Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No.04
Pages: 236-245
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.4.005

Internet of Things (IoT) Authentication and Access Control by Hybrid Deep Learning Method - A Study

Dr. Joy Iong Zong Chen,
Professor, Department of Electrical Engineering,
Da-Yeh University, Taiwan.
Email id: jchen@mail.dyu.edu.tw

Kong-Long Lai,
Department of Electrical Engineering,
Da-Yeh University, Taiwan.

Abstract- In the history of device computing, Internet of Things (IoT) is one of the fastest growing field that facing many security challenges. The effective efforts should have been made to address the security and privacy issues in IoT networks. The IoT devices are basically resource control device which provide routine attract impression for cyber attackers. The IoT participation nodes are increasing rapidly with more resource constrained that creating more challenging conditions in the real time. The existing methods provide an ineffective response to the tasks for effective IoT device. Also, it is an insufficient to involve the complete security and safety spectrum of the IoT networks. Because of the existing algorithms are not enriched to secure IoT bionetwork in the real time environment. The existing system is not enough to detect the proxy to the authorized person in the embedding devices. Also, those methods are believed in single model domain. Therefore, the effectiveness is dropping for further multimodal domain such as combination of behavioral and physiological features. The embedding intelligent technique will be securitizing for the IoT devices and networks by deep learning (DL) techniques. The DL method is addressing different security and safety problems arise in real time environment. This paper is highlighting hybrid DL techniques with Reinforcement Learning (RL) for the better performance during attack and compared with existing one. Also, here we discussed about DL combined with RL of several techniques and identify the higher accuracy algorithm for security solutions. Finally, we discuss the future direction of decision making of DL based IoT security system.

Keywords: *Deep learning, Cyber security, Reinforcement Learning*

1. INTRODUCTION

The IoT consist of physical components integrated with software and mobile application and other technologies. In short, this purpose of integrating all is for exchanging data and transferring data to other device through an internet. This construction is adopted easily with real time environment and has provided more flexibility [1].

Recently, passwords or PINs as a secure method of accessing a system or directory is moving towards physiological features (face, eye or finger print and etc). This biometric identification tells very prompt identification that “who we are” which is safest techniques than existing methods. Accessing of IoT devices very careful way should be top priority. Otherwise the causes or losses cannot be measured at all [2, 3, 4]. The advantage context of internet of things is shown in figure 1.

ISSN: 2582-2640 (online)
Submitted: 16.12.2020
Accepted: 12. 01.2021
Published: 19.01.2021

Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No.04
Pages: 236-245
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.4.005

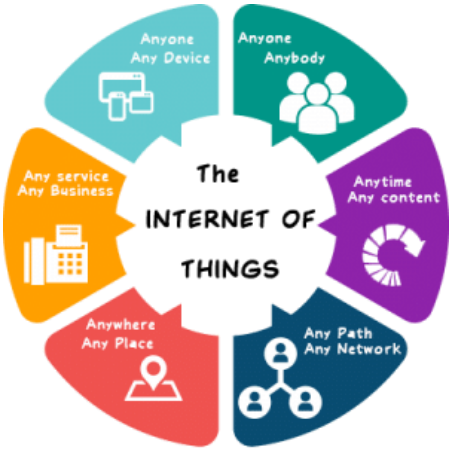

Figure 1 The Internet of Things

The ability to observe IoT devices showing intelligence provides a major answer to new or zero-day attacks. DL is powerful ways of knowledge exploration for learning concerning 'normal' and 'abnormal' behavior in line with however IoT elements and devices perform at intervals the IoT atmosphere [5]. Consequently, DL ways are necessary in reworking the safety of IoT systems from just facilitating secure communication between devices to security-based intelligence systems. IoT security threats that are associated with inherent or fresh introduced threats are given, and numerous potential IoT system attack surfaces and also the attainable threats associated with every surface are mentioned [6]. There are many security challenges for IoT devices is notified in the figure 2. We have a tendency to then completely review DL ways for IoT security and gift the opportunities, blessings and shortcomings of every methodology. We have a tendency to discuss the opportunities and challenges concerned in applying DL to IoT security.

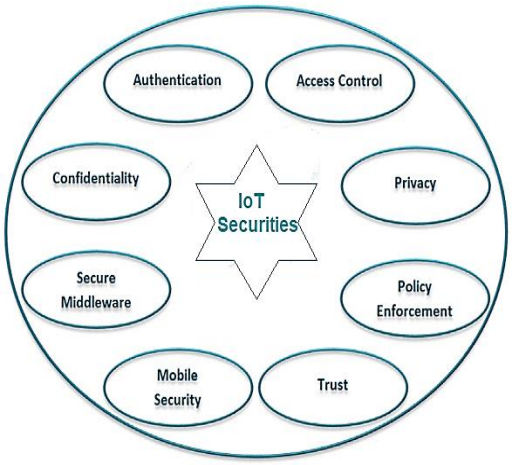

Figure 2 Requirement of IoT device security challenges

In a peer-to-peer environment, biometric based authentication for IoT devices offers good security system and the model overall structure is notified in figure 3. There are two common authentication operations as follows; (a) Mobile devices users' confirmation in order to access (b) From remotely the user accessing through mobile.

ISSN: 2582-2640 (online)
Submitted: 16.12.2020
Accepted: 12. 01.2021
Published: 19.01.2021

Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No.04
Pages: 236-245
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.4.005

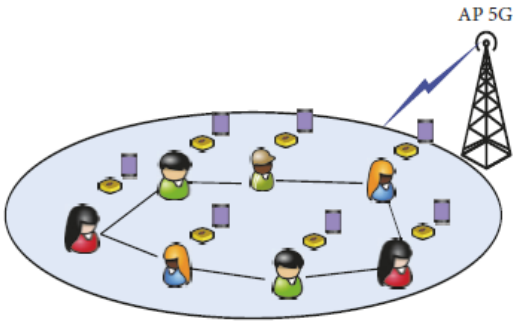

Figure 3 Biometric based authentication for IoT devices in a peer-to-peer environment

The main challenges that face biometric-based authentication schemes square measure (1) the way to style Associate in Nursing authentication mechanism that's free from vulnerabilities, which might be exploited by adversaries to form illicit accesses, and (2) the way to make sure that the user's biometric reference templates don't seem to be compromised by a hacker at the device level or the remote server level. The recent advancement of the deep learning algorithms are employed for IoT networks that discusses in this research article [7, 8, 9, 10]. These days, the mobile devices are essential one in our day to day life. The ranges of applications are huge and important in daily life. Due to two features authentication factors are identifying stronger for identity verification as "something you have" and "something you're," square measure combined. Many solutions that embody multi biometric and signature or voice recognition for smart campus, hospital and Tele-sector banks for more top security reason [11].

2. ORGANIZATION OF THE RESEARCH

The structure of the research article organized as follows; Section-3 gives literature survey of recent authentication and access control security by different approach. Section-4 provides the description of theoretical proposing analysis. Section-5 delivers future enhancement ideas and finally the conclusion with limitation is in section-6.

3. RELATED WORKS

Sathish et al discussed about adapting with certain domain of diverse features IoT. This analysis is based on domain, applications, environment parameter. Also it presents the survey of IoT devices in real time application [1]. Several researches have been conducted for checking the vulnerability of IoT systems. Granjal, Monteiro and Silva [12] highlighted the unsolved problems of IoT devices and suggest solutions for that. Zarpelão et al. [13] discussing many techniques for intrusion detection of IoT framework. Weber investigates on many regulatory approaches to compute privacy and security requirement for IoT framework [14]. Roman, Zhou and Lopez [15] investigates many challenges that should be addressed and discuss merits of IoT with the security concerns. The reviewing of ransomware attacks in IoT system discuss here [16]. Xiao et al. [17] discuss ML methods to shield data privacy and security in the IoT framework for further development. Also they discuss about backup security solution and fractional state observation for IoT system. [18, 19] These papers focus the uses of data mining and ML methods for security of intrusion detection. Many of the research papers consist of several reviews for recent advancement of DL methods and view point of IoT security.

There are many type of denial of service attacks for IoT devices. This kind of attack are establishing in the network domain to diminish gradually the resource of the service provider. There are many limitation of ML based algorithm for IoT devices. The processing for the IoT device is very small due to small appliances with less energy constrained one. So the ML techniques cannot connect directly in the resource environment.

Problem Statement

The destructive distribute denial of service is unique type of botnets that recently facing many attacks in IoT devices which is hard to solve. The IoT devices are transferring the data from one place to another. These data are generating and transferring diversely in nature. During processing of data are having many encoding, compression types. This will lead to heterogeneity property. The ML algorithms are not sufficient domain to this property and very challenging task too. The analysis of heterogeneous data is relatively tough task by ML algorithm. Obviously, the

ISSN: 2582-2640 (online)
Submitted: 16.12.2020
Accepted: 12. 01.2021
Published: 19.01.2021

Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No.04
Pages: 236-245
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.4.005

heterogeneous devices demand is an important in IoT networks. The ML algorithm capabilities are weaker to communicate heterogeneous device.

Proposed Solution

This research article considered this problem and using DL based algorithm for alternative to improve performance. Our research work will address the comparative analysis between DL algorithms and identify the higher accuracy algorithm for security solution. Also discuss about many challenges and future development of IoT security domain. This will enable the secure communication among IoT components with smart decision method named deep learning approach. Many unsolved problems in IoT network domain will be solved by deep learning approach.

4. SECURITY CHALLENGES AND THREAT MODELS IN IOT

The attackers will use many ways to attack IoT devices for example with the help of social engineering is one of the platforms to attack in physical. This perimeter of the networks is hard to mitigate. The IoT devices are having well known capability to create heterogeneous domain for process. ZigBee, WSN, MANET, WiFi, RFID, NFC techniques includes more complex process. The network layer level attacks will be at routing and traffic analysis, spoofing. The Sybil attack is used to create fake identities in the network for illusion [20, 21]. During the updating the routing information in routing tables, the attack can be possible such as spoofing or altering routing information in IoT network domain. Denial of Service (DoS) attack stick at transport layer in general during the framework of IoT. Resource constrained will not be scaled due to the nature of the IoT for traditional Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) at this layer [22, 23, 24].

4.1 General IoT Security Threats

The IoT domain identifies the threat surfaces. Generally the IoT attack surfaces are categorized as follows

1. Physical device
2. Network service
3. Cloud service
4. Web and Application interface.

The IoT devices should be working in an unreachable area for our daily comfort life. More over this system are more complex due to multi-level setup of individual function. So this will be concentrated security requirement in physical states itself [25, 26]. The potential threats occurrence is in IoT system shows figure 4.

The storing data in IoT devices should not be made known by attackers. Because these data contents are confidential, such as medical report, military report. The effective checking algorithm to detect received data is as an original or fake or modified content and malicious input like a fabricate inputs [27]. This feature can be ensured the IoT system by integrity property in any communication medium. IoT medical devices should have high effective integrity checking mechanism. There is more discussion about losing or modifying information leads to loss of human lives in the medical sector [28, 29]. The authentication is little tricky and it varies from device to device. This verification should be very healthy in the IoT framework. Otherwise it will lead to low security and easy attack by unauthorized person. Obviously there is need of an effective authentication that provides robust security domain for IoT devices. Very fundamental feature is continuous availability in all time for IoT security reason. In many IoT devices, no consideration of non-repudiation for security reason [30]. From our point of view, all these security parameter should be considered for effective IoT security communication. The block diagram for many types of IoT threats is notified in figure 4.

ISSN: 2582-2640 (online)
Submitted: 16.12.2020
Accepted: 12. 01.2021
Published: 19.01.2021

Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No.04
Pages: 236-245
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.4.005

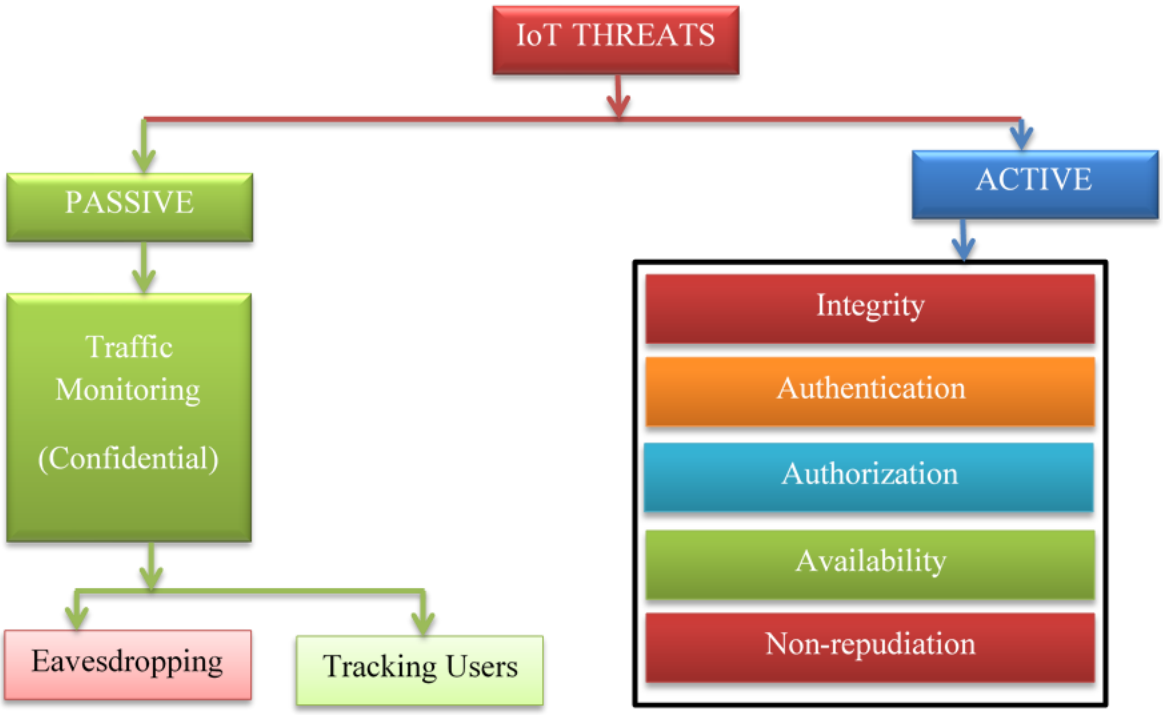

Figure 4 Types of threats in IoT device

4.2 Layer level attack

The layer level attacks include protocol layer attack and passive attack. The mitigation of passive attack is very hard in the network domain. The multi layered attacks could be launched on IoT infrastructure. This attack contains user information in the network. As we know, the data transfer is primary goal in IoT networks. So the passive attacks cannot be solved or prevent easily. Also it is an essential to guarantee for quality data transfer in the IoT real time environment. There are many attacks in layer level as discusses in following sections.

5. OVERVIEW OF PRACTICAL APPROACH

5.1 DL-based authentication and access control in IoT

DL algorithms are giving more impact on IoT system recently. It is a developing research topic currently. Because of handling large dataset, DL based algorithms are providing great effective performance than ML based framework for IoT devices. Usually, DL algorithm has capable of remove complex representations from data set [31]. Without human intervention, IoT based devices are interacting one another due to deep linking of unified protocol. In a smart home, all IoT devices should be deep-linked automatically for effective performance. The computational architecture contains several processing layers to learn about data set base of DL algorithm. Feature extraction will be suitable selection based on input defected data. The computing architecture is constructed hierarchical based representation. Our proposed work contains principle of based on both discriminative and generative learning named hybrid DL. There are many hybrid learning methods are Deep auto encoders (AEs), Deep Belief Network (DBN), Restricted Boltzmann Machine (RBMs), Generative Adversarial Networks (GANs) and ensemble of DL networks (EDLNs). The discriminative learning methods are named CNNs, RNNs for classification alone.

5.2 Proposed Architecture

The proposing architecture for IoT system comprises with three sections named Input, classifier, decision making section. The discussion of the sections as follows one by one.

ISSN: 2582-2640 (online)
Submitted: 16.12.2020
Accepted: 12. 01.2021
Published: 19.01.2021

Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No.04
Pages: 236-245
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.4.005

5.2.1 Input Section

The figure 5 shows simple smart home for IoT consists of several facilities with many sensors. For example, the central control devices connected with many appliances such as laptop, television, cameras, lights, fan and all home appliances.

Figure 5 Smart Home IoT

5.2.2 Training and Testing Section

Our classification framework believes in hybrid deep learning method and attack detection accuracy is high. The learning algorithm is at training phase with respect to trained model. The environment gives data to trained model as well to learning algorithm for training and testing purposes. Normally the attacks can happen in the different layers at IoT devices. Many of existing algorithms are cryptographic based one to detect the attack. This type of algorithms is suffering in accuracy and causes of false positives. Our suggesting algorithm is including DBN have been used. The general classification framework is shown in figure 6.

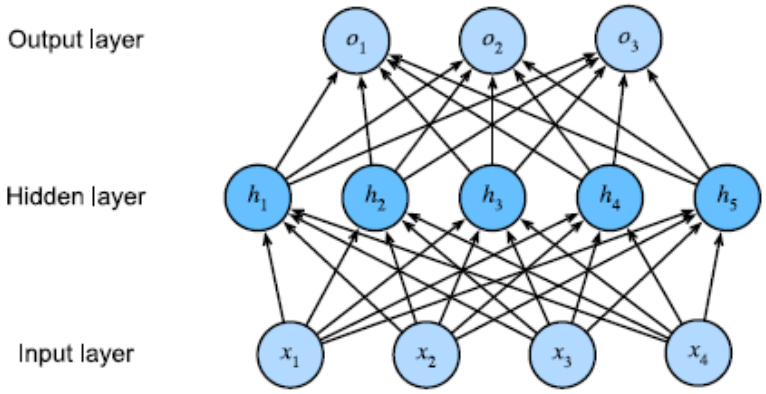

Figure 6 Classifier framework

ISSN: 2582-2640 (online)
Submitted: 16.12.2020
Accepted: 12. 01.2021
Published: 19.01.2021

Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No.04
Pages: 236-245
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.4.005

5.2.3 Output Section

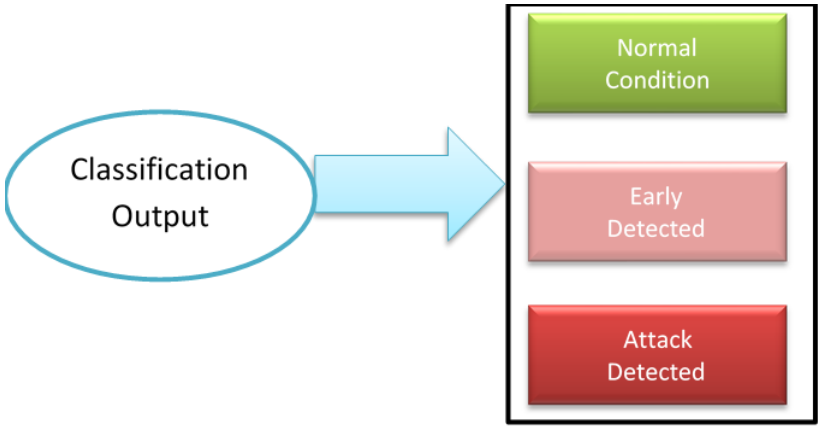

Figure 7 Structure of Decision Making

The decision making structure shows in figure 7. Generally the reinforcement learning starts learning by interacting with their past and previous outputs like as human learning structure. It also teaches DL algorithm that how and what to react in complex condition environment [30]. This RL is stimulated by the emotional and neuro logical views on machine algorithm controlling by its environment. RL comprises of making an agent learn how to map status quo to action accordingly to reach the maximum rewards. The decision making agent will get knowledge of present optimal action from strategy updated output which is from strategies learning algorithm. The most of the rewards is collected by attempting them through trial and error. The overall proposed system architecture is drawn here as block diagram in figure 8.

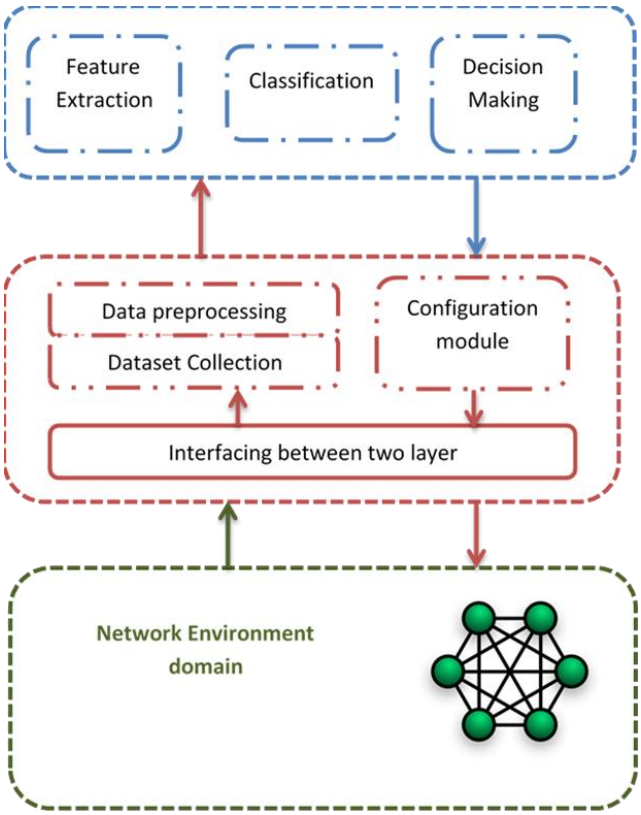

Figure 8 The Proposed system architecture

ISSN: 2582-2640 (online)
Submitted: 16.12.2020
Accepted: 12. 01.2021
Published: 19.01.2021

Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No.04
Pages: 236-245
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.4.005

The maximum rewards is depends on state of the environment. Our suggesting method comprises of DL and RL play together in the environment with dissimilar conditions. So the RL can have maximum rewards due to combine with DL. In this approach RL provides good learning experience of various environments input to DL that it can find best strategies for action value approximation [31, 32, 33].

The attack detection in our algorithm includes RL provides high accuracy than other ancient methods. The distributed attack detection can handle at near smart infrastructure with various parameters from hybrid learning mechanism. This learning mechanism is added on with RL algorithm which gives good results in accuracy. Because of this decision making algorithm can create the maximum rewards because of more iteration. Always the precipitation infrastructure is resource constrained for IoT network structure. During the time of attack or before that the data generating nodes are affected and it informed decision tree. The hybrid DL based decision approach in IoT realize the attack from primitive to mature stage and determining the optimal point for detection mechanism. It gives good accuracy and reduces inactive for communication & utilizes the resources. Our suggested approach proves that it can address DoS attacks in IoT [34, 35, 36, 37]. This table 1 is tabulated different hybrid deep learning solutions and shows their performance rating based on their results. Our suggesting combined version of deep learning and RL approach performs very high efficiency for IoT secured network. This paper comprises many potential requirements (confidential, authentication, authorization, integrity, availability and non-repudiation) for IoT network threats.

Table 1 Comparison of different solutions for IoT secured Network

Solutions	Confidential	Integrity	Authentication + Authorization	Availability	Decision Making	Overall Efficiency
AEs	Yes	No	No	No	*NA	Low
RBMs	NO	Yes	No	No	*NA	Low
GANs	Yes	Yes	No	No	*NA	Moderate
EDLNs	No	Yes	No	Yes	*NA	Moderate
DBNs	Yes	Yes	Partial	No	*NA	Moderate
DBN + RL	Yes	Yes	Yes	Yes	Early Attack detection	High Efficiency

*Not Available

6. FUTURE ENHANCEMENTS

The combination of DL & RL can construct great strategy to gain supreme effective term rewards. Because of an intelligent approach of DL, the RL can determine the best reward policy for performing an action. Some of the mis-classification problem arises due to complex pattern in the dataset. This kind of pattern will be leant by RL without any additional feature craft and solve automatically which arrange for efficient classification for DL algorithm.

7. CONCLUSION

The main influences of this research work are summarizing as follows; we presented the limitation of the ancient methods to solve the security problems in IoT networks by using ML methods. We presented new and efficient complete survey of hybrid DL methods (DBN algorithm) with RL technique in IoT. Also we focused an identifying overall higher accuracy and better effective performance for solving security threats. The deep belief network is proved that it is suitable RL approach for IoT devices due to its deep searching algorithm. The DBN method is acknowledged for effective security approach for RL method. At last this RL outcome is revising from feedback or old mistakes as behavior of human and animals. It starts with some operations in the real time environment and making precise decision from accurate output. This combined learning methods greatly helpful and will provide highest accuracy for dynamic applications such as real time robotics. This new era DL & RL approach will segregate the reward function continuously due to rectify failure rate and improve success rate towards highest accuracy; RL techniques are improving efficient in protecting attack whereas not knowing about previous history of data values. Further development of this research is that the environment will be sensed and to get the best out of both instantaneous and

ISSN: 2582-2640 (online)
Submitted: 16.12.2020
Accepted: 12. 01.2021
Published: 19.01.2021

Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No.04
Pages: 236-245
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.4.005

future prediction term rewards. The future challenges in IoT by this combination of DL & RL techniques are also discussed in previous section.

REFERENCES

[1] Sathish and Smys "A Survey on Internet of Things (IoT) based Smart Systems" Journal of ISMAC (2020) Vol.02/ No.04 Pages: 181-189, http://irojournals.com/iroismac/ DOI: https://doi.org/10.36548/jismac.2020.4.001
[2] Riahi Sfar, Arbia & Natalizio, Enrico & Challal, Yacine & Chtourou, Zied. (2017). A Roadmap for Security Challenges in Internet of Things. Digital Communications and Networks. 4. 10.1016/j.dcan.2017.04.003.
[3] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646-1685, thirdquarter 2020, doi: 10.1109/COMST.2020.2988293.
[4] V. Subbarao, K. Srinivas and R. S. Pavithr, "A SURVEY ON INTERNET OF THINGS BASED SMART, DIGITAL GREEN AND INTELLIGENT CAMPUS," *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India, 2019, pp. 1-6, doi: 10.1109/IoT-SIU.2019.8777476.
[5] Ferrag, Mohamed Amine & Maglaras, Leandros & Derhab, Abdelouahid. (2019). Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends. Security and Communication Networks. 2019. 10.1155/2019/5452870.
[6] Sathish, (2020). "Computer Vision on IOT Based Patient Preference Management System" Journal of Trends in Computer Science and Smart Technology. 2. 68-77. 10.36548/jtcsst.2020.2.001.
[7] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," in *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41-49, Sept. 2018, doi: 10.1109/MSP.2018.2825478.
[8] Gu, Rentao & Yang, Zeyuan & Ji, Yuefeng. (2020). Machine Learning for Intelligent Optical Networks: A Comprehensive Survey. Journal of Network and Computer Applications. 10.1016/j.jnca.2020.102576.
[9] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686-1721, thirdquarter 2020, doi: 10.1109/COMST.2020.2986444.
[10] E. L. C. Macedo *et al*., "On the security aspects of Internet of Things: A systematic literature review," in *Journal of Communications and Networks*, vol. 21, no. 5, pp. 444-457, Oct. 2019, doi: 10.1109/JCN.2019.000048.
[11] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, pp. 1125–1142, Oct 2017.
[12] 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 & Tutorials, vol. 17, no. 3, pp. 1294-1312, 2015.
[13] 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, vol. 84, pp. 25-37, 2017.
[14] R. H. Weber, "Internet of Things–New security and privacy challenges," Computer law & security review, vol. 26, no. 1, pp. 23-30, 2010.
[15] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266-2279, 2013.
[16] I. Yaqoob et al., "The rise of ransomware and emerging security challenges in the Internet of Things," Computer Networks, vol. 129, pp. 444-458, 2017.
[17] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning," arXiv preprint arXiv:1801.06275, 2018.
[18] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A Detailed Investigation and Analysis of using Machine Learning Techniques for Intrusion Detection," IEEE Communications Surveys & Tutorials, 2018.
[19] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015.
[20] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, "Security and privacy for cloud-based IoT: Challenges," IEEE Communications Magazine, vol. 55, no. 1, pp. 26-33, 2017.
[21] C. Bekara, "Security issues and challenges for the IoT-based smart grid," Procedia Computer Science, vol. 34, pp. 532- 537, 2014.

ISSN: 2582-2640 (online)
Submitted: 16.12.2020
Accepted: 12. 01.2021
Published: 19.01.2021

Journal of Soft Computing Paradigm (JSCP) (2020)
Vol.02/ No.04
Pages: 236-245
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2020.4.005

[22] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future generation computer systems, vol. 29, no. 7, pp. 1645-1660, 2013.
[23] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp. 2481-2501, 2014.
[24] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in Proceedings of the 2nd international conference on Embedded networked sensor systems, 2004, pp. 162-175: ACM.
[25] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems," Proceedings of
the IEEE, vol. 100, no. 1, pp. 283-299, 2012.
[26] K. Wan and V. Alagar, "Context-aware security solutions for cyber-physical systems," Mobile Networks and Applications, vol. 19, no. 2, pp. 212-226, 2014.
[27] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," Journal of biomedical informatics, vol. 55, pp. 272-289, 2015.
[28] J. Guo, I.-R, et al "A survey of trust computation models for service management in internet of things systems," Computer Communications, vol. 97, pp. 1 – 14, 2017.
[29] B. Schneier, Secrets and lies: digital security in a networked world. John Wiley & Sons, 2011.
[30] B. Jung, I. Han, and S. Lee, "Security threats to Internet: a Korean multi-industry investigation," Information & Management, vol. 38, no. 8, pp. 487-498, 2001.
[31] M. Abomhara, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," Journal of Cyber Security and Mobility, vol. 4, no. 1, pp. 65-88, 2015.
[32] 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.
[33] W. Zhou, Y. Zhang, and P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," arXiv preprint arXiv:1802.03110, 2018.
[34] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "IoT goes nuclear: Creating a ZigBee chain reaction," in Security and Privacy (SP), 2017 IEEE Symposium on, 2017, pp. 195-212: IEEE.
[35] M. Nitti, L. Atzori, and I. P. Cvijikj, "Friendship selection in the social internet of things: challenges and possible strategies," IEEE Internet of things journal, vol. 2, no. 3, pp. 240-247, 2015.
[36] M. Armbrust et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, 2010.
[37] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications, vol. 34, no. 1, pp. 1-11, 2011.

ISSN: 2582-2640 (online)
Submitted: 16.12.2020
Accepted: 12. 01.2021
Published: 19.01.2021