Journal of Advances in Science and Technology
Vol. 18, Issue No. 1, March-2021, ISSN 2230-9659

A Review of Intrusion Detection Techniques in IoT based Environment Systems

Devi Shalini K. B.[1]* Dr. Sanjay Kumar[2] Dr. Jambi Ratna Raja Kumar[3]

[1] PhD Student, Kalinga University, Raipur

[2] PhD Guide, Kalinga University, Raipur,

[3] Principal, GSMCOE, Pune

Abstract – Recently huze growth is observed in the utilization of Internet-connected devices, this will be alarming the security and privacy issues that turned into the significant obstructions ruining the broad reception of the Internet of Things (IoT). Security in IoT has become an important consideration for all, including the organizations, consumers, government, etc. While attacks on any system can't be completely secured perpetually, real-time detection of the attacks are significant to protect the systems in a compelling way. Privacy and security are the most significant concerns in the domain of realtime communication and predominantly in IoT's. With the advancements of IoT, the security of network layer has been drawn the core interest. The vulnerabilities of security in the IoT can create security threats dependent on any application. In this manner there is a basic prerequisite for security development and enhancement for the IoT system for preventing security attacks dependent on vulnerabilities of security. Here, this paper reviews the system, security attacks, security requirements and it's applications based on Machine learning (ML) approaches. The objective of this survey is to analyze the Machine learning strategies that could be utilized to develop and enhance the security methods for IoT frameworks."

Key Words – IoT, Security, Intrusion Detection, Cloud Computing Security and Machine Learning.

----------X----------

1. INTRODUCTION

The concept of IoT was created by an individual from the RFID group in 1999, and it has presently turned out increasingly significant to the practical world to a great extent on account of the development of mobile phones, embedded and universal communication, cloud computing and data analysis [1]. The IoT assumes a significant part in all aspects of our day-to-day lives. It covers several domains including industrial appliances, automobiles, healthcare, sports, entertainment, smart homes, and so on. The prevalence of IoT facilitates some daily activities, enhances the manner in which humans collaborate with the world and environment, and expands our social communications with others and objects [2]. The concept behind the IoT was to connect not just humans and computers as well as day-to-day objects to the Internet. This could be accomplished with outfitting things with computing and communication capacities hence altogether mapping the physical world to the digital one. This vision has originated from the way that individuals have constraints in time and precision with regards to information collection and generation, although if these procedures should be possible with no human intervene (i.e., by having exceptionally recognizable objects to report the condition, area, address, and so forth.), at that point the expenses and losses could be minimized significantly. The IoT can possibly change the methods for living and working with its new parts of interaction and communication, and creative service and application, e.g., practical objects observation, the web search engine for things, and so on. [3].

The initial years of the IoT mainly included data communication through machine to machine (M2M) communication. Though, the idea has developed quickly to incorporate human communication also, introducing a generation of IoE. Currently, our world incorporates billions of processing devices and sensors that are consistently sensing, gathering, combining, and dissecting the major measures of our own data. Such data may contain our place, browsing pattern, contact list, and fitness and health data. The sensing, gathering, and proliferating of such individual information by calculating devices are essentially propelled by accommodation: as devices gets smarter, they could respond better to our requirements, wishes, and even states of mind and deal with emergencies. However, this comfort comes at the cost of privacy and security difficulties: the private, customized data, if access to an unapproved, malicious operator, could lead to

critical harm to our wealth, status, and personal security.

These comprises fuses, firmware, and troubleshoot modes. Unapproved access to these resources could lead to the loss of a million of dollars in stolen copyrights, just as possibly critical exploitation of the resources. With the worldwide implementation of these devices, such security vulnerabilities could be disastrous [4].

2. IOT AND INTRUSION DETECTION METHODS

2.1 IoT Architecture

The architecture of IoT is discussed as Three-layer, Four-layer and Five-layer as represented below. These types of architectures are used for the IoT system development based on the performance model. The three different layers of IoT architecture is represented in fig.1.

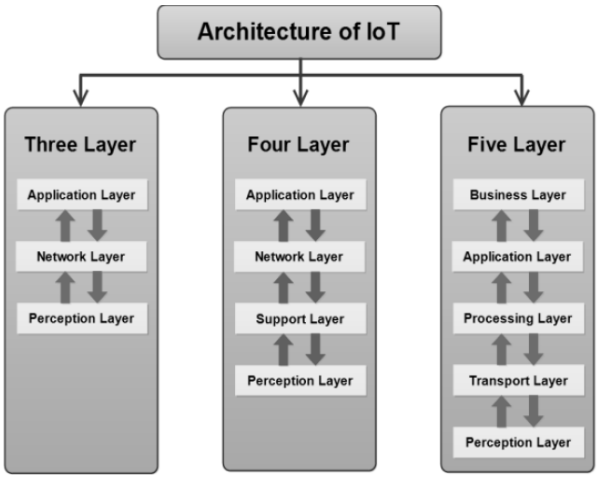

Fig. 1. Architecture Types of IoT

2.2 Security Requirements

Authenticity: Only valid users must be permitted to use the system or sensible data.

Authorization: The benefits of device segments and applications must be restricted so they can access just the resources they have to do their considered tasks.

Confidentiality: Data transmission among the nodes must be secured from intruders.

Integrity: Related data must not be altered

Availability and Continuity: So as to ignore any potential operational error and interference, accessibility and continuity in the arrangement of security services must be guaranteed [5]

2.3 Security Challenges

Interoperability: Related security solutions must not secure the function of interconnected heterogeneous devices in the system of IoT network.

Resource constraints: In IoT architecture, the vast majority of the nodes need storage capability, power, and CPU. They commonly utilize less-bandwidth transmission channel. Thus, it was unable to utilize some security strategies like frequency hopping transmission and the public key encryption algorithm. The arrangement of security system was very challenging under these conditions.

Data volumes: Although some IoT applications utilize brief and rare communication channel, there are an extensive quantity of IoT systems like logistics, sensor-based, and large- scale frameworks which have the possibilities to involve large volumes of information on servers or central network.

Privacy protection: Since a large amount of RFID systems were limited of appropriate authentication system, anybody could track labels and discover the ID of the objects transferring them. Hackers cannot just read the information as well as change or even delete information likewise.

Scalability: The network of IoT comprises of several nodes.

Autonomic control: Conventional computers require users for designing and adjust them to various application fields and distinctive transmission conditions. Nonetheless, objects in the network of IoT must setup links precipitously, and compose/design themselves to match for the stage they were working in. This sort of control additionally includes a few methods and systems like self-arranging, self-improving, self-management, self-protecting and self-healing [6].

2.4 Different Cyber Attacks on Applications of IoT

IoT networks are presented to different sorts of attacks both external and internal. Attacks are for the most part arranged by two type external and internal attacks. In external attack, the attacker is not a part of the network while in an internal attack the attack can be started through undermined or malignant nodes which are a segment of the network. In the accompanying, we analyze some potential digital attacks on IoT applications [7] [8]:

- “Sinkhole Attack
- Wormhole Attack
- Selective Forwarding Attack

- Sybil Attack
- Hello Flood Attack
- DOS Attack"

2.5 Intrusion Detection System

Intrusion was an undesirable or malevolent action that was dangerous for sensor nodes. Intrusion detection system can be a hardware or software tools. Intrusion Detection System could review and analyze machines and actions of user, find labels of well-known attacks and detect malignant network action. The Intrusion Detection System's objective was to monitor the networks and nodes, find various interruptions in the network, and alert the user after interruptions had been identified. The Intrusion Detection System performs as an alarm or network perceiver. It prevents from harm to the system through creating the alert previously the attacker ready to attack. It distinguishes both inside and outside attacks. Internal attacks were initiated through malignant or undermined nodes that are segment of the network while external attacks are initiated by third parties who are initiated by the external networks. Intrusion Detection System distinguish the network packet and determine if they are real users or intruders. There are mostly three parts of Intrusion Detection System: Monitoring, Analysis and detection, and Alarm. The monitoring module observes the network traffics, patterns and resources. The detection and analysis are the key part of Intrusion Detection System that identifies the intrusions as per specific algorithm. The alert module raises an alert if the intrusion was identified [10]. A normal Intrusion Detection System is made out of an analysis engine, sensors, and the reporting system. Sensor placed at various network locations or host and its primary objective is to gather information. The information gathered are transmitted to the analysis engine, which was capable to analyze the gathered information and identify intrusions. Once an intrusion is identified by the analysis engine, the reporting system produces an alert to the admin of network. Intrusion Detection Systems could be divided as Network-based Intrusion Detection System (NIDS) and Host-based Intrusion Detection System (HIDS). The implement of Intrusion Detection System relies upon environment. The Network-based Intrusion Detection System absorbs network traffic packets to identify malignant attacks and intrusions. A Network-based Intrusion Detection System could be software or else hardware-based system. (Fig. 2)."

The Host-based Intrusion Detection System was developed to be implement on a single system and to secure that system from malignant attacks or intrusions that would damage its OS or information [16], [17]. An Host-based Intrusion Detection System normally relies upon features in the host condition, like the activity files in the PC system. These features or metrics were utilized as input to the Host-based Intrusion Detection System decision engine. Along these, extraction of features from the host environment functions as the reason for any Host-based Intrusion Detection System [11],[12],[13],[14]."

TABLE 1: PERFORMANCE COMPARISON OF NIDS AND HIDS

"Performances	Network-Based IDS	Host-Based IDS
Intruder deterrence	Solid deterrence for external Intruders	Solid deterrence for internal intruders
Response time of threat	Strong response time against external intruders	Weak real-time response but performs better for a long term attack
Assessing damage	Very weak in assessing level of damage	Excellent in assessing level of damage
Prevention from Intruder	Better at avoiding external intruders	Better at avoiding internal intruders
Predicting Threat	Good at predicting and identifying malicious behavior patterns	It is also good at predicting and identifying malicious behavior patterns"

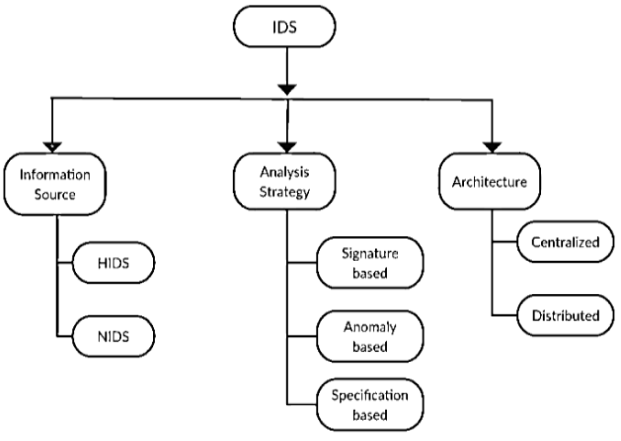

Fig. 2. Classification of IDS

3. DISCUSSION

Learning algorithms have been broadly accepted in several practical applications on account of their remarkable quality of solving issues. These algorithms deal with the development of machines which develops automatically by learning. Recently,

learning algorithms have been broadly used practically. The present improvement of learning algorithms has been directed through the advancement of new algorithms and the accessibility of big data, besides the development of less-computation cost algorithm. Commonly, learning algorithms intend to enhance execution in achieving the task with the assistance of training and learning from knowledge. For example, in learning intrusion identification, the task was for classifying the system's activity as abnormal or normal. An enhancement in execution could be accomplished through enhancing accuracy of classification, and experiences out of which the algorithms learn were an assortment of typical system activity. As discussed before Learning algorithms are characterized into four primary classes: Supervised, Semi- supervised, Unsupervised and Reinforcement Learning (RL). Machine Learning relates to intelligent techniques used to optimize the condition of the performance utilizing sample information or previous experience(s) through learning. All the more exactly, machine learning algorithms develop models of behaviors utilizing mathematical methods on large data collections. Machine learning additionally allows the capacity for learning without being specifically programmed. These methods were utilized as the reason for creating future expectations dependent on the new input information. Machine learning was interdisciplinary in quality and acquires its roots from numerous specialties of engineering and science that incorporate AI, data theory, optimization theory, and psychological science, to name the few.

TABLE 2. ML TECHNIQUES UTILIZED IN SECURITY ISSUES OF IOT

ML Technique	Description	Advantages	Disadvantages
SVM	SVM is the algorithm of supervised model with less computational complexity, utilized for regression and classification. It can perform with binary just as with multi-class conditions.	SVMs are known for their speculation capacity and appropriateness for information comprising of an enormous number of feature qualities however few sample points.	The optimal determination of a kernel is complex. Comprehending and interpreting SVM-based models are challenging.
K-NN	It is a basic and powerful supervised model and was utilized for connecting new data-points to the current comparative points via seeking through accessible data set. The system was trained and grouped by certain criteria and approaching information is analyzed for similarity in K neighbors.	KNN is a mainstream and successful machine learning strategy for intrusion detection.	The optimal k value for the most part differs starting with one data set then onto the next; in this way, deciding the optimal estimation of k might be a difficult and tedious procedure.
Naive Bayes	It is the algorithm of classification utilized with the multi-class and binary condition. It is called as "Naive", as over-rearranged suppositions are made for the computation of probabilities for the particular theory. Each feature is considered to be restrictively independent as opposed to figuring the real values.	NB is familiar for its simpleness, simple of usage, less training sample prerequisite and solid to inappropriate features.	NB handles features autonomously and in this way can't catch valuable parts of information from the connections and cooperation's between features.
PCA	PCA an unsupervised model and a multivariate method for compression of data. It executes dimensionality reduction	PCA could accomplish dimensionality reduction and subsequently decrease difficulty.	PCA was the feature reduction strategy. It must be utilized with various machine learning

	in huge datasets and extricates valuable data as the set included orthogonal factors called as "principal component". These components were composed in the expanding order of variation where the initial component was related with the most elevated difference of the information and it proceeds to the last. The least difference component having the least data could be removed.		strategies to build up a compellin g security approach.
Random Forest	RF was a supervised technique. It characterize s a model through actualizing specific rules deriving from the data features. Hence, this method was utilized to anticipate new variable targeted value.	RF was strong to over-fitting. RF derives feature selection and needs just some input parameters.	RF depends on developin g many DTs; therefore, it might be unreason able in particular practical applicatio n in which the necessar y training data set was enormous .
Decision Tree	The decision tree is utilized in regression and just as classification issues. Basically, these trees are utilized to divide the data set into many branches dependent on specific principles.	DT was a simple and transparent strategy.	DT requires huge storage as a result of its constructi on nature. Understa nding DT based technique s are simple just if not many DTs are included.
Neural Network	NN was the supervised technique to create the decision units in the form of cascaded chain to solve difficult issues. It basically builds network with a specific number of input to trigger output. Different sorts of NN have been proposed, for example, MLP, CNNs, and RNNs.	NN were flexible and could be utilized for both regression and classificatio n issues.	It was computati onally more costly and time consumin g to train with regular CPUs.
K-means Clustering	The most widely utilized familiar procedure is the K-mean clustering, the unsupervise d class of the machine learning family. It is utilized to classify or aggregate devices	Unsupervis ed techniques are commonly a better decision while creating the labelled information is complex. It could be utilized for private information anonymizati	It was less viable than supervise d technique s, particularl y in recognizi ng familiar attacks.

	dependent on features or parameters.	on in an IoT framework since it doesn't need labelled information.	
Q-Learning	It was utilized for "scheduling resource in spectrum management as well as security in IoT. It is associated to reinforcement learning class of the machine learning."	It is referred to attain long-term results which are very difficult to achieve.	It is not suitable for solving simple issues and needs huge data and huge computation.

ML was used if human skill either doesn't exist or can't be utilized like exploring a hostile location where people can't utilize their skill, for example, robotics, speech recognition, and so forth. It was likewise applied in circumstances where the solutions for some particular issue change in time (directing in the network of computer or discovering malignant code in an application or software) [29], [32], [33]. Moreover, it was utilized in real-time smart devices, for example, Google utilizes machine learning to dissect threats over mobile endpoint and application performing on Android. It was likewise utilized for distinguishing and eliminating malwares from infected devices. Moreover, Amazon has started the service Macie which utilizes machine learning to order and classify information saved in its cloud storage services. However, machine learning methods perform well in numerous domains; although, there was a possibility of FP and TN (Table. I). In this manner, machine learning methods need direction and changes to the model if the wrong prediction is made. Contrarily, in Deep Learning, another type of machine learning, the model could decide the precision of anticipation by itself. Because of self-service quality of deep learning methods, it was rendered as increasingly appropriate for classifications and task of prediction in new IoT applications with customized and contextual support [22],[24].

TABLE 3. ML METHODS FOR SECURITY ISSUES IN IOT

Objective/ Issues	ML Methods Used
Intrusion/ Anomaly Detection	• K-means Clustering and DT [27] • ANN [15]
	• Naive Bayes [30] • Decision Tree [19]
DDOS Attack	• KNN [23] • SVM [23] • Random Forest and Decision Tree [23] • Neural Network [23] • Q-Learning [31]
Attack Detection and Mitigation	• SVM [23] • K-NN and SVM [28]
Authentication	• Recurrent Neural Network [21] • Q-Learning and Dyna-Q [31] • DNN [28]
Malware Analysis	• SVM and PCA [25] • Recurrent Neural Network [27] • Ensemble Learning Algorithm Random Forest supervised classifier [18] • Artificial Neural Network [30] • Linear SVM [20]

Machine learning is utilized to make methods that were utilized to configuration, analyze, and train the datasets. These machine learning algorithms were utilized to distinguish potential patterns and similitudes in huge datasets and can perform predictions in new upcoming information. In any case, the basic confinement of machine learning technique is that it for the most part needs a data set to learn from, and afterward the method learned was utilized for real information. This occurrence might not enclose entire scope of properties and features of the information. In such manner, deep learning methods have been utilized to address the constraints of the machine learning methods (Table. II). Machine learning is viewed as major reasonable computational ideal models to present embedded intelligence in IoT systems. Machine learning could support smart devices and machines to induce valuable information out of the device or human-created information. It could likewise be characterized as capacity of the smart device to differ or computerize circumstance or conduct dependent on knowledge that was seen as a fundamental segment of the IoT solution. Machine learning methods have been utilized in operations like regression, classification, and density evaluation. Assortment of applications like computer vision, scam identification, bioinformatics, malware identification, validation, and speech recognition use machine learning algorithms and methods. Along these, machine learning can be utilized in IoT for giving intelligent services [26].

TABLE 4. APPLICATIONS OF MACHINE LEARNING TECHNIQUES IN IOT

Techniques	Applications in IoT
SVM	Identification of intrusions, malwares and attack in smart grid
KNN	Identification of intrusions and anomalies
NB	Detection of network Intrusion
RF	Identification of intrusions, DDoS attack, anomalies, and unapproved IoT device
DT	Identification of intrusions and suspicious traffic sources
K-means Clustering	Detection of Sybil in industrial WSNs and private data anonymization in an IoT system
PCA	It could be utilized for real-time detection models in IoT environments by reducing the model features

This review intends to present a usable manual which could motivate researchers to enhance the security of IoT from basically enabling secure transmission among IoT components to creating smart end-to-end IoT security-based methodologies (Tables 3 and 4).

4. CONCLUSION

The necessities for securing IoT systems have become challenge due to many advances, from physical devices and wireless communication to mobile and cloud models, should be protected and combined with different technologies. The development in Machine Learning has enabled the improvement of different incredible analytical strategies that could be utilized to upgrade IoT security. IoT privacy and security were fundamental significance and assume a critical role in the commercialization of IoT innovation. Conventional security and privacy arrangements affects from various issues that are identified with the dynamic quality of the IoT networks. In this survey deep review of IoT system is discussed and various IoT security threats and IoT security attacks are discussed. A brief review of machine learning techniques based on IoT security was analyzed in terms of its applications, objectives, advantages and disadvantages on IoT security. Different techniques are analyzed based on learning techniques.

REFERENCES

[1] K. K. Patel and S. M. Patel, —Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges‖, International Journal of Engineering Science and Computing, Vol. 6, Issue No. 5, pp.6122-6131, 2016.

[2] M. Ammar, G. Russello, and B. Crispo, —Internet of Things: A survey on the security of IoT frameworks‖, Journal of Information Security and Applications, Elsevier, Vol.38, pp.8-27, 2018.

[3] I. Alqassem and D. Svetinovic, —A Taxonomy of Security and Privacy Requirements for the Internet of Things (IoT)‖, Proceedings of the 2014 IEEE IEEM, pp.1244-1248, 2014.

[4] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, —Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice‖, Journal of Hardware and Systems Security, Vol.2, pp.97–110, 2018.

[5] J. K. Amfo and J. B. Hayfron-Acquah, —Modeling of Hybrid Intrusion Detection System in Internet of Things using Support Vector Machine and Decision Tree‖, International Journal of Computer Applications, Volume 181 – No. 15, pp.45-52, 2018.

[6] S. Geetha and A. V. Phamila, —Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems‖, Network Intrusion Detection and Prevention Systems for Attacks in IoT Systems, Chapter-6, IGI Global, pp.128-141, 2019.

[7] H. Jayakumar, K. Lee, W. S. Lee, A. Raha, Y. Kim, and V. Raghunathan, —Powering the Internet of Things‖, ACM Transactions, pp.375-380, 2014.

[8] E. Leloglu, —A Review of Security Concerns in Internet of Things‖, Journal of Computer and Communications, Vol.5, pp.121-136, 2017.

[9] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, —A survey of intrusion detection in Internet of Things‖, Journal of Network and Computer Applications, Elsevier, pp.1-13, 2017.

[10] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, —A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security‖, arXiv.org, pp.1-42, 2018.

[11] M. Hasan, Md. M. Islam, Md I. I. Zarif, and M.M.A. Hashem, —Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches‖, Internet of Things, Elsevier, Vol.7, pp.1-14, 2019.

[12] S. Jaiswal and D. Gupta, —Security Requirements for Internet of Things (IoT)‖, Proceedings of International Conference on Communication and Networks, Advances in Intelligent Systems and Computing, Springer, pp.419- 427, 2017.

[13] M. S. Alam and S. T. Vuong, —Random Forest Classification for Detecting Android Malware‖, IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, IEEE, pp.663- 6692013.

[14] A. Azmoodeh, A. Dehghantanha, and K. R. Choo, —Robust Malware Detection for Internet of (Battlefield) Things Devices Using Deep Eigenspace Learning‖, IEEE Transactions on Sustainable Computing, vol.4, no.1, pp.88-95, 2019.

[15] J. Canedo and A. Skjellum, —Using Machine Learning to Secure IoT Systems‖, Annual Conference on Privacy, Security and Trust (PST), IEEE, pp. 219-222, 2016.

[16] S. Rathore and J. H. Park, —Semi-supervised learning based distributed attack detection framework for IoT‖, Applied Soft Computing, Elsevier, pp.1-20, 2018.

[17] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, —Detecting Stealthy False Data Injection using Machine Learning in Smart Grid‖, IEEE Systems Journal, pp.1-9, 2014.

[18] H. H. Pajouh, R. Javidan, R. Khaymi, A. Dehghantanha and K. R. Choo, —A Two-layer Dimension Reduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks‖, IEEE, pp.1-11, 2016.

[19] H. H. Pajouh, A. Dehghantanha, R. Khayami, and K. R. Choo, —A deep Recurrent Neural Network based approach for internet of things malware threat hunting‖, Future Generation Computer Systems, Elsevier,2018, https://doi.org/10.1016/j.future.2018.03.007

[20] H. S. Ham, H. H. Kim, M.S. Kim, and M. J. Choi, —Linear SVM-Based Android Malware Detection for Reliable IoT Services‖, Journal of Applied Mathematics, Hindawi, pp.1- 10, 2014.

[21] F. Hussain, A. Anpalagan, A. S. Khwaja, and M. Naeem, —Resource allocation and congestion control in clustered M2M communication using Q-learning‖, Transactions on Emerging Telecommunications Technologies, Wiley Online Library, pp.1-12, 2016,.

[22] E. B. Karbab, M. Debbabi, A. Derhab, and D. Mouheb, —MalDozer: Automatic framework for android malware detection using deep learning‖, Digital Investigation, Elsevier, pp.48-59, 2018.

[23] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, —SINR-based DoS Attack on Remote State Estimation: A Game-theoretic Approach‖, IEEE, pp.1-10, 2015.

[24] N. An, A. Duff, G. Naik, M. Faloutsos, S. Weber, and S. Mancoridis, —Behavioral Anomaly Detection of Malware on Home Routers, International Conference on Malicious and Unwanted Software (MALWARE)‖, IEEE, pp. 47-54, 2017

[25] N. Nesa, T. Ghosh, and I. Banerjee, —Non-parametric sequence-based learning approach for outlier detection in IoT‖,FutureGenerationComputerSystems,Elsevier,2017,https://doi.org/10.1016/j.future.2017.11.021.

[26] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, —Machine Learning Methods for Attack Detection in the Smart Grid‖, IEEE Transactions on Neural Networks and Learning Systems, pp.1-14, 2015,.

[27] P. Shukla, —ML-IDS: A Machine Learning Approach to Detect Wormhole Attacks in Internet of Things‖, Intelligent Systems Conference, IEEE, pp.234-240, 2017.

[28] C. Shi, J. Liu, H. Liu, and Y. Chen, —Smart User Authentication through Actuation of Daily Activities Leveraging WiFi-enabled IoT‖, In Proceedings of Mobihoc '17, ACM, pp.1-10, 2017.

[29] J. Su et al., —Lightweight Classification of IoT Malware Based on Image Recognition‖, IEEE International Conference on Computer Software & Applications, IEEE, pp.664-669, 2018.

[30] E. Viegas, A. Santin, L. Oliveira, A. Francüa, R. Jasinski, and V. Pedroni, —A Reliable and Energy-Efficient Classifier Combination Scheme for Intrusion Detection in Embedded Systems‖, Computers & Security, Elsevier, pp.1-15, 2018.

[31] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, —PHY-layer Spoofing Detection with Reinforcement Learning in Wireless

Networks‖, IEEE Globecom 2015, IEEE, pp.1-11, 2015.

[32] W. Zhou and B. Yu, —A Cloud-Assisted Malware Detection and Suppression Framework for Wireless Multimedia System in IoT Based on Dynamic Differential Game‖, Computer System Security, China Communications, IEEE, pp.209-223, 2018.

[33] Saad Almutairi, S. Manimurugan, Majed Aborokbah, —A New Secure Transmission Scheme between Senders and Receiver Using HVCHC without Any Loss‖, EURASIP Journal on Wireless Communications and Networking, 2019:88, 2019, https://doi.org/10.1186/s13638-019-1399- z

[34] S.Manimurugan and C.Narmatha., —Secure and Efficient Medical Image Transmission by New Tailored Visual Cryptography Scheme with LS Compressions‖, International Journal of Digital Crime and Forensics (IJDCF), Volume 7, Issue 1, Pp 26-50, 2015.

Corresponding Author

Devi Shalini K. B.*

PhD Student, Kalinga University, Raipur