IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 24, 2019, accepted December 3, 2019, date of publication December 11, 2019,
date of current version January 17, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2959047

Malicious Insider Attack Detection in IoTs Using Data Analytics

AHMED YAR KHAN[1], RABIA LATIF[2], SEEMAB LATIF[3], (Senior Member, IEEE), SHAHZAIB TAHIR[4], (Member, IEEE), GOHAR BATOOL[5], AND TANZILA SABA[2], (Senior Member, IEEE)

[1]Information System Technology, Department of Securities Ex-change Commission of Pakistan, Karachi 44000, Pakistan
[2]College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[3]Department of Computing, School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan
[4]Department of Information Security, College of Signals, National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan
[5]Balochistan University of Information Technology, Engineering and Management Sciences, Quetta 75660, Pakistan

Corresponding author: Shahzaib Tahir (shahzaib.tahir@mcs.edu.pk)

This work was supported in part by the Artificial Intelligence and Data Analytics Lab (AIDA), Prince Sultan University, Riyadh, Saudi Arabia.

ABSTRACT Internet of Things (IoTs) are set to revolutionize our lives and are widely being adopted nowadays. The IoT devices have a range of applications including smart homes, smart industrial networks and healthcare. Since these devices are responsible for generating and handling large amounts of sensitive data, the security of the IoT devices always poses a challenge. It is observed that a security breach could effect individuals and eventually the world at large. Artificial intelligence (AI), on the other hand, has found many applications and is widely being explored in providing security specifically for IoT devices. Malicious insider attack is the biggest security challenge associated with the IoT devices. Although, most of the research in IoT security has pondered on the means of preventing illegal and unauthorized access to systems and information; unfortunately, the most destructive malicious insider attacks that are usually a consequence of internal exploitation within an IoT network remains unaddressed. Therefore, the focus of this research is to detect malicious insider attacks in the IoT environment using AI. This research presents a lightweight approach for detecting insider attacks and has the capability of detecting anomalies originating from incoming data sensors in resource constrained IoT environments. The results and comparison show that the proposed approach achieves better accuracy as compared to the state of the art in terms of: *a)* improved attack detection accuracy; *b)* minimizing false positives; and *c)* reducing the computational overhead.

INDEX TERMS Insider attacks, artificial intelligence, malicious threat.

I. INTRODUCTION

We live in an era where everything and everyone is interconnected through physical devices and physical objects. These embedded devices and objects interact over the internet. The IoT devices have many advantages that mainly include automated data gathering, monitoring and control in an efficient and effective manner. Although, IoT devices have to offer many benefits, they are also prone to security and privacy attacks. These security and privacy risks and concerns limit the adoption of the IoT devices on full scale especially in mission critical settings where sensitive data is involved. To mitigate the security and privacy attacks there has been emphasis on securing the devices and their communication, limiting unauthorized or illegal access, and preventing information leakage to third party [1], [2]. However there is little pondering on the possible insider attacks in an organization (within the system), and the damage that they might intentionally or unintentionally cause.

According to a recent report published in 2018 by IBM Security Intelligence Index [3], 60% of all the attacks are being carried out from the inside. The usual cause of insider threat is, when an individual or his/ her device within the network misuse their privileged access to cause a negative impact on the confidentiality, integrity or availability of the organization's systems. It is estimated that by

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

2020 over 20 billion Internet of Things (IoT) devices are set to come online [4]. Keeping in view the benefits of IoT devices, the state of the art technologies have fully transformed towards IoT. Although the IoT technology seems very promising but the other side of the picture is quite grim where we expect to experience a rise in IoT-specific attacks with the growth in wireless capabilities.

IoT is nearly transforming all the things that are part of our lives including consumer electronics, toys, appliances etc. All the equipment's surrounding us are becoming internet-enabled devices that traditionally have weak security configurations. These devices have limited power and computational resources such that they lack in even running an anti-malware, or lack in having the capability for intrusion detection. Protecting network-connected devices at such a large scale requires a paradigm shift in terms of the security of the IoT devices.

To adopt the IoT devices on a large scale, a proactive approach for the detection of the malicious insider attacks is to be followed. Artificial Intelligence (AI) has the ability to learn (acquire the information) and reason (reach a approximate or definite conclusion). Therefore, the use of AI in the IoT could lead to the timely detection of malicious insider attacks.

A. CONTRIBUTIONS

The existing approaches face a number of implementation challenges due to the deployment of resource constrained IoT devices which limits their use and effectiveness. This research makes the following contributions:

- This research addresses the security issues posed by malicious insider and presents a detection mechanism for IoT. The proposed algorithm is based on Artificial Intelligence (AI) and aims to ensure the security of critical and sensitive IoT data.
- Presents a methodology for smoothing input data to improve predictive performance and minimize false positives when compared to previous prediction approaches, which largely treat insider threat as a single category.
- The proposed technique is simulated in the R programming environment using the dataset generated through NS-2 simulation based on Computer Emergency Response Team (CERT) and a detailed analysis of the results is performed.

The remaining paper is organized as follows: Section II provides a literature review. Section III discusses the proposed work by presenting the preliminaries and framework. Section IV presents the proposed approach for detecting malicious activities in synthetic organizational records by presenting the algorithms involved in the technique. Section V discusses the experimental setup details and introduces the metrics for analysing the technique. The Section VI presents an evaluation of the proposed model. Finally, the conclusions and future work is drawn towards the end in the Section VII.

II. PREVIOUS WORK

The activities involved in an insider threat is with malicious intention, which occurs from within the system or network. The capabilities of detecting insider threats in Wide Area Networks (WAN) has been tested using various AI-based techniques such as neural network, deep learning, data sciences, K-Nearest Neighbor (KNN) and distance measurement. But very limited research is carried out previously on the use of AI to reduce malicious attacks in IoT networks.

A. MALICIOUS INSIDER ATTACK IN WAN

Effort has been put in to counter malicious insider attacks in different areas. Hall *et al.* [5] in their research define a methodology for performing pre-processing of organizational log data to derive user profiles for classification, and later on used to train multiple classifiers. Boosting is also applied to optimize classifier accuracy. Overall the models are evaluated through analysis using the associated confusion matrix and Receiver Operating Characteristic (ROC) curve, and the best performing classifiers are aggregated into an ensemble classifier. This meta-classifier has an accuracy of 96.2% with an area under the ROC curve of 0.988. Since this approach has a high complexity and computation overhead, therefore it cannot be used for IoT devices. Furthermore, Yuan *et al.* in [6] highlight that their approach requires "feature engineering" which is a difficult and time-consuming task.

A research based on Multi-criteria Aggregation method for Insider Threat Monitoring is presented in [7]. The approach is based on fusion for monitoring user behavior data. It executes temporal (multiple instance of time) and multi-criteria aggregation analyzes different types of user's activities on different instances under multiple criterion. Their approach improves the accuracy of detecting malicious insiders and gives a meaningful outcome. A Machine learning technique for detecting Insider attack using Hidden Markov Model (HMM) is presented in [8]. By using the synthetic dataset from Computer Emergency Response Team (CERT), based on different action or activities with assigned numbering, learning from previous activities, the normal behavior is identified and the model is trained. A new approach to detect insider threats is presented in [9], and proves to be better than the previous Distance Measurement (DM) techniques. It uses the same approach as used in HMM to detect malicious insider threat by applying different distance measurement techniques. AI techniques which were specifically used for Text and Speech analysis, is used to detect insider threat based on HMM, Damerau-Levenshtein (DL), Jaccard Distance (JD), and Cosine Distance (CD). Using previous data for normal behavior, assuming it is Benign, HMM was capable enough to detect the malicious activity. Techniques like DL, JD, and CD proved to be efficient.

An approach developed for Real-time Anomaly Detection in Heterogeneous Data Streams (RADISH) in [10], also identifies anomalous or malicious actions by concurrently analyzing incoming information to learn patterns of normal behavior. The technique searches for anomalous activity from recently learned behavior, such as any exploitation of privileges from within the organization or network. Characterization of benign behavior is performed automatically without any prior information with learning (RADISH-L) and alerting (RADISH-A) that run concurrently. A well-known Machine Learning (ML) approach K-Nearest Neighbor [11] with slight modification (Modified KNN) algorithm is used to detect malicious insider attack in a collaborative environment. The modified element in KNN includes a factor of weight and validity which show more prominent results, though this research is prone to false positives.

B. MALICIOUS INSIDER ATTACK IN IoT

The Isabelle Insider Framework [12] standardises the methods for modeling and analysing Insider threats. This framework integrates the physical and logical aspects by combining the policy invalidation with mathematical proofs, choosing a scenario for Malicious Insider Attack including attributes like the physical location of attacker and vulnerable devices. To detect malicious insider attacks in IoT, Isabelle insider framework has been implemented. The authors apply the standard methodology to detect violation in policy. In [13] the same Isabelle Insider Framework is used and the technique presents an improved approach for insider threats on the IoT based on attack trees. The authors implement and successfully characterize the intentions of the device or sensor as either malicious or accidental. The system is fully automated and all the attack vectors summarized in defined model can successfully detect a threat. But this solution cannot be used for AI-based malicious insider attack detection due to the complexity of the framework.

Existing techniques like unsupervised learning (recorded access logs) are not applicable due to IoT constraints such as low memory and computational power as the logs cannot be stored locally on the IoT device. Psychological and behavioral factors [14], have been used to detect Malicious Insider Attack which uses a 3- tier system. The first level detects policy violations, second level calculates anomalies based on behaviours and the third level detects deviations from the user's predefined profiles.

III. PROPOSED WORK

General principles of information security emphasize on securing the user or devices against attacks that originate from external sources. However, it is quite evident from recent research reports that insider threats are on the rise. It is reported [3] that 58% of the incidents originate from inside the network. This point is further highlighted by high impact cases; such as BBC Quote on Edward Snowden's whistle blower [15]. To mitigate the risks posed by an inside attacker, this section presents our novel malicious insider attack detection methodology.

A. PRELIMINARIES

This research proposes an artificial intelligence based solution for the evaluation and detection of malicious insider attacks in the IoT environment. The proposed framework mainly includes three stages: 1) data collection and classification, 2) applying threshold and 3) calculating malicious threats, checking malicious and benign activities and predicting the outcome. The proposed algorithm evaluates the level of maliciousness and also establishes the mechanism of distinguishing benign devices from malicious to facilitate the IoT environment. The proposed algorithm utilizes distance measurements against the IoT dataset derived from Computer Emergency Response Team (CERT). The conventional Artificial Intelligence (AI) algorithms such as Deep Learning, Neural Networks, Hidden Markov Model are considered resource intensive. Conventionally, Damerau-Levenshtein DM techniques have been applied to speech recognition and text analysis. The proposed work is based on the research by Lo. *et al.* [9]. This research focuses on insider attack detection using different distance measurement techniques discussed below:

1) DAMERAU- LEVENSHTEIN DISTANCE

The DL (Damerau Levenshtein) distance [16], which has been traditionally applied to string values, calculates the distance measurement between the numbers of operations that are required for one value to be changed to the another value. Changes allowed in DL algorithm include insertion, deletion, and replacement of values. Furthermore, transposition of adjacent values is included.

$$\begin{gathered} minimum(d[i-1,j-1]+cost), //substitution \\ d[i,j-1]+1, //insertion \\ d[i-1,j]+1, //deletion \\ d[k-1,l-1]+(i-k-l)+1+(j-l-1))//transposition \end{gathered}$$

2) JACCARD DISTANCE

Jaccard similarity coefficient [17] is a measure of similarity between two sets of data. The Jaccard distance calculates the difference between two sets, obtained by dividing the variance of the union and the intersection of two sets by their union.

$$\begin{aligned} Jaccard\ Coefficient &= \frac{|A \bigcap B|}{|A|+|B|-|A \bigcap B|} \\ Jaccard\ Distance &= 1 - Jaccard\ Coefficient \end{aligned}$$

3) COSINE DISTANCE

Cosine similarity [18] is a calculation of similarity between two sets of data comparative to the angle of Cosine between the two datasets. A similarity value of 1 means the two sets of data are the same and value of 0 represents non-similar datasets.

$$\begin{aligned} Cosine\ Similarity &= \frac{\sum_{i=1}^{n} A_i B_i}{\sqrt{\sum_{i=1}^{n} A_i^2}\sqrt{\sum_{i=1}^{n} B_i^2}} \\ Cosine\ Distance &= 1 - Cosine\ Similarity \end{aligned}$$

4) LV DISTANCE MEASUREMENT

This distance measurement technique "Levenshtein distance (LV)" is named after the Soviet mathematician Vladimir Levenshtein [19], that measures the similarity between two strings. Informally, it considers the minimum number of single-character edits (insertions, deletions or substitutions) required to change one word into the other. The final score of deviation is evaluated for decision making is given by:

$$\begin{gathered} minimum(d[i-1,j]+1), //deletion \\ d[i,j-1]+1, //insertion \\ d[i-1,j-1]+substitution\ cost)//substitution \end{gathered}$$

B. WORKFLOW

The proposed malicious insider threat detection system studies sensor's activities which is then classified further as benign or anomalous activity. In this IoT system, the outside data is collected first from the database or data stream and then features are mined that uncover relevant attributes related to a specific sensor. After feature extraction the data is filtered to an offline database for further activities including training and testing purposes. Finally the attack classification results are generated based on the distance measurement (DM) technique where it is used for further judgment. The proposed DM algorithm is discussed in section 3. Finally, the attack response is concluded in terms of week depending on the results from previous stages. The proposed framework is roughly categorized into three phases:

1) DATA GATHERING AND CLASSIFICATION

In this phase, data from the outside is collected first and a single sensor is selected so that the data can be filtered from among thousands of sensors. Afterwards it is assigned with activity number based upon known behaviors from the sensors. The collected data is taken forward to the smoothing algorithm or pre-processing stage for extracting features that are used to classify the threat later on. Figure 1 shows the data gathering and classification process. The data extracted from this phase will be fed as input to the next phase which is the threshold application and malicious threat calculation. It is also worth mentioning that all the sensors can be processed one-by-one depending upon the requirements/ need.

2) APPLYING THRESHOLD AND CALCULATING MALICIOUS THREAT

In this phase, the incoming traffic is passed through the threshold algorithm which basically smooths the traffic and removes the small spikes which usually are not malicious activities rather considered as benign. The smoothed data is then processed for malicious insider threat detection from the sensors and any malicious behavior from the sensor is recorded in terms of weeks, the Loop repeats itself by gradually changing the thresholds values until a malicious activity is discovered. Figure 2 represents the flow of events that take place while applying the threshold and calculating the malicious threat.

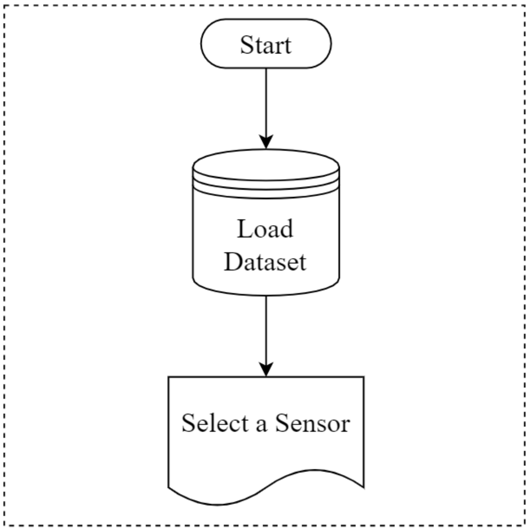


FIGURE 1. Data gathering and classification.

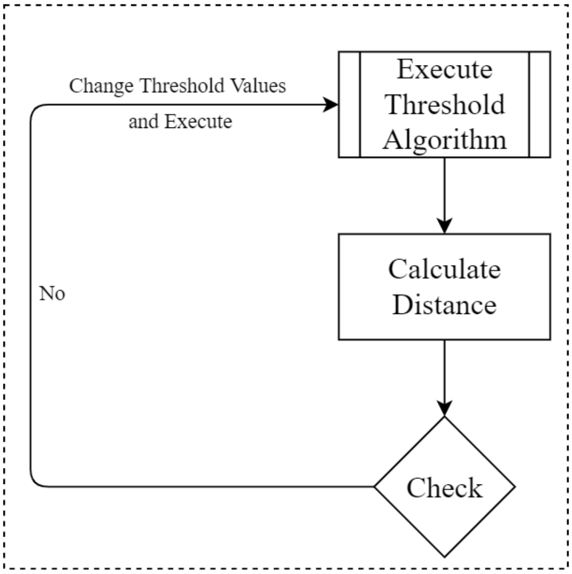

Change Threshold Values and Execute
Execute Threshold Algorithm
Calculate Distance
No
Check

FIGURE 2. Applying threshold and calculating malicious threat.

3) CHECKING FOR ANOMALY/ BENIGN AND CONCLUDING

In the final phase the goal of attack response module is to minimize false positives by allowing the legitimate traffic to move forward. The data is forwarded if the malicious activity is not found under the defined limits. The threshold algorithm is reapplied with specific values for normal behavior and the result is concluded as depicted in the figure 3.

C. SENSOR EXTRACTION AND LEARNING SEQUENCES

Figure 4 presents a bird's eye view of the proposed algorithm by depicting the sensor data extraction and learning sequence of the proposed framework. The complete flow is divided into number of steps discussed as follows:

- Data from every individual sensor in the IoT network is first extracted.

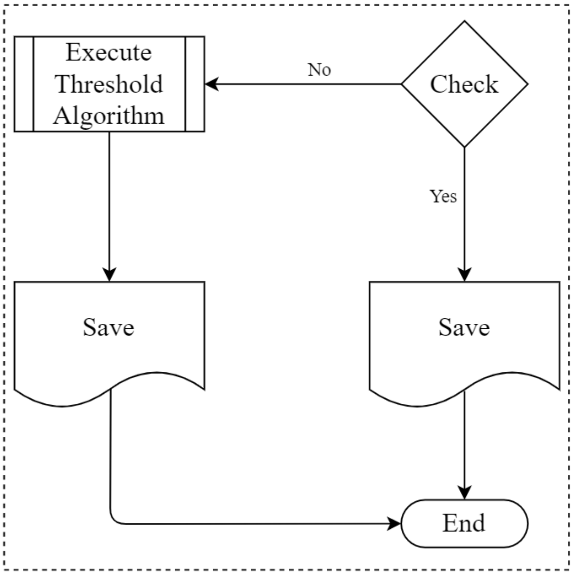


FIGURE 3. Checking for malicious/benign, concluding and calculating malicious threat.

- Later on the activities of the corresponding sensors are identified.
- Then these activities are grouped week-wise and distinguished as benign or normal.
- Activities are compared to previous week's activity and deviation greater than previous week's activity causes a spike/malicious behavior to be detected.

IV. PROPOSED ALGORITHM

In this section a dataset for IoT environment is used and analyzed for insider attack detection in the IoT environment. The proposed framework is represented as three phases and the associated algorithms are discussed in this section.

A. DATA EXTRAPOLATION AND THRESHOLD

In the proposed algorithm, first the malicious activity is taken into account for experimentation. The pseudocode code for insider attack is presented in the Algorithm 1. The algorithm is divided into two parts; in the first part libraries are loaded along with the dataset containing sensor data. Later on a single sensor is selected and the data is then categorized based on different activities. The data set is then formatted and presented week wise.

In the second part the data is smoothed to avoid any false positives. The threshold algorithm is based on the combination of three parameters; lag, threshold value and influence value. "lag" indicates the lag of the moving window, the "threshold value" is the z-score at which the algorithm signals, and "influence value" ranges between 0 and 1 of new signals on the mean and standard deviation. The average value (mean) and standard deviation are compared for the data to identify a signal as positive or negative. Influenced value is applied, filter is adjusted in the final phase and the resultant value based on the signal is stored.

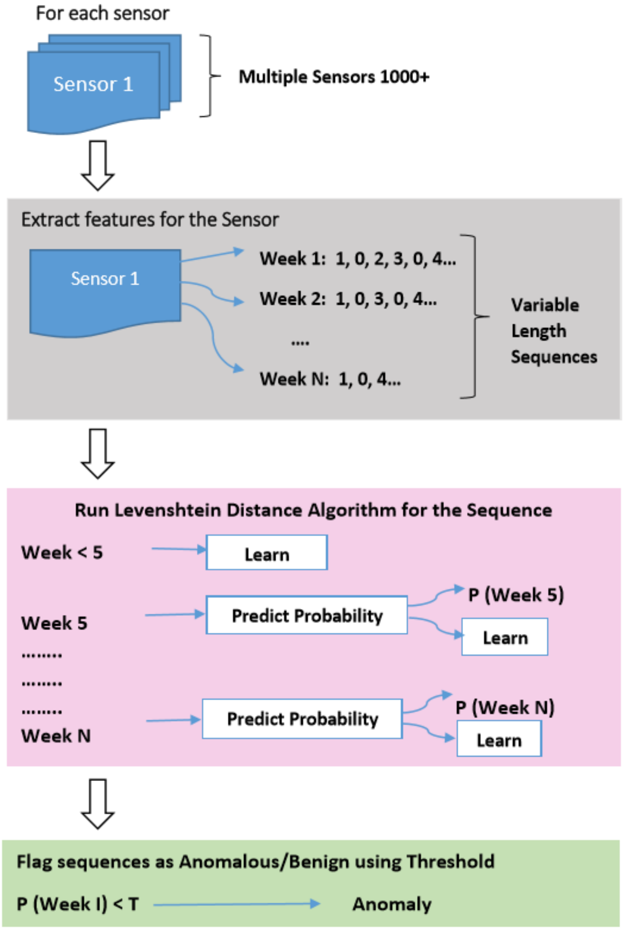


FIGURE 4. Sensor extraction and learning sequences.

B. DISTANCE CALCULATION MALICIOUS

In this phase data from the previous phase is bought forward and processed to calculate distance measurement for any malicious activity. Initializing the loop with the length of dataset, distance measurement is calculated using "stringdist" library. The function used is sequential distance where LV algorithm is selected, resultant week value is assigned with +5 increment considering the first 5 weeks as benign. Week value is compared with distance value to match the existence of malicious activity. If there is no malicious activity the values of ThresholdAlgo are readjusted gradually and the whole process is repeated. The distance measurement process is carried out again where threshold algorithm's parameter "lag" and malicious activity week is rechecked for different lag values. The parameters of lag are changed gradually if required. The pseudocode for the distance calculation is presented in the Algorithm 2.

C. BENIGN/ MALICIOUS

The last algorithm is for benign activity which is only required when no malicious activity is found previously. The parameters for benign activity are adjusted and the ThresholdAlgo is repeated. Then the distance measurement

Algorithm 1 Load Libraries & Data Extrapolation

```
BEGIN Procedure
Load Libraries
Load Dataset
Identify Sensor
Filter dataset according to relevant to sensor
Split sensor activities
Convert data into week format
################## Threshold and Data Extrapolation ##################
Initialize lag = 20, threshold Value 5, influence Value 0
repeat ################## Start Repeat Loop##################
Set ThresholdAlgo
Initialize signals, filteredy, avgFilter, stdFilter, avgFilter[lag] , stdFiltr[lag]
for (i in (lag+1):length(y))
    if (abs(y[i]-avgFilter[i-1]) > threshold*stdFilter[i-1])
        if (y[i] > avgFilter[i-1])
            then signals[i] <- 1
        else
            signals[i] <- 1
        end if
        then filteredy[i] <- influence*y[i]+(1-influence)*filteredy[i-1]
    else
        signals[i] <- 0, filteredy[i] <- y[i]
    end if
    Set avgFilter[i] <- mean(filteredy[(i-lag):i])
    Set stdFilter[i] <- sd(filteredy[(i-lag):i])
    Set return(list("signals"= signals,"avgFilter"= avgFilter,"stdFilter"= stdFilter))
end for
Set result <- ThresholdAlgo(y,lag,threshold,influence)
Set res<-result$signals
END Procedure
```

algorithms are executed. This could be considered as an extension to previous algorithm with altered parameters. The pseudocode for the categorization of activity as benign/ malicious is presented in the Algorithm 3.

V. IMPLEMENTATION AND PERFORMANCE METRICS

To assess the proposed malicious insider threat detection technique in IoT, simulation-based experiments are conducted. The proposed technique is evaluated and the comparison with existing techniques is performed separately using R programming platform. The dataset used in the experiment is generated using NS-2 simulation and based on Computer Emergency Response Team (CERT). To conclude, a detailed analysis is done based on the results gathered by simulating the proposed technique in comparison with simulation-based results acquired from existing distance measurement techniques. Accuracy and efficiency are among the most important parameters for evaluating an algorithm. Efficiency refers to the identification of a threat with less computational time and it is the measure of the time required to compute/ process one data frame. In terms of the computational complexity, the proposed technique has been compared with existing techniques discussed in the literature review presented in the section II. Table 1 presents a qualitative analysis of the existing schemes by highlighting whether the schemes can be used in the IoT environment and do they have AI capability. The analysis is based on three parameters; complexity (lightweight), IoT environment and AI compatibility. The complexity is analyzed to identify the lightweight property of the techniques under the identified parameters.

A. EXPERIMENTAL SETUP

The environment is setup for the analysis of the proposed scheme as mentioned below:

- The proposed algorithm based on LV distance measurement technique is implemented in R Studio using R programming language [20].
- Synthetic data for the IoT environment is generated by simulating in NS-2 using CERT dataset.
- R studio is installed on windows platform and the environment variable for R programming is set accordingly.
- Libraries for dataset, date formatting and distance measurement techniques were setup accordingly for evaluating existing mechanisms as well as for analyzing the proposed technique. The library used is stingiest readr lubridate HMM.

Algorithm 2 Distance Calculation Malicious

```
BEGIN Procedure
Initialize w
for(i in 6:length(res))
    if (i <= length(res))
        Set di <- seq_dist(na.omit(res[i]), na.omit(res[i-1]), method="lv")
        Set w[i - 5] <- di
    end if
end for
Set highestDist = 0;
for(result in w)
    if ((result) > highestDist)
        highestDist = result
    end if
end for
Set hd_week = match(highestDist, w) + 5
if (hd_week <= 6 && lag == 20)
    lag <- 25, print(lag)
else if (hd_week <= 6 && lag == 25)
    lag <- 10, print(lag)
else if (hd_week <= 6 && lag == 10)
    lag <- 35, print(lag)
else if (hd_week <= 6 && lag == 35)
    lag <- 40, print(lag)
else if (hd_week <= 6 && lag == 40)
    then break, print(lag)
end if
END Procedure
```

- All the project files are compiled, simulation is run and the threats are identified.

B. PERFORMANCE EVALUATION MATRIX

The proposed algorithm based on LV distance measurement is assessed using the following metrics to calculate the overall performance: accuracy for attack detection, false alarm rate, computational cost, and computational time. These performance metrics are vital for the evaluation of any attack detection technique.

C. ACCURACY OF ATTACK DETECTION

The accuracy of attack detection is the measure of proportion of number of true guesses to the total number of experimented examples. To measure accuracy of detection, accuracy matrix is depicted in table 2. The accuracy is detected as:

- True Positive = Tested activity that is correctly categorized as Malicious.
- True Negative = Tested activity that is correctly categorized as Benign.
- False Positive = Tested activity that is incorrectly categorized as Malicious.
- False Negative = Tested activity that is incorrectly categorized as Benign.

In general, the accuracy of proposed algorithm based on LV distance measurement is the combination of True Positive and True Negative with their ratio against the total number of tested sensors. The accuracy is calculated using equation 1.

$$\mathit{Attack\ Detection\ Accuracy} = \frac{\mathit{True\ Positives} + \mathit{True\ Negatives}}{\mathit{Total\ Number\ of\ Tested\ Samples}} \tag{1}$$

D. FALSE ALARM RATE

The number of false positives caused by proposed algorithm based on LV distance measurement is calculated as the mixture of both False Positives and False Negatives

E. FALSE POSITIVE RATE

False positive rate for proposed algorithm based on LV distance measurement is defined as a proportion of the total number of authentic activities recognized as anomalous to the total number of activities. The false positive rate is calculated using equation 2.

$$\mathit{False\ Positive\ Rate} = \frac{\mathit{Benign\ Sensor\ Incorrectly\ Classified\ as\ Malicious}}{\mathit{Total\ Number\ of\ Sensors}} \tag{2}$$

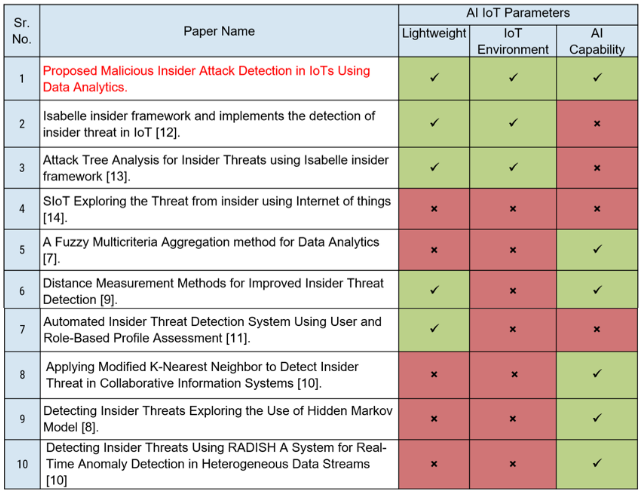
F. FALSE NEGATIVE RATE

False negative rate for the proposed algorithm based on LV distance measurement is defined as a proportion of the total number of malicious activities recognized as benign activity

Algorithm 3 Benign/Malicious

```
############# Distance Calculation Benign ################
else if (hd_week < 70)
Initialize lag = 30, threshold Value 10, influence Value 0
Set ThresholdAlgo
Initialize signals, filteredy, avgFilter, stdFilter, avgFilter[lag] , stdFiltr[lag]
for (i in (lag+1):length(y))
   if (abs(y[i]-avgFilter[i-1]) > threshold*stdFilter[i-1])
         if (y[i] > avgFilter[i-1])
            signals[i] <- 1
         else
            signals[i] <- 1
         end if
      filteredy[i] <- influence*y[i]+(1-influence)*filteredy[i-1]
   else
         signals[i] <- 0, filteredy[i] <- y[i]
      end if
      Set avgFilter[i] <- mean(filteredy[(i-lag):i])
      Set stdFilter[i] <- sd(filteredy[(i-lag):i])
      Set return(list("signals"= signals,"avgFilter"= avgFilter,"stdFilter"= stdFilter))
end for
Set result <- ThresholdAlgo(y,lag,threshold,influence)
Set res<-result$signals
############# Distance Calculation ################
Initialize w
for(i in 6:length(res))
      if (i <= length(res))
            Set di <- seq_dist(na.omit(res[i]), na.omit(res[i-1]), method="lv")
            Set w[i - 5] <- di
       end if
end for
Set highestDist = 0
for(result in w)
      if ((result) > highestDist)
            highestDist = result
       end if
end for
Set hd_week = match(highestDist, w) + 5
if (hd_week <= 6)
       Set hd_week <- 0
break
else
       print(lag), break
end if
End repeat
############# Distance Calculation Normal ################
else if (hd_week >= 70)
Initialize lag = 30, threshold Value 10, influence Value 0
Set ThresholdAlgo
Initialize signals, filteredy, avgFilter, stdFilter, avgFilter[lag] , stdFiltr[lag]
Set res<-result$signals
############# Distance Calculation ################
Set DistanceCalculationAlgo
End repeat
```

TABLE 1. Qualitative analysis.



Sr. No.	Paper Name	AI IoT Parameters		
		Lightweight	IoT Environment	AI Capability
1	Proposed Malicious Insider Attack Detection in IoTs Using Data Analytics.	✓	✓	✓
2	Isabelle insider framework and implements the detection of insider threat in IoT [12].	✓	✓	×
3	Attack Tree Analysis for Insider Threats using Isabelle insider framework [13].	✓	✓	×
4	SIoT Exploring the Threat from insider using Internet of things [14].	×	×	×
5	A Fuzzy Multicriteria Aggregation method for Data Analytics [7].	×	×	✓
6	Distance Measurement Methods for Improved Insider Threat Detection [9].	✓	×	✓
7	Automated Insider Threat Detection System Using User and Role-Based Profile Assessment [11].	✓	×	×
8	Applying Modified K-Nearest Neighbor to Detect Insider Threat in Collaborative Information Systems [10].	×	×	✓
9	Detecting Insider Threats Exploring the Use of Hidden Markov Model [8].	×	×	✓
10	Detecting Insider Threats Using RADISH A System for Real-Time Anomaly Detection in Heterogeneous Data Streams [10]	×	×	✓

TABLE 2. Accuracy matrix.

	Benign	Malicious
Benign	True Negative	False Positive
Malicious	False Negative	True Positive

to the total number of activity. It can be calculated using equation 3.

$$False\ Negative\ Rate = \frac{Malicious\ Activities\ Incorrectly\ Classified\ as\ Benign}{Total\ Number\ of\ SensorActivities} \quad (3)$$

LV distance measurement is compared with the existing techniques for insider attack detection algorithms in terms of false positive rate and false negative rate and simulated on R programming Studio.

G. COMPUTATIONAL COST

Computational cost is another major factor which focuses on the resource constraints of the IoT environment. It is very important to analyze the computational cost when assessing the performance of malicious insider attack detection technique specifically for the IoT. A computational cost matrix is used to help the decision making for categorizing a threat. It minimizes the cost of categorization by maximizing the correctness of classification. To calculate the computational cost of LV distance measurement, a computational cost matrix is shown in Table 3.

As the primary goal of the proposed algorithm based on LV distance measurement technique is to identify malicious activities, hence, the computational cost of false positive is predictably high. In this research false positives approximately cost five times higher than the cost of false negatives. The equation for calculating the computational cost is stated in equation 4.

$$Cost = (1 - Accuracy\ for\ Attack\ Detection) + (False\ Positive) \quad (4)$$

TABLE 3. Computational cost matrix.

	Benign	Malicious
Benign	0	λ
Malicious	1	0

where λ represents the high computational factor incurred due to the false positives.

TABLE 4. Benign sensor test results.

Sensor ID	DL	Jaccard	Cosine	Proposed
NGF0157	FALSE	FALSE	FALSE	TRUE
LRR0148	FALSE	TRUE	FALSE	TRUE
IRM0931	FALSE	TRUE	FALSE	TRUE
LAP0338	FALSE	TRUE	FALSE	TRUE
AHC0142	FALSE	TRUE	FALSE	TRUE
RRC0553	FALSE	TRUE	FALSE	FALSE
RZC0746	FALSE	TRUE	FALSE	TRUE
ATE0869	FALSE	FALSE	FALSE	TRUE
IIW0249	FALSE	FALSE	FALSE	TRUE
ESJ0670	FALSE	FALSE	FALSE	TRUE
FKK0055	FALSE	FALSE	FALSE	TRUE
JHP0583	FALSE	FALSE	FALSE	TRUE
RAW0915	FALSE	FALSE	FALSE	TRUE
JDC0030	FALSE	FALSE	FALSE	TRUE
YIC0195	FALSE	TRUE	FALSE	TRUE
Benign Sensor Tested (15)	0	7	0	14

H. COMPUTATIONAL TIME

Computational time is the measure of time required to compute one frame of data. Moreover Computational time is also a major factor for evaluating the efficiency of the proposed mechanism for the detection of insider attack. The computational time has been compared with existing techniques (presented in the section II) for the proposed algorithm based on LV distance measurement technique. The comparison is presented in the next section.

VI. SIMULATION RESULTS AND COMPARISON

The performance of proposed algorithm based on LV distance measurement is analyzed and compared with other distance measurement techniques. Since most of the existing techniques are based on the distance algorithms presented earlier in the section III, therefore this section also leads to a comparison against the state-of-the-art.

A. BENIGN SENSOR TEST RESULTS

As shown in Table 4, the summary of results for benign sensors are categorized with respect to the proposed technique, DL, Jaccard and Cosine techniques. The DL and Cosine techniques generates the highest false positives by alerting benign sensors as malicious, while Jaccard distance tagged majority of the benign sensors positively. Lastly the proposed technique based on LV is the most successful showing 90% sensors as benign.

B. MALICIOUS SENSOR TEST RESULTS

As shown in Table 5, the summary of results for malicious sensors are categorized with respect to the implemented technique. The DL and Cosine techniques detect the highest

TABLE 5. Malicious sensor test results.

Sensor ID	DL	Jaccard	Cosine	Proposed
KLH0596	TRUE	TRUE	TRUE	TRUE
MCF0600	TRUE	TRUE	TRUE	TRUE
AJR0932	TRUE	TRUE	TRUE	TRUE
DCH0843	TRUE	TRUE	TRUE	TRUE
MYD0978	TRUE	TRUE	TRUE	TRUE
RAB0589	TRUE	TRUE	TRUE	TRUE
HXL0968	FALSE	FALSE	TRUE	FALSE
IUB0565	TRUE	FALSE	TRUE	TRUE
LCC0819	TRUE	FALSE	TRUE	TRUE
GHL0460	TRUE	TRUE	TRUE	TRUE
EDB0714	TRUE	FALSE	TRUE	TRUE
PSF0133	TRUE	FALSE	TRUE	FALSE
JGT0221	TRUE	TRUE	TRUE	TRUE
RAR0725	TRUE	TRUE	FALSE	TRUE
RMW0542	TRUE	TRUE	TRUE	TRUE
Total Malicious Sensors (15)	14	10	14	13

TABLE 6. Accuracy matrix.

Accuracy Matrix	Attack Detection Accuracy
DL	32%
Jaccard	37%
Cosine	37%
Proposed	50%

TABLE 7. Computational cost matrix.

Computational Cost Matrix	Cost
DL	5.68
Jaccard	3.33
Cosine	5.63
Proposed	0.85

number of malicious sensors correctly, while Jaccard distance was not able to tag majority of the malicious sensors correctly. Lastly the proposed technique based on LV is nearly similar to Cosine and DL having the most successful detection of more than 90% sensors as malicious.

C. ATTACK DETECTION ACCURACY

As shown in Table 6, the accuracy percentage is summarized based on the equation 1. The result of accuracy percentage is categorized with respect to the implemented technique and compared with the existing techniques. It is observed that the DL technique has the lowest accuracy percentage, while Jaccard and Cosine techniques have moderate accuracy. Finally the Proposed technique based on LV is the most successful showing 50% accuracy overall.

D. COMPUTATIONAL COST MATRIX

As shown in Table 7, the computational cost matrix is based on equation 4. The results of computational cost are categorized with respect to the implemented technique. The DL and Cosine techniques have the highest computational cost, while the Jaccard technique has moderate computational cost. Finally, the proposed technique based on LV has the least computational cost.

The analysis shows that the insider attack detection is more accurate and decreases the false positives as compared to the existing techniques. Moreover, the simulation of the proposed technique was used to assess the performance of proposed technique. The summary of results depict the significance of threshold algorithm which minimizes the false positive rate. It is apparent from summary of results presented earlier that the computational cost of proposed algorithm is also less. Which itself is an advantage considering the resource constraints of the IoT environment. Therefore, the proposed technique is ideal for the IoT environment.

VII. CONCLUSION AND FUTURE WORK

Internet of Things is an emerging technology which has transformed our everyday life. Although, IoT offers tremendous benefits including on-demand availability of networked devices, these devices are prone to security threats. The security threats include data theft from unauthorized access, data leakage and insider attacks. In this regard an Artificial Intelligence-based algorithm is proposed to detect insider attack in IoT. In the IoT environment it is crucial to have an efficient, lightweight and low cost detection mechanism. This research proposes a mechanism to detect malicious insider attacks in the IoT environment by utilizing distance measurement techniques having Artificial Intelligence properties. The research includes comprehensive analysis of existing techniques for detecting malicious insider attacks in the IoT environment. The Levenshtein distance measurement technique is used in the proposed mechanism for the detection of malicious insider attack to ensure the security of critical and sensitive data of devices/sensors in the IoT environment. The proposed algorithm is based on three different mechanisms for the detection of insider attacks that includes data gathering and classification, threshold and distance calculation, and malicious/benign and conclusion. The results show that LV distance measurement technique is AI-based solution which has greater accuracy when compared with other existing techniques. The proposed solution requires less computations therefore it can be deployed in a resource constrained environment such as IoT. The future directions include better accuracy and attack prevention from insider attacks.

REFERENCES

[1] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for Internet of Things: A survey," *J. Netw. Comput. Appl.*, vol. 66, pp. 198–213, May 2016.

[2] S.-K. Choi, C.-H. Yang, and J. Kwak, "System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 2, pp. 906–918, 2018.

[3] M. Alvarez *et al.*, "IBM X-force threat intelligence index: A glimpse at 2017's notable security events," IBM Secur., Armonk, NY, USA, Tech. Rep. 77014377-USEN-02, 2018.

[4] M. Hung, "Leading the IoT-gartner insights on how to lead in a connected world," Gartner, Singapore, Tech. Rep., 2017.

[5] A. J. Hall, N. Pitropakis, W. J. Buchanan, and N. Moradpoor, "Predicting malicious insider threat scenarios using organizational data and a heterogeneous stack-classifier," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 5034–5039.

[6] F. Yuan, Y. Cao, Y. Shang, Y. Liu, J. Tan, and B. Fang, "Insider threat detection with deep neural network," in *Proc. ICCS*, 2018, pp. 43–54.

[7] I. Palomares, H. Kalutarage, Y. Huang, P. M. R. McCausland, and G. McWilliams, "A fuzzy multicriteria aggregation method for data analytics: Application to insider threat monitoring," in *Proc. 17th World Congr. Int. Fuzzy Syst. Assoc. 9th Int. Conf. Soft Comput. Intell. Syst. (IFSA-SCIS)*, Jun. 2017, pp. 1–6.

[8] T. Rashid, I. Agrafiotis, and J. R. Nurse, "A new take on detecting insider threats: Exploring the use of hidden Markov models," in *Proc. 8th ACM CCS Int. Workshop Manage. Insider Secur. Threats*, 2016, pp. 47–56.

[9] O. Lo, W. J. Buchanan, P. Griffiths, and R. Macfarlane, "Distance measurement methods for improved insider threat detection," *Secur. Commun. Netw.*, vol. 2018, Jan. 2018, Art. no. 5906368.

[10] B. Böse, B. Avasarala, S. Tirthapura, Y.-Y. Chung, and D. Steiner, "Detecting insider threats using radish: A system for real-time anomaly detection in heterogeneous data streams," *IEEE Syst. J.*, vol. 11, no. 2, pp. 471–482, Jan. 2017.

[11] P. A. Legg, O. Buckley, M. Goldsmith, and S. Creese, "Automated insider threat detection system using user and role-based profile assessment," *IEEE Syst. J.*, vol. 11, no. 2, pp. 503–512, 2015.

[12] F. Kammüller, "Isabelle modelchecking for insider threats," in *Data Privacy Management and Security Assurance*. New York, NY, USA: Springer, 2016, pp. 196–210.

[13] F. Kammüller, J. R. Nurse, and C. W. Probst, "Attack tree analysis for insider threats on the IoT using isabelle," in *Proc. Int. Conf. Hum. Aspects Inf. Secur., Privacy, Trust*. New York, NY, USA: Springer, 2016, pp. 234–246.

[14] J. R. Nurse, A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese, "Smart insiders: Exploring the threat from insiders using the Internet-of-Things," in *Proc. Int. Workshop Secure Internet Things (SIoT)*, Sep. 2015, pp. 5–14.

[15] (Dec. 2013). *Profile: Edward Snowden*. [Online]. Available: https://www.bbc.com/news/world-us-canada-22837100

[16] C. Zhao and S. Sahni, "String correction using the damerau-levenshtein distance," *BMC Bioinf.*, vol. 20, no. 11, p. 277, 2019.

[17] L. Hamers, "Similarity measures in scientometric research: The Jaccard index versus Salton's cosine formula," *Inf. Process. Manage.*, vol. 25, no. 3, pp. 315–318, 1989.

[18] B. Li and L. Han, "Distance weighted cosine similarity measure for text classification," in *Proc. Int. Conf. Intell. Data Eng. Automat. Learn.* New York, NY, USA: Springer, 2013, pp. 611–618.

[19] F. P. Miller, A. F. Vandome, and J. McBrewster, "Levenshtein distance: Information theory, computer science, string (computer science), string metric, Damerau-Levenshtein distance, Spell checker, Hamming distance," VDM Publishing House, Mauritius, Tech. Rep., 2009.

[20] *R: A Language Environment for Statistical Computing*, R Found. Stat. Comput., R Core Team, Vienna, Austria, 2017. [Online]. Available: https://www.R-project.org/

AHMED YAR KHAN received the bachelor's and master's degrees in computer engineering from the Balochistan University of Information Technology Engineering and Management Sciences, Pakistan. He is currently working as the Assistant Director of the Information System and Technology Department of Securities and Exchange Commission of Pakistan (SECP). His research interests include artificial intelligence, machine learning, and data sciences primarily in the field of security.

RABIA LATIF received the M.S. degree in information security and the Ph.D. degree in information security from the National University of Sciences and Technology, Pakistan, in 2010 and 2016, respectively. She is currently working as an Assistant Professor with the College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia. Her research interests include cloud computing security, healthcare data security, web security, cyber security, and network security. Her professional career consists of activities ranging from Conference Chair and Technical Program Committee member and reviewer for several international journals and conferences.

SEEMAB LATIF received the bachelor's degree in software engineering from Fatima Jinnah Women University, Pakistan, the master's degree in software engineering from the National University of Sciences and Technology, Pakistan, and the Ph.D. degree from The University of Manchester, U.K. She is currently working as an Assistant Professor with the Department of Computing, SEECS, National University of Sciences and Technology. Her research interests include artificial intelligence, machine learning, and natural language processing. Her professional services include Industry Consultations, Conference Chair, and Technical Program Committee member and reviewer for several international journals and conferences.

SHAHZAIB TAHIR received the B.E. degree in software engineering from Bahria University, Islamabad, Pakistan, in 2013, the M.S. degree in information security from NUST, Islamabad, in 2015, and the Ph.D. degree in information engineering from the City, University of London, U.K., in January 2019. He is currently an Assistant Professor with the Department of Information Security, NUST. He is also the Founder and the Chief Technical Officer of CityDefend Limited, U.K. His research interests include applied cryptography and cloud security. He has been a TPC member of many international IEEE conferences. He is a Reviewer of many high-impact journals, including the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, IEEE ICC, Elsevier FGCS, Springer *Cluster Computing*, Springer *Sadhna*, Springer *Science China Information Sciences*, and Springer *Neural Computing and Applications*. He is also an alumni of InnovateUK CyberASAP.

GOHAR BATOOL received the bachelor's degree in computer engineering from the Balochistan University of Information Technology Engineering and Management Sciences, Pakistan, where she is currently pursuing the master's degree in computer engineering. Her research interests include artificial intelligence and the Internet of Things (IoT), specifically spot localization in intelligent transportation systems.

TANZILA SABA received the Ph.D. degree in document information security and management from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia, in 2012. She is currently serving as an Associate Professor and the Associate Chair of the Information Systems Department, College of Computer and Information Sciences, Prince Sultan University, Riyadh, KSA. Due to her excellent research achievement, she is included in Marquis Who's Who (S & T) 2012. She has full command on a variety of subjects and taught several courses at the graduate and postgraduate level. On the accreditation side, she is a skilled with ABET and NCAAA quality assurance. She has more than one hundred publications that have around 1800 citations with H-index 28. Her mostly publications are in the biomedical research published in ISI/SCIE indexed. Her primary researches focus in recent years is medical imaging, pattern recognition, data mining, MRI analysis, and soft-computing. She is the Leader of the Artificial Intelligence and Data Analytics Research Laboratory, PSU, and an active professional member of ACM, AIS, and IAENG organizations. She received the Best Student Award from the Faculty of Computing, UTM, for 2012. She is currently an Editor and reviewer of reputed journals and on the panel of TPC of international conferences. She is the PSU WiDS (Women in Data Science) Ambassador with Stanford University.