iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.51963

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Cybersecurity Enhancement of Transformer Differential Protection

Annapoorani [1], Sampath R[2], Mohan. M[3], Srijayan. M[4]
[1]*Assistant Professor, Master of Computer Application, Paavai Engineering College, Namakkal, India.*
[2,3,4,] *PG Students , Master of Computer Application, Paavai Engineering College, Namakkal, India*

Abstract: ***The increasing use of information and communication technologies (ICT) in the operational environments of power grids has been essential for operators to improve the monitoring, maintenance, and control of power generation, transmission, and distribution; however, this has come at the expense of increasing the grid's exposure to cyber threats. This paper looks at cyberattack scenarios that target protective relays in substations, which can be the most important part of protecting power systems from abnormal conditions. The overall performance of the power grid could suffer significantly if the relays' operations are disrupted, possibly resulting in widespread blackouts. Utilizing the potential of machine learning to detect anomalous behavior in transformer differential protective relays, we investigate methods for improving substation cybersecurity. In order to find cyberattacks, the proposed method looks at operational technology (OT) data from the substation current transformers (CTs). Power frameworks recreation utilizing OPAL-RTHYPERSIM is utilized to create preparing informational collections, to simulate the cyberattacks and to evaluate the network safety enhancement capability of the proposed AI calculations. Terms in the index include differential protective relays, transformers, operational technology, cyber physical systems, and machine learning.***

Keywords: Optimization, Material Removal Rate, Surface Roughness.

I. INTRODUCTION

Over the course of the past ten years, the R APID implementation of interoperable and standard ICT in power systems has raised significant cybersecurity concerns among power utilities and regulatory agencies .This is principally on the grounds that the security-by-haziness reasoning utilized as a protective technique for restrictive ICT in power frameworks has become out of date in the arising standard and interoperable ICT worldview of brilliant networks .To address the developing network safety concerns, the North American Electric Dependability Partnership has laid out and authorized Basic Framework Insurance (CIP)
principles. Utilities are required by the CIP standards to identify, classify, and safeguard cyber assets that are crucial to the dependable operation of the bulk electric system . However, the cybersecurity measures and tools that should be developed to enhance the assets' cyber-resiliency are not outlined in the CIP standards. In order to develop cybersecurity measures and tools for cyber assets in power systems, a variety of standards and initiatives have been launched by National Standard Institutes (ISA) , research institutes (EPRI) , and government agencies (DOE) .

In light of recent successful cyberattacks on Ukrainian power infrastructures , the digitalization of power grids over the past ten years has increased the number of cyberattack surfaces across a variety of grid components and made cybersecurity enhancement of its assets, such as substation protective relays, a top priority for utilities and regulatory agencies. In a substation, defensive transfers structure the most basic guarded element of force framework against unusual conditions . As a result, their improper operations that are the result of cyberattacks may have significant effects on power systems, such as widespread blackouts.

II. SELECTION OF MATERIAL

We consider a substation mechanization plot that utilizes the IEC 61850 conventions GOOSE and SV for correspondence between defensive transfers and blending units. The simple estimations produced by the ongoing transformers CT1 and CT2 in Fig. 1 are combined into SV packets by combining units MU1 and MU2. The differential protective relay's GOOSE commands shown in Fig. 1 are passed on to the consolidating units MU1 and MU2 to set off activities separately on the circuit breakers CB1 and CB2.
The differential relaying is a powerful relaying principle that can be used for any asset like transformers, lines, buses, and so forth. The differential protective relays are designed to measure the geometrical difference between electrical quantities in particular current measurements and operate when the difference goes beyond a certain threshold.

©IJRASET: All Rights are Reserved

In either case, even if there are no physical faults, erroneous current measurements cause the differential protective relay to go off and de-energize the transformer. Despite the fact that substation and control center operators observe the transformer tripping, they cannot re-energize the transformer before conducting a comprehensive utility-based investigation into the cause. Having machine learning algorithms for anomaly detection would offer a preventative measure against cyberattack-caused differential protective relay malfunctions.

III. CYBERATTACK SCENARIOS

In the second scenario (referred to as Scenario), an attacker gains remote access to the substation process bus through the use of stolen legitimate operator credentials and a remote connection to the substation communication network. The attacker then performs false data injection attack by injecting falsified SV packets on the process bus forcing the differential protective to misoperate.

In both scenarios, falsified current measurements trigger the differential protective relay and de-energize the transformer in the absence of physical faults. Although substation and control center operators observe the transformer tripping, they would not be able to re-energize the transformer before performing a comprehensive investigation about the reason behind transformer tripping based on utility guidelines. Having machine learning algorithms for anomaly detection would provide a mitigation strategy to prevent differential protective relay misoperation caused by cyberattacks.Table.2. Levels of Input Parameters

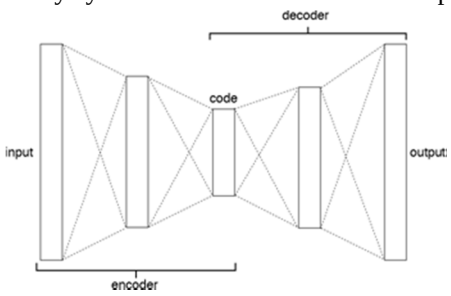


Fig.1. Autoencoder structure

IV. WORKING OF EDM

In either case, even if there are no physical faults, erroneous current measurements cause the differential protective relay to go off and de-energize the transformer. Despite the fact that substation and control center operators observe the transformer tripping, they cannot re-energize the transformer before conducting a comprehensive utility-based investigation into the cause. Having machine learning algorithms for anomaly detection would offer a preventative measure against cyberattack-caused differential protective relay malfunctions.

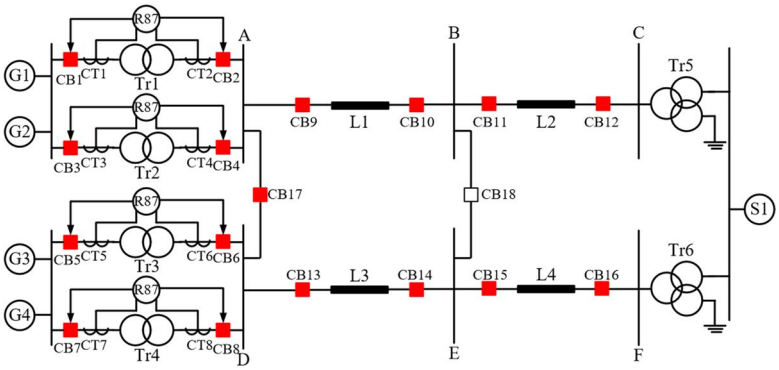


Fig.2.The IEEE PSRC D6 benchmark test system.

Cyberattacks are extremely uncommon in power systems, and attacks on power systems are uncommon. This is consistent with the literature's assumption regarding anomaly detection systems. Since the autoencoder has not been prepared on information containing cyberattacks, we conjecture that reproductions of odd estimations happening during assaults may not be remade well As a result, we intend to detect erroneous measurements that may indicate cyberattacks by employing a threshold of the autoencoder reconstruction error.

A. Test Framework

Fig. The IEEE power system relaying committee (PSRC) D6 benchmark test system is depicted in Figure 3 [29, 30]. A power plant with four generators G1G4 that are connected to the main grid via a 500 kV transmission system is the benchmark test system. The 500kV transmission framework comprises of four transmission lines L1-L4 and the fundamental matrix is demonstrated as a boundless transport S1. The power plant transformers Tr1-Tr4 are safeguarded by differential defensive transfers.

B. Preparing Informational Index

We utilized OPAL-RT HYPERSIM to carry out and reproduce PSRC D6 test framework and create the informational index for AI. In 50 MW steps, the generators G1-G4's operating points are changed between 200 MW and 400 MW. The three-stage inner shortcoming of the transformer Tr1 is simulated for 16 starting times chosen at random to guarantee that faults occur at various parts of the current waveforms. This equates to a thousand simulations.

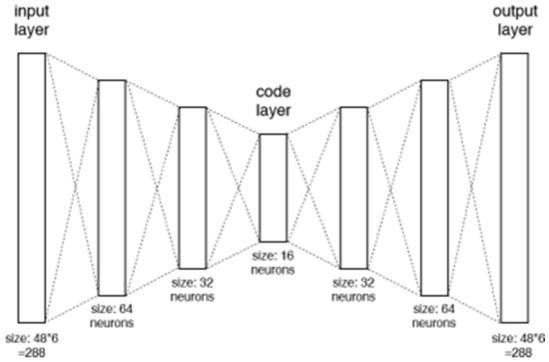


Fig. 4. Proposed Fully Connected Autoencoder Structure

V. EXPERIMENTAL WORK

Sets In the real world, attacks are rare and the anomaly detection data is heavily skewed. We have 2000 simulation data sequences to test, as we mentioned. We replace 100 of the sequences in each scenario with malicious data sequences to create an imbalanced data set. as was mentioned in Section II. B: Two possible cyberattacks on the transformer differential protective relay are taken into consideration. The aforementioned cyberattack scenarios serve as the basis for the generation of malicious data sequences. The differential protective relay on the transformer is triggered by scaling the current measurements from the current transformer CT1 in scenario 1. In Situation 2, the ongoing estimations from current transformer CT1 are supplanted by bogus information.

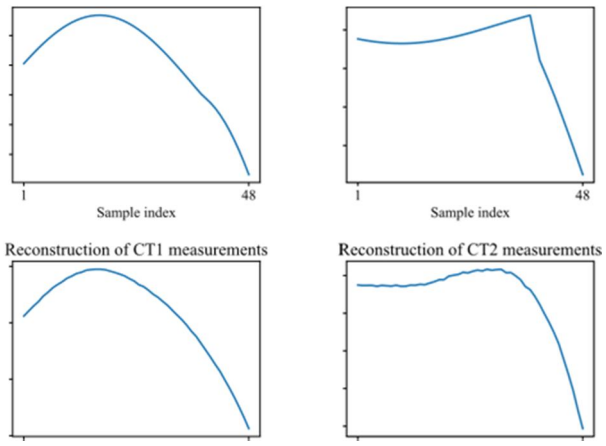


Fig. 5. During a physical fault in the transformer, reconstruction of phase

Fig.3. EDM spark

As will be covered in more detail later, three distinct values of the spark producing current (Ip), two different values of the thickness of the copper flat (t), and three different values of the pulse on duration (Ton) were selected in this case.

According to the diagram, the semiautomatic die-sinking machine has a dielectric rotational system with a filter, a pump, and a container for dielectric fluid. System for servo control and power development unit. Device for fixing electro-magnetic jobs that has a tank for a fully submerged workpiece in dielectric fluid while cleansing the outside.

The fully connected autoencoder's performance can be measured using the following two metrics: precision and recall.

A term "True Positive" refers to erroneous data that the fully connected autoencoder correctly identifies. Data from three-phase transformer faults that have been mistakenly classified as anomalous are represented by the False Positive status. Anomalies in the data that are determined to be transformers are represented by False Negative.

The Architecture of the Fully Connected Autoencoder, as depicted in Fig. 4 Data has been flattened to a vector size of (window size) (count of features) = 48.6 for the input layer. Subsequently, we have input layer of size 288, and yield layer with a similar size. The code size has been set to estimate 16. There are two hidden encoder/decoder layers in the autoencoder. There are 64 neurons in the encoder's hidden layers and 32 neurons in the decoder's hidden layers, respectively.

We analyzed various qualities for every boundary to tune hyper-boundaries of the autoencoder as summed up in Table I. The boundaries that delivered the most reduced approval blunders are chosen. It is important that the approval blunders are not revealed here for brevity. All layers use the Relu activation function, with the exception of the final layer, which uses the linear activation function. Further optimization uses the Adam Optimizer. The rate of learning is set to 0.01. The fact that we implemented the autoencoder using the Tensorflow and Keras libraries is noteworthy.

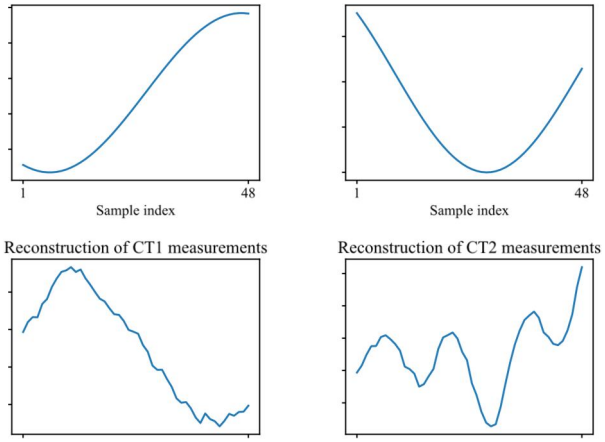


Fig. 5. During a physical fault in the transformer, reconstruction of phase
A current measurements from CT1 and CT2.

The parameters that have the fewest validation errors are selected. For the sake of conciseness, it is essential that the approval errors not be revealed here. With the exception of the final layer, which employs the linear activation function, all layers utilize the Relu activation function. The Adam Optimizer is used for further optimization. The learning rate is set to 0.01. It is noteworthy that we utilized the Tensorflow and Keras libraries to implement the autoencoder.

Parameter Values	Parameter Values
Learning rate {0.01, 0.001}	Learning rate {0.01, 0.001}
Hidden layers in the encoder/decoder {1, 2, 3, 4, 5}	Hidden layers in the encoder/decoder {1, 2, 3, 4, 5}
Neurons in the first hidden layer {32, 64, 128}	Neurons in the first hidden layer {32, 64, 128}

Table I
Parameter Values Examined For Hyper-Parameter Selection

VI. EXPERIMENTAL RESULT

The fully connected autoencoder has been put through its paces with the two cyberattack scenarios outlined in Section II.B. The autoencoder execution is analyzed for various changes in current estimation sizes. Current measurement scaling from 1.1 to 5 is thought about and tested. With 100 percent accuracy and recall, the fully connected autoencoder was able to identify the attacks. It is important that the autoencoder becomes dynamic when the get component of the differential defensive hand-off identifies an actual shortcoming on the transformer and becomes dynamic. In this manner, the autoencoder is equipped for recognizing and obstructing the irregular current estimations. Although this mitigation strategy can identify the source of a cyberattack before it causes differential protective relay misoperation and transformer false tripping, it cannot detect and prevent cyberattacks.

Fig. 6 shows an illustration of stage An ongoing estimations recreation for CT1 and CT2 during cyberattacks on MU1 utilizing an inventory network assault. As depicted in Figure, 6, with a high degree of error, the autoencoder reconstructs the phase A current measurements from CT1 and CT2.

The false data injection attacks were identified by the autoencoder with 100% accuracy and recall. This scenario employs a mitigation strategy that is comparable to that which was considered for Scenario 1.

Fig. Phase A current measurements reconstruction for CT1 and CT2 during false data injection cyberattacks is shown in Figure 7. As depicted in Figure, 7, the autoencoder recreates the stage An ongoing estimations from CT1 and CT2 with high blunder

In the subsequent situation (alluded to as Situation 2), an aggressor acquires remote admittance to the substation cycle transport using taken genuine administrator qualifications and a distant association with the substation correspondence organization. Following that, the attacker launches a false data injection attack by injecting forged SV packets onto the process bus, which causes the differential protective relay to malfunction.

In either case, even if there are no physical faults, erroneous current measurements cause the differential protective relay to go off and de-energize the transformer. Despite the fact that substation and control center operators observe the transformer tripping, they cannot re-energize the transformer before conducting a comprehensive utility-based investigation into the cause. Having AI calculations for oddity identification would give a moderation procedure to forestall differential defensive hand-off misoperation brought about by cyberattacks.

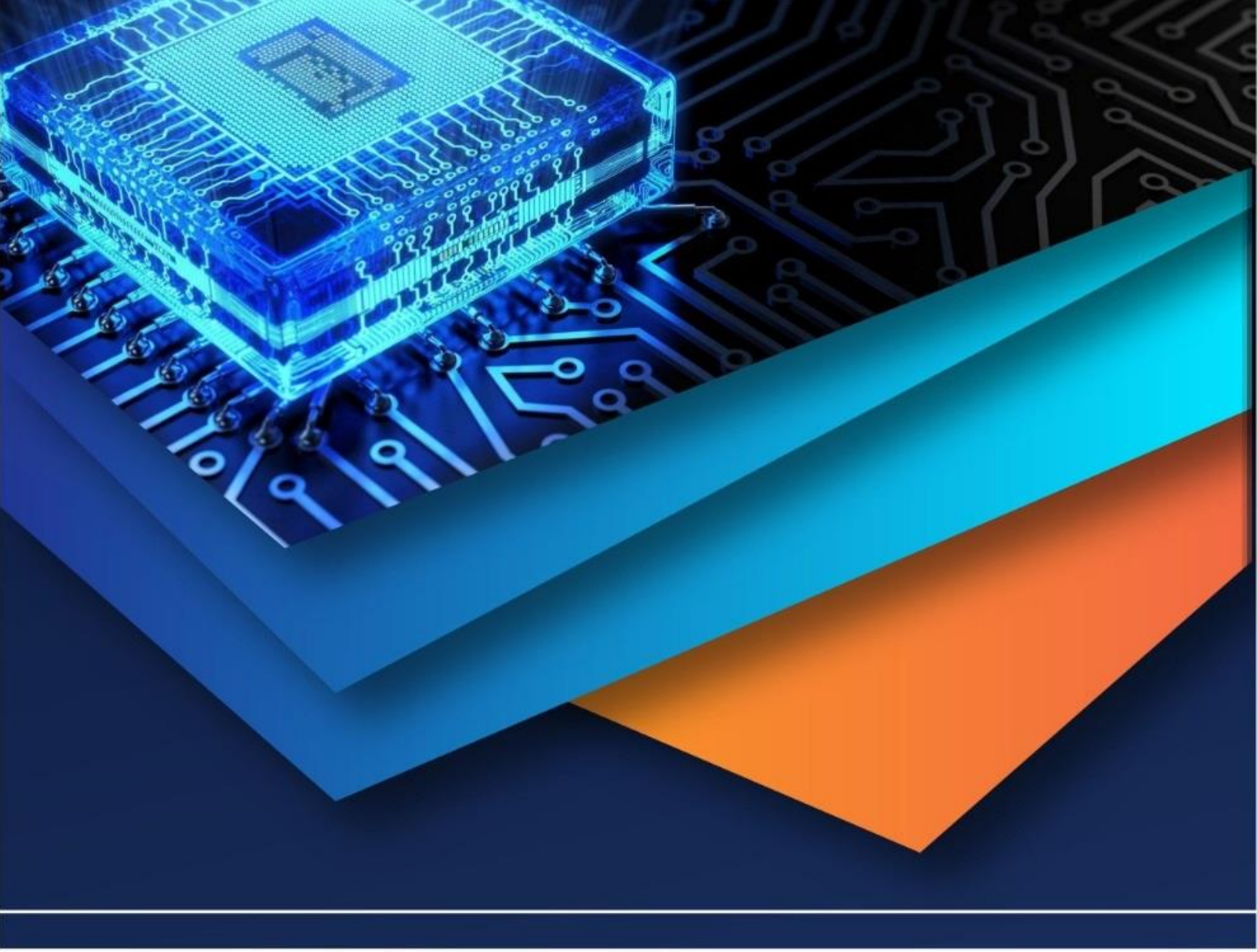
VII. CONCLUSION

Machine learning was used in this paper to improve the cybersecurity of transformer differential protective relays. A completely associated autoencoder is prepared utilizing sliding windows of 10-ms made out of the ongoing estimations at each side of the transformer. At each side of the transformer, the sliding windows contain 48 SV single-phase current measurements, or 144 SV three-phase current measurements. The informational indexes utilized for the autoencoder preparing are produced and documented involving OPAL-RT HYPERSIM for various working places of the test framework under review. After that, two distinct scenarios of a cyberattack are detected and mitigated using the proposed autoencoder. The simulation results show that the proposed machine learning algorithm is capable of detecting and preventing cyberattacks against transformer differential protective relays with high performance. While these outcomes are extremely reassuring, further exploration ought to research a bigger scope of situations to more readily grasp the scope of conditions where autoencoders perform well.

REFERENCES

[1] G. N. Ericsson, "Power system communication and cyber security: Fundamental pieces of a brilliant network foundation," IEEE Trans. Vol. Power Del. 25, no. 3, pp. 1501-1507, Jul. 2010.
[2] S. Ward and others, Concerns regarding protective relays' cyber security; c1 working gathering individuals from power framework transferring board," In Proc. IEEE Electric Power Soc. Gen. Conv., July 2007, pages 1-8.
[3] North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standards, http://www.nerc.com.
[4] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," NIST SP 800-82, 2015.
[5] E. Smith, S. Corzine, D. Racey, D. Patrick, H. Colin, and J. Weiss, "Going past network safety consistence," IEEE Power Energy Mag., vol. 14, no. 5, pp. 48-56, Sep. 2016.
[6] ISA99, Modern Computerization and Control Frameworks Security. As of August 2016,
[7] "Creating Security Metrics for the Electric Sector," December 2015, Electric Power Research Institute
[8] Roadmap to Achieve Energy Delivery Systems Cybersecurity, 2011, Department of Energy
[9] Multiyear Plan for Energy Sector Cybersecurity, 2018 from Department of Energy
[10] "Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case," by R. M. Lee, M. J. Assante, and T. Conway, Electricity-Information Sharing and Analysis Center (E–ISAC), March 2016.
[11] An Attack's Anatomy by J. Slowik: Defeating and Detecting CRASHOVERRIDE, a White Paper from Dragos Inc., October 2018.
[12] Blackburn, T. D. J., Protective Relaying: 4th ed., Principles and Applications CRC Press, 2014.

[13] Design, Modeling, and Evaluation of Protective Relays for Power Systems, by M. Kezunovic, J. Ren, and S. Lotfifard, Springer International Publishing, 2006.
[14] "Power system risk assessment in cyber attacks considering the role of protection systems," IEEE Trans., X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li. Vol. Smart Grid 8, no. 2, pp. 572–580 March 2017.
[15] M. Bahrami, M. Fotuhi-Firuzabad and H. Farzin, "Dependability assessment of force lattices considering respectability assaults against substation defensive IEDs," IEEE Exchanges on Modern Informatics, early access.
[16] A. Abiri-Jahromi, A. Kemmeugne, D. Kundur and A. Haddadi, "Cyberphysical assaults focusing on correspondence helped security plans," IEEE Trans. Power Control, early access 2019.
[17] IEEE Trans., “An intrusion detection system for IEC61850 automated substations,” by U. K. Premaratne, J. Samarabandu, and T. S. Sidhu. Vol. Power Del. 25, pp. 2376–2383, Oct. 2010.
[18] J. Hong et al., " Distance protection against cyberattacks and control of circuit breakers for digital substations,” IEEE Trans. Indust. Inform., vol. 15, no. 7, pp. 4332–4341, July 2019.
[19] SA. Ameli, A. Hooshyar, and E. F. El-Saadany, "Improvement of a cyberresilient line current differential hand-off," IEEE Trans. Indust. Inform., vol. 15, no. 1, pp. 305–318, Jan. 2019.
[20] IEEE Trans., "Anomaly detection for cybersecurity of the substations," by C. W. Ten, J. Hong, and C. C. Liu. Vol. Smart Grid 2, no. 4, pp. 865-873, Dec. 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)