Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.034551
Article

Tech Science Press

Detection of Phishing in Internet-of-Things Using Hybrid Deep Belief Network

S. Ashwini* and S. Magesh Kumar

Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (Deemed to be University), Chennai, Tamilnadu, India
*Corresponding Author: S. Ashwini. Email: ashwinisekar.achu@gmail.com
Received: 20 July 2022; Accepted: 13 December 2022

Abstract: Increase in the use of internet of things owned devices is one of the reasons for increased network traffic. While connecting the smart devices with publicly available network many kinds of phishing attacks are able to enter into the mobile devices and corrupt the existing system. The Phishing is the slow and resilient attack stacking techniques probe the users. The proposed model is focused on detecting phishing attacks in internet of things enabled devices through a robust algorithm called Novel Watch and Trap Algorithm (NWAT). Though Predictive mapping, Predictive Validation and Predictive analysis mechanism is developed. For the test purpose Canadian Institute of cyber security (CIC) dataset is used for creating a robust prediction model. This attack generates a resilience corruption works that slowly gathers the credential information from the mobiles. The proposed Predictive analysis model (PAM) enabled NWAT algorithm is used to predict the phishing probes in the form of suspicious process happening in the IoT networks. The prediction system considers the peer-to-peer communication window open for the established communication, the suspicious process and its pattern is identified by the new approach. The proposed model is validated by finding the prediction accuracy, Precision, recalls F1score, error rate, Mathew's Correlation Coefficient (MCC) and Balanced Detection Rate (BDR). The presented approach is comparatively analyzed with the state-of-the-art approach of existing system related to various types of Phishing probes.

Keywords: Cyber security; internet of things; phishing attacks; fault-tolerant devices; smart devices; cyber security attacks

1 Introduction

1.1 Vulnerable Attacks

Keeping the IoT connected devices and Systems to be saved from external honorable attacks, IoT security system is the dedicated module that protects from external attacks and identify the risk present in the network and fix the Vulnerable probes [1–10]. The best IoT keeping system for the complete solution, for availability, integrity, confidentiality of the service system.

1.2 Android Malwares

Most of the Android devices are continuously connected with publicly available network. Even though the device is secured with robust Firewall tools, malicious data is resilient and inserted into the device through various web contents. Frequently used systems that get more sensitive to phishing attacks through unauthorized emails and notification messages.

1.3 Impacts of Phishing Attacks

Massive information as per the global scenario are hacked from the email based phishing attacks. In many cases the initial probing is carried out through frequently used social media websites, E-commerce website, unknown blogs, notification messages etc. The research goal is to collectively model significant key points on phishing probes induced in the IT networks. The analysis is implemented through pattern recognition mechanism. The proposed framework is focused on creating a Novel Predictive analysis mechanism for detecting the various hints coming on way towards the IoT devices.

2 Literature Survey

Murali et al., presented a robust routing protocol to provide low power and lossless network. The author proposed an artificial bee colony algorithm (ABC) to detect the Sybil attack in smart phones. ABC algorithm considered as the light weight intrusion detection system, in which Sybil attack based on network behavior is presented. Three different types of Sybil attack is discussed in the presented system and achieved the detection accuracy of 96.8%. Further, from the conventional approach, probing attacks are required to be focused [11]. Liu et al., Presented a system to detect probe routed sinkhole attack is discussed. The system considers far-sink reverse routing, equal-hop routing, and minimum hop routing in order to find the sinkhole attack efficiently. Sinkhole attack detection need to reveal the signature ID, hence the probing based routing is not enough to locate the sinkhole. The so-called attack is created where the residual energy of the network exists. Fog computing and edge computing approaches are recommended to provide probing the sinkhole attacks [12]. Li et al., presented a paper in which false occurrence of data and practical scenario challenges are solved. A vibrational message passing algorithm is applied to check the network iteratively and find the closed convergence of attacks. The challenging problem is formulated with true posterior distribution on malicious nodes [13–17].

The benefits of IoT devices for an available in current scenario because of high profile accessibility, flexible, applications interfacing and business security [18]. Gradient boosted regression models are considered as one of the robust methodologies in detection of IoT probing attacks that enters into the IoT networks. The drawback of the Gradient boosted models is delay in processing the input patterns with respect to the trained patterns. For all kinds of datasets, gradient boosted algorithms may not get adopted [19]. IoT network enabled mobile edge tracking system is developed here. The presented framework by the author enhances the existing benefit of offloading computations. In case of better accuracy in tracking, multiple objects tracking with single connectivity is also enabled. Based on tracking mechanism, complete security and trust on the network is formulated [20]. Chen et al., presented a detection framework on detecting new GUI-Squatting attack that impact the android devices is presented. In case of security threats found, extensive procedure reveals the emergency attack detector and clearing mechanism. The system is further improved in order to detect many left over attack residuals ever after the complete goal is achieved. Confidence score of 3.9 is achieved on the whole of various phishing app detection. Tang et al., presented deep learning approach for detecting

phishing websites. The implemented framework provides browser plugins and formulates the real time prediction service.

The system focused on Sybil attack on peer-to-peer intrusion detection process. Further it needs to be included with deep consideration of Phishing entries. The attack scenario can focus on more feature consideration. The phishing probes can enter into the peer system towards the node edges. Query injection framework is concerned, multiple algorithms to attain hybrid model is recommended to improve the system performance on multiple feature extraction. On the other hand, distributed networks are highly impacted with malicious nodes in the IoT networks. In case of malicious nodes present in the massive network, the time taken to detect the suspicious node need to be reduced [21–23]. The occurrence of false positive statements is the reason for misclassification or weak classifications [24]. The more phishing impacts are produced in distributed systems. Development of real time data analysis is required with the model created using the standard data [25]. Improvements in smart city environment in future, demands more security in distributed systems. Hence to develop an ideal system suitable to considering real world scenarios, smart city IoT networks to consider distributed networks are keenly included here for making solution model [26].

3 Methodology

3.1 System Architecture

The system architecture is shown in Fig. 1. The proposed research works is motivated towards developing a robust architecture for detection of IoT probing attacks and display the feasible impact parameters that grab the attack scenario. In many publicly available networks, smart devices are getting connected frequently. In the meanwhile, ease of android connectivity enables the probing attacks get easily enter into the device through network [27–30].

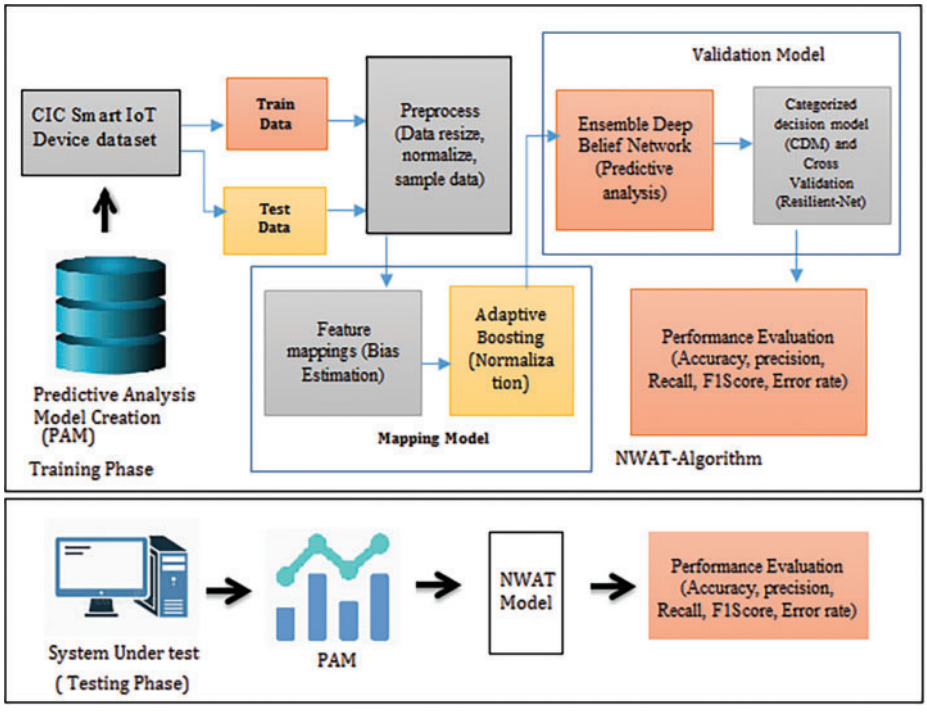

Figure 1: System architecture of proposed PAM enabled NWAT model

3.2 Dataset

The Canadian Institute of cyber security and communication security (CIC) establishment dataset is used to make the IoT based smart device attacking system. The variables of CIC dataset contain the background traffic and malicious traffic based on 7th sense of network attacks including brute force attack help maintain botnet attack, device attack, DDoS attack, web attacks and infiltration attacks. The CIC smart IoT device dataset is the freely available data that consists of various probing attack related feature points such as fake ID fake password, Android defender, email attack etc. The dataset preparation is initiated by reading the dataset, visualizing the data and sampling the data into training data and testing data. The normalization of the dataset his handled by self-organized mapping model. The dataset consists of user information and timestamps appropriate to the given probing attack framework.

3.3 Mapping Model

The dataset after Sampling and normalization process is required to map the unique attributes through Bayes estimation. Each data columns are summarized to find the unique points present in it through Bayes estimation process using self-organized mapping model. Feature fusion is evaluated by extracting unique information of the training data through different techniques. The first technique is focused on fetching the raw data into self-organizing mapping model to adjust the weights assigned to each feature points. The second method focus on calculating the mean median and statistical parameters such as variance standard deviation to formulate the identity of the given data.

3.4 Hybrid Deep Feature Fusion

The need for feature fusion is adopted in very peculiar cased in order to enhance the performance of the analysis model. The input raw data have unique feature points to be extracted. The hybrid approach of feature fusion, ensemble the levels of feed forward network with different training functions. The presented work considers feed forward network with Scaled conjugate gradient network (SCG), One Step Secant Method (OSS), Gradient descent adaptive learning (GDM) is used together for form a fusion of feature mechanism. The adaptive boost algorithm outperforms with effective feature points from the sequentially fused blocks of the SCG, OSS, GDM models.

Fig. 2 shows the Hybrid feature fusion mechanism that sequentially bootstraps the feed forward network of different transfer functions and formulates an adaptively boosted as well as bootstrapped feature vectors. The feature vectors are the transformed version of the input data.

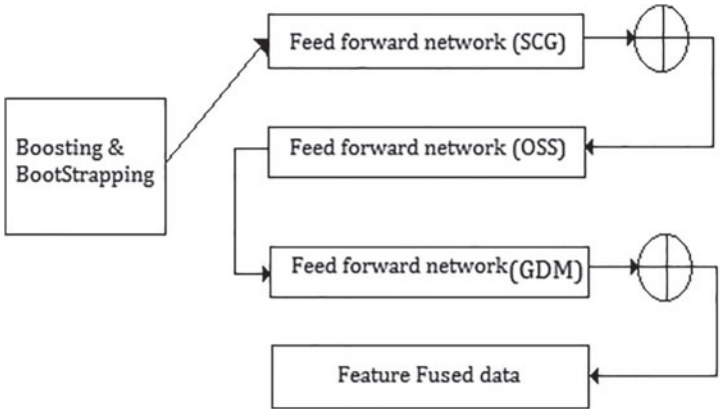

Figure 2: Hybrid feature fusion mechanism

3.5 Scaled Conjugate Gradient (SCG)

trainscg is a simple training function in neural networks used to convert the form of input data as long as the weights associated with the input net, transfer function have a significant derivative. SCG is derived from the below Eqs. (1)–(4),

$$Let\ \{d_1, d_2, \ldots .d_n\}\ be\ the\ input\ vector \tag{1}$$

$$Xscg \rightarrow minimum\ derivative\ of\ f(x) \tag{2}$$

$$\alpha_i \rightarrow Bias\ Weight\ of\ each\ data\ updated\ by\ FFNet \tag{3}$$

$$Xscg = \sum_{i=1}^{n} \alpha_i d_i \tag{4}$$

SCG based FFNet calculates the derivatives of performance function ***perf*.** With respect to the weighted bias variables α_i.

3.6 One Step Secant (OSS)

The secondary FFNet considered here is the one step secant function used as a transfer derivative of neural network. The OSS function for transforming the input data with a minimal search direction with less negative gradient is given by the Eq. (5) below.

$$Xoss = Xinp + \alpha_i * dX \tag{5}$$

3.7 Gradient Descent with Momentum (GDM)

The goal of the GDM perform with the enhanced angle of gradient search process in which, the function combines the adaptive learning benefit with momentum of training iterations. Each variable in the input is adjusted with gradient weight with a momentum function Eq. (6).

$$dX_{gdm} = mc * dX_{gdm}prev + lr * mc * dperf/dX \tag{6}$$

3.8 Process of Feed Forward Network (FFNet)

Training record (epoch and perf), returned as a structure whose fields depend on the network training function (net.NET.trainFcn). It can include fields such as

- Training pattern, data division rate, and performance validation functions and parameters are considered.
- Information division in light of preparing set, approval set and test sets
- Information division covers for preparing approval and test sets
- Number of ages (num_epochs) and the best age (best_epoch).
- A rundown of preparing state names (states).
- Fields for each state name recording its worth all through preparing
- Exhibitions of the best organization (best_perf, best_vperf, best_tperf)

Table 1 shows the Training of Network. Each time the FFNet iterates with maximum epochs, resulted with a new variant transformed data of the raw input, hybrid to form a sequential vectors.

Table 1: Configurations of FFNet

Unit	Initial value	Stopped value	Target value
Epoch	0	19	1000
Elapsed time	–	00:00:08	–
Perfomance	324	9.25e−05	0
Gradient	414	0.000292	1e−07
Mu	0.001	1e−05	1e+10
Validation checks	0	6	6

4 Validation Model

The proposed PAM enabled Novel Wait and Trap (NWAT) algorithm is developed by the boosting the input data after preprocess through Adaptive enhanced boosting algorithm. Further the boosted parameters are passed to validation model through predictive analysis. Predictive analysis holds many learning iterations to read and incorporate the relative pattern. The user information is split up into training data and testing data initially. The robust methodology train the given data set completely and form the labels through continuous iteration of learning process. The bias weights are updated at the end of every learning iteration. The predictive analysis of Deep and simple model enable the learning process more accurate and related to the pattern correlation process. The propose model is further provided with categorized decision making model in which the final decision on pattern correlation is performed based on the highest correlation factor of training data and testing data and exactly the type of IoT attack is detected. The dataset with 2362×85 of test sample is provided to the system under test. The novel system with Predictive analysis Model (PAM) iterates and learns the pattern, the NWAT model trap monitor the loop and trap the occurrence of Probing attacks. The output model with categorical decision model (CDM) is developed with Resilient Network with robust optimization rules. The performance evaluations of the percentage system is developed an updated using accuracy, precision, recall, F1score and error rate estimation. System is comparators with state-of-art approach of meaning existing implementations are discussed in Section 2.

4.1 Process Patterns

The Phishing process are reflected with various records and parameters are depicted in Table 2. For an example, the source port 33644 initiated the data transfer in the IOT networks,

Table 2: Sample record from the CIC dataset

Process parameter	Value recorded
Source port	33644
Destination port	443
Fwd packet length std	236
Bwd packet length max	1448
Fw packets/s	0.325939869
Flow duration	119653972

The destination port is around 443 only connected in active mode.

- The foremost suspicious activity is determined from the major difference between the forward packet length, backward packet length etc.
- As per the flow rate recorded, 0.3259 s approximately in the particular record, the required time to transfer the destination data that reflect back from the device in the network, approximately 443 destination ports got connected which is less than the source port.

4.2 Formation of NWAT algorithm

The Novel wait and trap (NWAT) algorithm is used to acquire the most relevant data from the training data. The dataset used here is the CIC dataset 2017 year that contains the overall recorded information on IoT connected 12 different devices attacked by the Victim probes from the overall devices. The dataset contains the raw information of recorded stampings of user login, mirror ports; source IP, destination IP etc. The main attribute considered here is the Data active duration, idle condition time, Data arrival frame, Flow of frame etc. The massive dataset is preprocessed by normalizing the data through removal of Nan values and scale the data into fixed frames of 800 samples each. The goal of NWAT algorithm is to monitor the loop completely and formulate the relevant match occurrences and its count. Once the network is initiated, the system start accepting the data frames. Once the pattern is trained by the proposed NWAT algorithm (refer to Table 3 for Pseudocode), it opens the ports and wait for the relevant pattern to occur.

Table 3: Pseudocode of NWAT algorithm

Begin
Read $CIC_{ds}, Ndata$
Store $Attri_{ndata(n_{column})}$
Normalize x
$\rightarrow$ $adpBoost\,(x, weight_{bias})$
Store $x1, x2, x3$
$\rightarrow$ $pattern\,(weights)$
$Split_{patterns} = Samples$
$\rightarrow$ $n_{sample_{length}}$
format $(Train_{data}, Test_{data})$
Initiate $Loop_{index} \rightarrow 1,$
Check $corr_{check(Train_{data}, Test_{data})}$
Store $Corr_{Const} \rightarrow 1$
Visualize $data_{plots}$
Store $Classified\_Results\_class$
End

Let $[x_1, x_2, x_3, ...x_n]$ be the sample test input of single attribute, whereas the preprocessed attributes are denoted as, $\{[x_1, x_2, x_3, \ldots .x_{kn}]\}$

where $k \rightarrow$ *attributes* are considered.

$$(H\,(n)) = sign\Big(\sum\nolimits_{k=1}^{N} \alpha_k h_k\,(n) \tag{7}$$

$N \rightarrow$ *length of attribute*

$n \rightarrow$ *total input feature columns considered*

Once the Data is enhanced after the scaling process, the NWAT system initiate the rule set by open the port of the systems and initiate the time t = 0;

At every iteration i, Eq. (7) is repeated for complete dataset. Further, the NWAT is performed as below Eq. (8),

$$pa_{cons(i)} = \sum_{i=1}^{\max\_iter} \{(H(n,i))\} \tag{8}$$

for $i < max_{iter} \rightarrow$ *decided on Complex input pattern*, $\alpha_k \rightarrow$ *ormalization constant*

$pa \quad 1$

$pa \quad 0$

$1 \rightarrow$ *for* max *correlation*,

$0 \rightarrow$ *minimum correlation*

For *max_iter i*, the correlation constants are evaluated and further the NWAT repeat the process until maximum correlation. The cross validation is performed using cross_entrophy by the formula given below Eq. (9).

$$H(p,q) = -\sum_{x \in total\ classes} p(x), \log q(x) \tag{9}$$

$p(x) \rightarrow$ *true probability distribution*

$q(x) \rightarrow$ *predicted distribution*

The NWAT model predicts the maximum match between the train data and test data through the occurrence of less error rate. The error rate is obtained through the Mean square error (MSE) formula mentioned below Eq. (10).

$$MSE(x) = \frac{1}{N} \sum_{i=1}^{N} (y_i - yk_i) \tag{10}$$

y_i, yk_i, the obtained result and predicted results respectively. The proposed system evaluated the predictions of the vulnerable attacks using the test scores produced from confusion matrix. Confusion matrix is a two-dimensional Matrix that represents the correlation of true conditions and predicted results. True positive describes the number of abnormal samples being accurately classified; True negative defines a number of normal samples being accurately classified. False positive specifies the number of normal samples being falsely classified as normal samples. False negative specifies the number of abnormal samples using being classified as false as normal samples. Various test scores were calculated using confusion matrix such as accuracy Precision recall and F1 score.

5 Results and Discussions

5.1 Existing Works and Comparative Results

Fig. 5 shows the various confidence score framework of various malfunctioning apps are detected from the IoT networks.

5.2 Performance Plots of Various Probing Test Input

The Probing inputs after preprocess, fetched directly into the prediction model, in which the performance of the overall iteration is shown in Fig. 3. Shows the instance, the best performance of the given iteration captured. Some of the Probing attacks focused on the proposed System are Android defender, Fake Application, Fake job Offers, Fake Virus shield, noisy data insertion and normal input also classified.

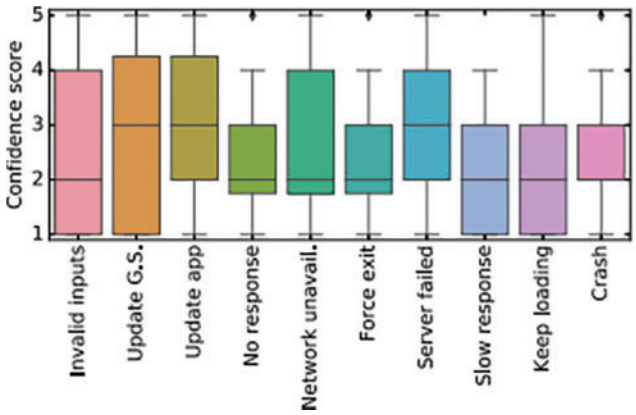

Figure 3: The confidence of treating apps as phishing apps according to different responses [24]

Fig. 4 shows the performance of the model get varies with respect to the complexity of the input pattern. For various test cases as inputs the NWAT architecture perform best trap at different ranges.

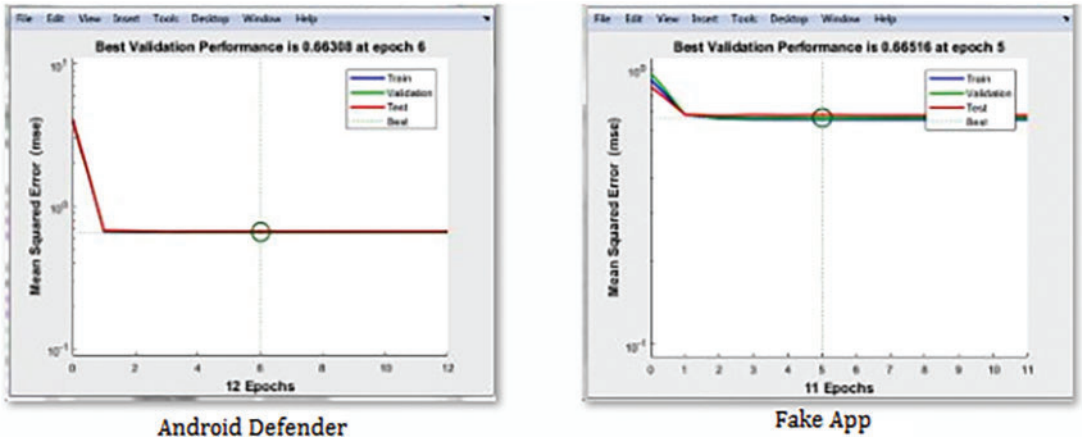

Figure 4: (Continued)

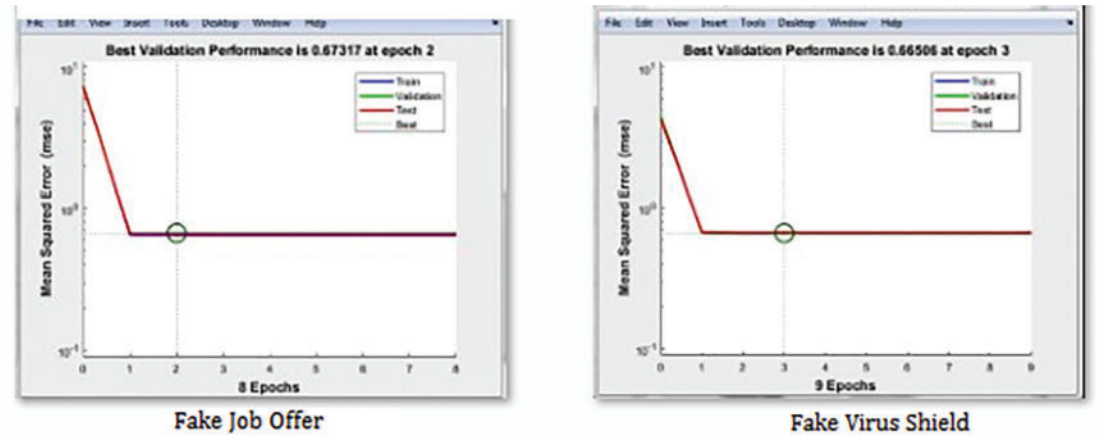

Figure 4: Captured best performance instance of given test inputs at different epochs

5.3 RMSE of HFF-EDBN

Fig. 5 shows the RMSE value of the proposed HFF-EDBN model in which the error rate reduced with respect to the increase in the iterations.

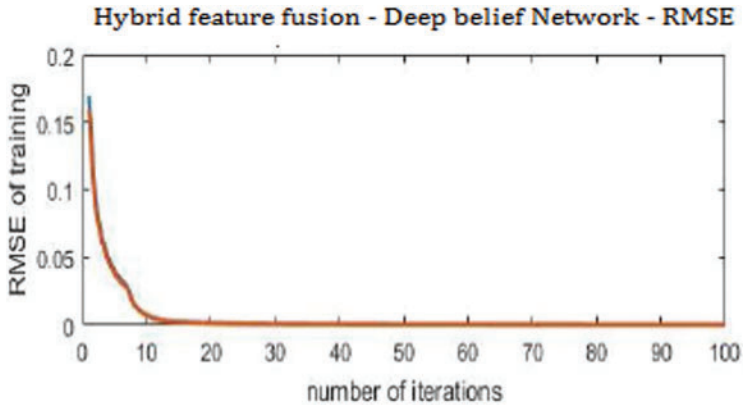

Figure 5: RMSE of proposed HFF-EDBN model at 100 iterations

Table 4 describes the number of attacks detected from the given CIC dataset with respect to the error rate.

Table 4: List of probing attacks & corresponding parameters

Sl. No	Attack name	Category	Error rate	RMSE	Sensitive iterations
1	FakeApp	ScareWare	0.02611	(0.15–0.00)	15
2	FakeJobOffer	ScareWare	0.0271	(0.22–0.00)	17
3	FakeVirusShield	ScareWare	0.009118	(0.16–0.00)	20
4	AndroidDefender	ScareWare	0.08001	(0.12–0.00)	10

5.4 Error Rate

Fig. 6 shows the error rate measured with respect to the probing attacks detected. Lower the error rate determine the best training happened in the optimization process.

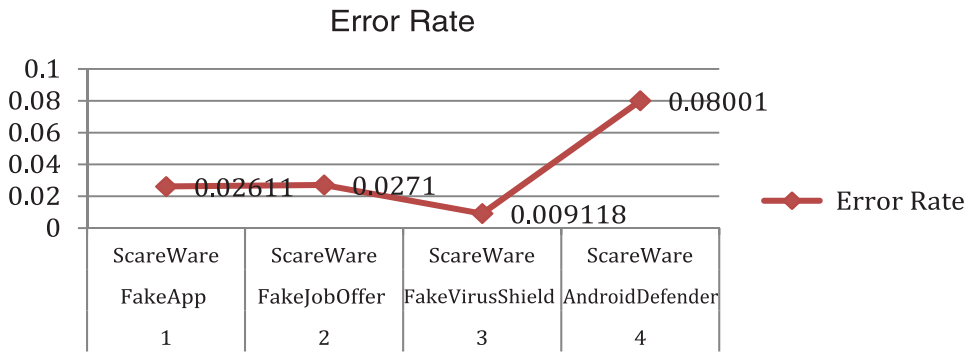

Figure 6: Error rate *vs*. attacks

Table 5 shows the Comparison results of existing systems and their results with respect to the proposed HFF-EDBN model,for the detection of proposed probing attacks.

Table 5: Comparison of existing systems with respect to proposed HFDBN model

Sl. No	Reference	Model description	Methodology	Attack type	Accuracy	Precision	Recall	F1Score
1	Murali et al.,	IoT Node attacks	ABC algorithm	Sybil attacks	96.80%	0.96	0.85	0.87
2	Wan et al.,	IoTAthena	SigMatch	Plug&Play attack	95%	0.95	0.88	0.85
3	Zhu et al,	SEDMDroid	PCA, MLP, SVM	Android malware	94.92%	0.94	0.89	0.68
5	Aassal et al.,	TPOT	DLN	Phishing attack	85.81%	093	0.85	0.94
6	Tang et al.,	RNN-GRU	DLN	Phishing attack	98.10%	0.98	0.97	0.87
7	Alsariera et al.,	Meta learning ETree	AI	Phishing attack	97%	0.97	0.95	0.88
8	Proposed method	Hybrid feature fusion DBN	N-WAT	Android probes	98.12%	0.98	0.91	0.89

Table 6 shows the elapsed time of processing the NWAT model is listed. Each attacks have a specific pattern of records, thus generated and interpreted in specific time slot.

Table 6: NWAT processing time

Sl. No	Attack name	Category	Elapsed wait_time	Elapsed trap_time	Sensitive iterations
1	FakeApp	ScareWare	40 S	5–7 S	15
2	FakeJobOffer	ScareWare	58 S	4–7 S	17
3	FakeVirusShield	ScareWare	30 S	4–8 S	20
4	AndroidDefender	ScareWare	36 S	5–8 S	10

6 Conclusion

The major challenge faced from the above implementation is the handling the complex dataset with a greater number of columns. This pattern is the complete recorded real time information and its time stampings. In order to read and sample those inputs the processing delay is highly increased. Further to improve such reading process and reduce the challenge, multi-spectral machine learning algorithms need to be developed. Behavior of IoT networks is more difficult to predict in real-time scenario. The number of destination ports connected, Source pc count, flow duration after the node gets connected, forward and backward flow rate etc. The proposed research work is focused on creating a robust detection model that detects the phishing probes activities in the IoT network using CIC dataset. Keeping the massive demands of security in 5G networks, and smart systems in future, identification of Impact parameters of the Phishing attacks are thoroughly verified and highlighted using Novel Wait and Trap algorithm (NWAT). Predictive Analysis Module (PAM) enabled algorithms are helpful in making the correlated peak points with iterative analysis. The novel algorithm runs to the repeated predetermined iterations to trap the attack pattern. The proposed system is achieved the accuracy of 98.12% with less error rate of 0.02611. Further the system needs to be improved by evaluating a Light-weight multi-Spectral machine learning models to reduce the processing delay. The Phishing process and legitimate process are identifying with the presented approach need to be improved with reducing the detection time. Prevention of phishing process is the explored research scope in IoT networks.

Acknowledgement: The authors would like to thank the Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (Deemed to be University) for providing facilities to carry out the research work.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Serror, S. Hack, M. Henze, M. Schuba and K. Wehrle, "Challenges and opportunities in securing the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2985–2996, 2021.

[2] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava *et al.*, "Enabling drones in the internet of things with decentralized blockchain-based security," *IEEE Internet of Things Journal,* vol. 8, no. 8, pp. 6406–6415, 2021.

[3] L. Zhang, J. Wang and Y. Mu, "Privacy-preserving flexible access control for encrypted data in internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 19, pp. 14731–14745, 2021.

[4] N. Ravi and S. M. Shalinie, "Semisupervised-learning-based security to detect and mitigate intrusions in IoT network," *IEEE Internet of Things Journal*, vol. 7, no. 11, pp. 11041–11052, 2020.

[5] V. Borgiani, P. Moratori, J. F. Kazienko, E. R. R. Tubino and S. E. Quincozes, "Toward a distributed approach for detection and mitigation of denial-of-service attacks within industrial internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4569–4578, 2021.

[6] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[7] M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah and M. Gidlund, "A machine-learning-based technique for false data injection attacks detection in industrial IoT," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8462–8471, 2020.
[8] A. N. Jahromi, H. Karimipour, A. Dehghantanha and K. -K. R. Choo, "Toward detection and attribution of cyber-attacks in IoT-enabled cyber– physical systems," *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13712–13722, 2021.
[9] V. Kumar and R. Kumar, "Detection of a phishing attack using visual cryptography in ad hoc network," in *Int. Conf. on Communications and Signal Processing (ICCSP)*, Melmaruvathur, pp. 1021–1025, 2015.
[10] R. B. Basnet and T. Doleck, "Towards developing a tool to detect phishing URLs: A machine learning approach," in *IEEE Int. Conf. on Computational Intelligence & Communication Technology*, Ghaziabad, 2015.
[11] S. Murali and A. Jamalipour, "A lightweight intrusion detection for sybil attack under mobile RPL in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 379–388, 2020.
[12] Y. Liu, M. Ma, X. Liu, N. N. Xiong, A. Liu *et al.*, "Design and analysis of probing route to defense sink-hole attacks for internet of things security," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 356–372, 2020.
[13] S. Malani, J. Srinivas, A. K. Das, K. Srinathan and M. Jo, "Certificate-based anonymous device access control scheme for IoT environment," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9762–9773, 2019.
[14] F. Li, Y. Shi, A. Shinde, J. Ye and W. Song, "Enhanced cyber-physical security in internet of things through energy auditing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5224–5231, 2019.
[15] M. Naveed Aman, S. Taneja, B. Sikdar, K. C. Chua and M. Alioto, "Token-based security for the internet of things with dynamic energy-quality tradeoff," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2843–2859, 2019.
[16] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan and R. Jain, "Machine learning-based network vulnerability analysis of industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6822–6834, 2019.
[17] Y. Li, S. Ma, G. Yang and K. -K. Wong, "Secure localization and velocity estimation in mobile IoT networks with malicious attacks," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6878–6892, 2021.
[18] S. Park, J. Park and J. Oh, "Design and implementation of trusted sensing framework for IoT environment," *Journal of Communications and Networks*, vol. 23, no. 1, pp. 43–52, 2021.
[19] J. Su, S. He and Y. Wu, "Features selection and prediction for IoT attacks," *High-Confidence Computing*, vol. 2, no. 2, pp. 100047, 2022.
[20] Y. Wu, P. Tian, Y. Cao, L. Ge and W. Yu, "Edge computing-based mobile object tracking in internet of things," *High-Confidence Computing*, vol. 2, no. 1, pp. 100045, 2022.
[21] J. Wang, S. Hao, R. Wen, B. Zhang, L. Zhang *et al.*, "IoT-praetor: Undesired behaviors detection for IoT devices," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 927–940, 2020.
[22] Y. Wan, K. Xu, F. Wang and G. Xue, "IoTAthena: Unveiling IoT device activities from network traffic," *IEEE Transactions on Wireless Communications*, vol. 21, no. 1, pp. 651–664, 2022.
[23] H. Zhu, Y. Li, R. Li, J. Li, Z. You *et al.*, "SEDMDroid: An enhanced stacking ensemble framework for android malware detection," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 984–994, 2021.
[24] S. Chen, L. Fan, C. Chen, M. Xue, Y. Liu *et al.*, "GUI-squatting attack: Automated generation of android phishing apps," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 2551–2568, 2021.
[25] A. El Aassal, S. Baki, A. Das and R. M. Verma, "An in-depth benchmarking and evaluation of phishing detection research for security needs," *IEEE Access*, vol. 8, pp. 22170–22192, 2020.
[26] Y. -W. Lee, H. Lim, Y. Lee and S. Kang, "Robust secure shield architecture for detection and protection against invasive attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 10, pp. 3023–3034, 2020.

[27] S. Mathupriya, S. S. Banu, S. Sridhar and B. Arthi, "A survey of the impact of digital twin technology on IoT, industries, and other smart environments," *Journal of Computational Science and Intelligent Technologies*, vol. 3, no. 1, pp. 17–23, 2022. https://doi.org/10.53409/MNAA/JCSIT/e202203011723

[28] S. F. Noori and B. B. Ahamad, "A deep web data extraction framework enhancement method," *Journal of Computational Science and Intelligent Technologies*, vol. 3, no. 1, pp. 33–42, 2022. https://doi.org/10.53409/MNAA/JCSIT/e202203013342

[29] M. N. Reem, Q. A. Asrar, S. F. Jameelah and M. Q. Albalawi, "Smart logistics using internet of things (IoT)-study," *Journal of Computational Science and Intelligent Technologies*, vol. 2, no. 2, pp. 24–34, 2021. https://doi.org/10.53409/mnaa/jcsit/2204

[30] R. Khilar, K. Mariyappan, M. S. Christo, J. Amutharaj, T. Anitha *et al.,* "Artificial intelligence-based security protocols to resist attacks in internet of things," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1440538, pp. 1–10, 2022. https://doi.org/10.1155/2022/1440538