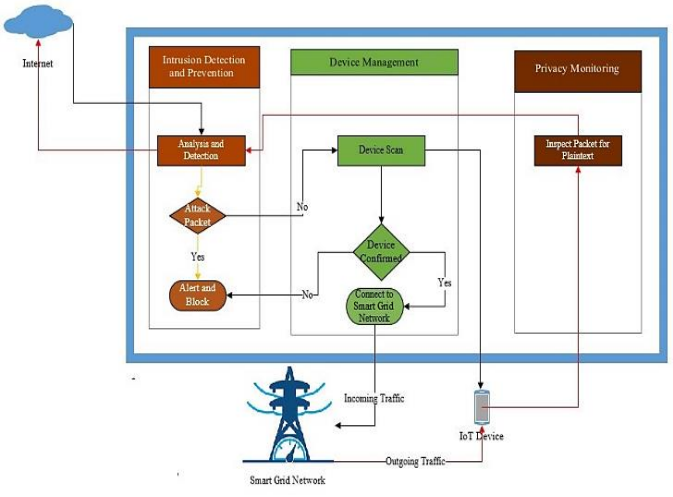

Figure 1: Conceptual Framework for Smart Grid Security Threats

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 383-392 | e-ISSN: 2347-470X

Figure 1 shows conceptual framework that can be used to guide the security advance of IoT smart grid architecture. Our framework can be used to detect the potential vulnerabilities and the applicable mitigation mechanism [21].

4.1 Support Vector Machines

In the 1990s, SVM gained popularity in machine learning since they were shown to be extremely effective. Support vector machines draw a line to categories two sets of points when utilized in a classification issue in machine learning. The line with the greatest distance between boundary line points within each group is discovered. The support vectors, on which the entire algorithm is predicated, are these two extreme points.

4.2 KSVM

To create a mapping function that increases the dimension, use the first option, Mapping to a Higher Dimension. Consider *figure 2*, which shows non-separable data points in a single dimension. Even with the following Equation, we are unable to completely detached all.

$$f = x - 5 \quad (1)$$

But if we square *equation 1*, we obtain *equation 2*, which yields *figure 3*. It is now obvious that the green and red points in *figure 3* can be linearly separated.

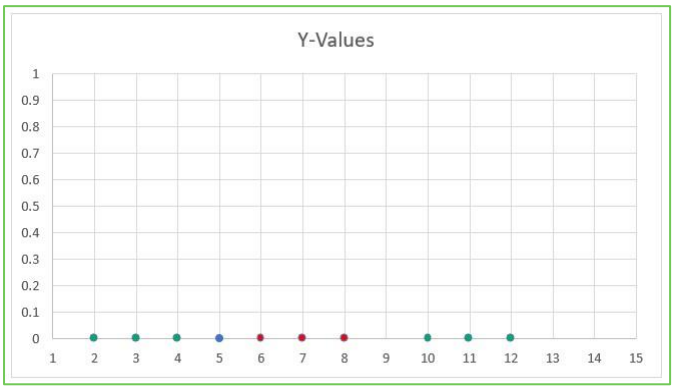

Figure 2: Separable Dataset if Not Linear

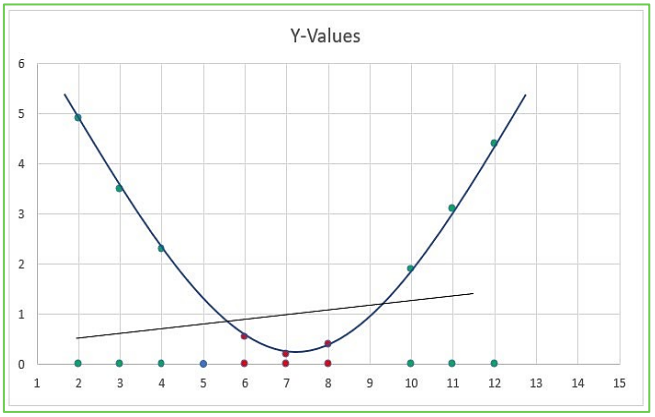

Figure 3: Separable Dataset if Linear

Increasing the dimensionality is the name of this strategy.

$$f = (x - 5) \wedge 2 \quad (2)$$

Equation 2 is the Squaring *equation 1*. In some circumstances, this procedure might be more difficult, but that is outside the purview of this study. Although this strategy seems to be effective, it also consumes a lot of resources.

4.3 KNN

A simple knowledge serves as the foundation for the K-Nearest Neighbors categorization method. Algorithm does follow:

1. Decide on K as the no. of neighbors. This is essentially a default value; however, 5 neighbors are a frequent choice.
2. Count the K Euclidean distance closest neighbors to the new data point. Although there are several ways to calculate distance, the Euclidean approach is the most popular.
3. Determine how many of these data points fit into each group. As an illustration, look at *figure 4*, where we have two green and three red.
4. Put the new data point in the group with the most neighbors. Given that we have more red neighbors; the new point is categorized as red in this instance.

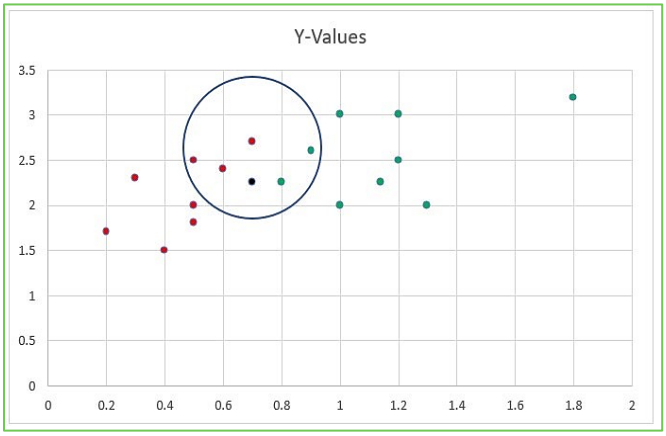

Figure 3: Classification Algorithm of K-Nearest Neighbors

Five of the new black point's neighbors are depicted in Figure 27 according to their Euclidean distance from it. Between Two Dots

$$ED = \sqrt{(x2 - x1)^2 + (y2 - y1)^2} \quad (3)$$

4.4 Logistic Regression (LR)

We can use a distinct type of regression called logistic regression to analyse data that has been distributed in a particular way. An example of a usual linear regression line is shown in *figure 5*.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 383-392 | e-ISSN: 2347-470X

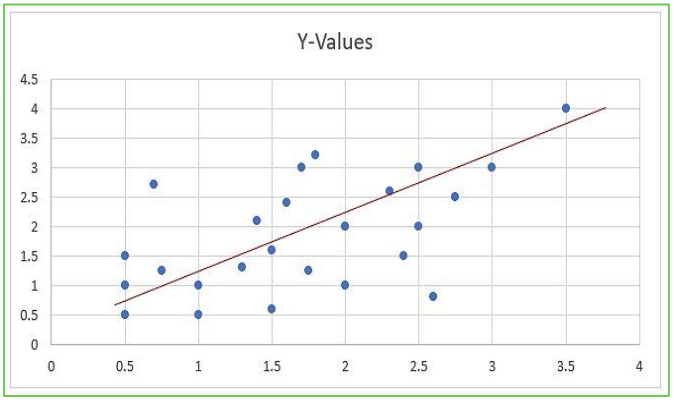

Figure 5: Usual Linear Regression

The following is the usual regression Equation for the above figure:

$$y = b0 + b1 * x \quad (4)$$

Consider the distribution below, where we would mail an offer to clients of various ages. Age is shown on the x-axis, while acceptance of the offer is represented on the y-axis as the dependent variable.

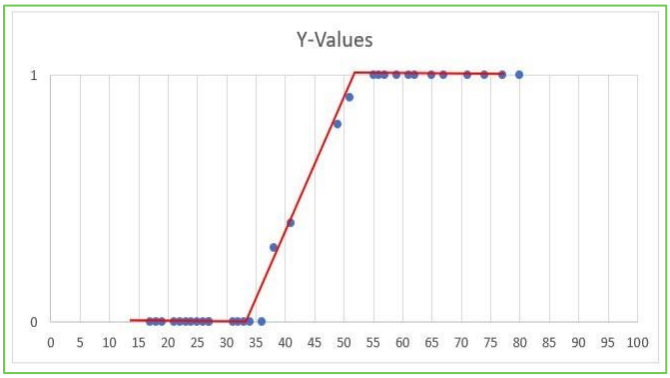

Figure 6: Classification Algorithm of Logistic Regression (LR)

A spreading of data for an offer we deliver to clients is shown in *figure 6* above. Customers' ages are shown on the x-axis, while acceptance of the offer (denoted by 1) or rejection (denoted by 1) are shown on the y-axis (denoted by 0). It is clear that this distribution does not lend itself to a linear regression.

Here,

$$p = \frac{1}{(1 + e^{-y})} \quad (5)$$

The logistic regression equation is then obtained by solving for y in the earlier equation.

$$\ln\left(\frac{p}{1-p}\right) = b0 + b1 * x \quad (6)$$

Figure 6's logistic regression clearly fits the data considerably better than linear regression would have.

4.5 Naïve Bayes

A supervised machine learning technique called the Naive Bayes classifier is centered on the Bayes Theorem, which is depicted in *equation 7* below.

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)} \quad (7)$$

where

P(A|B): The Posterior Probability

P(B|A): The Likelihood

P(A): The Prior Probability

P(B): The Margin Likelihood

Applying the Bayes Theorem to each scenario and comparing the results will allow us, for example, to establish if the designated x-designated black point below is a member of the red or green group of points. Given a certain point's characteristic, what is the probability?

So, as per situation:

As per situation 1:

$$P(Red|X) = \frac{3|10 * 10|30}{4|30} = 0.75$$

As per situation 2:

$$P(Green|X) = \frac{1|20 * 20|30}{4|30} = 0.25$$

We can see that 0.75 > 0.25 by comparing the two outputs, and as a result, the Naive Bayes classifier labels the black point *x* as red. *Figure 7* depicts Naive Bayes as a classifier.

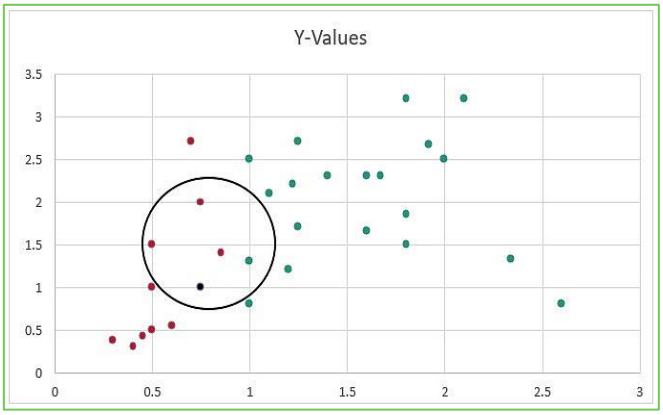

Figure 7: Classification Algorithm of Naive Bayes (NB)

4.6 Random Forest (RF)

RF is based on a machine learning concept called ensemble learning, which combines various machine learning techniques to accomplish a task more effectively. Several Decision Trees are used by Random Forest as part of a single large machine learning method. How Random Forest functions is explained in the next few steps:

a) Randomly selecting K.
b) Using these K data points, construct a decision tree.
c) Select decision tree for N.
d) Used for each N-tree of trees to predict a new data point's categorization, place the dot as receives the bulk of votes.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 383-392 | e-ISSN: 2347-470X

4.7 Decision Tree(DT)

It can be quite challenging to convey the mathematical concepts underlying decision trees for categorization.

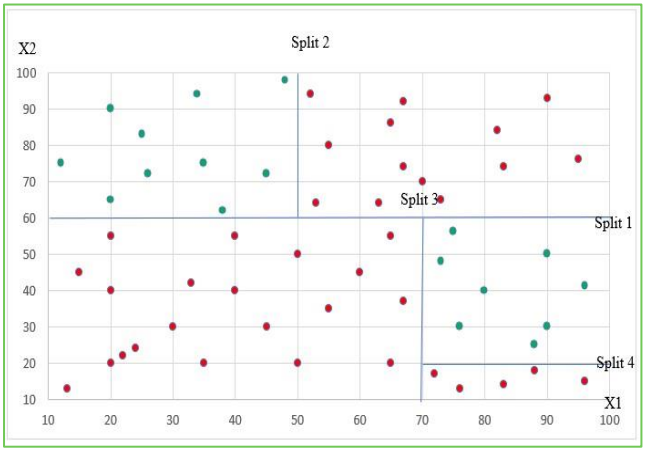

Figure 8: Dividing DT

Simply put, decision trees divide data into categories by conducting numerous splits until they reach the terminal leaves, where the categories are finalized. Decision trees are capable of classifying data from many groups. We choose two groups in the example below: a group in red and a group in green. According to *figure 8 and 9*.

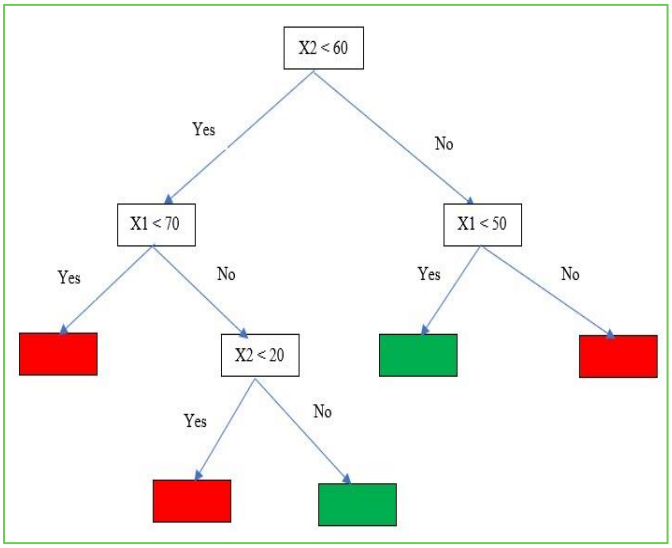

Figure 8: Constructing DT

5. METHODS

The framework is derived from the problem analysis as illustrated in *figure 10*. This framework focuses solely on employing the various encryption and machine learning techniques of threat tracing to the source, for a thorough, albeit challenging [22], but more effective way of countering the threats posed by the discovered threats.

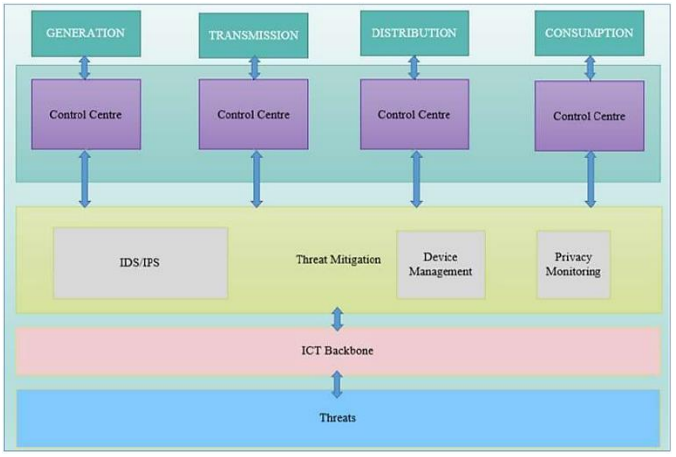

Figure 10: Derived Efficient Smart Grid Security Framework

Each of the seven techniques mentioned above section had to be turned into a machine learning model, and we had a 20% testing and an 80% training in order to train each model from CICID'17. *Table 2* depicts the comparison of various ML used Confusion Matrices.

Table 2. Comparison of various ML used Confusion Matrices

	SVM	KSVM	KNN	LR	NB	RF	DT
TP	30770	30994	31131	30914	18396	31147	31139
TN	1065	1100	1348	1015	1352	1351	1361
FP	378	154	17	234	12752	1	9
FN	303	268	20	353	16	17	7

In this paper, we compared our solution to four others that were created to safeguard the smart grid Internet of Things environment.

The following selection of evaluation with Threat Mitigation Framework:

a) Model of the WFS-IDS [23]
b) Model of the GA-SVM [24]
c) Model of the A-IDS [25]
d) Model of the Beget [26]

For the various smart grid applications that include sensors for the Internet of Things (IoT) and cyber-physical systems, there is an urgent need for advancements in security technology (CPS). One sort of framework does not suffice for all security applications in the majority of sensors used for sensing stimuli like pressure and temperature. Hence, many layers of protection for sensors become crucial.

6. RESULTS

To evaluate the performance of the security framework, we use precision, recall, F1-score and confusion matrix table metrics, which are defined as follow:

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 383-392 | e-ISSN: 2347-470X

Accuracy: Ratio of samples with accurate predictions How frequently is our classifier accurate, in other words?

$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN) \quad (8)$$

Precision: How frequently does the classifier succeed in predicting true values?

$$\text{Precision} = TP / (TP + FP) \quad (9)$$

Recall: Likewise called sensitivity. The proportion of correctly predicted positive samples to all positive samples.

$$\text{Recall} = TP / (TP + FN) \quad (10)$$

F-Measure: Likewise known as F-Score or F1. The model is most valuable when recall and precision are balanced. contemplates both recall and precision.

$$F - \text{Measure} = 2 * (\text{Recall} * \text{Precision}) / (\text{Recall} + \text{Precision}) \quad (11)$$

Where,

TP: This value represents the proportion of normal samples that the model correctly identified as normal. It is referred to as True Positive.
TN: Correctly classified as attacks for no. of sample. It is referred to as True Negative.
FP: Mistakenly detected as attacks for no. of sample that is normal. It is referred to as False Positive.
FN: Mistakenly detected as normal for no. of sample that is attack. It is referred to as False Negative.

The comparison of Threat Mitigation Framework conducted using software features of Python that is an interpreted language with a design philosophy that prioritizes code readability. CICIDS2017 DDoS dataset was used to compare Threat Mitigation Framework with the other four models. *Table 3* presents the test results in detail. *Table 3* clearly demonstrates that the Threat Mitigation Framework model lags behind the Beget model in detecting True Negatives and WFS-IDS and GA-SVM in recognizing True Positives.

Table 3. Comparison of Confusion Matrixes for TMF and Alternative Solutions

	TMF	WFS-IDS	GA-SVM	A-IDS	Beget
TP	37,551	38,138	37,942	17,186	2,453
TN	51,147	49,102	49,550	51,111	51,206
FP	1,572	1,038	1,044	21,944	36,438
FN	28	2,020	1,762	57	201

Threat Mitigation Framework came in first for identifying False Negatives but came in third for identifying False Positives, trailing only GA-SVM and WFS-IDS. Threat Mitigation Framework, however, performed better than all models while recognizing more TP + TN combinations and less FP + FN combinations. This demonstrates unequivocally that TMF outperforms the other four models.

Table 4 demonstrates that the Threat Mitigation Framework performed better than further models since it had the highest matrices scores. The model's lightness is quantified by the running time comparison. We computed the time the model required for both training and testing and the average running time was determined ten times for the training and testing phases.

Table 4. Evaluation Statistically of Compared TMF

Matrices	TMF	WFS-IDS	GA-SVM	A-IDS	Beget
Accuracy	.9824	.9662	.9689	.7563	.5943
Precision	.9994	.9498	.9557	.9968	.9244
Recall	.9599	.9735	.9733	.4393	.0632
F-Measure	.9792	.9615	.9644	.6098	.1182

This was done to be more precise. running comparison between training and testing time for the five models in *table 3* reveals that TMF fared better than the other four models. The running time is measured in sec. *Figure 11* shows comparison of Running Time among five model including TMF.

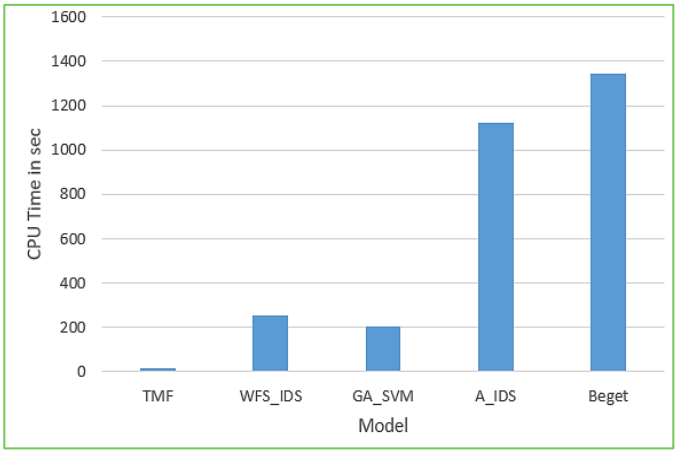

Figure 11: Running Time Comparison

In the above article, we conducted a comprehensive comparative analysis of existing security approaches for smart grid IoT and introduce the novel Threat Mitigation Framework (TMF) as a promising solution through *table 5*.

Table 5. Existing Model Comparison with TMF

Feature	Existing	TMF
IoT Security Focus	Traditional Approaches	Machine Learning-based
Threat Mitigation	Limited to Known Patterns	Adaptive & Dynamic
Device Management	Basic Device Listing	Intelligent Device Analysis
Modes of Operation	N/A	Single & Dual Modes
Virtual Testing	Not Mentioned	Simulated Attack Scenarios
Quantification of Attacks	Not Detailed	Attack Proportion Analysis

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 383-392 | e-ISSN: 2347-470X

6.1 Mode I: Simulated in a Virtual Setting for Attack XSS

By introducing malicious code into a website, XSS attacks function. As most websites demand that users leave JavaScript turned on, XSS attacks are fairly popular [27]. We used the XSSER simulation tool, which is pre-installed in Kali Linux, to model XSS attacks.

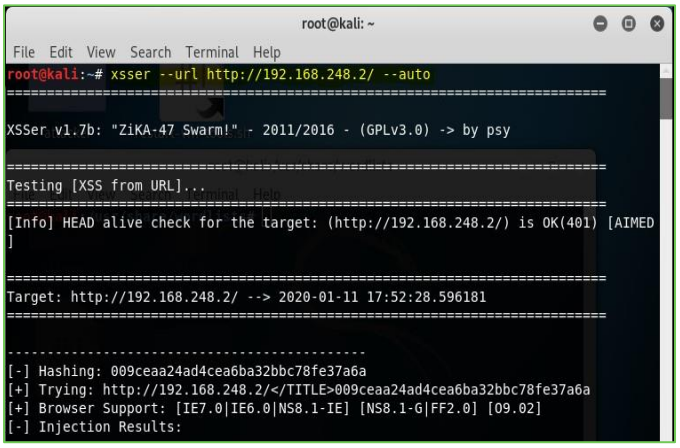

Figure 12: Performing XSS Attacks using XSSER

Figure 13: Displaying the Impact of the XSS Attack having Tool XSSER

As a result, since the tool already offers the answer, we do not need to record and count the no. of packets that Threat Mitigation Framework has classified as an attack. *Figure 12* depicts the command Performing XSS Attacks using XSSER.

Figure 13 depicts the Displaying the Impact of the XSS Attack, XSSER tool was unable to identify a vulnerability.

6.2 Mode II: Simulated XSS Attacks in a Virtual Setting with RPi

Using Kali's installed XSSER attack tool, we conducted five simulations of Cross Site Scripting (XSS) attacks against the smart grid router.

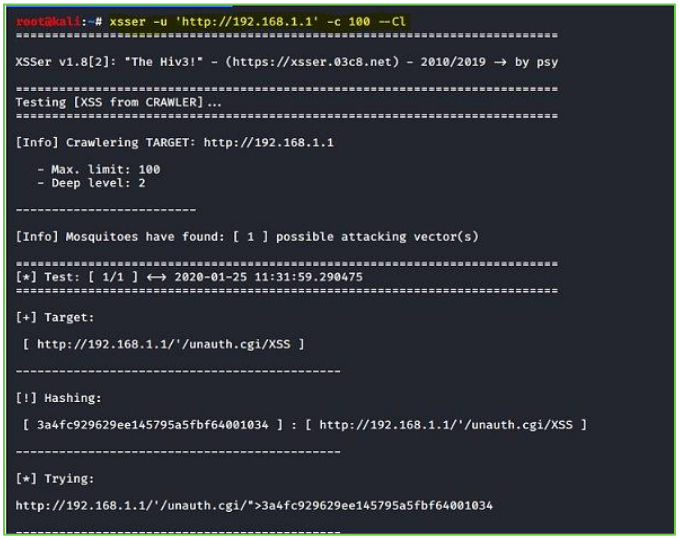

Figure 14: Mode II: XSSER Sending XSS Attacks on RPi

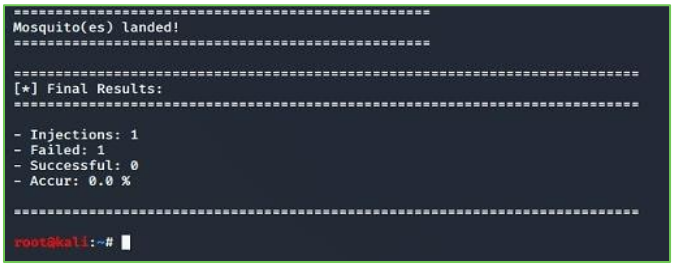

Figure 15: Mode II: Demonstrating XSS Attack Is Not Successful

The test results demonstrated that Threat Mitigation Framework accurately identified XSS threats. A screenshot of an XSS attack sent by XSSER is shown in *figure 14*. *Figure 15* demonstrates that the XSS attack failed

7. DISCUSSIONS

Concerning all introduced machine learning approaches from above section with the gained knowledge of the data characteristics, in this work, an efficient framework will be pursued. The two Threat Mitigation Framework modes are contrasted in this section, along with each mode's advantages and disadvantages. In each of the two TMF modes, the Device Management technique operates slightly differently. For instance, the configuration could block the attacker's IP address when in mode I but not for other. Router set up with Threat Mitigation Frameworks can record packets delivered from the attacker to the victim in that scenario and label them as attacks because they are mode I with the flow [28]. The virtual setting is first and foremost a more regulated environment. All traffic sources can be blocked, leaving just simulation attacks launched through attacker tools. This manner, we can be certain that every packet is an attack and determine the quantity or proportion of attacks vs normal packets. Second, we can create two networks in a virtual Setting: an internal network that houses the Threat Mitigation Framework and the victim system, and attacker system.

A comparison of TMF *Mode I* and *Mode II* is shown in Table 6.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 383-392 | e-ISSN: 2347-470X

Table 6. TMF Mode I vs. Mode II Comparison

TMF Mode I	TMF Mode II
○ Integrated inside a router or other device, such as a Raspberry Pi, in direct. ○ Functions as an IPS, which can identify and stop threats before warning the user. ○ Prevents suspected harmful activity from gaining access to networks for smart grids.	○ Put on a non-traffic-oriented device, like a Raspberry Pi, and ○ Identify risks and notify the user of them. ○ If malicious behaviour is found, immediate alarms are sent. ○ Virus tracking to assess how it is spreading via systems (if discovered).

Above *table 5* highlights the importance of a well-controlled and regulated virtual environment in evaluating the Threat Mitigation Framework. By focusing on simulation attacks and creating network segments, researchers can gain deeper insights into the framework's behavior, responsiveness, and adaptability. This approach enhances the accuracy of assessing the TMF's performance and its ability to handle different modes of operation, ultimately contributing to the development of an efficient and robust security framework for IoT-based smart grid systems.

8. CONCLUSIONS

In conclusion, the Internet of Things (IoT) has emerged as a significant player in delivering online automated services to millions of users through various organizations. As the adoption of IoT continues to grow, customers are increasingly seeking more advanced security features to enhance the smart grid IoT paradigm. This demand is driven by the desire for greater traceability, automation, and security while maintaining cost-effectiveness.

This paper introduced the Threat Mitigation Framework (TMF) as a robust security system designed to cater to non-technical smart grid controllers. The TMF comprises three key techniques that collectively enhance the security of the smart grid network. The first technique, Device Management, constitutes the initial section of the TMF. It involves scanning the smart grid network and presenting a user-friendly GUI interface to list all connected devices [29]. This empowers the user, who may lack technical expertise, to review and identify any devices that they consider unauthorized or suspicious. This level of control enables the user to disconnect devices that pose potential security risks.
The second technique leverages an Intrusion Detection and Prevention System (IDS/IPS) approach, utilizing the Decision Tree machine learning classification algorithm [30]. This method actively monitors the network for any signs of attacks, aiming to detect and mitigate threats in real-time. By employing machine learning, the system can adapt and improve its threat detection capabilities over time.

The third technique, known as "Privacy Monitoring," focuses on safeguarding the confidentiality of data transmitted within the smart grid network. It achieves this by monitoring the content of packet payloads sent in plaintext. Upon detecting any plaintext data, the system alerts the smart grid controller, granting them the authority to disconnect the transmission if it is deemed a security concern.

Collectively, the Threat Mitigation Framework (TMF) offers a comprehensive approach to securing the smart grid IoT paradigm for non-technical users. Its three techniques – Device Management, IDS/IPS with machine learning, and Privacy Monitoring – address different aspects of security, enabling enhanced protection, detection, and response capabilities. As the IoT landscape continues to evolve, solutions like TMF play a pivotal role in ensuring the integrity, reliability, and security of smart grid systems.

Two testing scenarios were used to evaluate the Threat Mitigation Framework. Threat Mitigation Framework outdone the WFS-IDS, GA-SVM, A-IDS, and Beget models, as explained in the method section [31].

The scope of the article will focus on improving TMF's usability, particularly the requirement for a self-trained system. In order to anticipate future threats, the Threat Mitigation Framework should be able to learn from fresh data and train itself. Many algorithms might be combined with other Deep Learning techniques. This would eliminate the requirement for manually training the algorithm and manually updating the training dataset. Future research will focus on creating a completely automated system that can educate and train itself [32]. Establishing reliable simulation tools for threats recognizing and retort, for a stable system, as well as providing more palatable models for handling security risks to the Smart Grid by basis cataloging for the required resiliency, may be considered in future study.

9. ACKNOWLEDGMENTS

We sincerely acknowledge Maharaja Agrasen University for providing access to various subscribed online databases which are very helpful for this paper.

REFERENCES

[1] Jovanovic, B., 2021. Internet of things statistics for 2021 - taking things apart [WWW Document]. Internet of Things statistics for 2021 - Taking Things Apart. URL https://dataprot.net/statistics/iot-statistics/
[2] P. H., F., J., J., 2021. A review on the feasibility of deployment of renewable energy sources for electric vehicles under Smart Grid Environment. International Journal of Electrical and Electronics Research 9, 57–65.
[3] Baig, Z.A., Amoudi, A.-R., 2013. An analysis of smart grid attacks and countermeasures. Journal of Communications 8, 473–479.
[4] OWASP, 2018. OWASP Internet of Things Project, *28/09/2018*, *64* (9), 2489–2509.
[5] Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., Fu, X., 2017. Security vulnerabilities of internet of things: A case study of the smart plug system. IEEE Internet of Things Journal 4, 1899–1909.
[6] Sivaraman, V., Gharakheili, H.H., Fernandes, C., Clark, N., Karliychuk, T., 2018. Smart IOT devices in the home: Security and privacy implications. IEEE Technology and Society Magazine 37, 71–79.
[7] Sivaraman, V., Gharakheili, H.H., Vishwanath, A., Boreli, R., Mehani, O., 2015. Network-level security and Privacy Control for smart-home IOT devices. 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).
[8] Ali, M.H., Al Mohammed, B.A., Ismail, A., Zolkipli, M.F., 2018. A new intrusion detection system based on fast learning network and particle swarm optimization. IEEE Access 6, 20255–20261.

International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 12, Issue 2 | Pages 383-392 | e-ISSN: 2347-470X

[9] Ul Rehman, S., Manickam, S., 2016. A study of smart home environment and its security threats. International Journal of Reliability, Quality and Safety Engineering 23, 1640005.
[10] Gupta, N., Gupta, K., Rani, S., Koundal, D., Zaguia, A., 2021. Smart Architecture Energy Management through dynamic BIN-packing algorithms on cloud. Symmetry 13, 2298.
[11] Huang, H., Khalid, R.S., Liu, W., Yu, H., 2017. A fast online sequential learning accelerator for IOT network intrusion detection. Proceedings of the Twelfth IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis Companion.
[12] Kumar, A., Sharma, S., Goyal, N., Singh, A., Cheng, X., & Singh, P. (2021). Secure and energy-efficient smart building architecture with emerging technology IOT. Computer Communications, 176, 207–217.
[13] Zhang, Y., Li, P., Wang, X., 2019. Intrusion detection for IOT based on improved genetic algorithm and deep belief network. IEEE Access 7, 31711–31722.
[14] AbuNaser, M., Alkhatib, A.A.A., 2019. Advanced survey of blockchain for the internet of things smart home. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT).
[15] Gunduz, M.Z., Das, R., 2020. Cyber-security on Smart Grid: Threats and potential solutions. Computer Networks 169, 107094.
[16] Mantri, A., Dutt, S., Gupta, J. P., & Chitkara, M., 2008. Design and evaluation of a PBL-based course in Analog Electronics. IEEE Transactions on Education, 51(4), 432–438.
[17] Komninos, N., Philippou, E., Pitsillides, A., 2014. Survey in Smart Grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials 16, 1933–1954.
[18] Gupta, B.B., Akhtar, T., 2017. A survey on Smart Power Grid: Frameworks, tools, security issues, and solutions. Annals of Telecommunications 72, 517–549.
[19] Li, X., Liang, X., Lu, R., Shen, X., Lin, X., Zhu, H., 2012. Securing Smart Grid: Cyber-attacks, countermeasures, and challenges. IEEE Communications Magazine 50, 38–45.
[20] Kumar, P., Lin, Y., Bai, G., Paverd, A., Dong, J.S., Martin, A., 2019. Smart Grid Metering Networks: A survey on security, privacy and open research issues. IEEE Communications Surveys & Tutorials 21, 2886–2927.
[21] Dubey, G.P., 2021. Investigating the impact of feature reduction through information gain and correlation on the performance of error back propagation based ids. International Journal of Electrical and Electronics Research 9, 27–34.
[22] Kumar, R., Gupta, R., Kumar, S., 2022. IOT security on Smart Grid: Threats and mitigation frameworks. ECS Transactions 107, 14623–14630.
[23] Li, Y., Wang, J.-L., Tian, Z.-H., Lu, T.-B., Young, C., 2009. Building lightweight intrusion detection system using wrapper-based feature selection mechanisms. Computers & Security 28, 466–475.
[24] Tao, P., Sun, Zhe, Sun, Zhixin, 2018. An improved intrusion detection algorithm based on Ga and SVM. IEEE Access 6, 13624–13631.
[25] Aljawarneh, S., Aldwairi, M., Yassein, M.B., 2018. Anomaly-based Intrusion Detection System through feature selection analysis and building hybrid efficient model. Journal of Computational Science 25, 152–160.
[26] Jan, S.U., Ahmed, S., Shakhov, V., Koo, I., 2019. Toward a lightweight intrusion detection system for the internet of things. IEEE Access 7, 42450–42471.
[27] Farraj, A., Hammad, E., Kundur, D., 2018. A distributed control paradigm for smart grid to address attacks on data integrity and availability. IEEE Transactions on Signal and Information Processing over Networks 4, 70–81.
[28] Ni, Z., Paul, S., 2019. A multistage game in Smart Grid Security: A reinforcement learning solution. IEEE Transactions on Neural Networks and Learning Systems 30, 2684–2695.
[29] Goyal, M., Dutta, M., 2018. Intrusion detection of Wormhole attack in IOT: A Review. 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET).
[30] Teng, L., Teng, S., Tang, F., Zhu, H., Zhang, W., Liu, D., Liang, L., 2014. A collaborative and adaptive intrusion detection based on SVMS and decision trees. 2014 IEEE International Conference on Data Mining Workshop.
[31] Srikantha, P., Kundur, D., 2016. A der attack-mitigation differential game for Smart Grid Security Analysis. IEEE Transactions on Smart Grid 7, 1476–1485.
[32] Abdullayev, V., Bhadouria, R.P., 2020. Overview of the conversion of traditional power grid to internet energy. International Journal of Electrical and Electronics Research 8, 36–39.