Research Article

Saif Mohammed Ali, Amer S. Elameer, and Mustafa Musa Jaber*

IoT network security using autoencoder deep neural network and channel access algorithm

<https://doi.org/10.1515/jisys-2021-0173>

received August 04, 2021; accepted September 21, 2021

Abstract: Internet-of-Things (IoT) creates a significant impact in spectrum sensing, information retrieval, medical analysis, traffic management, etc. These applications require continuous information to perform a specific task. At the time, various intermediate attacks such as jamming, priority violation attacks, and spectrum poisoning attacks affect communication because of the open nature of wireless communication. These attacks create security and privacy issues while making data communication. Therefore, a new method autoencoder deep neural network (AENN) is developed by considering exploratory, evasion, causative, and priority violation attack. The created method classifies the transmission outcomes used to predict the transmission state, whether it is jam data transmission or sensing data. After that, the sensing data is applied for network training that predicts the intermediate attacks. In addition to this, the channel access algorithm is used to validate the channel for every access that minimizes unauthorized access. After validating the channel according to the neural network, data have been transmitted over the network. The defined process is implemented, and the system minimizes different attacks on various levels of energy consumption. The effectiveness of the system is implemented using TensorFlow, and the system ensures the 99.02% of detection rate when compared with other techniques.

Keywords: internet of things, attacks, network security, autoencoder deep neural network, channel access algorithm

1 Introduction

All manuscripts must be in English. These guidelines include complete descriptions of the fonts, spacing, and related information for producing your proceedings manuscripts.

Nowadays, the Internet-of-Things (IoT) [1–3] is one of the effective growing internet-enabled devices that utilized fitness trackers to smart health care systems. The IoT devices are integrating with different services [4] such as driverless cars, smart cities, smart brushing, smart farming, etc. These devices are worked along with the emerging techniques such as Artificial Intelligence because it is a fragment of the fourth industrial revolution. From the report of McKinsey, around a quarter of the business process [5] uses the IoT techniques, and it has been gradually increased in 2025. The IoT devices create a great impact in every industry and research application, but they can be misused and create risk because of privacy and

* **Corresponding author: Mustafa Musa Jaber**, Department of Computer Science, Dijlah University College, Baghdad, Iraq; Department of Computer Science, Al-Turath University College, Baghdad, Iraq, e-mail: Mustafa.musa@duc.edu.iq

Saif Mohammed Ali: Department of Computer Science, Dijlah University College, Baghdad, Iraq, e-mail: Saif.alameri@duc.edu.iq

Amer S. Elameer: Biomedical Informatics College, University of Information Technology and Communications (UOITC), Baghdad, Iraq, e-mail: Amerelameer@yahoo.com

security issues [6,7]. Generally, a greater number of IoT devices are interconnected to make the information transmission that time cybersecurity needs to be considered. The data transmission is hacked by malicious hackers [8] and creates thousands of attacks to access the private information, channel access, crippling infrastructure, and unsecured device access. Hence, the IoT devices are developed by withstanding the vulnerability and security issues. By considering these vulnerabilities, industries are planning to create IoT devices without having their firmware, software, and password details. Then, the devices are continuously changing their username and password at the time of installation; the created passwords are unique to every IoT device [9,10]. Finally, the firmware and software are the latest version that helps to mitigate the vulnerabilities.

Although the industries provide enough security measures to IoT devices, connectivity of IoT devices creates a specific set of security-related issues [11,12]. The IoT devices handle heterogeneity, scale, latency, proximity, interconnectivity, cost, structure (network attacks), dynamic configurations, and privacy-related issues. These IoT complexities created numerous impressions while transferring data from one location to another. Therefore, the Machine learning (ML) technique [13] is pragmatic in IoT security because it was able to adapt to changing parameters and also adjust changing environments successfully. Moreover, the ML technique's ability to detect intermediate attacks and unknown malicious activities [14] is predicted by using the learning process. Along with this, known attacks like Distributed Denial of Services (DDoS) [15] are detected from learned patterns with maximum accuracy. From the various ML techniques, deep learning (DL) approaches [16] are highly utilized in this field to identify the attack in IoT. The DL concept is able to extract the features automatically by scanning data. Moreover, this concept has a fast learning process that correlates the extracted features effectively. These advantages are the main reason to utilize the DL network to predict intermediate attacks and unauthorized access.

Although the DL network works perfectly, few research works fail to concentrate on various attacks such as priority violation, jamming, and spectrum position attacks. The network characteristics and channel status are considered less priority, which create complexity and latency issues while transmitting data over a network. To overcome these issues, an autoencoder deep neural network (AENN) along with a channel access algorithm is implemented to manage the security in the IoT environment. During this process, the system analyzes different attack characteristics that are used to predict attacks in the IoT environment. The discussed system was implemented using TensorFlow, and the effectiveness of the system was evaluated using different metrics such as precision, recall, accuracy, detection rate, false alarm rate, and error rate. Then, the rest of the paper is organized as follows: Section 2 analyzes the different researcher's opinions about IoT security, Section 3 discusses the autoencoder DL technique-based data security, and the effectiveness of the system is evaluated in Section 4. Conclusion is discussed in Section 5.

2 Related works

Ullah et al. [17] apply DL techniques in IoT-based communication for detecting security threats. Here, TensorFlow deep network approach is used to analyze the pirated software and malware-infected files over the network. This process aims to identify the malicious activities with maximum prediction accuracy. During the analysis, system uses the Google Code Jam dataset information, which is utilized to investigate the malware samples from the malign dataset.

Tsogbaatar et al. [18] discovered anomaly activities in the IoT using a deep ensembling learning algorithm (DEL). This system aims to resolve the data heterogeneity, data imbalance issues while predicting anomaly activities in the IoT environment. This goal is achieved by integrating the software-defined networking in IoT to handle the various network features. The introduced system predicts the device status whether it is a normal or abnormal one.

Balasundaram et al. [19] detected intrusion activities using the bat extreme learning approach (BEL) in smart IoT environment. The system aims to design a scalable system to predict the security-related activities. This process use the data analyzer mechanism to examine the IoT network characteristics to predict

malicious activities and attackers. This system is implemented using the API NDNOMNet smart automation tool. This system predicts the reply, spoofing, man-in-the-middle, and DDoS attacks effectively.

Basati et al. [20] detected intrusion activities in IoT environment using asymmetric parallel auto-encoder approach. This network uses the three layers of convolution filters that are used to extract the local features from input. The channel attention module is applied in the convolution layer to identify the intrusion activities. The discussed system is implemented using CICIDS2017, UNSW-NB15, and KDDCup99 dataset, and the system predicts the intrusion activity.

Swarna Priya et al. [21] detected intrusions on the Internet-of-Medical Things environment using gray wolf optimization along with DL network. This system examines the input, and various features are extracted according to the principal component analysis approach. With the help of the features, abnormal activities are detected, which improves the overall data security accuracy.

Hafeez et al. [22] introduced fuzzy C-means clustering with fuzzy interpolation techniques to predict malicious activities in an IoT environment. This process examines the user inputs and the similar activities are clustered, and abnormal activities are predicted with a minimum false positive rate. The successful determination of network access conditions helps to improve the overall prediction accuracy.

Fortino et al. [23] resilient framework is introduced in IoT to predict malicious activities. The system aims to minimize the delay and enhance trustworthiness while transmitting data in the network. This system uses the reputation model that provides effective solutions to identify attackers in the IoT environment.

Ullah and Mahmoud [24] detecting anomalous activities in IoT network using two-level flow approach. This system uses the flow-based approach to inspect the packet headers while transmitting data over the network. After that, a decision tree classifier is applied to predict the IoT Botnet attacks with high detection accuracy. The effectiveness of the system was evaluated using a cross-fold validation approach.

According to the above research activities, DL and ML techniques are utilized to investigate intermediate access and attacks effectively. By considering their opinion, in this work neural networks and channel access algorithms examine the intermediate access effectively. The detailed working process of the introduced system is discussed in the following section.

3 Proposed deep neural network for IoT network security

As discussed earlier, the ML techniques especially neural networks played a vital role in maintaining IoT network security. The IoT devices continuously transmit information from one location to another. During this time, intermediate attackers are aimed to access the network and transmitted packets to reduce the quality of the transferred data. This causes changes in data and creates complexity while making further data analytics.

The authorized access of the data minimizes the trust between the user and service provider in a network environment. Therefore, several ML techniques are incorporated with this IoT data transmission process but they are consuming time, high parameters are required to identify the threat patterns; latency and reliability are one of the serious problems. To overcome these issues, in this work, AENN is utilized. The network predicts the intermediate attacks by considering the behavior of evasion, exploratory, priority violation, and causative attacks. The created AENN approach investigated the packet or information transmission behavior to predict the attacks and unauthorized activities. This process directly indicates that the system cannot utilize the input samples to predict the intrusions in IoT. This process overcomes the data overfitting and unwanted data analysis time, because the input samples may contain noisy samples that differ from original data. Moreover, the information is transmitted by examining the channel status (busy or idle) then only the network receives the output (“No Ack” or “Ack”) status. The autoencoding neural network decides the intermediate attacks based on how the data transmission is performed in the single that considers the channel characteristics. The network effectively works in the unsupervised environment which means it is able to predict the unknown attack patterns using the learning parameters.

The AENN approach utilizing few general settings to identify the Internet mediate attacks in the IoT-wireless communication process. The $\mathfrak{T}$ transmission process should examine the data spectrum sensing and channel idle status to identify the data transmission. The $\mathfrak{T}$ is only performed if the network channel is idle else the data transmission should hold until the channel is free. During this process, the background transmitter $\mathfrak{B}$ has 0.8 rate (λ) while the packet arrived to the receiver. Therefore, before transmitting data in the IoT network, $\mathfrak{A}$ and $\mathfrak{T}$ should examine the channel current status to transmit the data, which help to eliminate the intermediate attacks in the earlier stage. Most of the attacks happened during the busy channel status; therefore, the single background transmitter $\mathfrak{B}$ is considered. The multiple $\mathfrak{B}$ causes to create the difficulties to examine the channel status that create the unwanted access in the IoT environment. Moreover, this single $\mathfrak{B}$ setting does not create any impact the attack or defense in the IoT data transmission process.

Here, the AENN network predicts the intermediate access in three phases such as sensing, transmission, and feedback phase. $\mathfrak{T}$ transmission process gathering the channel information, and the channel status (idle/busy) has to be investigated using neural network in the sensing phase. Suppose, the $\mathfrak{T}$ predicted channel is idle, then information is transmitted to the receiver $\mathfrak{R}$ (transmission phase) and then they acknowledge (Ack) to the $\mathfrak{A}$ once they get the data (feedback phase). At the time, the high parameter optimization problem high $\mathfrak{T}$ is resolved by parameter updating which is done by a deep neural network approach. This parameter updating process reduces the variation between the misdetection probabilities, ($v_{MD}(\mathbb{C})$)-busy slot is predicted as an idle and false alarm probability value ($v_{FA}(\mathbb{C})$)-idle slot predicted as busy. Therefore, the deep network-based parameter updating process minimizes the variation of $\max(v_{MD}(\mathbb{C}), v_{FA}(\mathbb{C}))$ in the network. This variation minimization helps to resolve the latency and reliability issues in IoT-based data transmission.

According to the discussion, this paper investigates the $\mathfrak{T}$ transmission channel behavior to identify and classify the channel status. Therefore, the overall working process of three phases has been illustrated in Figure 1.

Figure 1: Three-phase of AENN IoT data transmission process.

In the sensing phase, the autoencoder network is utilized for sensing the channel using sample attributes and network behavior for making data transmission. The autoencoder is one of the effective neural networks that has efficient coding-based learning mechanism that helps to predict the patterns for unlabeled data. The encoding process regenerates the input patterns by performing the encoding process. During this process noise data, irrelevant information is eliminated to improve the overall channel status identification process. The network has two phases such as encoder and decoder; the encoder process maps the given input to the coding and the decoder process regenerates the input from coding. This process helps to maintain the input quality because it aims to preserve the data quality while making data transmission. The network has three layers similar to the multi-layer perceptron but the number of nodes in the input layer is similar to the output layer. Here, the aim is to identify the status of the channel but maintaining the input similarity. During the reconstruction process, the input $\mathfrak{X}$ and output $\mathfrak{Y}$ prediction variation should be minimum. The encoder (ϕ) and decoder (ψ) process of a neural network is defined as follows.

$$\phi = \mathfrak{X} \rightarrow \mathfrak{F}, \quad (1)$$

$$\varphi = \mathfrak{F} \rightarrow \mathfrak{X}. \quad (2)$$

The deviation of (ϕ) and (ψ) is defined as follows.

$$\phi \text{ and } \psi = \arg \min_{\phi, \psi} \|\mathfrak{X} - (\varphi \circ \phi) \mathfrak{X}\|^2. \quad (3)$$

This computation deviation helps to reduce the latency difficulties while predicting the channel status (idle/busy) and attacker prediction process. The input x in $\mathfrak{X}$ transferred to hidden layer that maps in hidden layer as follows:

$$h = \sigma(Wx + b). \quad (4)$$

The mapping process defined in equation (4) is represented as $h \in \mathbb{R}^p = \mathfrak{F}$. Here, h is defined as code that is generated from the encoding process. Element-wise activation function is referred to as σ which is normally sigmoid activation function. The weight matrix is W and the node bias value is b . The defined W and b values are updated continuously according to the backpropagation learning. This updating minimizes the deviation of output estimation. During this process, network behaviors, number of data transmissions, time of data transmission, and network characteristics are examined for every data sample. Based on these characteristics, coding value is computed. Then, the code has been reconstructed in the decoding stage that is done as follows:

$$x' = \sigma'(W'h + b'), \quad (5)$$

Here, h autoencoder mapping is reconstruction x' of input x which is done by using the decoder weight (W'), bias (b'), and activation function (σ'). During this process, the variations are minimized according to equation (6).

$$\mathcal{L}(x, x') = \|x - \sigma'(W'(\sigma(Wx + b)) + b')\|^2. \quad (6)$$

Based on the above process, the network behavior decision is handled for every sample trying to send in the network. As discussed, sample S_i has a different number of features $\{f_{i1}, f_{i2}, f_{i3}, \dots, f_{iM}\}$. These features are classified according to above-defined procedures; the class label $C(S_i)$ is given for a specific sample. These labels help to identify the testing features related patterns, and the deviation between the computed and predicted labels are estimated using error probability value $n_{\text{error}}/n_{\text{test}}$. Based on the above process, channel idle and busy state have been identified. If the channel is in an idle state, the data have been transferred to the network. During the data transmission process, the labeled data helps to identify the characteristics of data. Suppose the network characteristics are changed that are treated as intermediate attacks, then the data transmission is eliminated in the earlier stage.

Further, the unauthorized access is eliminated by validating users using the channel access algorithm. The data have been transmitted from one station to another in wireless communication. Assume the IoT-based collected data consists of a number of stations information system (IS) which has upper boundary U , the transmitted data length has normalized to 1 which is denoted as β and transmission propagation delay

is denoted as λ . During the data transmission, the collected IoT data has buffered in a channel with a probability value of 1. Each data has certain slots with δ values that are developed using the probability density function $g(x)$ value $[0,1]$. The station analyzes the channel status from previous analysis with transmitted packet length. If there are obstacles predicted in a carrier, the data have been transmitted else; the busy tone will ring and the data have been allocated in a buffer. Then, the overall authorized channel access algorithm is defined as follows (Table 1):

Table 1: Channel access algorithm

```

Initialize:  $g(x)$ ,  $\lambda$ ,  $\beta$ 
For every slot
  If Buffer (B)  $\neq$  empty then
    Realize the data generate backoff value following  $g(x)$   $[0,1]$ 
    Examine the channel at time  $\beta$ 
  If carrier  $\neq$  not presented
    Data transmission immediately.
  Else
    Cancel the data transmission in that slot.
  End
End
If not transmission then
  Check slot for collision
  If Collision occur then
    The busy tone will ring
  End
End
If packet = transmission then
  No busy not ring and delete the packet from buffer
End
End
End

```

According to the autoencoder, the network-based network validation and channel status examination process help to identify unauthorized activities effectively. The neural network utilizes the attack behaviors and characteristics while examining the network during the data transmission process. The created system effectiveness is evaluated using experimental results and discussion.

4 Results and discussion

This section examines the effectiveness of the AENN and channel access algorithm-based data transmission in an IoT environment. The introduced method reduces the security issues with minimum latency and reliability. Moreover, the system is able to consider the different attacks and their behavior, which is used to eliminate the intermediate and unauthorized access. The effectiveness of the system was evaluated using various metrics such as precision, recall, error rate, and mean-square-error rate. The AENN network uses the input samples and respective features to evaluate the network status. The identified status helps to predict the channel's current position. The current status is used to predict the time of data transmission. For every data, it has a specific time to transmit from one place to another. If the network consumes more time to transmit specific data, then the system is considered as something such as collision, intermediate access, and unauthorized activities are happening in the network. In addition to this, the system uses the

channel access algorithm that verifies channel status for every transmission which leads to improving the overall network precision and recall value. The obtained value is illustrated in Figure 2.

Figure 2: (a) Precision and (b) recall.

The successful formulation and reconstruction of inputs in the encoding process help to identify the channel state correctly. This process helps to minimize the deviation of output with respect to the input $\|x - \sigma'(W'(\sigma(Wx + b)) + b')^2\|$. In addition to this, the channel access algorithm checks the network every time in terms of network characteristics and collision. This helps to identify the exact channel location, and the alert has been ringed correctly. This indicates that the system has a minimum false alert to the user. The

Table 2: Overall efficiency

Attacks	Misdetecation (%)	False alarm rate (%)	Normalized throughput (%)	Detection accuracy (%)
No attack	2.18	1.01	97.89	98.39
Jamming attack	2.02	1.03	98.23	98.76
Poisoning attack	2.13	1.24	97.3	97.9
Priority violation attack	2.04	1.06	98.12	98.45

minimum deviation and false alert rate show that the AENN approach has a high attack prediction rate on various attacks. The obtained results are illustrated in Table 2.

Table 2 clearly indicates that the AENN approach recognizes the various attacks such as jamming, poisoning, priority violation attacks with high detection rate, minimum misdetection, and minimum false alarm rate. The obtained system effectiveness is further evaluated with existing techniques, and the obtained results are illustrated in Table 3.

Table 3: Attack detection rate

S. No	Methods	Accuracy	Detection rate
1	DL [17]	95.57	96.13
2	DEL [18]	96.24	96.98
3	BEL [19]	97.48	97.46
4	AENN	99.18	99.02

Table 2 depicted that the AENN and channel access algorithm recognizes the attacks and authorizes the channel with a maximum detection rate (99.02%). In addition to this, the method predicts the channel condition such as idle and busy with high recognition accuracy (99.18%). Thus, the system improves the overall IoT security with minimum latency, false error rate, deviation, and high detection accuracy.

5 Conclusion

Thus, the paper analyzes the AENN with channel access algorithm to improve security in IoT-based data transmission. The network examines the data transmission channel using three layers of autoencoder neural network. The network maps and reconstructs data using a coding process. This approach continuously updates the network parameters using backpropagation learning that helps to minimize the deviations and reduce the false alarm rate. The learning process improves the overall channel status identification accuracy because it uses the various attacks related parameters and characteristics. Here, the channel access algorithm also utilizes that investigates the data transmission network in terms of their characteristics and collision status. According to the network information, channel status has been checked and authenticated for every data transmission slot. Then, the effectiveness of the system implemented using TensorFlow and the system ensures the 99.02% of detection rate when compared with other techniques. In the future, the effectiveness of the system improved using an optimized classifier for reducing the computation complexity.

Acknowledgments: We would like to thank Dijlah University College for funding this research.

Funding information: This research was supported by the Dijlah University College I [grant number G2021-1].

Conflict of interest: Authors state no conflict of interest.

References

- [1] Hasan M, Islam MM, Zarif MI, Hashem MM. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet Things*. 2019;7:100059.

- [2] Hussain F, Abbas SG, Shah GA, Pires IM, Fayyaz UU, Shahzad F, et al. A framework for malicious traffic detection in IoT healthcare environment. *Sensors*. 2021;21(9):3025.
- [3] Hafeez I, Ding AY, Antikainen M, Tarkoma S. Real-time IoT device activity detection in edge networks. In *International Conference on Network and System Security*. Cham: Springer; 2018. p. 221–36.
- [4] Dian FJ, Vahidnia R, Rahmati A. Wearables and the internet of things (IoT), applications, opportunities, and challenges: a survey. *IEEE Access*. 2020;8:69200–11.
- [5] Bughin J, Chui M, Manyika J. Clouds, big data, and smart assets: Ten tech-enabled business trends to watch. *McKinsey Q*. 2010;56(1):75–86.
- [6] Alfandi O, Khanji S, Ahmad L, Khattak A. A survey on boosting IoT security and privacy through blockchain. *Clust Comput*. 2020;24(1):1–19.
- [7] Mohanta BK, Jena D, Ramasubbareddy S, Daneshmand M, Gandomi AH. Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet Things J*. 2020;8(2):881–8.
- [8] Reddy YB, Latifi S. Trust and access controls in IoT to avoid malicious activity. In: *Cloud Network Management*. London, UK: Chapman and Hall/CRC; 2020. p. 87–103.
- [9] Bhatt P, Bhatt S, Ko M. Poster: IoT SENTINEL-An ABAC approach against cyber-warfare in organizations. In: *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*; 2020. p. 223–5.
- [10] Islam MR, Aktheruzzaman KM. An analysis of cybersecurity attacks against internet of things and security solutions. *J Computer Commun* 2020;8(4):11–25.
- [11] Fan R, Pan J, Huang S. ARM-AFL: coverage-guided fuzzing framework for ARM-based IoT devices. In: *International Conference on Applied Cryptography and Network Security*. Cham: Springer; 2020. p. 239–54.
- [12] Alferidah DK, Jhanjhi NZ. A review on security and privacy issues and challenges in internet of things. *Int J Computer Sci Netw Security IJCSNS*. 2020;20(4):263–86.
- [13] Waheed N, He X, Ikram M, Usman M, Hashmi SS, Usman M. Security and privacy in IoT using machine learning and blockchain: threats and countermeasures. *ACM Comput Surv (CSUR)*. 2020;53(6):1–37.
- [14] Chanal PM, Kakkasageri MS. Security and privacy in IOT: a survey. *Wirel Personal Commun*. 2020;115(2):1667–93.
- [15] Chen YW, Sheu JP, Kuo YC, Van Cuong N. Design and implementation of IoT DDoS attacks detection system based on machine learning. In: *2020 European Conference on Networks and Communications (EuCNC)*. United States: IEEE; 2020. p. 122–7.
- [16] Ujjan RM, Pervez Z, Dahal K, Bashir AK, Mumtaz R, González J. Towards flow and adaptive polling sampling for deep learning based DDoS detection in SDN. *Future Gener Comput Syst*. 2020;111:763–79.
- [17] Ullah F, Naeem H, Jabbar S, Khalid S, Latif MA, Al-Turjman F, et al. Cyber security threats detection in internet of things using deep learning approach. *IEEE Access*. 2019;7:124379–89. doi: 10.1109/ACCESS.2019.2937347.
- [18] Tsogbaatar E, Bhuyan MH, Taenaka Y, Fall D, Gonchigsumlaa K, Elmroth E, et al. DeL-IoT: a deep ensemble learning approach to uncover anomalies in IoT. *Internet Things*. 2021;14:100391.
- [19] Balasundaram J. A novel optimized bat extreme learning intrusion detection system for smart Internet of things networks. *Int J Commun Syst*. 2021;34(7):e4729.
- [20] Basati A, Faghih MM. APAE: an IoT intrusion detection system using asymmetric parallel auto-encoder. *Neural Comput Applic*. 2021;2021:1–21. doi: 10.1007/s00521-021-06011-9.
- [21] Swarna Priya RM, Maddikunta PK, Parimala M, Koppu S, Gadekallu TR, Chowdhary CL, et al. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Comput Commun*. 2020;160:139–49.
- [22] Hafeez I, Antikainen M, Ding AY, Tarkoma S. IoT-KEEPER: detecting malicious IoT network activity using online traffic analysis at the edge. *IEEE Trans Netw Serv Manag*. 2020;17(1):45–59.
- [23] Fortino G, Messina F, Rosaci D, Sarnè GM. ResIoT: an IoT social framework resilient to malicious activities. *IEEE/CAA J Automatica Sin*. 2020;7(5):1263–78.
- [24] Ullah I, Mahmoud QH. A two-level flow-based anomalous activity detection system for IoT networks. *Electronics*. 2020;9(3):530.