International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-10, August 2020

Detection of Cyber-Attack in Broad-Scale Smart Grids using Deep and Scalable Unsupervised Machine Learning System

Simran Koul, Simriti Koul, Prajval Mohan, Lakshya Sharma, Pranav Narayan

Abstract*: The increase in the reliability, efficiency and security of the electrical grids was credited to the innovation of the smart grid. It is also a fact that the smart grids a very dependable on the digital communication technology that in turn gives rise to undiscovered weaknesses which have to be reconsidered for dependable and coherent power distribution. In this paper, we propose an unsupervised anomaly detection which is mainly focused the statistical correlation among the data. The main aim is to create a scalable anomaly detection system suitable for huge-scale smart grids, which are capable to denote a difference between a real fault from a disruption and an intelligent cyber-attack. We have presented a methodology that applies the concept of attribute extraction by the use of Symbolic Dynamic Filtering (SDF) to decrease compilation drift whilst uncovering usual interactions among subsystems. Results of simulation obtained on IEEE 39, 118 and 2848 bus systems confirm the execution of the method, proposed in this paper, under various working conditions. The results depict a precision of almost 99 percent, along with 98 percent of true positive rate and less than 2 percent of false positive rate.

***Keywords*: Anomaly, cyber-attack, smart grid, statistical property, machine learning, unsupervised learning**

I. INTRODUCTION

The present power frameworks comprise of a system of sensors and attached generators which permit two-way interaction inside the framework's network along with production of reliable energy through combination of Distributed Energy Resources (DERs) with Advanced Metering Infrastructure (AMI). While this complicated interaction framework has enormous lead, by positively enhancing dependability, efficiency, and feasibility, it expands the framework's vulnerabilities relating to cyber-attacks because of the gigantic number of gadgets and nodes that work outside the conventional regulatory domain. Since the flops in the power grid in turn leads to calamitous occurrences, it is profoundly critical to examine the impacts of cyber-attacks in a power framework. As recorded in [1], absence of framework recognition is the primary cause in the North American power outages, which feature the significance of cyber-attacks analysis to keep up a stable and authentic performance of the power supply. A cyber-attack can bring about overcharge that will harm the tools, or fake request demand that surely brings about loads of energy created. Furthermore, a mischievous attack can likewise cause fake negatives, i.e., fake overburden condition within a power framework. Different interruptions in various parts of the smart grid, electric automobile foundation is additionally feasible. It is appeared in [2-3] that vindictive attacks through obstructive interactions with a gadget can stop facilities in small computers. Subsequently, constant cyber-attack detection is fundamental for the dependable execution of the basic foundation including smart grids. Uninterrupted and active framework surveying is a prerequisite to identify intended cyber-attacks and accomplish attack flexibility.

Usually, every sensor in a huge-scale network is the primary objective of security concessions. An undermined insider can without much of a stretch access data stored in a compromised node. In principle, key disavowal of any compromised node is feasible by applying a verification system to sensor systems. Be that as it may, confirmation approaches dependent on cryptography or security computing, for example, the one portrayed in [5-6], are not conceivable because of the compilation and storage limitations of the framework. The existing theories inside the smart power grid primarily concentrate on the systems administration security of the cyber components, propelled anomaly detection strategies, and safeguard control conjecture dependent on various state estimation methods.

In spite of the fact that the previously mentioned solutions are able to immunize the power frameworks, greater part of them are numerically costly, genuinely unreasonable and not versatile for enormous scope complex system. These days, enormous measure of information is produced everywhere throughout the grids which gives increasing access for real-time framework supervising.

Revised Manuscript Received on August 30, 2020.
* Correspondence Author
Simran Koul* School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India. E-mail: simran.koul@yahoo.com
Simriti Koul School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India. E-mail: simriti.koul@yahoo.com
Prajval Mohan School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India. E-mail: prajval.mohan23@gmail.com
Lakshya Sharma School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India. E-mail: lakshya99sh@gmail.com
Pranav Narayan School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. E-mail: pranavnarayan79@gmail.com

Investigating this information enormously upgrades the supervision of performance, diagnosis, and predictability of anomaly in complicated frameworks. Authentic information depicting the framework's tasks can help recognize anomalies and possible attacks.

Notwithstanding, customary Bad Data Detection (BDD) strategies are most certainly not arranged for issues brought by executional and storage due to the large volume of information produced in the smart grid. These challenges open up the chance of utilizing data analytical strategies, for example, Machine Learning (ML), to handle complicated structure of datasets with AI to distinguish and avert cyber-attacks. Machine learning algorithms can be utilized to investigate different blends of data through states, AMI, and control steps by learning their patterns. It can identify False Data Injection (FDI) attack by understanding the nonlinear, complicated connection between data. This should be possible along these lines to fruitful methods applied to another power framework issues as found discovered research survey [7]. There are restricted theories on the utilization of Machine learning towards the cyber security of the smart grids. Many machine learning algorithms are examined and differentiated in [8] for uncovering of FDI attacks. General interpretations were concluded the accomplishment of machine learning in grouping FDI attacks. It was proposed by [10] a blend of interruption detection strategy dependent on customary path mining technique to distinguish unusual power framework occasions from PMU data, transfers, and energy management system (EMS) logs. A cyber-attack identification methods dependent on the relationship among two PMU limitations utilizing Pearson correlation coefficient as utilized in [11]. This strategy broke down the variation in correlation among two PMU limitations utilizing Pearson correlation coefficient. Authors in [12] used Gaussian procedure joined with ML to display the attack methodology for anomaly recognition. The identification of a cyber-deception attack taking place during the state estimation process was proposed by an administered ML-based strategy. A deep learning technique which detected significant aspects of FDI attacks in current scenarios is also mentioned in [14]. Implementation of the current, information- driven attack identification strategies can be enhanced utilizing Probabilistic Graphical Models (PGM) to demonstrate complicated framework execution. Among PGMs, Dynamic Bayesian Networks (DBN) are instruments that are helpful as they have the ability to represent complex frameworks advancing in time utilizing the usual connections within framework modules. In addition, new strategies ought to be created to deal with the complicated and great dimensional data to keep up the strength, scalability and precision of the attack identification schemes. To diminish the executional load in huge datasets, attribute extraction can be utilized to change the initial aspects into a much more important portrayal by rebuilding its inputs and it includes diminishing the measure of resources required [15-16]. Identification methods that don't depend on training information which are grouped beforehand are necessary, as there exist anomalies which can't be estimated or generated.

In this paper, an anomaly recognition technique for smart grid is proposed to draw out the samples of transformations in FDI attack. The uncovered features are utilized to identify the attacks in current scenario. Symbolic Dynamic Filtering (SDF) is utilized to fabricate an executional productive element extraction program to find usual communications among the smart grids subsystems via DBN. Mutual Information (MI), DBN and developing techniques are utilized to identify inconspicuous cyber-attacks dependent on free energy as the anomaly token. Our objective is to apprehend reliabilities among factors through linking of a directional energy to every factor, which serves as an extent of concord. The flexibility of this method is analyzed on different IEEE test frameworks which was demonstrated on PSS/E program. The outcomes show extensive precision and less of false alarm under various functioning conditions. It ought to be referenced that the presented technique doesn't just depends on the similar routines followed while training the data sets yet it additionally utilizes the theory of free energy to distinguish among the level of energy in the attack and day-to-day data sets. In this manner, even unknown and inconspicuous attack can be recognized.

The principle benefactions of this paper are as per the following:

• Creation of an unsupervised outlook to identify an anomaly in smart grids with no need of naming datasets.

• Presenting an adaptable technique by decreasing executional load via data reduction by SDF.

• Creating a solid model with learning ability dependent on DBN.

• Presenting an outlook without a specific model that can be utilized in hierarchical and topological networks for various attack situations.

Now, the paper is composed as follows: Numerical definitions are depicted in Section II. Presented cyber-attack recognition technique is introduced in Section III. Section IV talks about the case investigations and simulation results followed by the conclusion in Section V.

II. MATHEMATICAL REPRESENTATION

A. Generator's Model

In this model, smart grid is demonstrated as a multi-operator, digital physical framework where every one of these operators incorporate a generator, an estimation gadget, an administered control operator, also, a storage for energy framework that can infuse or assimilate actual power in the framework. The dynamic and static positions of the framework are portrayed as follows:

$$x = f(x,u,n) \quad \text{.....(1)}$$

$$z = h(x,u,w)$$

where,

x →framework's state which includes both the static and dynamic states of the network

f →non-linear and dynamic performance of the generators

h →estimation of the non-linear function

u → outputs vectors

z →measurement vectors

The 4th order of the two axis representation of the generator I's can be depicted as follows:

$\delta_i = \Omega_s \Delta\omega_i$

$\dot{\omega_i} = \omega_s/(2H_i)\,(P_{Mi} - P_{Ei} - D_i\Delta)$

$$E_{qi} = 1/(T_{di}')\,(-E_{qi} - (X_{di} - X_{di}')) + V_{fi}) \quad \ldots.(2)$$

$$E_{di}' = 1/(T_{qi}')\,(-E_{di}' + (X_{qi} - X_{qi}')I_{qi})$$

$$E_{qi}' = V_{qi} + R_{ai}I_{qi} + X_{di}' I_{di}$$

$$E_{di}' = V_{di} + R_{ai}I_{di} - X_{qi}' I_{qi}$$

Where,

δ→ rotor angle

$\Delta\omega$→rotor speed

Ω_s→frequency of the system

D→damping coefficient

E_d'→transient electromotive force in d-axis

E_q'→transient electromotive force in q-axis

V_f→ field voltage

H→machine inertia constant/unit

I_d, I_q→stator current of d- and q-axis

R_a→armature resistance

X_d, X_q→reactance of d- and q-axis

X_d', X_q'→transient reactance of d- and q-axis

T_d' , T_q' →open loop time constant of d- and q-axis

P_E→torque of electrical output

P_M→torque of mechanical input

In the case of synchronous generator i, the field voltage is controlled by the excitation system, and the associated speed governor controls the mechanical torque. However, the electrical output is as follows:

$$P_{Ei} = E_{di}' I_{di} + E_{qi}' I_{qi} + (X_{qi}' - X_{di}') \quad \ldots (3)$$

Let the integral voltage of generator i be denoted as Ei, then PEi can be denoted as [18]:

$$PEi = \sum_{(k=1)}^{N} [\![|Ei||Ek|]\!]\,(Gik\cos(\delta i - \delta k) + Bik\sin(\delta i - \delta k)) \quad \ldots(4)$$

Where,

$B_{ik} = B_{ki}$ is the susceptance between generators i and k

$G_{ik} = G_{ki}$ is the conductance between the generators i and k

In our paper, the main objective is the prediction of the dynamic behavior of smart grid to recognize the anomaly or cyber-attacks. There are various tools like SDF, DBN, and RBM which perform like compilation tools and are used for the identification of communications among subsystems.

B. Representation of Attack

Customarily, the validity of the state estimation process is confirmed through BDD technique by compiling the L-norm of estimation residue. The existence of bad dataset is decided upon the following equation:

$$||z - H\hat{x}|| > T_r \quad \ldots. (5)$$

Where,

$z \in R^N$ is the estimation vector

$\hat{x} \in R^D$ is the approximate state vector

$H \in R^{N \times D}$ is the Jacobian matrix

A threshold T_r is characterized beforehand to keep up the precision of the state estimation. Beside the way that cyber-attacks sidestep the current BDD method, estimation discharge required for BDD approaches makes them unrealistic for smart grid innovation. In cognitive cyber-attacks, explicitly FDI attacks, the objective of the contender is to have a subset under control of the estimations and control the state factors subjectively. It tends to be finished by infusing a fake data vector $z_a \in R^N$ that avoid conventional BDD methods. Assume the pernicious attack purposefully controls the meter readings by z_a. In like manner, the attack-induced estimation change can be denoted as:

$$z = H\hat{x} + z_a + \epsilon = H(\hat{x} + c_a) + q_a + \epsilon \quad \ldots.(6)$$

$$\hat{x_a} = \hat{x} + c_a$$

Where,

ϵ →measurement noise

$\hat{x_a}$ →faulty estimate state

The infused fake data (z_a) can be broken down into two parts $a = Hc_a$ and q_a, where $c_a \in R^D$ is an infused vector of data which avoids BDD tests as it has its place in the column of H, and qa is the main discernible part that lies in the corresponding space where $(HT\ H)^{-1}\ H^T\ q_a = 0$. In a nut shell, the secrecy attack vectors (z_a) consistently exists regardless of whether the contender can get fractional access to the system topography furthermore, line limitations to build malevolent attacks which totally reside in (H), i.e., $q_a = 0$, subsequently avoiding the existing BDD techniques.

The accompanying presumptions are taken into account in the display of the attack:

• In this work, the presumption that will be that the attacker has constrained provided inputs and these could just control restricted number of estimation readings. This could be either power infusion or power flow data, for a time span $T_a \subseteq T$. This is a sensible presumption on the grounds that, with regards to the power systems it isn't sensible to expect that every sensors apprise flawed estimations at the exact time. In addition, as a general rule, trading off all estimations brings about immense expense and exertion for contenders.

• Complete information on the framework is actually incomprehensible for an attacker that has not been involved in the network. Along these lines, the contender has partial information on the framework areas and security systems. Such information can be acquired by statistical analysis of data transferred from the remote terminal units (RTUs) to the control system or by seizing the security data implanted in a node. In this paper, key sparse FDI attack with least absolute shrinkage and selection operator (LASSO) is examined. Jacobian grid (H) is broken down on the basis of a row-wise methodology. A sub Matrix $HS = (H_{ji,:}, H_{jN-|S|,:})$, of H is made to represent the reliable estimations, where $H_{ji,:}$ is the j_i -th row of H, with the end goal that $H^S c_a = 0$. In like manner, sub-matrix H^A is built for attacked estimations. At long last, the contender's system is characterized in a manner to discover a solution c_a which streamline the below expression:

$$\text{Minimize } \|H_A c_a\|0$$

$$\text{Subject to } H^S c_a = 0 \quad \ldots. (7)$$

$$\|c_a\|_\infty \geq \tau,$$

Where,

$R \geq 0$ →given constant

LASSO and Regressor Selection algorithms are used to solve compilation problems. [20] Has given access to further details regarding the building of an attack.

The attacker's objective is to control the speed of the rotor and the angle of FDI attack through hacking into the interaction framework.

Thus, $\forall\ t \in T_a$, for generator i, the expression for the FDI attacks on the framework are denoted as:

$x_i{}^a(t) = x_i(t) + \gamma_i x_i(t) + C_I$ ……. (8)

where,

γ_i →constant coefficient

C_i →constant bias during the attack sequence

Thus, the attacker would aim to modify the system state by γ_i and C_i. taking into account that the z_a will be designed by the attacker in such a way that it will make the attack vector seem unobservable for the rest of the operators and conventional BDD techniques. In the analysis made through the experiments, it is presumed that λ-measurements will be accessed by the attacker, as λ-sparse attack vector would randomly be chosen to be generated.

III. PROPOSED METHODOLOGY FOR THE DETECTION OF ENERGY-BASED CYBER-ATTACK

Here, we propose a cyber-attack identification system which utilizes DBN representation, and for dataset training, it uses attribute extraction via MI and RBM. DBN and MI are applied to smart grid test frameworks with broad estimations, and the RBM is utilized to take into account the similarities in framework execution that are extricated by the supervised DBN model. The proposed knowledge driven system for anomaly recognition is delineated in Fig. 2. Initially, the framework is divided into a few sub-frameworks. Furthermore, causal reliance between ostensible aspects of subsystems is taken into account utilizing SDF. The presented technique is a executional proficient tool, which decrease the computational load by: 1) choosing a subset of estimations through attribute selection and SDF, and 2) by break down of specialization and data handling on a many subsystems consequently, as opposed to managing entire framework altogether.

A. Symbolic Dynamic Filtering

The attribute extraction method that we have proposed which is based on SDF, the conversion of time series data initially results into symbol sequences, and later DBN are derived from the resultant sequences to narrow down the data into low-dimensional statistical routines. Eq. (1) denotes the phase of the system space which is divided into fixed number of cells. Ω is a compact region which introduces a B that is a partition, denoted as $B \Xi \{B_0, \ldots, B_{m-1}\}$ which contains 'm' mutually exclusive and exhaustive cells. The time series data, as described by the dynamic system, is denoted as $0 \Xi \{\beta_0, \ldots, \beta_{m-1}\}$, $\beta_i \in \Omega$, that is observed to pass through the cells located in the partition B. Fig. 1 depicts a system that portrays the concepts of mapping as well as partitioning into the symbol alphabet. Let S be a random variable, with value $s \in A$, which represents the cell visited by a trajectory. Set A contains 'm' different symbols where each symbol denotes different elements in the partition. Every state in the beginning $\beta_0 \in \Omega$ generates a sequence containing symbols that are used for mapping from phase space into that of the symbol space as described below:

$\beta_0 \rightarrow s_{i0}\, s_{i1} \ldots s_{ik}$ ……. (9)

Symbolic dynamics was earlier described in Eq. (8). The multi-dimensional space is converted into a symbol series and later into a DBN. This process is called symbolization process.

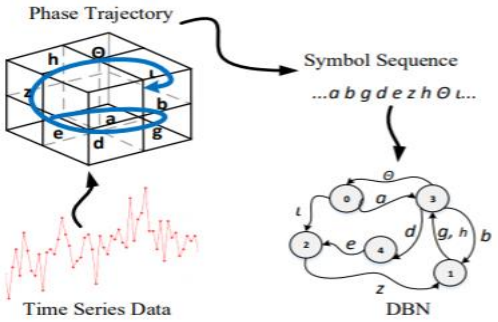

Fig.1. Steps leading to generation of DBN using SDF-based attribute extraction

B. Dynamic Bayesian Network

The main uses of DBNs are the probabilistic graphical models which are capable to depict system's state as a set of factors, and portray the probabilistic dependencies of those factors between time periods. Here, a high order DBN on ξ factors $x_t = \{x1,t, \ldots, x_{\xi,t}\}$ at various time intervals, the points $t = 1, \ldots, T$ is taken into account. Every $x_{i,t}$ denotes the expression of state i at time t. SDF provides a variable set from which symbol series is derived. Let S_n denote the occurrence probability as DBN would satisfy the $\mathscr{L}$-th order of Markov property as follows:

$(s_n | s_{n-1} \ldots s_{n-\mathscr{L}} \ldots s_0) = (s_n | s_{n-1} \ldots s_{n-\mathscr{L}})$ …….(10)

Let Π denote the state transition matrix that portrays the $\mathscr{L}$-th order of Markov property, which can be presented on the basis of training data. Let q_k denote the state at that particular instance of time, k. The ij-th element of Π can be depicted as follows:

$\Pi_{ij} \triangleq (q_{k+1} = s_i \mid q_k = s_j)$ …… .(11)

In this paper, as there are a lot of time sequences involved, an improved version of Markov chain is suggested [20] to predict, for new symbol, the occurrence probability in sequence A by utilizing the last $\mathscr{L}$ symbol for another sequence B. For the sub-systems A and B in $\mathscr{L}$-th order of Markov property, they are defined as Π^A and Π^B respectively. Cross state transition matrices like Π^{AB} and Π^{BA} represent the normal dependencies of A on B and B on A, respectively.

Atomic patterns (APs) and the one for x$\mathscr{L}$-th order of Markov property are denoted as features from $\mathscr{L}$-th order of Markov chain and are called as relational patterns (RPs). Π^{AB} and Π^{BA}, state transition matrices, can be depicted as:

$\pi_{kl}{}^{\mathbb{AB}} \triangleq (q_{n+1}{}^{\mathbb{B}} = l | q_n{}^{\mathbb{A}} = k)\ \forall n$ ……. (12)

$\pi_{ij}{}^{BA} \triangleq (q_{n+1}{}^{A} = j | q_n{}^{B} = i)\ \forall n$ ……. (12)

Where,

$j,k \in Q^A$

$i,l \in Q^B$

Q^A →state vector corresponding to sequence A

Q^B →state vector corresponding to sequence B

The symbol sequence, S, is generated with partitioning in any multivariate time series. An extensive order DBN is utilized to denote further states and transition probabilities among vertices. Here, we suggested the use of MI criteria to capture essential feature of an AP or an RP. We use MI as it creates a general linear correlation coefficient which estimates the relationship among 2 random factors.

To signify that 2 variables are independent towards each other can be done when MI gives a non-zero value as output. I^{AB} is an Importance metric in MI which denotes the state series between q^A and q^B, and can be depicted as follows:

$$I^{\mathbb{AB}} = (q_{k+1}\,;\, q_{k+1}{}^{\mathbb{A}}) = H(q_{k+1}{}^{\mathbb{B}}) - H(q_{k+1}{}^{\mathbb{B}}\,|q_k{}^{\mathbb{A}}) \quad \ldots.(13)$$

Where,

$$H(q_{k+1}{}^{\mathbb{B}}) = -\sum_{i=1} Q^B \;\; P(q_{k+1}{}^{\mathbb{B}} = i)\log_2 P(q_k{}^{\mathbb{B}} = i)$$

$$H(q_{k+1}{}^{\mathbb{B}}\,|q_k{}^{\mathbb{A}}) = -\sum_{i=1} Q^A \;\; P(q_k{}^{\mathbb{A}} = i)\, H(q_{k+1}{}^{\mathbb{B}}\,|q_k{}^{\mathbb{A}} = i)$$

$$H(q_{k+1}{}^{B}\,|q_k{}^{a} = i) = -\sum_{j=1} Q^B \;\; P(q_{k+1}{}^{\mathbb{B}} = j|q_k{}^{\mathbb{A}} = i)\log 2\, P(q_{k+1}{}^{\mathbb{B}} = j|q_k{}^{\mathbb{A}} = i)$$

[19] Has provided detailed information about MI-based casualty. The variation in I^{AB} between 2 instances of time can be depicted as follow:

$$(I) = I_{t1}{}^{\mathbb{AB}} - I_{t2}{}^{\mathbb{AB}} \quad \ldots. (14)$$

δ denotes the strong predictive and data link in AP/RP which can help to differentiate among 2 kinds of clients.

When the programs are ready, RBM would learn the similarities in the routines of the system's execution. To predict the output, the test data is used for computation. We have also suggested the use of Restricted Boltzmann Machine (RBM) for this issue.

C. Restricted Boltzmann Machine

Boltzmann Machine is a productive technique to display the obscure spread of information. In contrast to the greater part of the Machine Learning methods that separate a few data vectors for other people, Boltzmann Machine can likewise produce new information with given combined dissemination, as well as pattern execution if there should be an occurrence of absent inputs. It is additionally thought of more aspect-rich and versatile. RBM has a place with the class of stochastic Energy-based Models (EM). In EM, each state of the framework is related to a particular energy level. Such a framework can be depicted by a system of stochastic binary neurons (few factors $v = \{v_1, \ldots, v_N\}$) which are associated with a lot of concealed factors $h = \{h_1, \ldots, h_K\}$.

Framework's state can be portrayed as reliable on combined arrangements of the obvious and concealed factors. It is demonstrated that model estimation in RBM sums to expand the probability of the datasets in training with less energy state. Accordingly, an anomaly will show up as a design with less possibility or more energy. Given binary factors v and concealed factors h, the joint probability of a state ($Pr(v, h)$) can be portrayed in light of the energy level of that state ($En(v, h)$), with a Boltzmann dissemination work:

$$(v, h) = (\exp(-\text{En(v,h)}))/(\sum \text{v,h} \exp(-\text{En(v,h)})) \quad \ldots.(15)$$

Where,

$$(v, h) = -\sum_{i=1} N\; a_i v_i + \sum_{k=1} K(b_k + \sum N_{i=1} w_{ik} v_i)\; h_k \quad \ldots.(16)$$

Where,

a, b, w →parameters set by the model

Model parameters are computed by maximizing the training data probability with less energy state.

Data density is depicted as:

$$(v) \propto \sum_h \exp(-En(v, h)) = \exp(-F(v)) \quad \ldots\ldots.(17)$$

Where,

(v) • free energy

It can be represented as:

$$(v) = -\log(\Pr(v)) + constant \quad \ldots\ldots.(18)$$

In this manner, free energy can be utilized as the anomaly list to prioritize information cases in direct time. The trained RBM is utilized to recognize a cyber-attack dependent on the likelihood and energy level of an instance. Anomaly consists of an instance with more energy or less possibility. The presumption usually made is that cyber-attacks change the communication between the lower systems and brings about various patterns in DBN. For main purpose of training, $I^{\mathbb{AB}}$ can be standardized into either of the two states (0 and 1 for less and more values) for APs and RPs. At last, variations in the conditions associated with the acknowledged patterns are utilized to recognize cyber-attacks. A dissemination of free energy is utilized to identify less probability instances or cyber-attacks dependent on distance measurement. For the ordinary task limitation, free energy will have comparative dissemination to that of the training information. The presumption is that the data training are for the most part gathered from ordinary task condition. Consequently, the learnt RBM can successfully take into account the normal executions of the framework.

To evaluate the distinction between the energy disseminations to train and test information, Relative Entropy (RE) metric is utilized. The relative entropy between two probable instances is an estimate of the distance between them. RE for two probability distributions, P and Q on a fixed set X,

$$(P\|Q) = \sum_X (x) \log (\text{P(x)})/(\text{Q(x)}) \quad \ldots\ldots.(19)$$

Where,

P →free energy dissemination in normal instance

Q → free energy dissemination in cyber-attack instance

(v^n) →free energies in regular execution condition

(v^{ca}) →free energies in cyber-attack condition

(v^n) and (v^{ca}) can be computed using Eq. (14). A similar RE distance was characterized in [24],

$$(P\|Q) = (P\|Q) + RE(Q\|P) \quad \ldots.(20)$$

This can also be utilized as a key for anomaly detection, to further compare it with Detection Threshold (DT) to identify and cyber-attack. In case the thresholds are way too less than expected, it is bound to give fake attack detections, while it's also an instance that very high thresholds may lead to unknown attack. In this paper, a few of the RE values are unexpected while the rest of the values which are computed through training are expected to be constant. To evaluate DT, the easiest way is to use normal distribution. It is presumed that 95 per cent of information is consisted among two standard deviations of the mean. $\forall\, D\tilde{T}$' satisfies

$|\{RE_i : D\tilde{T}' \geq RE_i\}| = 0.95|\{REi\}|$, i=1,2,…,n that DT = min $\{D\tilde{T}'\}$

Where,

RE_i • i-th RE in training dataset

Anomaly will be detected when RE(t) ≥ DT. The steps are provided as follows:

Change time sequences information to specific series.

• Display the systems involved and their communications utilizing DBN.

• Determine the data based measurement values utilizing MI (I^{ij}).

• Produce a binary vector of length L utilizing I^{ij}, and relegate a state 0 or 1 to each I^{ij}.

• Use RBM with noticeable nodes relating to APs furthermore, RPs to become familiar with the standard of behavior.

• Recognize anomaly by computing the event probability of the current perception dependent on trained RBM.

The anomaly detection process algorithm is depicted in Algorithm 1.

IV. RESULTS DERIVED FROM CASE INVESTIGATIONS AND SIMULATION

In this segment a contextual investigations under various tasks condition are created to approve execution of the proposed strategy. Case 1 is displayed as a multi-operator cyber-physical framework dependent on IEEE-39 bus model where each operator involves a generator similar to the one depicted in Section II, an estimation gadget, a dispersed control operator, and an energy storage framework as depicted in Fig.4. The depiction of the energy storage is such that can be an input into the framework by diverse small grid or inexhaustible resources. A similar analysis is considered for all contextual investigations, be that as it may, for space just the outputs of Case 1 are involved for this segment.

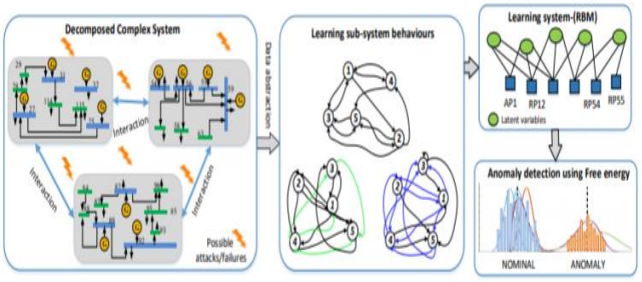

Fig.2. Proposed network for cyber-attack recognition utilizing unsupervised learning

Algorithm 1: Anomaly Detection
1. Gather normal and testing dataset
2. Compute the regular pattern ($I^{AB}(t)$, $I^{AB}_{norm}(t)$, $I^{AB}_{test}(t)$)
3. Choose RBM structure, visible and concealed units (v,h)
4. Input $I^{AB}_{norm}(t)$ into RBM
5. Derive weights and biases for trained RBM
6. Calculate the free energy F(v) of the normal data
7. Compute RE and RE_d
8. Determine the threshold DT
9. Revise the inputs $I^{AB}_{test}(t)$
10. Determine free energy of revised $I^{AB}_{test}(t)$
11. Calculate RE and RE_d on the basis of current and past inputs
12. Contrast current RE_d with DT to identify anomaly

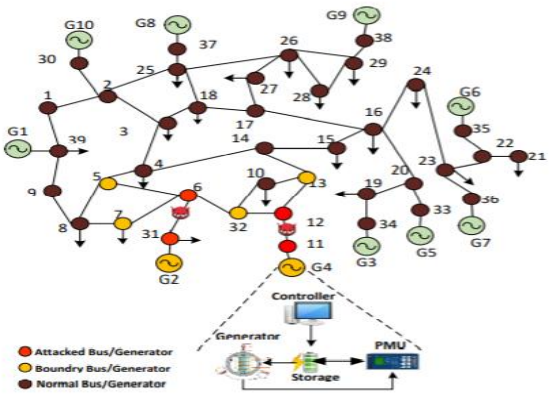

Fig.3. IEEE-39 bus system under cyber-attack in line 6-31 and 11-12

A. Test System

The below table lists the details of the cases studied and they are adapted from Matpower [21]. The provided case examinations are presumed to be completely evident. It is also presumed that the framework networks remain constant over a period of time. Matlab R2017a is used to carry out the implementation of the case studies and complied on the Core™ i7-7700 CPU, 3.6 GHz, and a RAM of 32.00GB.

UNITS FOR MAGNETIC PROPERTIES

S. No.	Number of Buses	Number of Generators	Number of Lines	Number of States	Number of measurements
1	39	10	46	40	171
2	118	54	186	216	609
3	2848	547	3776	2188	12673

By investigating the MI index, reliability among a subset of factors that impact each other in the ordinary condition is utilized for anomaly identification. The model created by RBM signifies the ordinary framework since the vast majority of the gathered information gathered is from the ordinary conditions. It ought to be stated that gathered information are marked as ‘normal’ or ‘anomalous’. Acquiring and formatting this data is further utilized to creating the benchmark for the ordinary condition which will be utilized for choosing the edge for the anomaly. A window in motion in a subset of the training data (with distribution factor P) is utilized to calculate the distribution Q signifying the dynamic execution of the framework. So as to estimate the separation among Q and P, the RE metric is applied in every subset. Comparable setting is utilized for the testing data. At long last, the two RE are contrasted to identify anomalous condition (in this instance, it is cyber-attack). The attack technique is intended to over-burden lines 6-31 and 11-12. The attack locale is appeared in Fig. 3. Standardized estimation under ordinary execution condition, main cause allotted to cyber-attacks introduced in Fig.4 for Case 1. It tends to be seen that all the estimations residuals due to cyber-attacks have nearly a similar extent as the estimation lingering under normal execution environment which suggests that traditional residual test can't distinguish the secretive digital assaults. It ought to be noticed that shortcomings will provide outcomes remaining in the estimation leftover as appeared in Fig. 4. If there should be an occurrence of a deficiency in the framework, the administrator will be informed and clear the flaw. Consequently, the shortcoming won't influence the conditions of the framework.

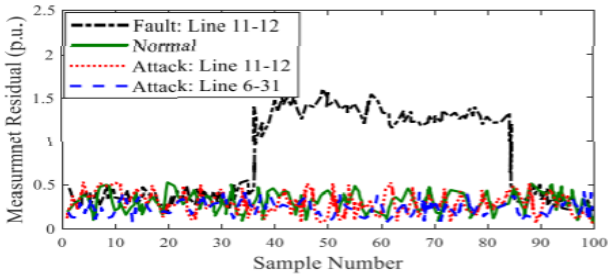

Fig.4. Estimation residual on Case 1 pre- and post the cyber-attack

From Fig. 5, we discover that the variation in the lower plot is in an acceptable zone. We notice that in the top plot, there is a significant increase in the variation when the attack takes place between sample numbers 35-65. This, then, signals towards a potential threat of cyber-attack which is quite possible to have gone unnoticed during bad data detection. Thus, predicted states which involve more error could be treated as an input for the rest of the framework, which in turn results in irrevocable damages.

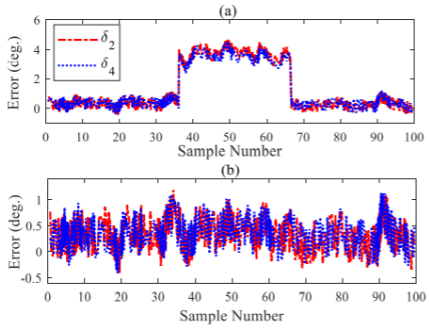

Fig. 5. a) Variation on state measurement error with no cyber-attack, b) variation on state measurement error during cyber-attack on Case 1.

B. Accuracy, False Positive and True Positive

During the analysis of smart grid, the main area of concern has not just been the identification of cyber-attacks, but it has also been the ability to prevent the fake alarms. Thus, execution of our presented strategy is on the basis of the True Positives (TP), False Positives (FP), True Negatives (TN) and False Negatives (FN) that are displayed in the table below:

UNITS FOR MAGNETIC PROPERTIES

	Attacked	Secure
Classified as Attacked	TP	FP
Classified as Secure	FN	TN

The capability to learn and memorize are properties of the algorithms, which are estimated by False Positive Rate (FPR), True Positive Rate (TPR), and Accuracy (Acc) factors, that are depicted as follows:

FPR = FP/(TN+FP)
TPR = TP/(TP + FN) …….(21)
ACC = (TP + TN)/(TP + TN + FP + FN)

Less value of FPR of 0 per cent implies that no secure estimations are misread as attacked. When the value of TPR is 100 per cent, it means that no attacked estimations are misread as secure. When the Accuracy is 100 per cent, it implies that these estimations categorized as an attacked estimation, and every estimation categorized as a secure estimation.

1. Impact of Threshold on FPR:

Fig. 6 depicts the difference of FPR as a function of identification edge for single attack (SA) and many attacks (MA) on state variables δ_2, δ_4. DT ranged from 0.25DT to 1.5DT, in every case, in Section 3, DT is the threshold. As depicted in the figure, FPR reduces as the detection edge increases. This implies that when the threshold is low, it causes the algorithm to behave a little more forceful in attack detection, which further suffers from high fake-alarm rate.

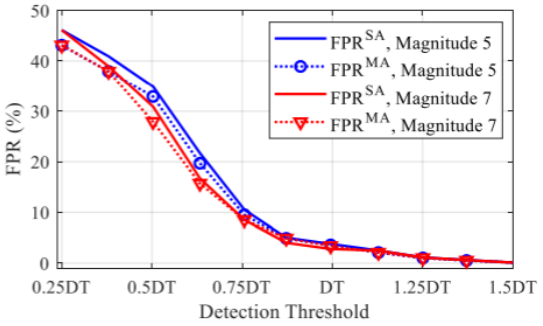

Fig.6. For 2 separate attack magnitudes in Case 1, FPR is displayed under single and multiple cyber-attack

The change in the magnitude of attack along with the number of attacks doesn't have any impact on FPR drastically. Furthermore, FPR becomes negligible when the threshold is observed to be greater than DT. Thus, we can use DT as the threshold for our proposed technique, as well as, there were a lot of changes to be taken into account for FPR in comparison to the edge for other states.

2. Impact of Magnitude of Attack on TPR and ACC:

For 2 attack cases where state variables are $\delta 2$, $\delta 4$, the variation in TPR and ACC which is considered to be the function of attack magnitude, is depicted in Fig. 7. 1 per cent of initial estimate signifies less magnitude of attack and 10 per cent of initial estimate signifies more magnitude of attack. Magnitude that is neither high nor low, medium, is signified by 5. This magnitude is of regular type of attack. To crosscheck the impact that detection threshold has on TPR and ACC, the output is presented on the below graph.

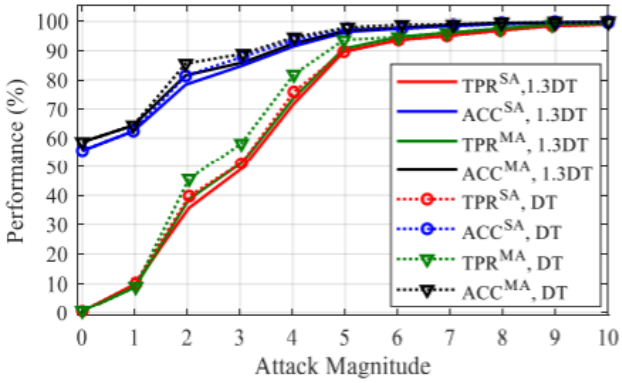

Fig.7. For 2 separate attack magnitudes in Case 1, TPR and ACC is displayed under single and multiple cyber-attack

As appeared in Fig.7, by expanding the magnitude of the attack, TPR as well as ACC immediately moved toward 100 per cent. Also, it tends to be seen that when the threshold extremely high, it negatively influences the TPR and affects the base size identifiable attack. The outcomes show that DT characterized in Section III can successfully identify an attack with moderate and high quality with practically 99 per cent precision and 98 per cent TPR.

A similar pattern was seen in the transformations of TPR and ACC in comparison to the attack size for all states. Synopsis of the outcomes for various contextual investigations are announced in the below table.

RESULTS SYNOPSIS FOR MEDIUM ATTACK MAGNITUDE IN MONO ATTACK (AVERAGE) (in %)

S. No.	TPR^{SA}	TPR^{MA}	FPR^{SA}	FPR^{MA}	ACC^{SA}	ACC^{MA}
1	98.0	98.1	2.01	1.98	98.9	99.1
2	98.1	98	1.96	1.96	99.1	99.0
3	98.1	98.1	1.98	1.97	99.0	99.1

3. Impact of Sparcity of an Attack on TPR and ACC:

To investigate the impact of attack sparsity, attacks with distinguishable sparsities $\lambda/N \in [0, 1]$ are produced. N signifies the absolute number of estimations in the framework. As appeared in Fig. 8, both TPR as well as ACC increment as the quantity of debased estimations increments. Here, sparsity 1 implicates all estimations are controlled by the aggressor. The figure depicts that the algorithm presented in this paper has extremely high TPR (around 94 per cent) and ACC (around 90 per cent) when just 35 per cent of the estimations are influenced. When partial the estimations are attacked, which is a reasonable presumption for non-futile attack execution from the aggressor's side, the algorithm used is exceptionally successful with 99 per cent TPR and 98 per cent ACC.

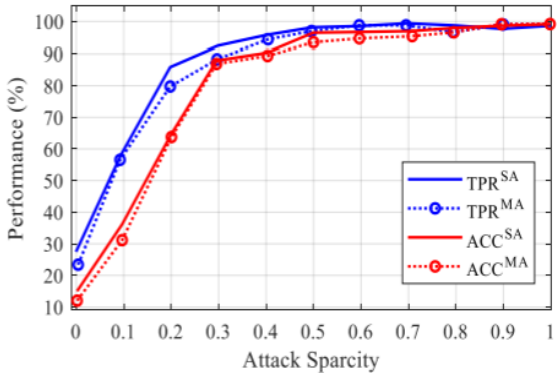

Fig.8. For separate attack magnitudes in Case 1, TPR and ACC is displayed under single and multiple cyber-attack

C. Performance Analysis under Various Execution Limitations

To approve the efficient execution of the proposed technique, four various situations are taken into consideration:

1) ordinary state without attack
2) arbitrary attack
3) single FDI attack on 6-31
4) various, synchronous FDI attacks on lines 6-31 and 11-12.

Proposed strategy is contrasted and the two most well-known BDD techniques; LNR test and Chi-Square test. 3σ is the fixed threshold while σ is the standard deviation, to limit the fake positives because of the residual data, in this manner FPR, due to residual data, is under 1 per cent. For exact and elaborated examination, the threshold is standardized for all indicators. A similar rule is taken into consideration for setting limitation in LNR test. Indicator's outcomes are portrayed in Fig. 9. As appeared in Fig. 9 (a), in standard execution condition, the outcome of all detectors is below threshold which determines that there is no hint of bad information or cyber-attack in the framework. Fig. 9 (b) shows that all techniques can distinguish the arbitrary attack. As the attack is ignorant, it will drop its trail in the datasets and the administrator will be apprised regarding any existence of an attack. The arbitrary bad information, which was infused to the estimation set, brings about critical variations in the estimation surplus vector that prompts the expansion in cost execution. In an ideal state measurement, we assess the cost work dependent on the residual of the estimations. In the standard task condition, without bad information in the framework, the cost function follows a standard dissemination with zero mean. Under an unexpected attack, the expense capacity will proceed through the threshold for ideal state estimation. In this manner, both LNR and chi-square tests will alert the alarm effectively. If there should be an occurrence of single or numerous FDI attacks, as can be seen in Fig. 9 (c) and (d), the cost for executing both LNR and Chi-Square indicator remained in the genuine scope of predefined thresholds. The two methodologies brought about their standardized excess factors underneath the predetermined threshold and in this way they couldn't distinguish the attack in the framework. Nonetheless, in a similar environment, outcome of the proposed indicator is over the given threshold and can trigger the alarm.

The principle reason is that the LNR test and Chi-Square test depend on excess of the estimation vector while cyber-attacks are cautiously made to avoid the statistical identifier with no trail in excess vector. Comparative outcomes were watched for all case examples. Normal recognition time for all contextual analyses was 1ms with 0.2ms deviations.

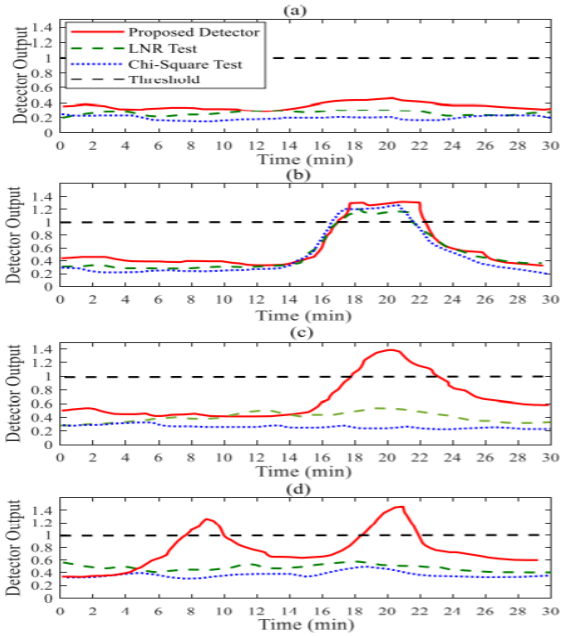

Fig.9. Case 1 depiction of detector outcomes in a) standard limitation, b) arbitrary attack, c) single cyber-attack, d) continuous cyber-attacks

As a rule, any kind of FDI attack in line or framework brings about similar difference in the system with minor moderation. Along these lines, the strategy we proposed can effectively identify different FDI attacks from various inputs. Moreover, since the strategy that was proposed examines the similarities between the undermined information and the standard information, its accuracy rate doesn't rely upon the attack situations.

V. CONCLUSION

With regards to smart grid anomaly detection, the provisions proposed theoretically are chiefly disconnected techniques with limitation to manage powerfully advancing cyber commination. This paper presents a realistic and computationally effective tool for anomaly identification that using attribute extraction technique and time sequences dividing to uncover usual communications among the systems. DBN theory and learning algorithms on the basis of Boltzmann Machine are utilized to recognize undetectable attacks dependent on free power as the anomaly token. Execution of the algorithm discussed was assessed on various IEEE test frameworks and under various execution limitations for a various measures (TPR, FPR, and ACC). The outcomes exhibited that the framework accomplishes a precision of 99 per cent, TPR of 98 per cent and FPR of under 2 per cent.

REFERENCES

1. J. Dagle, “Postmortem analysis of power grid blackouts-the role of measurement systems”, IEEE Power and Energy Magazine, vol. 4, no. 5, pp. 30-35, Sept 2006.
2. M. Masera, I. Nai Fovino, “Effects of intentional threats to power substation control systems”, Int. Jour. Cri. Infr., vol. 4, no. 1, pp.129143, 2008.
3. T. Morris, S. Pan, J. Lewis, J. Moorhead, B. Reaves, N. Younan, R. King, M. Freund, V. Madani, “Cybersecurity testing of substation phasor measurement units and phasor data concentrators”, in Proc. of CSIIRW, pp. 12-14, Oct. 2011.
4. Prajval Mohan, Pranav Narayan, Lakshya Sharma, Tejas Jambhale, Simran Koul, "Iterative SARSA: The Modified SARSA Algorithm for Finding the Optimal Path". International Journal of Recent Technology and Engineering (IJRTE). ISSN: 2277-3878, Volume-8 Issue-6, March 2020.
5. H. Haddad Pajouh, R.Javidan, R.Khaymi, A. Dehghantanha and K.R.Choo, “A Two-layer Dimension Reduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks”, IEEE Trans. on Eme. Topics in Computing, 2016.
6. R. Khan, K. Mclaughlin, D. Laverty, S. Sezer, “Design and implementation of security gateway for synchrophasor based realtime control and monitoring in smart grid”, IEEE Access, vol. 5, no. , pp. 11626-11644, June 2017.
7. H. Karimipour, V. Dinavahi, “Robust Massively Parallel Dynamic State Estimation of Power Systems Against Cyber-Attack”, IEEE Access, vol. 6, pp. 2984-2995, Dec. 2017.
8. M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor,“Machine learning methods for attack detection in the smart grid,” IEEE Trans. on Neural Net. & Learning Syst., vol. 27, no. 8, pp. 1773–1786, Aug 2016.
9. Prajval Mohan, Adiksha Sood, Lakshya Sharma, Simran Koul, Simriti Koul, “PC-SWT: A Hybrid Image Fusion Algorithm of Stationary Wavelet Transform and Principal Component Analysis”. International Journal of Engineering and Advanced Technology (IJEAT)’, ISSN: 2249-8958, Volume-9 Issue-5, June 2020.
10. S. Pan, T. Morris, and U. Adhikari, “Developing a hybrid intrusion detection system using data mining for power systems”, IEEE Trans. Smart Grid, vol. 6, no. 6, pp. 3104_3113, Nov. 2015.
11. J. Landford et al., “Fast sequence component analysis for attack detection in synchrophasor networks”, 5th Int. Conf. Smart Cities Green ICT Syst. (SmartGreens), Rome, Italy, 2016.
12. S. Ahmed, Y. Lee, S. Hyun and I. Koo, “Feature Selection-Based Detection of Covert Cyber Deception Assaults in Smart Grid Communications Networks Using Machine Learning”, IEEE Access, vol. 6, pp. 27518-27529, 2018.
13. Simran Koul, Yash Raj, Simriti Koul, “Analyzing Cyber Trends in Online Financial Frauds using digital Forensics Techniques”. ‘International Journal of Innovative Technology and Exploring Engineering (IJITEE)’, ISSN: 2278-3075 (Online), Volume-9 Issue-9, July 2020, Page No. 446-451.
14. Y. He, G. J. Mendis and J. Wei, “Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism”, IEEE Trans. on Smart Grid, vol. 8, no. 5, pp. 2505-2516, Sept. 2017.
15. S. Mohammadi, H. Mirvaziri, M. G. Ahsaee, H. Karimipour, “Cyber Intrusion Detection by Combined Feature Selection Algorithm”, Journal of Inf. Sec. and App., pp. 80-88, vol. 44, Feb. 2019.
16. C. A. Murthy, “Bridging feature selection and extraction: compound feature generation”, IEEE Transactions on Knowledge and Data Engineering, vol. 29, no. 4, pp. 757-770, 1 April 2017.
17. A Bergen and V. Vittal, “Power Systems Analysis”, Prentice-Hall, Second ed., 2000.
18. Y. Liu, M. K. Reiter, and P. Ning, “False data injection attacks against state estimation in electric power grids”, ACM Trans. Inf. Syst. Secur., vol. 14, pp. 1-33, 2011.
19. M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, “Sparse attack construction and state estimation in the smart grid: Centralized and distributed models,” IEEE J. Sel. Areas Commun., vol. 31, no. 7, pp. 1306–1318, Jul. 2013.
20. S. Sarkar, S. Sarkar, K. Mukherjee, A. Ray, A. Srivastav, “Multisensor data interpretation and semantic fusion for fault detection in aircraft gas turbine engines”, Journal of Aerospace Engineering, vol. 227, no. 12, pp. 1988–2001, Dec. 2013.
21. R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, “MATPOWER:
Steady-state operations, planning, and analysis tools for power systems research and education,” IEEE Trans. Power System, vol. 26, no. 1, pp. 12–19, Feb. 2011.
22. Simriti Koul, “Contribution of Cognitive Science and Artificial Intelligence in the Simulation of the Complex Human Mind”. ‘International Journal of Recent Technology and Engineering (IJRTE)’.
23. Simran Koul, “Contribution of Artificial Intelligence and Virtual Worlds Towards Development of Super Intelligent AI Agents”. ‘International Journal of Engineering and Advanced Technology (IJEAT)’, ISSN: 2249-8958 (Online), Volume-9 Issue-5, June 2020, Page No. 800-809

AUTHORS PROFILE

Simran Koul was born in Jammu, India, on 10th November 1998. She completed her senior high school in FAIPS DPS, Ahmadi, Kuwait. She is currently pursuing for her Bachelor’s Degree in Computer Science and Engineering at Vellore Institute of Technology, Vellore, India. She is currently working on projects which involve concepts of Digital Forensics, Robotics, Artificial Intelligence, Cyber-security and Natural Language Processing.

Simriti Koul was born in Jammu, India, on 10th November 1998. She completed her senior high school in FAIPS DPS, Ahmadi, Kuwait. She is currently pursuing her Bachelor's Degree in Computer Science Engineering at Vellore Institute of Technology, Vellore, India. She is currently working on projects which involve concepts of Artificial intelligence, Data Analytics, Digital Forensics, Cyber-security and Natural Language Processing.

Prajval Mohan was born in Hyderabad, India, on 23rd October 1998. He completed his Senior High School from FIITJEE Junior College, Hyderabad, graduated with 96.1 percent, and received the Honorary Certificate of Merit in the year 2016. Prajval is currently pursuing his B. Tech in Computer Science and Engineering from Vellore Institute of Technology, Vellore, India. His areas of interest include Robotics, Machine Learning, Artificial Intelligence, and Cloud Computing. He has advanced working knowledge of Robotics and Database handling, which were strengthened by completing various projects and internships in the respective fields. He also has ongoing research in the field of Deep Learning, Software Engineering, and Parallel Distributed Computing.

Lakshya Sharma was born in Jaipur, India, on 25th January 1999. He was raised in Delhi, India, and completed his Senior high school from DAV Public School. He is currently pursuing B. Tech in Computer Science Engineering from Vellore Institute of Technology, Vellore. His research interests include Deep learning, artificial intelligence, autonomous object avoiding and path planning robots. He has worked on several machine learning, deep learning projects and has ongoing research in offline signature recognition using Siamese networks.

Pranav Narayan was born in Thane, India on July 29, 1999. He completed his senior high school in Indian School Muscat, Oman. He is currently pursuing his Bachelor's in Computer Science and Engineering from Vellore Institute of Technology, Vellore. He is currently working on projects which involve computer science concepts like Operating Systems, Robotics and Software Engineering.