DOI: 10.21917/ijct.2021.0358

A COMPARATIVE STUDY ON CYBER SECURITY THREATS DETECTION IN INTERNET OF THINGS

P. Vijayalakshmi and D. Karthika
Department of Computer Science, P.K.R. Arts College for Women, India

Abstract

Internet of Things (IoT) is an evolving digital technology, which is mainly meant to bridge physical and virtual world. New business model has been emerged because of people, objects, machines and Internet connectivity along with new interactions amid humanity and remaining world. IoT is considered as a gateway for cyber-attacks since various resources such as systems, applications, data storage, and services are connected through IoT that relentlessly provide services in the organization. IoT security is challenging factor due to prevailing software piracy and malware attacks presently. The economic and reputational damages are caused by these threats due to crucial information burglary. IoT malware detection is yet another challenging factor due to security design deficiency besides IoT devices specific characteristics such as processor architecture heterogeneity, particularly on identifying cross-architecture IoT malware. Hence, IoT malware detection area is main objective of this research by security community recently. The familiar dynamic or static analyses to detect IoT malware is greatly deployed in various researches with its benefits. A systematic review relating to latest research studies and technologies of classical, Deep Learning (DL) and Machine Learning (ML) methodologies for cyber security threats recognition are outlined and are view is given in this paper. Every approach pertaining to its objective, approach and outcomes have been examined for every selected work. Deep Learning (DL) approach is greatly utilized for malware infected files and pirated software recognition in IoT network in cloud. Several software piracy and malware attack detection methods has been analyzed in this paper with respect to its advantages and disadvantages. The source code plagiarism is detected through DL methodology and dataset collection is done from Google Code Jam (GCJ) for software piracy investigation. Rather than this, Deep Convolutional Neural Network (DCNN) is mainly involved in identifying malicious infections in IoT network. Mailing dataset is utilized for obtaining malware samples which is used for experimental purpose. It is thereby substantiated that suggested method namely Tensor Flow Deep Neural Network (TF-DNN) classification performance for assessing cyber security threats in IoT are enhanced when compared with classic approaches such as Support Vector Machine (LBP+SVM), Gray Level Cooccurrence Matrix with Support Vector Machine (GLCM+SVM) pertaining to F-measure (F1) and Classification Accuracy (CA).

Keywords:

Internet of Things, Deep Convolutional Neural Network, Tensor Flow Deep Neural Network, Support Vector Machine, Google Code Jam

1. INTRODUCTION

Internet of Things (IoT) is one amid technologically evolving area for bridging physical and virtual worlds. New business models are emerged due to people, objects, machines and Internet connectivity apart from new interactions amid humankind and remaining world. The physical moving objects "Things" interconnection by internet embedded with sensors, electronic chip and various hardware forms is mainly referred as IoT. The unique identification of every device redone globally through Radio Frequency Identifier (RFID) tags. These smart objects remote controlling and monitoring are attained by communicating with other connected nodes. The ubiquitous connectivity to an extensive array of service industries, smart physical objects, cloud computing services, besides applications. IBM enumerated that connected devices count by internet is estimated to upsurge up to 50 billion by 2020 [1]. Cloud infrastructure is greatly utilized for sharing smart objects connection along with amount of big data by increasing the number of communication networks. IoT enabled technologies are employed for emerging smart cities, health, e-shopping, education system, e-banking, and for entertaining as well as defending people [2].

The design complexity and implementation in both hardware and software, apart from security functions and capabilities lagging, IoT devices has been grabbing attention towards cyber criminals taking benefit of poor authentication, malwares and outdated firmware for conceding IoT devices. There is estimation that all 25% cyber-attacks targets IoT devices in 2020 [3]. These attacks are increasingly rapidly due to evolving IoT technologies. Malware is one amid mostdangerous threats to IoT devices. Mira malware family reported in October 2016 that Dyn was one among prevalent and potent DDoS attacks. About 1.2 million IoT devices has been affected along with several common online services like Amazon, Google, etc. Hence, enhancing IoT devices security aspects is one of the researcher's challenges, particularly when handling with IoT malware [4]. Various research studies have been carried out for IoT devices. In which, Granjal et al. [5] concentrated on investigating existing protocols as well as mechanisms for secured IoT communications. Kouicem et al. [6] suggested a wide-ranging prevailing recommended security and privacy key top down survey in IoT.

IoT devices might be utilized for an open attack owing to continuously prevailing on network. Malware infection and pirated software are easily caused which in turn affect Industrial IoT-cloud as well security is compromised [7]. Software piracy is nothing but software development for reusing source codes illegitimately from other's research and disguised as unique version. Cracker through reverse engineering processes in addition same logic designing is being done in another source codes type [8] copies the original software logic. It is regarded as serious threat to internet security by which pirated software, open source codes are supported and pirated versions advertises are downloaded infinitely which is increased drastically apart from offering massive economic forfeiture to IT industry.

Business Software Alliance (BSA) 2016 report confers that public software piracy ratio is roughly 39%, ensuing in business compensations up to 52.2$ billion each year. The plagiarized source codes in pirated software are obtained by these intelligent software plagiarism methods. Various plagiarism detection methods such as source code similarity recognition, clone detection, software bugs analysis, software birthmark exploration

etc. are suggested. Hence, if a cracker to another programming language type reuses original software logic, then it is difficult in catching because of dissimilar structure behaviour.

IoT nodes privacy, computer systems and smartphones are affected by these malware attacks over the internet. There are two malware identification classification analysis. They are static and dynamic based analysis. Malware files patterns are learned through dynamic analysis despite the fact that executing code in real-time virtual atmosphere. It is revealed from manifold researches in which malicious behaviour observation can be done through function parameters exploration, function calls, information flow, instruction traces, visual codes analysis. Malicious codes are dynamic behaviour are examined by many automated online tools. However, it is considered as time consuming approach for the reason of observing every dynamic source code behaviour [9]. In addition, static malware analysis approaches do not necessitate source codes real-time execution. The malware executable binaries format information is captured by this approach. The signature-based malware recognition methods are static based, i.e. string signature, n-gram, opcode frequency and control flow graph.

In recent days, mostly concentrated research topic is DL's application to IoT systems [38]. In large datasets, superior performance is exhibited by DL when compared with traditional ML. Huge data are produced by various IoT systems. So, for such systems, DL techniques can be used. From data, complex representations can be extracted automatically using DL [38]. The IoT environment's deep linking is enabled by DL techniques [39]. A type of unified protocol is deep linking, where, without human intervention, automatic interaction between IoT devices with its applications are permitted. For instance, a fully smart home is formed by permitting automatic interaction between IoT devices in a home [38]. A computational architecture by combining various processing levels called layers are provided by Dl methods for learning representations with various abstraction levels. The state-of-the-art applications are enhanced considerably by DL techniques when compared with traditional ML techniques. Human neurons and brains working mechanism to process a signal is inspired in DL.

For unsupervised (generative) and supervised learning (discriminative), constructed the deep networks. These learning types combination is termed as hybrid DL. A discriminative DL technique's examples includes recurrent neural networks (RNNs) and CNNs. Examples of DL techniques includes ensemble of DL networks (EDLNs), generative adversarial networks (GANs), restricted Boltzmann machines (RBMs), deep belief networks (DBN), Deep autoencoders (AEs).

1.1 CHALLENGES

- **Software Piracy**: Presently, all third installed software application pirating is done. Since this software are globally easy to get on the internet, there is no physical intellectual digital property along with software authorship rights which leads to tough in sustaining. Attacker might crack original software and logic needs to redesign into another programming language type. Due to diverse syntax and semantic structures for programming language, there lies a great challenge for catching crackers' malevolent activities in cross-domain source codes.
- **Malware Detection**: Traditional techniques are greatly utilized for coding complication concerns, nonetheless huge computational cost is desired concerning texture feature mining by malware visualizations. This feature extraction procedures categories do not accomplish well with huge malware data examination.

This review analyses preeminent DL methodology for pirated and Malware attacks identification on industrial IoT cloud. Tensor Flow Deep Neural Network (TF-DNN) is mainly intended for capturing the pirated software via source code plagiarism. Additionally, malware malicious patterns are captured viabinary visualization by means of DCNN design. The suggested methodology combined solutions are considered to be proficient in terms of classification performance.

The paper structure is as follows. Background study is given in section 2. There are three-sub sections in section 2. Traditional approaches for cyber security threats recognition in discussed in first subsection 2.1. Machine Learning (ML) approaches for cyber security threats recognition in given in second subsection 2.2, Deep Learning (DL) approaches for cyber security threats recognition in last subsection 2.3. The prevailing approaches are discussed in section 3succeeded by solution in section 4. Subsequently, results and discussion are given in section 5. Lastly, a conclusion summary in offered in section 6.

2. BACKGROUND STUDY

Many researches are being carried out on malware detection and software plagiarism recognition for effective threat detection in IoT atmosphere and thereby attaining high identification performance, and reduce time cost. The Software plagiarism detection diverse aspects impact has been revealed by enormous research work but single programming language is utilized for various prevailing work. A cracker for other data structure in identical programming language chiefly alters the source code logic, which confers that current literature is valued. Moreover, unsupervised learning methodology was greatly deployed for assessing source codes similarity and diverse source codes similar functionalities are engaged for plagiarism detection. In addition, static, dynamic, hybrid, as well as visualization analysis for malware detection are also presented in earlier studies. Binary data extraction tools are exploited for features extraction via static means from binary files through static analysis methods. Dynamic analysis methodologies are typically on basis of binary samples execution in a controlled way for features extraction contained by a virtual machine. Hybrid methodology outclasses in an enhanced way when compared to combined methodology instead of static and dynamic approaches running distinctly.

2.1 REVIEW OF CONVENTIONAL METHODS FOR CYBER SECURITY THREATS DETECTION

Dovom et al. [10] utilized fuzzy and fast fuzzy pattern tree approaches for developing an OpCodes into a vector space for malware recognition besides classification. These approaches are considered to be proficient in malicious codes recognition in an accurate manner which is superior compared with Support Vector Machine (SVM), Random Forests (RF), Decision Trees (DT), K-Nearest Neighbor (KNN). On basis of experimental outcomes, it

is substantiated that malware classification and benign for IoT is achieved precisely using Vx-Heaven dataset with enhanced accuracy. Higher accuracy for both datasets with reduced run-time is attained through fast fuzzy pattern tree using Potential Heuristics. Feature extraction along with fuzzy classification are greatly utilized for attaining robust, more potent edge computing malware recognition and classification technique. Also, fuzzy pattern tree accuracy might be enhanced in future by suggesting fuzzy pattern tree distributed variation which is further proficient concerning edge computing over an IoT network.

Sun et al. [11] recommended an system named Cloud Eyes, cloud-based anti-malware system for proficient as well as consistent security services for resource-constrained devices. A new signature detection process on basis of reversible sketch structure by suggesting suspicious bucket cross-filtering for affording retroactive and precise malicious signature fragments orientations. A lightweight scanning agent implementation is attained using CloudEyes for client by exploiting signature fragments for dramatically reducing accurate matching range. Moreover, sketch coordinates transmission is done along with modular hashing, thereby low-cost communications and data privacy are ensured through Cloud Eyes. Lastly, CloudEyes performance assessment is attained through normal and campus suspicious traffic files. CloudEyes mechanism are proved as effective as well as practical which outclasses other prevailing systems with reduced communication and time consumption.

Shen et al. [12] designed a system namely Multistage Privacy-Preserved Malware Detection Game (MPMDG) by using Perfect Bayesian Equilibrium (PBE) for malware recognition. An Intrusion Detection System (IDS) is greatly utilized for realizing Malware detection infrastructure with fog and cloud computing for solving IDS deployment issues in smart objects because of their restricted resources as well as heterogeneous sub networks. The interactions amid smart objects and conforming fog node are disclosed by using a signaling game due to malware uncertainty in smart objects. The optimal strategies are developed for minimizing smart objects privacy leakage as well maximizing malware recognition probability via theoretical game PBE computation. Furthermore, parameters manipulating malicious smart object diffusing malware optimal probability as well features influencing fog node performance in defining an infected smart object. Lastly, suppressing malware diffusion practical applications in IoT networks have been suggested.

Naeem [13] suggested a Malware Threat Hunting System (MTHS) precisely and robust model for malware recognition in IoT environment. Malware binary is transformed into a color image by this suggested method following which machine or deep learning examination is done for effective malware detection. The visual similarities amid malware binaries computation is achieved through machine learning and depth learning examination. Abaseline has been formulated for MTHS performance comparison with customary malware detection methodologies. It is thereby substantiated that suggested method attained an extraordinary classification rate with a marginally low runtime cost on malimg database. Experimentations are carried outon two public Windows and Android software datasets. MTHS response time and detection accuracy outperforms in an enhanced way in contradiction with earlier machine learning and deep learning methodologies.

Yan et al. [14] suggested a methodology namely Multi-Level DDoS Mitigation Framework (MLDMF) for Industrial Internet of Things (IIoT) to defend against DDoS attacks, encompassing edge computing, fog-computing, besides cloud computing level. There are three major layers in IIoT architecture specified as perception, network, application layer. SDN-based IIoT gateways is greatly utilized by edge computing level for managing as well as safeguarding IIoT perception nodes. Fog computing level chiefly comprises an IIoT management control unit. A Software Defined Networking (SDN) controllers cluster besides applications are employed by IMCU for DDoS attacks detecting and counteracting. Big data and intelligent computing are deployed by cloud computing level for analysing network traffic, thereby attaining an intelligent attack recognition and alleviation outline for defending against DDoS attacks. It is thereby validated through simulation outcome that an edge computing amalgamation offers quick response capability, fog computing's state awareness capability, cloud computing's powerful computing aptitude, and SDN's networking programmability. SDN is utilized for managing massive IIoT devices as well mitigating DDoS attacks in IIoT. Also, suggested methodology effectiveness are proved through experimental outcomes.

Hossain and Muhammad [15] accomplished health monitoring in cloud environment by suggesting Healthcare Industrial IoT (Health IIoT) which is considered as significant monitoring methodology. This methodology is considered to be interconnected apps, communication technologies, Things (sensors and devices), people integration that would perform in combined way as one smart system for monitoring, tracking, and storing patients' healthcare evidence for ongoing care. Mobile devices and sensors in case of Health IIoT-enabled monitoring structure perform ECG and other healthcare information collection and thereby sending to cloud in a secure way for seamless access to healthcare experts. Watermarking, signal enhancement, other associated analytics are utilizing by healthcare experts for avoiding distinctiveness theft or clinical error. Investigational assessment and simulation help in validating this methodology appropriateness using health monitoring service based on an IoT-driven ECG in cloud. Healthcare data watermarking is performes before being directed to cloud for protected, safe as well as superior health monitoring. In forthcoming research, testing of suggested Health IIoT monitoring structure for notification functions and data security, along with test trial realization with real-world patients and health experts might be performed.

Habib et al. [16] achieved malicious behaviors recognition in IoT network traffic by framing a Multi-Objective Particle Swarm Optimization (MOPSO). MOPSO performance has been validated against multi-objective Non-dominating Sorting Genetic Algorithm (NSGA-II), general customary machine learning algorithms, and certain traditional filter-based feature selection approaches. Thereby it is substantiated through acquired outcomes, MOPSO is viable, outclasses NSGA-II, customary machine learning approaches, filter-based techniques for almost datasets.

Son et al. [17] suggested a system namely Parse Tree Kernel (PTK) for identifying code plagiarism. A similarity value among two source codes pertaining to their parse tree similarity are estimated by this method. The essential source codessyntactic

structure are encompassed in parse trees, due to which system efficiently manages structural data and its contribution are two-fold. Initially, PTK optimization is performed for program source code. It is validated through evaluation that system founded on this kernel outclasses eminent baseline systems. A university programming class is greatly opted for gathering massive real-world Java source codes. The plagiarized source codes are recognized in three steps by suggested methodology. All source codes are signified as trees by system initially. At that moment, similarity values amid all pairs are computed through suggested kernel. At last, source code pairs which are further alike than definite predefined threshold are identified as plagiarized pairs. This system is implemented in Java platform, however with other languages like C, C++ and Pascal are utilized for implementation. Manual investigation is done by this test set where two independent human annotators are tagged for marking plagiarized codes tag which is greatly utilized for several detection systems performance assessment in real-world environments. Thereby it is substantiated that plagiarism detection system performance attains highest level of human annotators.

Modiri et al. [18] utilized fuzzy and fast fuzzy pattern tree approaches to develop OpCodes into a vector space for malware recognition and classification. In addition to it, variations of fast fuzzy pattern trees and fuzzy pattern are implemented. On basis of experimental outcomes with Vx-Heaven dataset, fuzzy pattern tree might precisely categorize malware with 99.384% and benign with 100% accuracy for IoT. With much lesser run-time, for both datasets, fast fuzzy pattern treeby Potential Heuristics achieved 100% accuracy. Both approaches are deployed for Kaggleand Vx-Heaven datasets and attained 97.0427% accuracy for malware and 88.76% accuracy for benign through fuzzy pattern tree as well 90.093% for malware and 93.132% accuracy for benign through fast fuzzy pattern tree. In forthcoming work, fuzzy pattern tree accuracy needs to be enhanced by suggesting a fuzzy pattern tree distributed variation which is more proficient edge computing method over an IoT network. Higher accuracy degree is attained in the course of reasonable run times particularly for fast fuzzy pattern tree. This system is greatly utilized for attaining robust, more potent edge computing malware recognition and classification technique

Table.1. Inferences of Conventional Methods for Cyber Security Threats Detection

Method name	Advantages	Disadvantages
DT, RF, KNN, SVM, fuzzy and Fast Fuzzy Pattern Tree [10]	Accurately classify malware	Prediction stage might be slow
CloudEyes [11]	Reduce accurate matching range	Not support large data reduction rates
MPMDG use PBE [12]	Maximize malware detection	Malware's mutual influences and diversity are not considered
MTHS [13]	High classification rate	It is only focused on malware threat detection
MLDMF [14]	Identify and counteract DDoS attacks	It is not appropriate for larger dataset
Health IIoT [15]	High-quality, safe and secured health monitoring	Test trials are not done with health professionals and real-world patients
MOPSO [16]	IoT network traffic, recognizing malicious behaviors	low convergence rate
PTK [17]	Plagiarism detection system attains highest human annotators level	Consumes more time
OpCodes [18]	Malware detection and categorization	It is not appropriate for software piracy

2.2 REVIEW OF MACHINE LEARNING (ML) METHODS FOR CYBER SECURITY THREATS DETECTION

Yin et al. [19] identified a system for DDoS attacks identification and reduction by establishing a Software-Defined Internet of Things (SD-IoT) on basis of SDx paradigm. Generally, this system has controller pool encompassing SD-IoT switches, SD-IoT controllers, incorporated with IoT gateway, and devices. An algorithm is suggested for DDoS attacks identification as well as reduction in the suggested SD-IoT context in which packet-in message rate's vectors cosine similarity at boundary SD-IoT switch ports helps in determining whether DDoS attacks ensue in IoT. Lastly, suggested algorithm possess the ability in identifying IoT device which launches DDoS attack is done within diminutive time period, rapidly handle as well as alleviate DDoS attack, and eventually enhances unveiled glaring vulnerabilities in IoT, where terminal devices tend to possess computational as well as memory requirement restrictions. It is thereby substantiated through experimental outcomes, suggested algorithm tend to possess improved performance and IoT security is also strengthened with heterogeneous and vulnerable devices by adapting this framework. The forthcoming work might emphases on proactively defending action against DDoS attacks in SD-IoT. Additionally, in controller pool, dynamic load-balancing algorithms might be implemented and designed along with SD-IoT background algorithms.

Cosma and Joy [20] implemented source-code plagiarism recognition and exploration by PlaGate uses Latent Semantic Analysis (LSA)formulation. This new PlaGateis incorporated with prevailing plagiarism detection tools for plagiarism detection performance improvement. A novel approach for examining similarity among source-code files in view of collecting evidence for substantiating plagiarism is also implemented. The source-code fragments examination is permitted which is presented through graphical representation for substantiating plagiarism. Also, specified source-code fragments across files in a corpus comparative significance are indicated through this graphical evidence which is attained by LSA information retrieval method for detecting the importance within definite files under exploration in association to other files in corpus.

Zhou and Yu [21] suggested an approach namely Support Vector Machine (SVM) for cloud-assisted malware recognition along with dynamic differential game. Initially, malware detection model based on SVM's construction is done with data sharing in security platform at cloud and various malware-infected nodes having physical infectivity of susceptible nodes estimation is done accurately on basis of Wireless Multimedia System (WMS) transmission attributes. Then, modified epidemic model is used to define state transition amid WMS devices. Moreover, target cost function and dynamic differential game derivation are done in successful manner for Nash equilibrium among WMS and malware system. Depending on this, saddle-point malware recognition and suppression algorithm is offered on basis of optimal and modified epidemic model approaches computation. Hence it is validated through numerical outcomes that suggested algorithm can upsurge WMS utility resourcefully and effectually.

Sharma et al. [22] suggested a system namely Software Defined Network (SDN) for realizing safe smart home environment (SHSec) for forecasting malicious events. It mainly emphases on proficiencies crucial for providing a flexible generic policy and open source service creation components modularity for user-friendly smart home via implementing conventional software-defined network model. Also, an agile, modular, significant infrastructure is offered in this methodology. For evading several manual evaluations, recommendations through administrators, security should routinely adjust to any threat in immediate background. Network performance is tested for suggested model through simulation and feasibility in the course of link failures and switching in a normal background. The suggested model performance evaluation is done on basis of several metric factors. Simulation outcome reveal that SHSec management is capable for attack detection and mitigation, besides can also be exploited for system security, defend user security, accompanied by heterogeneous local network enhancement. Higher accuracy, sensitivity whereas predicting malicious events are also attained by suggested model.

Shafiq et al. [23] suggested a Decision Tree C4.5, Naïve Bayes (NB), Random Forest (RF), BayesNet, Random Tree (RT) for BoT-Internet of Things (BoT-IoT) malicious and anomaly traffic recognition. Initially, BoT-Internet of Things (BoT-IoT) identification dataset is greatly utilized. For Machine Learning (ML) algorithm, its 44 effective features selection are done from various features. Malicious and anomaly traffic identification is done by selecting five effective ML algorithm and most extensive ML algorithm performance assessment metrics. A bijective soft set approach and its algorithm is greatly utilized for finding out effective ML algorithm as well for intrusion traffic identification and choosing IoT anomaly. The suggested algorithm on basis of bijective soft set methodology is greatly utilized. Thus, it is revealed through experimental outcomes that suggested model is effective for selecting ML algorithm in various existing algorithms.

Alrashdi et al. [24] implemented a system for solving IoT cyber security threats in a smart city by formulating Random Forest (RF) for Anomaly Detection-IoT (AD-IoT), which is an intelligent anomaly detection on RF machine learning algorithm basis. This method might efficiently identify compromised IoT devices at distributed fog nodes. The model accuracy is illustrated by assessing model and modern dataset. Also, training final model parallel distributed amid fog nodes is performed as well as centralized IDS in master fog node for detecting cyber-attacks and identifying normal or attack traffic activities in urban life. Likewise, only suggested preliminary model is tested for network traffic categorization, subsequently will endure allocating IDS besides final model are compared on basis of fog network detection systems. For attaining the objective for identifying IoT attack networks in smart city, also distributed computing open sources are utilized for model distribution in fog nodes for cyber-attacks recognition and handling massive data passing via final model detection. Hence it is validated thatefficiently highest classification accuracy with lowest false positive rate are attained.

Rathore and Park [25] suggested an approach namely Extreme Learning Machine (ELM) based Semi-supervised Fuzzy C-Means (ESFCM) for distributed attack recognition. Fog computing paradigm is greatly utilized in fog-based attack detection context and also in suggested approach. As an cloud computing extension, attack detection at network edge are enabled by fog computing along with distributed attack detection. A Semi-supervised Fuzzy C-Means (SFCM) is deployed by ESFCM technique for handling labeled data issue as well ELM algorithm is exploited for providing worthy generalization performance at more rapidly detection rate. ELM functional in suggested context can further effect in lower performance because of input bias and weights arbitrary assignment. A serious issue might be caused by such random input bias and weights in which classification returns more than one solution and the assessment was done on NSL-KDD dataset signifying that suggested context attained improved performance than centralized attack detection framework. More definitely, 11 milliseconds detection time is recorded and increased accuracy rate.

Moustafa et al. [26] suggested a Decision Tree (DT), Artificial Neural Network (ANN), Naive Bayes (NB) for ensemble intrusion detection method for malicious events mitigation, in specific botnet attacks in contrast to Message Queue Telemetry Transport (MQTT), Hyper Text Transfer Protocol (HTTP), Domain Name System (DNS) protocols exploited in IoT networks. On basis of their potential properties, new statistical flow features generations are done from protocols. Then, AdaBoost ensemble learning technique is suggested by three machine learning techniques, specifically DT, NB, and ANN, are utilized for assessing these features effect and detecting malicious events efficiently. NIMS and UNSW-NB15 botnet datasets with simulated IoT sensors' data are deployed for suggested features extraction besides assessing ensemble technique. The suggested have potential normal as well as malicious activity features by correntropy as well as correlation coefficient measures. Additionally, recommended ensemble technique offers high detection rate and low false positive rate associated with every classification method encompassed in this context and three other customary techniques.

Shafiq et al. [27] suggested CorrAUCby using Decision Tree (C4.5), Naive Bayes (NB), Support Vector Machine (SVM), Random Forest (RF) for malicious Bot-IoT traffic recognition. Initially, novel feature selection technique termed as CorrAUC is proposed, and then based on CorrAUC, a new feature selection algorithm called Corrauc is designed, which is a wrapper technique used for accurate features filtering and effective

features selection for a selection of Machine Learning (ML) algorithm via Area Under Curve (AUC). Then, Shannon Entropy and applied integrated TOPSIS on basis of bijective soft set to validate selected features for malicious traffic identification in IoT network. The suggested methodology assessment is done through Bot-IoT dataset and four various ML algorithms. Hence, suggested technique is substantiated through experimental evaluation offering effective outcomes on average.

Table.2. Inferences of Machine Learning (ML) methods for cyber security threats detection

Method name	Advantages	Disadvantages
SD-IoT [19]	Detecting and mitigating DDoS attacks	It is only suitable for DDoS attacks detection
PlaGate uses LSA [20]	Source-code plagiarism recognition and exploration	parameter settings for languages other than Java are not analyzed
SVM [21]	Cloud-assisted malware detection	It is does not perform very well when the data set has more noise
SDN [22]	Achieves a higher accuracy, sensitivity	Reduced security level
NB, DT (C4.5), BayesNet, RF, RT [23]	Malicious and anomaly traffic identification	Assumption of independent predictor features
RF [24]	Highest classification accuracy with lowest false positive rate	It also requires much time for training
ELM based ESFCM [25]	Lower detection time and an accuracy rate increased	Few/many hidden nodes employed would lead to under- fitting/over-fitting
DT, ANN, NB [26]	High detection rate, low false positive rate	Unexplained functioning of the network
CorrAUC uses C4.5, NB, SVM, RF [27]	Malicious Bot-IoT traffic detection	They are often relatively inaccurate

2.3 REVIEW OF DEEP LEARNING (DL) METHODS FOR CYBER SECURITY THREATS DETECTION

Jeon et al. [28] explicate a detection method for finding intelligently evolved new IoT and existing IoT malware variant to decrease the IoT device damage caused by the malware known as Dynamic analysis for IoT Malware Detection (DAIMD). Nested cloud environment is utilized by DAIMD to analyze the malwares in IoT dynamically and Convolution Neural Network is used for learning IoT malware. Numerous amounts of behavior data are compressed in behavior images and IoT malware in nested cloud based VM environment is learned on CNN models. Without the limitation of hardware, the IoT malware variant which is complicated or whose code value is changed is detected and analyzed accurately because the DAIMD is analyzed dynamically the IoT malware in nested virtual atmosphere instead of IoT devices. CNN is trained and classified by utilizing the behavior images which is formed by converting analyzed and extracted the behavior data. The dynamic analysis is used for learn the generated enormous amount of behavior data to visualized the malware which reduces the IoT devices damage caused the infections through DAIMD. For malware detection and analyzation maximum amount of extracted action data is utilized by converting it into image. In DAIMD, the IoT malware is accurately classified by one type of CNN network known as ZFNet which is trained by behavior image.

Ye et al. [29] formulated a DeepAM for detecting the malware by utilizing Restricted Boltzmann Machines (RBMs). The intelligent malware detection is based on depth of the learning architecture design which is studied by windows application programming interface calls derived from portable executable files. The new unknown malware is detected by the proposed deep learning architecture made up of an associative memory layer with multilayer RBMs stacked up on auto encoder. Supervised learning for fine-tuning parameter is performed after unsupervised feature learning carried out by the operation of greedy layer-wise training in the proposed deep learning model. For feature learning, in the proposed system is various from the existing model by top to bottom utilization of heterogeneous deep learning model which used unlabeled and labeled file samples to pre trained it multilayers and utilization of class label files (either malicious or benign) in training phase. Many malware detection methods are compared in the work by experimental study on the Comodo Cloud Security Centre's larger real time data. While comparing with the traditional malware detection methods such as anti-malware scanners, shallow learning methods and heterogenous framework deep learning methods the proposed method shows improved performance. It can also utilize for other malware detection task.

Xiao et al. [31] proposed a novel cloud platform integrated malware detection in IoT environment called as Behavior based Deep Learning Framework (BDLF). API calls extracted from data is utilized to construct the behavior graphs for better malware detection in the first step of the proposed model. Followed by that, form the behavior graph the high-level features are extracted by neural network-Stacked Auto Encoders (SAEs). SAEs layer is added one after another and some added classifiers is connected to the last layer of SAEs. 6000-2000-500 are the SAEs architecture. 1.5% of average detection precision is increased by the proposed BDLF by the behavior graph through which the semantic of higher-level malicious behavior learning is occurred.

Naeem et al. [32] introduced a color image transformation integrated Deep Convolutional Neural Network (DCNN) for malware attack detection in Industrial Internet of Things (MD-IIOT). The DCNN model take color images as an input which is formed from the extracted raw android files. The files are classified as benign or malware by comparing the behavior database and the fingerprint file in the analyzer unit. The system administrator is warned to take necessary action by the response unit if any malicious activity is detected in network. DCNN and color image visualization combined methodology is used for in-depth malware analysis. The detection accuracy and the predictive time of the detection of the proposed method is higher than the

other compared existing deep learning and machine learning methods to detect malware.

Al-Hawawreh and Sitnikova [33] formulated Batch Normalization integrated Deep Neural Network (DNN-BN) for Ransomware detection in environment of Industrial Internet of Things. The malicious behavior is accurately detected by the extraction of latent representation of collected high dimension data through deep learning technique. Variational Auto-Encoder (VAE) and Classical Auto-Encoder (CAE) technique is integrated in hybrid manner with one another for feature engineering process performing in the proposed method. The collected system activity good representation and data dimension reduction is carried by the hybrid technique. The DNN-BN classifier is tested and trained by the new feature vector obtained from the two methods. The decision engine generalization capability, ransomware attack dynamic behavior analyzation and detection process effectiveness are improved by the suggested method. From experimental outcomes it shows that enhanced ransomware detection than the other traditional models.

Diro and Chilamkurti [34] proposed Deep Learning model for detecting distributed attacks in Internet of Things (IoT). Neural Network Algorithm and CPU improvement has an eminent partin DL applications in practical field. The DL high-level feature extraction capability is utilized in novel attacks or resilient mechanism to small mutation for detection of attacks in the cyberspace. The discrimination of attacks from the benign traffic is performed by the discovery of the hidden pattern from the training data because of the compression and the self-taught capability of DL. The attacks on the social IoT detection in cyber security is enabled by incorporating the novel DL approach. The detection of disturbed attack is compared with centralized detection system and proposed system performance is compared with the existing machine learning approaches. Compared to centralized detection systems and DL shallow counter parts, the proposed system shows effective and superior performance in disturbed attack detection from the experimental results.

Parra et al. [35] formulated distributed deep learning context based on cloud for detection as well as mitigation of Botnet attack and phishing with Long-Short Term Memory (LSTM) and Distributed Convolutional Neural Network (DCNN). Proposed model consists of two main security mechanism cooperatively working with one another. There are: (1) To detect Botnet attack at back end, cloud-based temporal LSTM network model is hosted and it is also observed distributed phishing attacks in numerous IoT devices by embedding ingest CNN. (2) For DDoS attacks detection in application layer and Phishing detection in IoT devices DCNN model incorporated as IoT device micro-security add-on. The phishing attack detection and defended at the origin in the IoT devices is carried out by incorporate the distributed CNN in ML at the client IoT device. The LSTM model at the backend is trained by selected N_BaIoT dataset and the recommended CNN add-on security model trained by created dataset combines the non-phishing and phishing URLs. The maximum utilization of the extracted useful features, minimal resources and communication requirements are the benefits of joint training method. The overall performance of the system is improved through multiple request fusion by scheme aggregation. The F-1 score higher accuracy in the detection of phishing attack is achieved by IoT micro-security add-on in suggested CNN model. From investigational outcomes, it is observed that in distributed fashion, suggested model identify attacks in both back-end level and at device.

Haddadpajouh et al. [36] proposed a network for hunting malware threat in Internet of Things (IoT) known as Recurrent Neural Network (RNN) approach. Execution operation codes (OpCodes) of the ARM- based IoT applications is analyzed using RNN. 270 benign ware and 281 malwares are combined to form a utilized dataset of IoT application to trained the proposed models. Secondly, along with configurations of three distinguish Long Short-Term Memory (LSTM) trained model is evaluate with 100 new IoT malware samples. From the experimental result, new malware samples detection shows higher accuracy in second configuration with 2-layer neurons from analyzation of 10-fold cross validation. In the conclusion, the best possible outcome is delivered by the LSTM approach which is also represented by the machine learning classifiers.

Kim and Song [37] proposed Behavior-based Malware Detection utilizing deep learning (BMD-DL) for the Internet of Things (IoT)'s security environment. Since numerous devices are connected in the IoT networks, the IoT environment is easily accessed by numerous different smart devices with larger number of users, it increases the chances of various attacks on the infrastructure and devices of IoT and tampering of data through malicious code. Due to continuous variation and learning of smart devices data derivation and learning model is essential for IoT environment to detect the malwares. The device id, state, behavior, location and the time values are normalized to generate metadata for malware detection. In IoT security background, various studies are carried out of malware detection, to reduce the security threats. Deep learning is utilized by BMD-DL for learning and detecting the malicious codes and behavior-based metadata collection for malicious behavior. BMD-DL along with learning model disconnecting malicious devices from the IoT network which creating malicious behavior to the IoT environment. The persistent malware detection is carried out by BMD-DL through applying outcomes of deep learning models. The models are trained by the behavioral data collected from various IoT device by BMD-DL.

Table.3. Inferences of Deep Learning (DL) Methods for Cyber Security Threats Detection

Method name	Advantages	Disadvantages
DAIMD uses CNN [28]	precisely categorize and identify IoT malware	Lack of ability to be spatially invariant to the input data
DeepAM uses RBMs [29]	the overall performance in malware detection	Not focus on how sparsity constraints are imposed on Auto Encoder
DBN and ANN [30]	malicious threat detection	Not appropriate for other attack detection
BDLF [31]	increase the average detection precision	Large time-consuming
DCNN [32]	predictive time and detection accuracy increased	slow convergence and time consuming

DNN-BN [33]	Ransomware Detection	Problem of categorizing multiple ransomware families
DL [34]	Distributed attack detection	High computational cost and large time-consuming
DCNN and LSTM [35]	Botnet attack detection and mitigation	Not suitable for identifying emerging attacks which targets IoT systems and devices
RNN [36]	malware threat hunting	Computation is slow
BMD-DL [37]	malware detection in IoT environment	It is only focused on behavior-based malware detection

3. ISSUES FROM EXISTING METHODS

Recently, the data storage, applications, service, and connect systems of IoT turn out to be root cause for cyber-attacks, since constant services have provided by them to the organization. i) the security of IoT becomes uncertain due to malware threats and software piracy. An important information may be lost through security threats that damages the reputation and economy. ii) The emergence of malware threats makes conventional host-based security solution puffy, and limits its application. Besides, the cloud-based security solution is inadequate in concurrently accomplishing the high-performance detection as well as the data privacy protection. iii) Smart objects privacy are preserved by malware diffusion and seek optimal malware detection approaches in IoT networks and attaining malware diffusion suppression. iv) Handling massive IIoT devices is difficult and not convenient. (v) Program plagiarism recognition is challenging for identifying plagiarized code pairs amid a source code set.

4. SOLUTION

The mentioned issues are mitigated through following methods (i) A combined deep learning methodology for malware infected and pirated software files detection in IoT network. Tensor Flow Deep Neural Network (TF-DNN) for pirated software identification by source code plagiarism, (ii) CloudEyes, offering proficient and trusted security services for resource-constrained devices. A suspicious bucket cross-filtering, which is an innovative signature detection mechanism is provided by CloudEyes on reversible sketch structure basis for cloud server. It also offers malicious signature fragments retrospective and accurate orientations. (iii) Utilizing optimal approaches which enhances malware detection probability through theoretically calculating Game Perfect Bayesian Equilibrium (iv) for IIoT, Multi-level DDoS mitigation framework (MLDMF) for defending against DDoS attacks, which encompasses edge computing, fog computing, cloud computing level, (v) code plagiarism detection system by deploying parse tree kernel.

5. RESULTS AND DISCUSSION

During the experiments, the performance results of Tensor Flow Deep Neural Network (TF-DNN) and other preeminent methods, like Local Binary Pattern with Support Vector Machine (LBP+SVM) and Gray Level Co-occurrence Matrix with Support Vector Machine (GLCM+SVM) are compared. In the pirated software, the code similarity is examined through the software plagiarism measure. With respect to software piracy, the proposed approach is analyzed through source code dataset collected from Google Code Jam (GCJ). For each source, the beneficial tokens accompanying frequency details are obtained initially by preprocessing the dataset, during which stemming, root word, minimum and maximum length of token, minimum and maximum frequency of token, etc., are included. Then, weighting of tokens is retrieved using the extraction and features selection methods, such as Logarithm Term Frequency (Log TF) and Term Frequency and Inverse Document Frequency (TFIDF). Besides, from Mailing dataset, the malware samples are collected. Empirical findings clearly depict the efficiency of the Tensor Flow Deep Neural Network (TF-DNN) based on the performance parameters, like F-measure (F1) and Classification Accuracy (CA). The suggested deep learning-based malware detection classification performance and prevailing machine learning-based malware detection methods are compared in Table.4.

Table.4. Comparison of Classification Performance Between Earlier Methods and Suggested Model

Metrics / Methods	F-measure (F1) (%)	Classification Accuracy (CA) (%)	Precision (%)
LBP+SVM	77.5	78.1	70
GLCM+SVM	91.9	92.1	75
TF-DNN	97.5	97.6	85

In Table.4, the F-measure (F1) values of the proposed TF-DNN classifier, and the existing LBP+SVM, GLCM+SVM classifiers are compared. The results depict that the proposed classifier is capable of outperforming the existing classifiers, since the proposed method secures 97.5% F-measure rate, whereas the existing LBP+SVM, and GLCM+SVM methods solely obtain 77.5%, and 91.9%, correspondingly.

The Precision (P) values of the proposed TF-DNN classifier, and the existing LBP+SVM, GLCM+SVM classifiers are compared. From the results, the proposed classifier is capable of outperforming the existing classifiers, since the proposed method secures 85% precision rate, whereas the existing LBP+SVM, and GLCM+SVM methods solely obtain 70% and 75% correspondingly.

The Classification Accuracy (CA) obtained by the proposed TF-DNN classifier, and the existing LBP+SVM, GLCM+SVM classifiers is further compared. The results represent the efficiency of proposed classifier to outperform the existing classifiers, since the proposed method secures 97.6% Classification Accuracy (CA), whereas the existing LBP+SVM, and GLCM+SVM methods solely obtain 78.1%, and 92.1%, correspondingly.

6. CONCLUSION

The key research objective is IoT malware detection domain. In this review, a detailed study on cyber security threats detection using Machine Learning (ML), conventional, Deep Learning (DL) methods are clearly presented. Several researches on intelligent malware detection is carried out by utilizing conventional and machine learning techniques. The chosen methodology for review are analyzed with respect to its objective, approach and outcomes.DL methods are introduced for detecting pirated software and malware infected files in IoT network in cloud. Existing work on software piracy and malware attack detection approaches has been investigated pertaining to its merits and demerits. Apart from this, Convolutional Neural Network (DCNN) is chiefly suggested in recognizing malicious infections in IoT network. It is thereby substantiated that suggested method namely TensorFlow Deep Neural Network (TF-DNN) classification performance for assessing cyber security threats in IoT are enhanced when compared with classic approaches such as LBP+SVM, GLCM+SVM pertaining to F1 and CA. Final conclusion is that, deep learning methodologies outclasses the prevailing approaches.

REFERENCES

[1] G.J. Joyia, R.M. Liaqat, A. Farooq and S. Rehman, "Internet of Medical Things (IOMT): Applications, Benefits and Future Challenges in Healthcare Domain", *Journal of Communication*, Vol. 12, No. 4, pp. 240-247, 2017.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities", *IEEE Internet of Things*, Vol. 1, No. 1, pp. 22-32, 2014.

[3] Q.D. Ngo, H.T. Nguyen, L.C. Nguyen and D.H. Nguyen, "A Survey of IoT Malware and Detection Methods based on Static Features", *ICT Express*, Vol. 6, No. 4, pp. 280-286, 2020.

[4] V. Ramalingam, D.B. Mariappan, R. Gopal and K.M. Baalamurugan, "An Effective Social Internet of Things (SIoT) Model for Malicious Node Detection in Wireless Sensor Networks", *CRC Press*, 2020.

[5] J. Granjal, E. Monteiro and J.S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", *IEEE Communications Surveys and Tutorials*, Vol. 17, No. 3, pp. 1294-1312, 2015.

[6] D.E. Kouicem, A. Bouabdallah and H. Lakhlef, "Internet of Things Security: A Top-Down Survey", *Computer Networks*, Vol. 141, pp. 199-221, 2018.

[7] S. Jabbar, K.R. Malik, M. Ahmad, O. Aldabbas, M. Asif, S. Khalid, K. Han and S.H. Ahmed, "A Methodology of Real-Time Data Fusion for Localized Big Data Analytics", *IEEE Access*, Vol. 6, pp.24510-24520, 2018.

[8] F. Ullah, J. Wang, M. Farhan, M. Habib and S. Khalid, "Software Plagiarism Detection in Multiprogramming Languages using Machine Learning Approach", *Concurrency and Computation: Practice and Experience*, Vol. 33, No. 4, pp. 1-12, 2018.

[9] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker, "Security Threats to Critical Infrastructure: the Human Factor", *Journal of Supercomputing*, Vol. 74, No. 10, pp. 4986-5002, 2018.

[10] K.M. Baalamurugan, R. Gopal and V. Ramalingam, "An Energy-Efficient Quasi-Oppositional Krill Herd Algorithm-Based Clustering Protocol for Internet of Things Sensor Networks", *CRC Press*, 2020.

[11] H. Sun, X. Wang, R. Buyya and J. Su, "CloudEyes: Cloud-based Malware Detection with Reversible Sketch for Resource-Constrained Internet of Things (IoT) Devices", *Software: Practice and Experience*, Vol. 47, No. 3, pp. 421-441, 2017.

[12] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan and Q. Cao, "Multistage Signaling Game-based Optimal Detection Strategies for Suppressing Malware Diffusion in Fog-Cloud-based IoT Networks", *IEEE Internet of Things*, Vol. 5, No. 2, pp. 1043-1054, 2018.

[13] H. Naeem, "Detection of Malicious Activities in Internet of Things Environment Based on Binary Visualization and Machine Intelligence", *Wireless Personal Communications*, Vol. 108, No. 4, pp. 2609-2629, 2019.

[14] Q. Yan, W. Huang, X. Luo, Q. Gong and F.R. Yu, "A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things", *IEEE Communications Magazine*, Vol. 56, No. 2, pp. 30-36, 2018.

[15] M.S. Hossain and G. Muhammad, "Cloud-Assisted Industrial Internet of Things (IIoT)-Enabled Framework for Health Monitoring", *Computer Networks*, Vol. 101, pp. 192-202, 2016.

[16] K.M. Baalamurugan and D.S.V. Bhanu, "Analysis of Cloud Storage Issues in Distributed Cloud Data Centres by Parameter Improved Particle Swarm Optimization (PIPSO) Algorithm", *International Journal on Future Revolution in Computer Science and Communication Engineering*, Vol. 4, No. 1, pp. 303-307, 2018.

[17] J.W. Son, T.G. Noh, H.J. Song and S.B. Park, "An Application for Plagiarized Source Code Detection based on a Parse Tree Kernel", *Engineering Applications of Artificial Intelligence*, Vol. 26, No. 8, pp. 1911-1918, 2013.

[18] A. Modiri, N. Dehghantanha and K. Parizi, "Fuzzy Pattern Tree for Edge Malware Detection and Categorization in IoT", *Journal of System Architecture*, Vol. 5, No. 2, pp. 1-19, 2018.

[19] D. Yin, L. Zhang and K. Yang, "A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework", *IEEE Access*, Vol. 6, pp. 24694-24705, 2018.

[20] G. Cosma and M. Joy, "An Approach to Source-Code Plagiarism Detection and Investigation using Latent Semantic Analysis", *IEEE Transactions on Computers*, Vol. 61, No. 3, pp. 379-394, 2012.

[21] W. Zhou and B. Yu, "A Cloud-Assisted Malware Detection and Suppression Framework for Wireless Multimedia System in IoT based on Dynamic Differential Game", *China Communications*, Vol. 15, No. 2, pp. 209-223, 2018.

[22] P.K. Sharma, J.H. Park, Y.S. Jeong and J.H. Park, "Shsec: SDN based Secure Smart Home Network Architecture for Internet of Things", *Mobile Networks and Applications*, Vol. 24, No. 3, pp. 913-924, 2019.

[23] M. Shafiq, Z. Tian, Y. Sun, X. Du and M. Guizani, "Selection of Effective Machine Learning Algorithm and Bot-IoT Attacks Traffic Identification for Internet of Things in Smart City", *Future Generation Computer Systems*, Vol. 107, pp. 433-442, 2020.

[24] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy and H. Ming, "Ad-IoT: Anomaly Detection of IoT Cyberattacks in Smart City using Machine Learning", *Proceedings of Annual Conference on Computing and Communication*, pp. 305-310, 2019.

[25] S. Rathore and J.H. Park, "Semi-Supervised Learning based Distributed Attack Detection Framework for IoT", *Applied Soft Computing*, Vol. 72, pp. 79-89, 2018.

[26] N. Moustafa, B. Turnbull and K.K.R. Choo, "An Ensemble Intrusion Detection Technique based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things", *IEEE Internet of Things*, Vol. 6, No. 3, pp. 4815-4830, 2018.

[27] M. Shafiq, Z. Tian, A.K. Bashir, X. Du and M. Guizani, "Corrauc: A Malicious Bot-IoT Traffic Detection method in IoT Network using Machine Learning Techniques", *IEEE Internet of Things*, Vol. 12, No. 2, pp. 1-13, 2020.

[28] J. Jeon, J.H. Park and Y.S. Jeong, "Dynamic Analysis for IoT Malware Detection with Convolution Neural Network model", *IEEE Access*, Vol. 8, pp. 96899-96911, 2020.

[29] Y. Ye, L. Chen, S. Hou, W. Hardy and X. Li, "DeepAM: A Heterogeneous Deep Learning Framework for Intelligent Malware Detection", *Knowledge and Information Systems*, Vol. 54, No. 2, pp. 265-285, 2018.

[30] S. Huda, S. Miah, J. Yearwood, S. Alyahya, H. Al-Dossari and R. Doss, "A Malicious Threat Detection Model for Cloud Assisted Internet of Things (CoT) based Industrial Control System (ICS) Networks using Deep Belief Network", *Journal of Parallel and Distributed Computing*, Vol. 120, pp. 23-31, 2018.

[31] F. Xiao, Z. Lin, Y. Sun and Y. Ma, "Malware Detection based on Deep Learning of Behavior Graphs", *Mathematical Problems in Engineering*, Vol. 14, No. 2, pp. 1-10, 2019.

[32] H. Naeem, F. Ullah, M.R. Naeem, S. Khalid, D. Vasan, S. Jabbar and S. Saeed, "Malware Detection in Industrial Internet of Things based on Hybrid Image Visualization and Deep Learning Model", *Ad Hoc Networks*, Vol. 34, No. 2, pp.1-22, 2020.

[33] M. Al-Hawawreh and E. Sitnikova, "Leveraging Deep Learning Models for Ransomware Detection in the Industrial Internet of Things Environment", *Proceedings of International Conference on Military Communications and Information Systems*, pp. 1-6, 2019.

[34] A.A. Diro and N. Chilamkurti, "Distributed Attack Detection Scheme using Deep Learning Approach for Internet of Things", *Future Generation Computer Systems*, Vol. 82, pp. 761-768, 2018.

[35] G.D.L.T. Parra, P. Rad, K.K.R. Choo and N. Beebe, "Detecting Internet of Things attacks using Distributed Deep Learning", *Journal of Network and Computer Applications*, Vol. 163, pp. 1-13, 2020.

[36] H. HaddadPajouh, A. Dehghantanha, R. Khayami and K.K.R. Choo, "A Deep Recurrent Neural Network based Approach for Internet of Things Malware Threat Hunting", *Future Generation Computer Systems*, Vol. 85, pp. 88-96, 2018.

[37] H.W. Kim and E.H. Song, "Behavior-based Malware Detection using Deep Learning for Improve Security of IoT Infrastructure", *International Journal of Advanced Science and Technology*, Vol. 28, No. 5, pp. 128-134, 2019.

[38] H. Li, K. Ota, and M. Dong, "Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing", *IEEE Network*, Vol. 32, No. 1, pp. 96-101, 2018.

[39] Z. M. Fadlullah, "State-of-the-Art Deep Learning: Evolving Machine Intelligence toward Tomorrow's intelligent Network Traffic Control Systems", *IEEE Communications Surveys and Tutorials*, Vol. 19, No. 4, pp. 2432-2455, 2017.