Volume: 5, Issue: 3
Page: 61-70
2021

International Journal of
Science and Business
Journal homepage: ijsab.com/ijsb

IJSAB International

# Deep Learning Models for Cyber Security in IoT Networks: A Review

**Kosrat Dlshad Ahmed & Shavan Askar**

## Abstract:

The IoT systems and connectivity provide improved experience and improve the quality of service for the users in different perspectives. Recent development of the technological prospects and management of the sufficient aspects for the delivery of performance need to be ensured in this regard. The concept of IoT is related with the widely connected features, systems, data storage facilities, management processes, applications, devices, users, gateways, services and thousands of other elements. As the importance of IoT applications has been growing in recent times, the prospects for development and management are immense for the development opportunities. In recent times, cybersecurity and ensuring privacy for the users have attracted attention of the users. With growing popularity of the social media platforms, more and more people are becoming connected. With growing opportunity of connectivity, people need more secured space to connect. In this article, different aspects of the cybersecurity based on the deep learning models and analyzing the concepts of machine learning, understanding the concept of security and privacy, contributing to the development and management of cybersecurity etc. To demonstrate the understanding of cybersecurity in the IoT networks, effective deep learning models such as MLP, CNN, LSTP and a hybrid model of CNN and LSTP have been analyzed. To contribute to the learning process, future research opportunities have also been identified.

**IJSB**
**Literature review**
Accepted 1 February 2021
Published 3 February 2021
DOI: 10.5281/zenodo.4497017

***Keywords:*** *Deep Leaning, Machine Learning, Cyber Security, Internet of Things, Privacy, Cyber Security.*

About Author (s)

**Kosrat Dlshad Ahmed,** Information System Engineering, Erbil Polytechnic University, Erbil, Iraq. Email: kosrat.ahmed@epu.edu.iq.

**Shavan Askar (Corresponding Author)**, Assistant Professor, Erbil Polytechnic University, Erbil, Iraq. Email: shavan.askar@epu.edu.iq.

## 1. Introduction

Technological development and emerging prospects have redefined the way human interact and connect with each other (Bengio et al., 2013). Providing necessary development and management processes for dealing with the deep learning processes, different aspects of the internet security and management processes are vital to analyse (Schmidhuber, 2015). Considering the continuing growths and expansion of the IoT networks and management capabilities, modern day practices for developing the security criteria need to be utilized (Sulaiman & Askar, 2015; Farez & Askar, 2016). Modern IoT 4th generation networks and processes are intricate in nature and require effective utilization of the available resources. As the concept of IoT system and networks deal with interrelated components which allow the users to communicate and inter connect via sub networks, ensuring security for different components and subnetworks are challenging at times (Zhang et al., 2018). Each SN or sub network is allowed to work for specific task and relevant aspects of the architecture (Axelsson, 2000). In this way, overall determination and management of the IoT networks require effective utilization of the capabilities and management processes, so that different neural engines can be connected effectively. These connected networks and sub networks need to be designed to address the challenges and prospects that are required to evaluate the context of security (Sulaiman & Askar, 2015; Fares & Askar, 2016). In the context of IoT security, the CIA or Confidentiality, Availability and Integrity are considered as the fundamental elements of secured workspace (Kasongo and Sun, 2020). In order to explore the contexts of cybersecurity, relevant models and prospects have been evaluated in this regard in order to develop relevant criteria and management criteria.

## 2. Literature Review

### 2.1 Deep Learning

Deep Structured Learning or simple Deep Learning can be referred to as member of broader Machine Learning Family (Bengio et al., 2015). Considering the scopes and opportunities for different deep learning methods and facilities, modern day digital world has adopted effective strategies to address different deep learning and machine learning methods and strategies (Ciresan et al., 2012). Different computer and system network architecture require different forms of deep learning models.

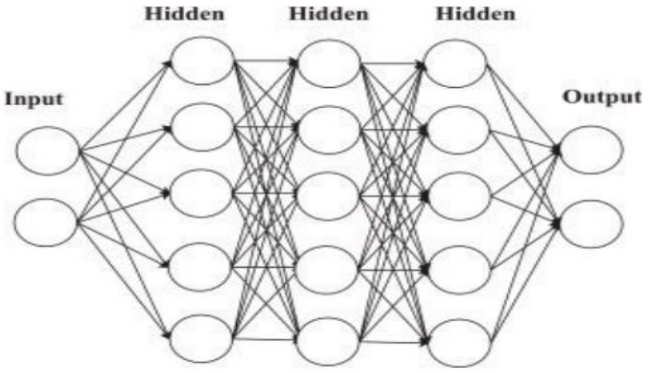


Figure 1. Deep Learning Architecture

The basic formation of the DL model consists of single input layer and several hidden layers (Ferrag et al., 2020). These hidden layers in the model lead to output layer (Li et al., 2019). CNN or Convolutional Neural Network is widely used to determine and utilize the concepts of the IoT application and management development (Ge et al., 2019). Recurrent Neural Network or RNN is the type of deep learning process which has provided effective

development of the network management (Parker et al., 2019). LSTM model and RNN are similar in the evolution and development prospects which need to be determined in order to develop different criteria for the effective management of the cybersecurity prospects. Different deep learning processes and methods have intrinsic implications on the computer and network systems such as speech recognition, image processing, AI applications, health care management, driving and management etc. (Shinde et al., 2019). Considering the growth and prospects of the sector of IoT enabled deep learning setting, the security prospects are important so that different criteria for development can be ensured. The context of deep learning can also be expanded to the aspect of decentralized computer networks as well as in the centralized networks. With growing needs and increasing usage, development of the IoT networks and deep learning have roots in the development of the modern technological development aspects.

### 2.2 Cyber Security in IoT Networks

To understand the concept of cyber security, this is necessary for the research processes to understand the concept of privacy. IoT networks are connected layers of controllers and physical components, edge computing considerations and computing levels, connective level considerations, management of the security components and determination of the outcomes of the processes, data abstraction processes, accumulation of data and information, application process, IoT security level determination, collaboration and management of the security processes etc. (Axelsson, 2000). In order to determine the aspects of cybersecurity, this is necessary to understand the aspects of privacy, and security in the networks.

## 3. Privacy

In digital world practices, this is important for the practitioners to implement the privacy and security concerns so that maintaining individual privacy is possible (Krizhevsky et al., 2012). Cybersecurity is termed as the collective approach for ensuring protection of computer networks and systems from damage or any kind of external theft relating to the prospects of hardware, system, electronic data and software etc. (Al ameedee, 2018). Modern digital world is becoming increasingly dependent on the effective use and management of computer systems. Due to rapid growth of technological advancements, smart devices and technologies, wireless network systems such as Bluetooth, Wi-Fi etc. security is becoming important in present day applications. Jarvis Thomson argued that the concept of property and liberty can be regarded as privacy but the context of privacy differs from the sole concept of liberty and property claims (elkhodr, 2016). Solove regarded 8 exact concepts of privacy to demonstrate the concept of security.

Right to be alone: If a person wishes to be alone from other persons' contact, he or she can maintain the secrecy (Al-Rubaie, 2018). The concept of privacy and security are dependent on how individual processes the concept of security.

Limited Access: This notion is dependent on the prospect that a person can take part in different societal affairs irrespective of the rules and information barriers (Elgan, 2016). Considering the needs and challenges for the personal development and management can be considered in this regard.

Control: The right to control over the information and management on self management and prospects can be considered in this regard (Komando, 2017).

Privacy State: The state of individual's privacy and management can be considered in this stage. Managing the privacy and management can be effectively maintained to ensure cybersecurity for different persons (Cha et al., 2016).

Secrecy: The right to secrecy and management of personal information needs to be established considering individual requirements (Michael and Whitman, 2016).
Autonomy and Personhood: Autonomy and personhood for given security contexts need to be maintained for delivering effective management support (Jo et al., 2011). Autonomy of the selection process needs to be maintained for this purpose.
Personal Growth : Personal growth opportunity and management considerations for the security prospects can be ensured (Al-Rubaie et al., 2016).
Intimate Relationships: The right to secure the relationships and interactions with the friends and partners need to be secured in this purpose.

## 4. Cybersecurity in IoT

The concept of cybersecurity is based on the idea to promote safe practice and integrity of the digital world and practices (Bipraneel and Cheung, 2018). Cybersecurity is considered as the practice of protecting and safeguarding the online practices, interaction, programs and networks etc. In recent times, there have been multiple cyber-attacks endangering the safeguarding and management of the security in the first place. Successful cybersecurity approaches always consider the elements for privacy of the individuals, integrates the organisational approach with the individual interests, and offer multiple layers of security to promote safe practices. Considering the elements and management of the cybersecurity practices, different aspects of the evaluation and management of cybersecurity considerations need to be evaluated (Emmanuel et al., 2020). In different layers and architecture of the IoT networks, providing required cyber security is challenging for the developers. Internet of things is considered as the next big thing for the digital world (Kozik et al., 2018). In this way, the user specific applications and management capability for the processing of organisational capability can be ensured. IoT applications and development of the integrated processes target to provide enhanced quality of the operation, interaction and management capability for the professionals (Yan et al., 2018). IoT applications and system usually consist of the technologies, smart objects around the world which are connected via secured network. Cybersecurity in the IoT applications plays vital part as this can ensure effective management of the interaction with the human and objectives. IDS or Intrusion Detection System is used widely for the determination and management of the threats in the cyber space. In this way, the developers can securely ensure effective performance and management capability of the cyber threats that may put the system in danger (Zhang et al., 2018; Askar, 2017; Fizi & Askar, 2016; Askar, 2016; Keti & Askar, 2015). Considering the growth and management capability for the cyber security, relevant architecture and management capability need to be addressed. QoS or Quality of Service of the IoT applications and devices are important aspects for effective determination of the performance and management of the capability assessment. IDS can detect the potential cyber attacks and harms may cause in the cyber platforms (Bipraneel and Cheung, 2018). Low latency applications and system performance need to be upgraded for the evaluation of the performance and management considerations for the safe cyber space (Askar et al., 2011; Al Majeed et al., 2014).

## 5. Secured IoT Architecture

Secure IoT management and network tools require sufficient development and processing of the information management. In this regard, digital technology and capability assessment for the technological tools and assembling the architecture are vital (Scully, 2017). Considering four layer architecture for the development of the secure IoT networks have been designed in this case (Scully, 2017). Four different layers for the IoT networks are device layer, communication layer, loud layer and lifecycle management layer. All these layers have

significant impact on the development of the structure and components for secure structure and development.

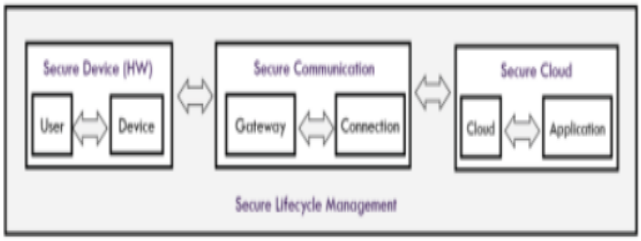


Figure 2. Four Layers of cybersecurity in IoT networks

### 5.1 Secure Layer – Device

Secure device layer is the first step while ensuring and designing secured cyber space (Santos et al., 2011). Considering the development and management considerations for the secure workspace and network facility, the management of secured network layer is significantly important for the cloud – server interactions. Utilizing TPM or trusted platform modules can resolve the chip security required for the network management. Developers often use different forms of RSA keys which are used for the encryption purpose (Scully, 2017). Developers also use AIK or attestation identity key for the development of the secure device layer. Secure booting and physical security protection are also important for the management of the secure device and components. Modern usage also implies the importance of the firmware integrity of the solutions and providers for effective utilization of the resources. The device management also needs to ensure the encryption facilities, proxy management, firewall inspection as required, components for the secure connection facility, and analyse the data while receiving and sending (Kalash, et al., 2018). Modern day usage implies importance on the integrity of the interaction of the server management.

### 5.2 Secure Layer – Communication

For the secure layer of communication, the system management needs to be able to ensure data centric evaluation and encrypting data while required (Kumar et al., 2018). Avoiding compromise on the development and management of data security, effective controlling of the data management needs to be secured. Connection initiation in the network needs to be maintained while maintaining the required protocols and service processes (Cui et al., 2018). This layer is also dependent on the inherent evaluation and management of security to the outer layers.

### 5.3 Secure Layer – Cloud

This layer contributes to the development of the cloud based security and management in different perspectives (Bipraneel and Cheung, 2018). In this way, the developers may use the utilization of the strong security procedures and controlling facilities. Considering the development and management of the cloud based models for security management, developers can ensure sufficient management capability for the users (Mohammad et al., 2019). Analysing the components and management processes of the cloud layer, evaluation of the IoT applications need to be considered for improved prospects.

### 5.4 Secure Layer – Lifecycle Management

This layer targets to secure the lifecycle management to be effective and manageable for the users. Evaluating the processes and management capabilities for the client – server

evaluation and interaction, the lifecycle management can be ensured. Log monitoring is also important for the processing the management of the organisational capability.

## 6. Analysis

### *6.*1 Related Works

Comparison of some of the relevant works on deep learning and cybersecurity space are presented.

TABLE I. COMPARISON OF LITERATURE

| Authors | Analysis |
|---|---|
| Kasongo and Sun (2020) | The authors discussed about the deep learning methods and implications for the developers in modern day applications. In order to provide sustainable solution, the authors opted for wrapper based concpet that will allow the users to extract the requried data for the detection systems. In this way, the authors were able to determine the outcomes for effective solution for the problem.<br>[a.] WFEU compiled with FFDNN model used. |
| Li et al. (2020) | The authors proposed a robust detection model for the security management process applicable for the IoT enabled applications. For the industrial usage of IoT applications, development of the multi CNN fusion need to be authorised.<br>[b.] CNN model used. |
| Tian et al. (2020) | Tian and the authors used distributed solution for the deep learning method. In the edge provided services, detection of the intrusion and attacks have been utilised. Web enabled services were also utilised in this analysed.<br>[c.] CNN and GRU model used. |
| Ferrag et al. (2020) | The authors discussed about the approaches, comparative study and datasets on the cyber security systems and processes. Considering the growth and management processes, the authors used cyber security processes and solutions to evaluate the considerations for the security intrusion detection processes.<br>[d.] RNN, CNN and DNN methods used. |

### *6.2* Review of Deep Learning Models

Some effective deep learning methods will be reviewed in this chapter.

#### 6.2.1 DL Model – MLP

In this segment, a very basic architecture of the MLP deep learning model will be evaluated. In this MLP deep learning model, there is single input layer which is followed by three consecutive dense layers (Hwang et al., 2019). In the system model, output from different layers becomes the input for the next layer. From the proposed layer of MLP system, different outputs and measures can be considered (Bae et al., 2019). In the system, one dropout layer is selected in order to prevent the system from heating. In this process, the overall system is operated under the sigmoid function in order to provide the output.

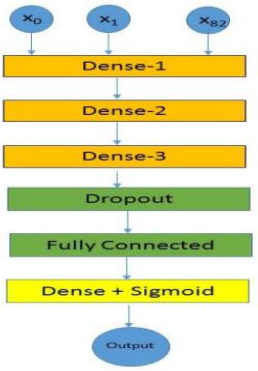


Figure 3. Deep Learning Method – MLP

### 6.2.2 DL Model – CNN

In the CNN deep learning model, there are mainly three forms of layers (Tian et al., 2019). These layers are pooling layer, dense layer and convolution layer. These layers collectively form 3D format such as channels, steps and batch. Analyzing the concepts and determinations of these models, effective models of deep learning models are evaluated.

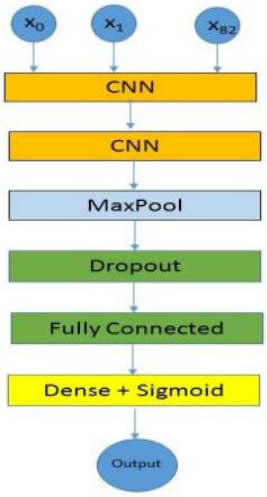


Figure 4. Architecture of CNN DL Model

### 6.2.3 DL Model – LSTM

Unlike the CNN model, the deep learning LSTM model is based on the improvement of the learning process of the system (Tian et al., 2019). The concept of LSTM model is based on a RNN system which targets to decrease the pressure, lag in the performance and enhance the output in different aspects of the operation. In this system, the operation is conducted by a sigmoid function which is translated into the desired outcome of the functions (Nsunza et al., 2018). Relating to the outcomes and management of the system approach, this LSTM model can be used for future scaling and management of the performance of the deep learning processes (Pratomo et al., 2018).

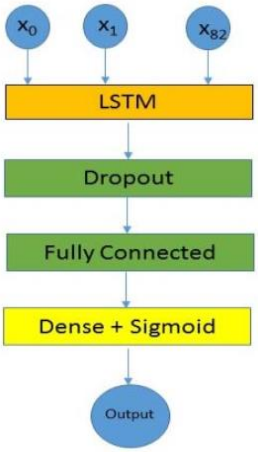


Figure 5. LSTM DL Model

### 6.2.4 DL Model – CNN + LSTM

The hybrid model of CNN and LSTM represent a collective approach for the determination of the deep learning outcomes (Zhou,et al., 2018). Considering the architecture, this model is considered a hybrid model (Diro and Chilamkurti, 2018). This model of deep learning has greater performance to input ratio (Aminanto et al., 2017).

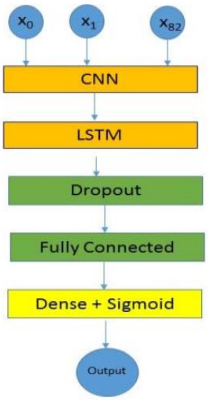


Figure 6. LSTM and CNN Hybrid Model

## 7. Conclusion

Modern IoT technologies, and system offer greater prospects for the integrated management of the technology, services and management capability for the digital world (Kasongo and Sun, 2020). People are becoming more and more connected and intuitive as a result of integrated development of the technology. As a consequence of growing technological capability, the security concerns are becoming more and more important. Considering the growth and management opportunities for the professionals, need to be justified for the effective management of the technological tools and development opportunities. In this analysis, different aspects of the IoT applications, considerations for the deep learning etc. have been discussed to analyse the security implications for the modern technology.

## References

Al Majeed, S., Askar, S. & Fleury, M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application. UKSim-AMSS 16th International Conference on Computer Modelling and Simulation (UK), Cambridge (pp. 292-297), doi: 10.1109/UKSim.2014.59.

Al-Rubaie (2018). "Privacy Preserving Machine Learning: Threats and Solutions," IEEE, Florida, 2018.

Al-Rubaie, Chang, J. M., Morris, (2016) "Reconstruction Attacks Against Mobile-Based Continuous Authentication Systems in the Cloud," IEEE Transactions on Information Forensics and Security,, p. 2648–2663, 2016.

Aminanto, R., Choi, H. C., Tanuwidjaja, P. D., Yoo, and K. Kim, (2017). "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," IEEE Trans. Inf. Forensics Secur., vol. 13, no. 3, pp. 621–636, Oct. 2017.

Askar S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Evaluation of Classified Cloning Scheme with self-similar traffic. 3rd Computer Science and Electronic Engineering Conference (CEEC), Colchester, 2011, pp. 23-28, doi: 10.1109/CEEC.2011.5995819.

Askar, S. (2016). Adaptive Load Balancing Scheme For Data Center Networks Using Software Defined Network. Journal of University of Zakho, Vol. 4(A), No.2, Pp 275-286,

Askar, S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5, pp.1047-1056

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Service differentiation for video applications over OBS networks. 1*6th European Conference on Networks and Optical Communications*, Newcastle-Upon-Tyne, pp. 200-203.

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). A novel ingress node design for video streaming over optical burst switching networks. Optics Express, Vol. 19 (26), pp. 191-194

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Adaptive Classified Cloning and Aggregation Technique for Delay and Loss sensitive Applications in OBS Networks. in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2011, OSA Technical Digest (CD) (Optical Society of America, 2011), paper OThR4.

Axelsson, (2000). "Intrusion Detection Systems: A Survey and Taxonomy," 2000.

Bae, S., Jang, M., Kim, and Joe, I. (2019). “Autoencoder-based on anomaly detection with intrusion scoring for smart factory environments,” in Communications in Computer and Information Science, 2019, vol. 931, pp. 414–423.

Bengio, Y., Courville, A., and Vincent, P. (2013). "Representation Learning: A Review and New Perspectives". IEEE Transactions on Pattern Analysis and Machine Intelligence. 35 (8): 1798–1828. arXiv:1206.5538. doi:10.1109/tpami.2013.50. PMID 23787338. S2CID 393948.

Bengio, Yoshua; LeCun, Yann; Hinton, Geoffrey (2015). "Deep Learning". Nature. 521 (7553): 436–444. Bibcode:2015Natur.521..436L. doi:10.1038/nature14539. PMID 26017442. S2CID 3074096.

Roy, B. and Cheung, H. (2018). A deep learning approach for intrusion detection in internet of things using bi-directional long shortterm memory recurrent neural network. In 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), pages 1–6. IEEE, 2018.

Cha, C.-Y., Dai and Chen, J.-F. (2016) "Is there a tradeoff between privacy and security in BLE-based IoT applications: Using a smart vehicle of a major Taiwanese brand as example," in IEEE 5th Global Conference on Consumer Electronics, Kyoto, Japan, 2016.

Ciresan, D., Meier, U., and Schmidhuber, J. (2012). "Multi-column deep neural networks for image classification". 2012 IEEE Conference on Computer Vision and Pattern Recognition. pp. 3642–3649. arXiv:1202.2745. doi:10.1109/cvpr.2012.6248110. ISBN 978-1-4673-1228-8. S2CID 2161592.

Cui et al., (2018). Detection of malicious code variants based on deep learning. IEEE Transactions on Industrial Informatics, 14(7), 3187-3196.

Diro and Chilamkurti, N. (2018). “Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications,” IEEE Commun. Mag., 56 (9), 124–130.

Elgan, "Does Google listen in on your life," 10 dec 2016.

Elkhodr, "preservation and management of location privacy in the internet of things," proquest llc, sydney, 2016.

Fares, N., Askar, S. (2016). A Novel Semi-Symmetric Encryption Algorithm for Internet Applications. Journal of University of Duhok, 19 (1), 1-9

Ayo et al. (2020) Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection. Information Security Journal: A Global Perspective, 1–17.

Ferrag, L., Maglaras, Moschoyiannis, S., and Janicke, H. (2020). “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” J. Inf. Secur. Appl., 50.

Fizi, F., & Askar, S. (2016). A novel load balancing algorithm for software defined network based datacenters, International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), Graz, 2016, pp. 1-6, doi: 10.1109/COBCOM.2016.7593506.

Ge, X., Fu, N., Syed, Z., Baig, G., Teo, and Robles-Kelly, A. (2019). “Deep learning-based intrusion detection for IoT networks,” in Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC, 2019, vol. 2019-Decem, pp. 256–265.

Hwang, M. C., Peng, V. L., Nguyen, and Chang, Y. L. (2019). “An LSTM-Based Deep Learning Approach for Classifying Malicious Traffic at the Packet Level,” Appl. Sci., 9(16), 3414

Jo. F. and J. A. K. , (2011). "Fingerprint Reconstruction: From Minutiae to Phase," IEEE Transactions on Pattern Analysis and Machine Intelligence.

Kalash, M., et al. (2018). Malware classification with deep convolutional neural networks. in 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). 2018. IEEE.

Kasongo and Sun, Y. (2020). “A Deep Learning Method With Wrapper Based Feature Exaction For Wireless Intrusion Detection System,” Comput. Secur., 92.

Keti, F., Askar, S. (2015). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. *6th International Conference on Intelligent Systems, Modelling and Simulation*, Kuala Lumpur, 2015, pp. 205-210, doi: 10.1109/ISMS.2015.46.

Komando (2017) "How to stop your devices from listening to (and saving) what you say," 29 sept 2017. (Online). Available: https://www.usatoday.com/story/tech/columnist/komando/2017/09/29/how-stop-your-devices-listening-andsaving-what-you-say/715129001/.

Kozik, M., Chora Å. Z., Ficco, M. and Palmieri, F. (2018) “A scalable distributed machine learning approach for attack detection in edge computing environments,” Journal of Parallel and Distributed Computing, 119, 18 – 26.

Krizhevsky, A, Sutskever, I., Hinton, G. (2012). "ImageNet Classification with Deep Convolutional NeuralNetworks" (PDF). NIPS 2012: Neural Information Processing Systems, Lake Tahoe, Nevada.

Kumar et al. (2018)Malic. ious Code Detection based on Image Processing Using Deep Learning. in Proceedings of the 2018 International Conference on Computing and Artificial Intelligence.ACM.

Li et al. (2020). “Robust detection for network intrusion of industrial IoT based on multi-CNN fusion,” Meas. J. Int. Meas. Confed., 154..

Li, A., Shinde, Y., Shi, J., Ye, X., Li, Y. and Song, W. (2019). "System Statistics Learning-Based IoT Security: Feasibility and Suitability," IEEE Internet Things J., 6 (4) 6396–6403.
Li, L., Deng, M., Lee, and Wang, H. (2019). "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," Int. J. Inf. Manage., 49, 533–545.
Michael E. W. (2016). Principles of Information Security, Cengage Learning, 2016.
Hassan, M. M., Gumaei, A., Alsanad, A., Alrubaian, M. and Fortino. G. (2019). A hybrid deep learning model for efficient intrusion detection in big data environment. Information Sciences, 513,386–396.
Moustafa, N., Turnbull, B., and Choo. K.R. (2018). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. IEEE Internet of Things Journal, 6(3), 4815–4830.
Nsunza, A,. Tetteh, R. and Hei, X. (2018). Accelerating a Secure Programmable Edge Network System for Smart Classroom, IEEE SmartWorld,
Parker, P. D, Yoo, T. A., Asyhari, L., Chermak, Y., Jhi, and Taha, K. (2019). "Demise: Interpretable deep extraction and mutual information selection techniques for IoT intrusion detection," in ACM International Conference Proceeding Series, 2019, 1–10.
Pratomo, P. Burnap, and Theodorakopoulos, G. (2018). "Unsupervised Approach for Detecting Low Rate Attacks on Network Traffic with Autoencoder," in 2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018.
Rana A. .A. (2018). exploiting user privacy from iot devices using deep learning and its mitigation," proquest.
Santos, I., Nieves, J. and Bringas, P.G. (2011). Semi-supervised learning for unknown malware detection. in International Symposium on Distributed Computing and Artificial Intelligence. Springer.
Schmidhuber, J. (2015). Deep Learning in Neural Networks: An Overview. Neural Networks. 61: 85-117.
Scully, (2017). Understanding IoT Security, iot-analytics, 19.
Sulaiman, S., Askar, S. (2015). Invetigation of the Impact of DDoS Attack on Network Efficiency of the University of Zakho. Journal University of Zakho, 3(2) , 275-280.
Tian, C., Luo, J., Qiu, X. Du, and Guizani, M. (2020). A Distributed Deep Learning System for Web Attack Detection on Edge Devices, IEEE Trans. Ind. Informatics, 16 (3), 1963–1971.
Tian, J., Li, and H. Liu, (2019). A Method for Guaranteeing Wireless Communication Based on a Combination of Deep and Shallow Learning," IEEE Access, 7, 38688–38695.
Yan, Y. Qi, and Q. Rao, (2018). Detecting malware with an ensemble method based on deep neural network," Security and Communication Networks.
Zhang, M., Zhou, and Fortino, G. (2018). Security and trust issues in fog computing: A survey, Future Generation Computer Systems, 88, 16 – 27.
Zhou, M., Han, L., Liu, J., He, S., and Wang, Y. (2018). Deep learning approach for cyberattack detection," in INFOCOM, IEEE Conference on Computer Communications Workshops, 2018, 262–267

## Cite this article:

**Kosrat Dlshad Ahmed, Shavan Askar** (2021). Deep Learning Models for Cyber Security in IoT Networks: A Review. *International Journal of Science and Business, 5*(3), 61-70. doi: https://doi.org/10.5281/zenodo.4497017
Retrieved from http://ijsab.com/wp-content/uploads/686.pdf

# Published by