Faculty of Natural and Applied Sciences Journal of Computing and Applications
Print ISSN: 3026-8133
www.fnasjournals.com
Volume 3; Issue 1; March 2026; Page No. 130-136.
DOI: https://doi.org/10.63561/jca.v3i1.1244

An optimised transformer-based intrusion detection framework for IoT networks using Fisher score feature selection and SMOTE balancing technique.

***[1]Ganiyu, O.A., [1]Hamzat, O. A., & [2]Enesi, F.A.**
[1]Department of Computer Science, Federal University of Technology, Minna, Nigeria.
[2]Department of Information Technology, Federal University of Technology, Minna, Nigeria.

***Corresponding author email**: ganiyu.pg2113803@st.futminna.edu.ng

Abstract
The proliferation of Internet of Things (IoT) devices has brought about significant advantages in areas such as smart homes and industrial automation. However, this widespread adoption has also rendered these systems more susceptible to cyberattacks, underscoring the critical need for robust intrusion detection systems. The proposed model presents an optimised approach to intrusion detection in IoT networks using a transformer-based architecture, renowned for its exceptional performance across diverse machine-learning tasks. This model was validated on the BoT-IoT Network Intrusion dataset, which encompasses a variety of IoT network traffic scenarios. The Synthetic Minority Oversampling Technique (SMOTE) was leveraged to address the imbalanced dataset. Furthermore, we improved efficiency by employing Fisher's score to select the most critical features. The Transformer-based model, leveraging the self-attention mechanism, was utilised to classify network traffic as normal or malicious. Our findings demonstrate the remarkable effectiveness of this approach, yielding an accuracy rate of 99%, precision of 99%, recall of 99%, F1 score of 99%, and an Area Under the Receiver Operating Characteristic Curve (AUC) of 99%. These scores confirm that our model can accurately detect and classify intrusions with minimal to no errors.

Keywords: Transformer, Fisher's Score, SMOTE, IoT, IDS

Introduction

The security-related threats and vulnerabilities increase as the number of connected devices in the Internet of Things (IoT) grows. The IoT nodes create a dynamic topology and perform their tasks without human intervention, making it more complex to address security issues in IoT. The privacy and security challenges in IoT become more troublesome with limited resources. Furthermore, the substantial growth and adoption of IoT devices across all aspects of human life underscore the need to consider these security threats before implementing countermeasures. An Intrusion Detection System (IDS), is a security mechanism designed to protect a system by alerting administrators of security breaches and taking measures to block intruders (Axelsson, 2019). The Internet of Things (IoT) refers to the interconnected network of physical devices, such as home appliances, industrial machines, and wearable technology that communicate and exchange data over the Internet. These devices make our lives easier and more efficient by automating tasks and providing real-time information. However, as the number of IoT devices grows, so does the potential for security threats. Cyber-attacks on IoT devices can lead to significant issues, such as data breaches, loss of privacy, and even physical harm in some cases. This is where Intrusion Detection Systems (IDS) come into play (Khraisat and Alazab, 2021). IoT applications span healthcare, logistics, smart cities, smart homes, and agriculture. However, due to its limited resources, IoT is prone to vulnerabilities that attackers can easily exploit. The number of unsecured IoT devices connected to the global network is increasing rapidly (Colakovi & Hadziali, 2018). Several researchers have focused on utilising deep learning techniques for IDS in IoT environments. These approaches generally aim to improve detection accuracy and reduce false positive rates. For instance, Aboelwafa *et al.* (2020), employed the Spider Monkey Optimisation (SMO) algorithm and a stacked-deep polynomial network (SDPN) for detecting various types of attacks in IoT environments. Similarly, Cristiano et al. (2020), introduced a hybrid DNN-

Cite this article as:
Ganiyu, O. A., Hamzat, O. A., & Enesi, F. A. (2026). An optimised transformer-based intrusion detection framework for IoT networks using Fisher score feature selection and SMOTE balancing technique. *FNAS Journal of Computing and Applications, 3*(1), 130-136.https://doi.org/10.63561/jca.v3i1.1244

kNN model, which combines deep neural networks with k-Nearest Neighbour (kNN) for binary classification of network records. The focus of these studies is on leveraging deep learning architectures to enhance intrusion detection in IoT systems. Feature selection is a critical aspect of improving IDS efficiency by reducing the dimensionality of input data and focusing on the most relevant features. Bace and Mell (2020), proposed a feature extraction method that combines feature selection with deep learning algorithms, aiming to enhance both accuracy and time efficiency. In a similar vein, Riyaz and Ganapathy (2020), developed an incremental feature selection algorithm incorporating Conditional Random Fields (CRF) and Linear Correlation Coefficient-aware feature selection methods, which was used alongside Convolutional Neural Networks (CNN) for classifying network records. The existing body of research in IoT IDS is rich with innovations, particularly in leveraging deep learning and hybrid approaches to improve detection capabilities. However, there are still gaps in optimising feature selection techniques and in further reducing detection latency, especially in resource-constrained IoT environments. This study proposes an optimised feature selection technique to reduce the input dataset size by identifying the most significant features. Additionally, a Transformer model is applied for efficient and effective record classification (Otounm & Nayak, 2019).

Intrusion detection has been studied for over 25 years, with the RAID (Recent Advances in Intrusion Detection) workshop being one of the first dedicated events, held in 1998. Network Intrusion Detection Systems (NIDS) for IoT are software- or hardware-based systems designed to detect potential security threats, such as hacking, malware, and other malicious activities. Machine learning algorithms have been used to improve IoT NIDS by automatically learning normal behaviour patterns and spotting deviations that might indicate an attack (Tahsien et al., 2020). Traditional NIDS often rely on signature-based methods, which detect known attack patterns by matching incoming data with a set of predefined attack signatures (Masdari & Khezri, 2020). However, this method can struggle to detect new or unknown attacks. Another approach is anomaly detection, which compares incoming data to a baseline of normal behaviour to find deviations that may signal an intrusion. The effectiveness of this method can be limited by the quality of the baseline and the accuracy of the deviation detection algorithms (Alsoufi *et al.*, 2021).

Deep learning (DL) has become popular in intrusion detection due to its ability to process large amounts of data and recognise complex patterns (Ferrag et al., 2020). DL algorithms can achieve higher accuracy and performance than traditional machine learning methods by learning from and improving on more data. This has led to the development of several DL-based NIDS models that have shown promising results in detecting various intrusion types, including network attacks, insider threats, and malware.

Arp *et al*. (2020), reviewed the effective and ineffective uses of machine learning in computer security at the USENIX Security Symposium. Advanced ML methods are now used in commercial IDS systems, such as Darktrace (2022). Ashiku et al. (2021) developed an adaptive and resilient NIDS using deep learning to detect and classify network attacks. Satam and Hariri (2021), proposed a Wireless Intrusion Detection System (WIDS) that uses anomaly detection to accurately identify Wi-Fi network attackers with few false alarms.

The diverse nature of IoT introduces unique challenges and security concerns that can affect the privacy and safety of smart home users. Various research approaches aim to improve NIDS solutions for this heterogeneous data (Oseni et al., 2023).

Mahadik *et al*. (2022), proposed an advanced NIDS to identify and counteract different types of DDoS attacks in IoT environments. Bertoli et al. (2023), discussed using stacked-unsupervised federated learning (FL) to enhance intrusion detection across diverse networks.

Based on the related literature survey of various approaches in IDS, it is concluded that:

- Intrusion detection has over 25 years of research history, with significant milestones such as the RAID workshop in 1998. This indicates a mature field with a rich background of knowledge and advancements.
- Modern IDS systems, especially for IoT, benefit from machine learning and deep learning algorithms, which can learn normal behaviour patterns and detect deviations, improving accuracy and performance.
- Deep learning-based NIDS models can handle large datasets and perform complex pattern recognition, leading to better detection of various intrusions, including network attacks and malware.
- Recent advances include Transformer-based models, which have shown improved accuracy and efficiency in threat detection through learning from past data and identifying new threats.

Cite this article as:
Ganiyu, O. A., Hamzat, O. A., & Enesi, F. A. (2026). An optimised transformer-based intrusion detection framework for IoT networks using Fisher score feature selection and SMOTE balancing technique. *FNAS Journal of Computing and Applications, 3*(1), 130-136.https://doi.org/10.63561/jca.v3i1.1244

- Various novel approaches, such as stacked-unsupervised federated learning, semi-supervised frameworks, and combined architectures (e.g., CNN-Transformer), enhance IDS's handling of heterogeneous and complex IoT environments.

Based on the review, it is evident that while most Intrusion Detection System (IDS) methods have achieved high accuracy, often exceeding 90%, further improvements in the field remain challenging. To the best of our knowledge, the following challenges remain critical in the development and implementation of IDS:

- Traditional NIDS methods, like signature-based detection, rely on regular updates to detect known attack patterns. Many IoT devices do not receive consistent updates, leaving them vulnerable to new or evolving threats.
- Anomaly detection methods depend on the quality of the baseline of normal behaviour and the accuracy of deviation detection algorithms. Poor baselines can lead to false positives or undetected intrusions.
- Some advanced IDS methods, particularly those combining multiple deep learning techniques (e.g., CNN-LSTM), can have high computational costs, making them less feasible for resource-constrained IoT devices.
- Techniques such as Visual Transformer (ViT) and hybrid sampling methods attempt to address data imbalance but often do not fully resolve the quantitative imbalance, potentially affecting detection accuracy.

Methodology

System Model Architecture

In recent years, machine learning (ML) and deep learning (DL) techniques have shown promise in enhancing the capabilities of IDS. Among these techniques, the Transformer model, originally designed for natural language processing, has emerged as a powerful tool for sequence modelling and classification. As shown in Figure 1, our proposed Transformer-based IDS was evaluated through two major experiments. The first experiment employed Fisher's Score Algorithm for feature selection, while the second employed SMOTE to balance our dataset.

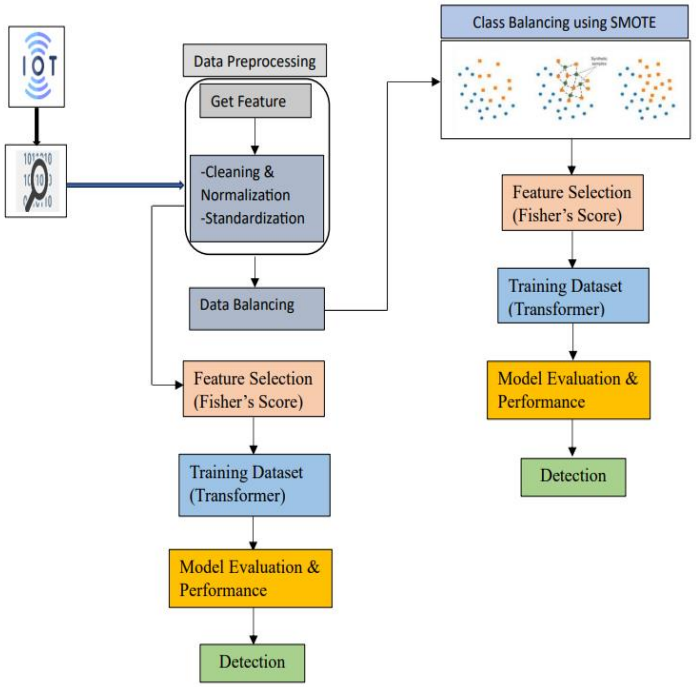

Figure 1: Proposed Model Architecture

Dataset Description

The BoT-IoT 2023 dataset was used in this study. It contains realistic IoT network traffic, including normal behaviour and multiple attack categories such as DoS, DDoS, OS scanning, keylogging, and data exfiltration.

Cite this article as:
Ganiyu, O. A., Hamzat, O. A., & Enesi, F. A. (2026). An optimised transformer-based intrusion detection framework for IoT networks using Fisher score feature selection and SMOTE balancing technique. *FNAS Journal of Computing and Applications, 3*(1), 130-136.https://doi.org/10.63561/jca.v3i1.1244

Data Pre-processing
Data cleaning involved removing duplicates, handling missing values, encoding categorical attributes, and applying Min–Max normalisation. To address class imbalance, SMOTE was applied to generate synthetic samples for minority classes.

Feature Selection Using Fisher's Score
Fisher's Score was employed to rank features based on their discriminative power between normal and attack classes. Only top-ranked features were selected, significantly reducing dimensionality while preserving classification performance.

Transformer-Based Classification
The Transformer model utilises self-attention mechanisms to capture relationships between network traffic features. Multi-head attention, feed-forward neural networks, residual connections, and positional encoding were implemented to enhance classification accuracy.

Experimental Results and Discussion
Two experiments were conducted: one using the original imbalanced dataset and another using SMOTE-balanced data. Results show that the Transformer model achieved 97.90% accuracy without SMOTE and improved to 98.88% accuracy after balancing. Precision, recall, F1-score, and AUC values consistently exceeded 98%, outperforming existing IDS models reported in the literature.

The findings confirm that combining Fisher's Score and SMOTE significantly enhances Transformer-based IDS performance, particularly in handling imbalanced IoT datasets.

Experiment I: Training BoT-IoT dataset without smote technique
During the class distribution, we have Normal (0): 61 instances and Attacked (1): 440,162. This experiment was conducted using Fisher's score for feature selection and the Transformer model for classification without the Smote technique. The number of epochs we trained for was 12. Figures 2 and 3 show the validation accuracy, validation loss and confusion matrix.

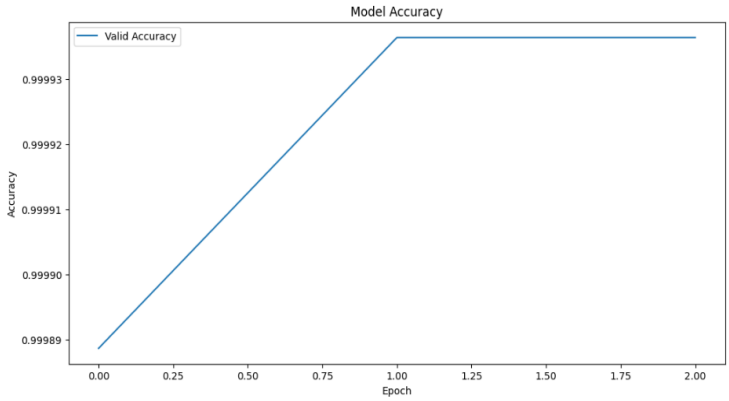

Figure 2: Validation accuracy

Cite this article as:
Ganiyu, O. A., Hamzat, O. A., & Enesi, F. A. (2026). An optimised transformer-based intrusion detection framework for IoT networks using Fisher score feature selection and SMOTE balancing technique. *FNAS Journal of Computing and Applications, 3*(1), 130-136.https://doi.org/10.63561/jca.v3i1.1244

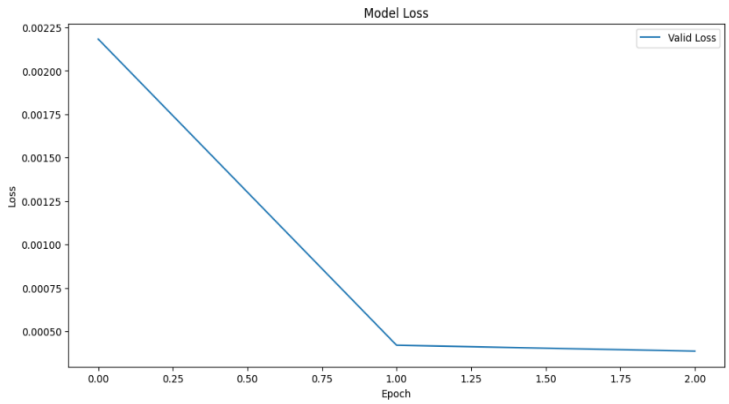

Figure 3: Validation loss

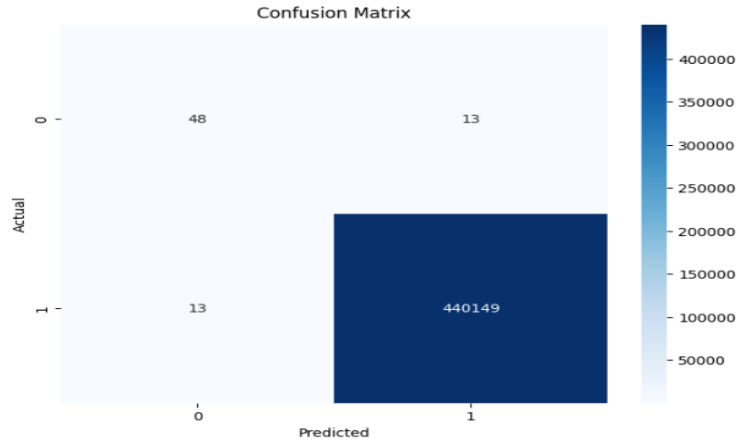

Figure 4: Confusion Matrix

Classification Report Summary **Table 1**

Accuracy	Precision	Recall	F1 Score	AUC
97.90%	98.68%	98.50%	99.70%	98.60%

4.2 Experiment II: Training BoT-IoT dataset with SMOTE technique

During the class distribution, we have Normal (0): 440,162 instances and Attacked (1): 440,162 instances. This experiment was conducted using Fisher's score for feature selection and the Transformer model for classification with the SMOTE technique. The number of epochs trained was 12. Figures 5 and 6 show the validation loss and confusion matrix.

Cite this article as:
Ganiyu, O. A., Hamzat, O. A., & Enesi, F. A. (2026). An optimised transformer-based intrusion detection framework for IoT networks using Fisher score feature selection and SMOTE balancing technique. *FNAS Journal of Computing and Applications, 3*(1), 130-136.https://doi.org/10.63561/jca.v3i1.1244

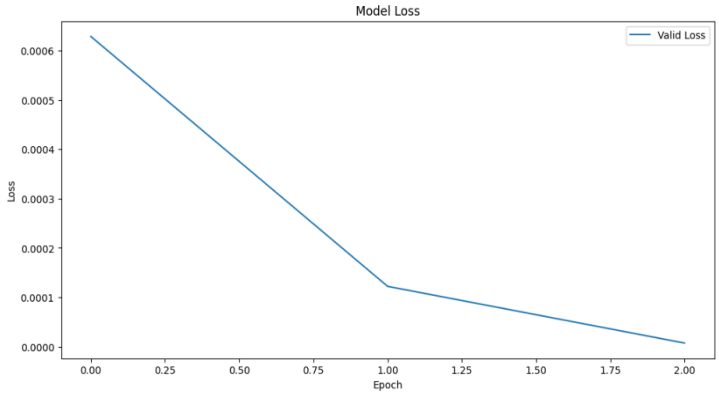

Figure 5: Validation loss

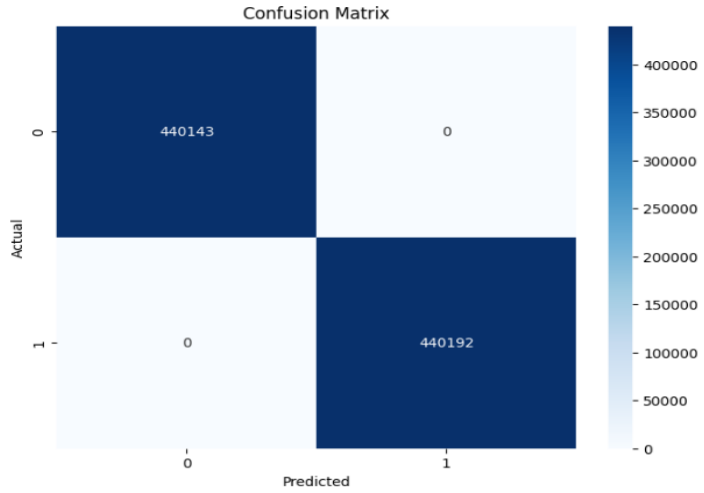

Figure 6: Confusion Matrix

Classification Report Summary **Table 3**

Accuracy	Precision	Recall	F1 Score	AUC
98.88%	99.75%	100.00%	99.83%	99.90%

Conclusion

This study presents a highly effective Transformer-based IDS for IoT environments. By integrating Fisher's Score feature selection with SMOTE, the proposed model achieves superior detection accuracy while reducing computational complexity. Future research will focus on real-time deployment, scalability, and adaptive learning for evolving attack patterns.

Declaration of Competing Interests

The authors declare that there are no known financial interests or personal relationships that could have influenced the research presented in this study.

Cite this article as:
Ganiyu, O. A., Hamzat, O. A., & Enesi, F. A. (2026). An optimised transformer-based intrusion detection framework for IoT networks using Fisher score feature selection and SMOTE balancing technique. *FNAS Journal of Computing and Applications, 3*(1), 130-136.https://doi.org/10.63561/jca.v3i1.1244

References

Aboelwafa, M. M. N., Seddik, K. G., Eldefrawy, M. H., Gadallah, Y., & Gidlund, M. (2020). A machine-learning-based technique for false data injection attack detection in industrial IoT. IEEE Internet of Things Journal, 7(9), 8462-8470. https://doi.org/10.1109/JIOT.2020.2970501.

Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in IoT using deep learning: A systematic literature review. *Applied Sciences, 11*(8383). https://doi.org/[CrossRef].

Arp, D., Quiring, E., Pendlebury, F., Warnecke, A., Pierazzi, F., Wressnegger, C., Cavallaro, L., & Rieck, K. (2020). Dos and don'ts of machine learning in computer security. arXiv. https://arxiv.org/abs/2010.09470.

Ashiku, L., & Dagli, C. (2021). Network intrusion detection system using deep learning. Procedia Computer Science, 185, 239–247. https://doi.org/[CrossRef].

Axelsson, S. (2019). Intrusion detection systems: A survey and taxonomy.

Bace, R., & Mell, P. (2020). Intrusion detection systems.

Bertoli, G. D. C., Junior, L. A. P., Saotome, O., & dos Santos, A. L. (2023). Generalizing intrusion detection for heterogeneous networks: A stacked-unsupervised federated learning approach. *Computers & Security, 127,* 103106. https://doi.org/[CrossRef].

Colakovic, A., & Hadzialic, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks. https://doi.org/10.1016/j.comnet.2018.07.017.

Cristiano, A. de Souza, Westphall, C. B., Machado, R. B., Sobral, J. B. M., & Vieira, G. dos S. (2020). Hybrid approach to intrusion detection in fog-based IoT environments. Computer Networks, 180, Article 107417. https://doi.org/10.1016/j.comnet.2020.107417.

Darktrace. (n.d.). Available online: https://darktrace.com/ (accessed on March 3, 2022).

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419. https://doi.org/10.1016/j.jisa.2020.102419.

Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the Internet of Things: Techniques, deployment strategy, validation strategy, attacks, public datasets, and challenges. Cyber Security, 4(18). https://doi.org/10.1186/s42400-021-00077-7

Mahadik, S., Pawar, P. M., & Muthalagu, R. (2022). Efficient intelligent intrusion detection system for heterogeneous Internet of Things (HetIoT). Journal of Network and Systems Management, 31(2). https://doi.org/10.1007/s10922-022-09620-4

Masdari, M., & Khezri, H. (2020). A survey and taxonomy of the fuzzy signature-based intrusion detection systems. Applied Soft Computing, 92, 106301. https://doi.org/10.1016/j.asoc.2020.106301

Oseni, A., Moustafa, N., Creech, G., Sohrabi, N., Strelzoff, A., Tari, Z., & Linkov, I. (2023). An explainable deep learning framework for resilient intrusion detection in IoT-enabled transportation networks. IEEE Transactions on Intelligent Transportation Systems, 24, 1000–1014. https://doi.org/10.1109/TITS.2022.3179132

Otounm, Y., Liu, D., & Nayak, A. (2019). DL-IDS: A deep learning-based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies, Article No. e3803, 1-14. https://doi.org/10.1002/ett.3803

Riyaz, B., & Ganapathy, S. (2020). A deep learning approach for effective intrusion detection in wireless networks using CNN. Soft Computing, 24, 17265–17278.

Satam, P., & Hariri, S. (2021). WIDS: An anomaly-based intrusion detection system for Wi-Fi (IEEE 802.11) protocol. IEEE Transactions on Network and Service Management, 18, 1077–1091.

Tahsien, S., Karimipour, H., & Spachos, P. (2020). Machine learning-based solutions for Internet of Things (IoT) security: A survey. *Journal of Network and Computer Applications, 161,* 102630. https://doi.org/10.1016/j.jnca.2020.102