International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 03, 2021

Deep Learning Techniques In Internet Of Things (Iot) Security

Sanjay V[1] , Dr.N.Suganthi[2]

[1]ME- Scholar, Department Of CSE, Kumaraguru College Of Technology, Coimbatore
[2]Professor, Department Of CSE, Kumaraguru College Of Technology, Coimbatore

Abstract: Iot Integrates Many Devices With Less Human Involvement That Can Communicate With One Another. With This Feature Iot Improves The Reliability In Various Applications Such As Healthcare, Smart Agriculture, Home Security, Industries, Smart Cities, Etc., However The Nature Of Iot Infrastructure And The Components Involved In The Deployment Provides New Security Issues. The Prior Security Measures Like Encryption, Access Control Are Ineffective In Detecting The Attacks. Therefore The Previous Security Mechanism Has To Be Enhanced In Order To Provide A Secure Iot Environment. The Advancement Of Deep Learning Approach Presents The Embedded Intelligence In Iot That Solve The Several Security Issues. This Paper Presents The Survey On Various Deep Learning Approaches For Securing The Iot Devices From Various Attacks. In Addition The Advantages And Disadvantages Of These Methods Are Also Discussed That Serve As The Scope For Further Studies.

Keywords: Iot Application, Internet Of Things, Security, Deep Learning, Attack Prevention,

1. INTRODUCTION

Iot Is The Emerging Communication Technology That Enhances The Quality Of Life [1] By Modernizations. It Is The Fastest Developing Technology In Field Of Smart Applications Like Smart Agriculture, Smart Cities, Education, Automations, Home Security, Etc., Iot Has Large Benefits However The Nature Of Iot Infrastructure And The Components Involved In The Deployment Provides New Security Issues.

Iot Architecture Is Complex With Integrative Modules. So Retain The Security In Wide Range Is Really A Difficult Task. The Prior Security Measures Like Encryption, Access Control Are Ineffective In Detecting The Attacks. Therefore The Previous Security Mechanism Has To Be Enhanced In Order To Provide A Secure Iot Environment.

In Recent Years The Deep Learning Architecture Provides The Effective Result In Securing The Iot Devices From Intruder's Attack By Learning The Behavior Of Those Devices In Both Normal And Abnormal Conditions. Figure 1 Illustrates The Role Of Deep Learning Approach In Enhancing The Iot Security. The DL Mechanism Detects The Abnormal Behavior At The Initial Stage Itself By Analyzing The Normal Pattern Through Investigating The Input Data Of Iot Devices. In Addition The DL Approach Perform Well In Predicting The Upcoming Malicious Behavior With The Training Of Prior Data.

Various Researchers Have Been Carried Out Using The Data Mining Techniques And Traditional Machine Learning Approaches For Securing The Iot Devices [2][3][4]. But This Paper Mainly Focuses On Deep Learning Architecture And Aims At Presenting A Survey On Latest Deep Learning Architecture In Order To Identify The Suitable DL Approach For

Securing The Iot Devices From Intruder Attacks. The Remaining Section Of This Article Is Organized As Follows: Section 2 Describes DL Methods Applied In Iot Security. Eventually The Summary Of This Review Article Is Described In Section III.

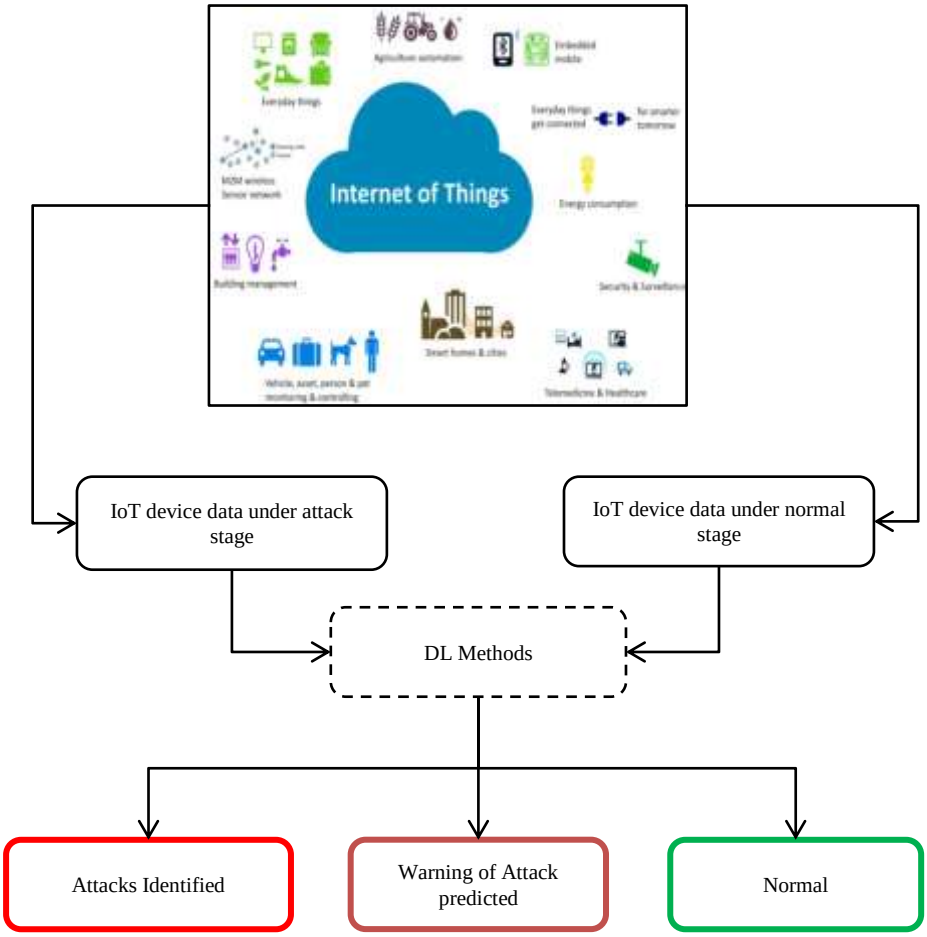

Fig 1. DL Role In Iot Security

2. RELATED WORKS

Recently, Deep Learning In Iot Security Application Has Becoming The Interesting Research Areas Among Several Researchers. The Development Of DL Methods Provides The Superior Performance Compared To ML Approaches. This Section Describes The Latest DL Methods In Detail.

2.1 Convolutional Neural Networks (Cnns)

CNN Is Developed To Minimize The Parameters Applied In Artificial Neural Network. Later CNN Outperforms In Many Decision Making Applications. The Working Flow Of CNN Based Iot Security System Is Shown In Figure 2. Initially The Convolution And Pooling Layers Are Used In Feature Selection To Extract The Deep Features Of The Iot Data And Classifies The Normal And Abnormal Condition Using The Fully Connected Layers. The Layers In Feature Selection Convolute The Attributes With Several Filters[20]. Simultaneously The Pooling Layers Reduce The Size Of Modules With The Help Of Max Pool Layers. Abhinaya Nagisetty And Govind P. Gupta [5] Introduced The CNN Using

Keras Platform To Identify The Malicious Behavior Of Iot Devices. This Study Was Tested On NSL-KDD99 Dataset Which Is Available Publically.

Bambang Susilo And Riri Fitri Sari [6] Introduced The Deep Learning Based Attack Detection System Using CNN Technique. The Study Discusses The Iot Threats And Attempts To Detect The Denial Of Service Attack In Iot Environment[21]. The Python Platform Is Used To Implement The Security System. This Study Is Compared With Best Performing ML And DL Approaches. Compared To Other Method CNN Achieved The Great Result.

Tarundhardiwan Et Al [7] Presents A DL Based Approach For Iot Data Security Using The CNN Architecture. The CNN Is Companied With LSTM To Classify The Normal And Abnormal Condition Of Iot Devices[22]. This Study Achieves The 98% Accuracy In Detecting The Attacks. The Problem In This Study Is Execution Time. Since CNN Does Nor Need Any Additional Feature Selection Algorithm It Takes More Time For Execution.

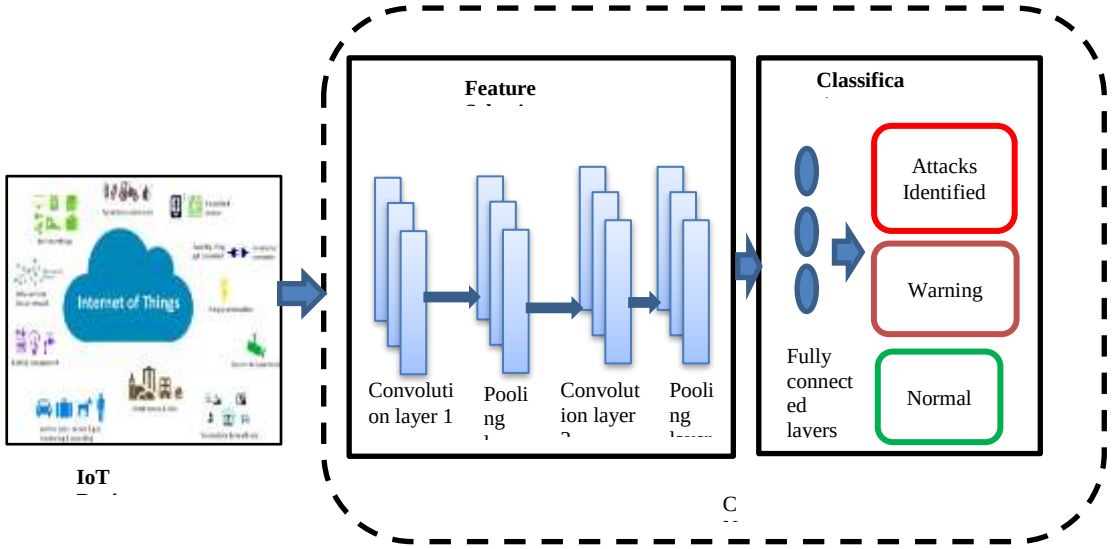

Figure 2. Working Procedure Of CNN In Attack Detection

CNN Work Well In Extracting The Features From The Input Data And Training It And Predict The Result Based On The Existing Trained Information. It Has High Computational Cost So It Is Difficult For Implementing With Less Resource. So Light Weight Neural Network Is Introduced [8] With Few Subset Of Class For Deep Classification. In The Prior Study [9] Proves That CNN Can Be Easily Breakup Able.

2.2 Recurrent Neural Networks (Rnns)

RNN Is A Powerful Deep Learning Architecture Developed To Process The Sequential Data Effectively. This Section Discuss About The RNN Based Iot Security Model. Chen-Hung Liao Et Al [10] Applied The Recurrent Neural Network In Iot Network To Predict The Storage Failure. Likewise Nadra Guizani And Arif Ghafoor [11] Introduced The RNN And RNNLSTM In Identifying The Abnormal Behavior Of Iot Devices In A Timely Manner. This Study Achieves 78% And 98% Accuracy In Classifying The Normal And Abnormal Behavior Using RNN And RNNLSTM.

Shin Hyuk Park Et Al [12] Presents The RNN For Malicious Attack Detection By Using The LSTM As Feature Extraction And Cosine Similarity As Scoring Function. This Study Achieves The 89.5% Accuracy In 90% Boundary Region. M. Shobana And S. Poonkuzhali [13] Make An Attempt To Detect The Malware System Calls Sequence Occurs During The Runtime In Iot Device. The System Calls Are Collected And Preprocessed Using N-Gram Approach. Based On The System Call RNN Classifies The Malicious Behavior. This Study Identifies The 175 Malware System Call From IOTPOT Dataset.

Jagmohan Chauhan Et Al [14] Utilized The RNN Model To Enhance The Security In Homes. This Study Integrates The ML And DL Approach To Predict The Unauthorized Access In Smart Homes. The Embedded Approach Is Performed By Integrating The Support Vector Machine And LSTM Architecture. The Feature Extraction Is Performed With Java Based Toolkit That Extracts The Mel-Frequency Cepstral Coefficients Features And Classifies The Normal And Abnormal State Effectively. LSTM Provides The Better Result Compared To SVM But LSTM Takes More Time To Execute.

Hamed Haddadpajouh Et Al [15] Used Recurrent Neural Network Architecture To Detect The Malware In Opcodes Which Is The Iot Based Application. Feature Selection Is Performed With Term Frequency And Inverse Document Frequency Methods. This Study Is Evaluated On Iot Dataset With Total Of 551 Samples. This Study Achieves 98% Accuracy In Malware Detection. The Problem In This Study Is It Provides The Efficient Result For Small Dataset.

2.3 Deep Belief Networks (Dbns)

It Consists Of Stacked A Restricted Boltzmann Machine That Provides The Robust Performance In Classification. Yuanfang Chen Et Al [16] Introduced A Successful Malicious Attack Detection Model Using DBN Architecture. DBN Effectively Learns The Malicious Features And Predict The Attacks In Early Stage. This DBN Based Architecture Achieved 96% Accuracy.

From The Literature It Is Clear That The Previous Study On Enhancing The Iot Security Is Performed Effectively With Deep Learning Architecture. However The Deep Learning Framework Is Complex And Taking More Time For Training And Provides The Less Accuracy In Small Dataset. DL Is Suitable For Large Dataset. The DL Approaches Need Optimization In Hyper Parameters To Achieve Better Result That Can Be Applicable In Real Time Iot Security.

Peisong Li And Xinheng Wang [17] [23]Presents Genetic Algorithm Based DBN Architecture To Detect The Malware In Iot Devices. This Study Was Evaluated On NSL-KDD Dataset And Achieves The Great Result In Finding The Misbehavior Of Iot Devices. Using The Different Types Of Malware Is Identified Using The Genetic Algorithms. The Problem In This Study Was It Provide The Great Result In Small Dataset.

2.4 Generative Adversarial Networks (Gans)

GAN Is The Best Performing Deep Learning Approach Recently Used In Many Applications. In Iot Security GAN Provides The Efficient Result And This Section Presents The Study Related To GAN Based Iot Security. The Architecture Of The GAN Is Shown In Figure 3. The Data From Iot Device Is Collected And Generator And Discriminator Work Together To Classifies The Normal And Abnormal Behavior.

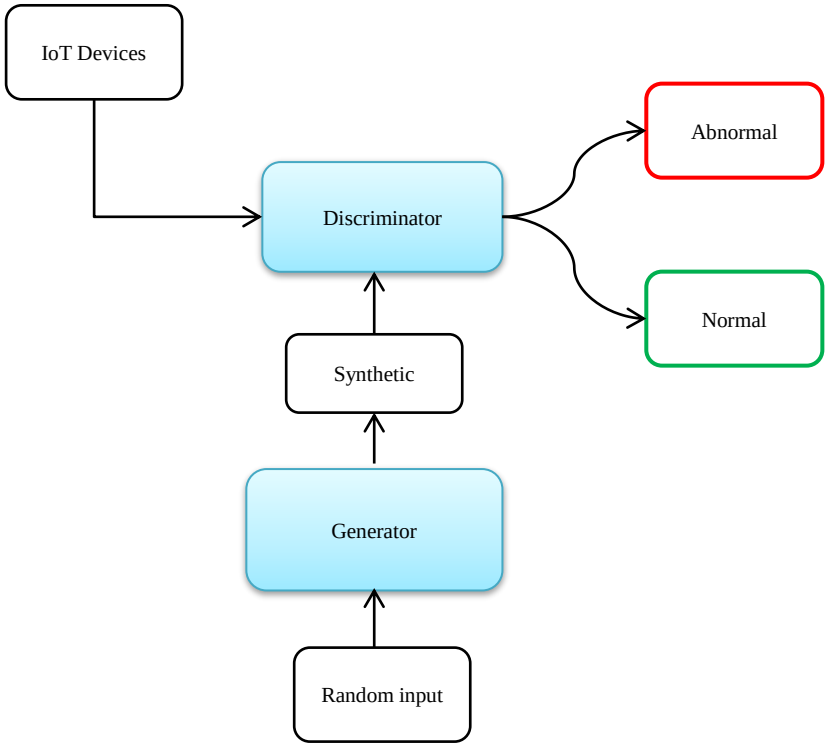

Figure 3. Working Procedure Of GAN

Aidin Ferdowsi And Walid Saad [18] Introduced The GAN Based Architecture To Detect The Malwares In Iot. With The Help Of Generator And Discriminator The Anomalous Behavior Is Identified Effectively. Compared To The Existing Study This Method Achieves 20% Improvement In Accuracy.
Kevin Merchant ; Bryan Nousain [19] Introduced The GAN To Identifies The Deep Features Of Iot Data And Detect The Abnormal Behavior Effectively. The Study Was Tested On Iot Dataset And Achieves The Great Result With Less Error Rate. This Adversarial Model Works Well Against The Iot Attacks And Enhance The Security Using It Advancement.

3. CONCLUSION

In Recent Days The Security On Iot Device Plays A Significant Role In Commercialization Of This Technology. However The Security Have Become Difficult Due To Several Iot Factors Like Physical Devices, Data Transmission Among The Physical Device To Cloud, Etc., The Best Performing DL Algorithm In Identifying The Malware Is Investigated In This Article. The Development In Deep Learning Allows Building An Enhanced Mechanism That Can Improve The Security Of Iot. This Study Retrospect's The Various DL Methods Applied For Iot Security With Their Merits And Demerits. This Article Aims To Present The Useful Research Direction That Can Assists The Researchers To Develop An End To End Model For Iot Security.

4. REFERENCES

[1] Dastjerdi, A. V., & Buyya, R. Fog Computing: Helping The Internet Of Things Realize Its Potential. Computer, 49(8), 112-116 (2016) .

[2] Kotsiantis, S. B., Zaharakis, I., & Pintelas, P.. Supervised Machine Learning: A Review Of Classification Techniques. *Emerging Artificial Intelligence Applications In Computer Engineering*, *160*(1), 3-24 (2007).

[3] Kim, G., Lee, S., & Kim, S.. A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection With Misuse Detection. *Expert Systems With Applications*, *41*(4), 1690-1700 (2014).

[4] Chang, Y., Li, W., & Yang, Z. Network Intrusion Detection Based On Random Forest And Support Vector Machine. In *2017 IEEE International Conference On Computational Science And Engineering (CSE) And IEEE International Conference On Embedded And Ubiquitous Computing (EUC)* 1, 635-638 2017.

[5] Nagisetty, A., & Gupta, G. P. Framework For Detection Of Malicious Activities In Iot Networks Using Keras Deep Learning Library. In *2019 3rd International Conference On Computing Methodologies And Communication (ICCMC)* 633-637 (2019).

[6] Susilo, B., & Sari, R. F. Intrusion Detection In Iot Networks Using Deep Learning Algorithm. *Information*, *11*(5), 279 (2020).

[7] Tarundhardiwan, Dr. Siddartha Choubey, Dr. H.S. Hota, "A Novel Hybrıd Approach For Cyber Securıty In Iot Inetwork Usıng Deep Learnıng Technıques", International Journal Of Advanced Science And Technology, 29(6) 4169–4179 (2020).

[8] De Coninck, E., Verbelen, T., Vankeirsbilck, B., Bohez, S., Simoens, P., Demeester, P., & Dhoedt, B. Distributed Neural Networks For Internet Of Things: The Big-Little Approach. In *International Internet Of Things Summit,* 484-492 (2015).

[9] Maghrebi, H., Portigliatti, T., & Prouff, E. Breaking Cryptographic Implementations Using Deep Learning Techniques. In *International Conference On Security, Privacy, And Applied Cryptography Engineering* 3-26 (2016).

[10] Liao, C. H., Shuai, H. H., & Wang, L. C. RNN-Assisted Network Coding For Secure Heterogeneous Internet Of Things With Unreliable Storage. *IEEE Internet Of Things Journal*, *6*(5), 7608-7622 (2019).

[11] Liao, C. H., Shuai, H. H., & Wang, L. C. RNN-Assisted Network Coding For Secure Heterogeneous Internet Of Things With Unreliable Storage. *IEEE Internet Of Things Journal*, *6*(5), 7608-7622 (2019).

[12] Guizani, N., & Ghafoor, A. A Network Function Virtualization System For Detecting Malware In Large Iot Based Networks. *IEEE Journal On Selected Areas In Communications*, *38*(6), 1218-1228 (2020).

[13] Park, S. H., Park, H. J., & Choi, Y. J. RNN-Based Prediction For Network Intrusion Detection. In *2020 International Conference On Artificial Intelligence In Information And Communication (ICAIIC)* 572-574 (2020).

[14] Shobana, M., & Poonkuzhali, S.. A Novel Approach To Detect Iot Malware By System Calls Using Deep Learning Techniques. In *2020 International Conference On Innovative Trends In Information Technology (ICITIIT)* 1-5 (2020).

[15] Chauhan, J., Seneviratne, S., Hu, Y., Misra, A., Seneviratne, A., & Lee, Y. Breathing-Based Authentication On Resource-Constrained Iot Devices Using Recurrent Neural Networks. *Computer*, *51*(5), 60-67 (2018).

[16] Haddadpajouh, H., Dehghantanha, A., Khayami, R., & Choo, K. K. R.. A Deep Recurrent Neural Network Based Approach For Internet Of Things Malware Threat Hunting. *Future Generation Computer Systems*, *85*, 88-96. (2018)
[17] Chen, Y., Zhang, Y., & Maharjan, S.. Deep Learning For Secure Mobile Edge Computing. *Arxiv Preprint 1709.08025* (2017).
[18] Zhang, Y., Li, P., & Wang, X. Intrusion Detection For Iot Based On Improved Genetic Algorithm And Deep Belief Network. *IEEE Access*, *7*, 31711-31722 (2019).
[19] Ferdowsi, A., & Saad, W. Generative Adversarial Networks For Distributed Intrusion Detection In The Internet Of Things. In *2019 IEEE Global Communications Conference (GLOBECOM)* 1-6 (2019).
[20] Merchant, K., & Nousain, B.. Securing Iot RF Fingerprinting Systems With Generative Adversarial Networks. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)* Pp. 584-589 (2019).
[21] Sujatha, K & Shalini Punithavathani, D 'Extraction Of Well Exposed Pixels For Image Fusion With Sub Banding Technique For High Dynamic Range Images. International Journal Of Image And Data Fusion', Taylor & Francis, DOI: 10.1080/ 19479832.2016.1226967.
[22])Malar, A.C.J., Kowsigan, M., Krishnamoorthy, N. S. Karthick, E. Prabhu & K. Venkatachalam (2020). Multi Constraints Applied Energy Efficient Routing Technique Based On Ant Colony Optimization Used For Disaster Resilient Location Detection In Mobile Ad-Hoc Network. Journal Of Ambient Intelligence And Humanized Computing, 01767-9.
[23] M. Kowsigan, J. Rajeshkumar, B. Baranidharan, N. Prasath, S. Nalini, And K. Venkatachalam, "A Novel Intrusion Detection System To Alleviate The Black Hole Attacks To Improve The Security And Performance Of The MANET," *Wireless Personal Communications*, Pp. 1-21, 2021.