International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
***Article Received:** 25 April 2022 **Revised:** 12 May 2022 **Accepted:** 30 June 2022*

Security Challenges and Solutions in IoT-Based Image Processing Using Machine Learning Techniques

Sushma T Shedole[1], Naheeda Tharannum B[2], Poornima[3]

[1]Assistant Professor, Department of Computer Science and Engineering, Government Engineering College, Raichur, Karnataka, Pin-Code:584135. Email: stshedole@gmail.com
[2]Assistant Professor, Department of Electronics and Communication Engineering
Government Engineering College, Raichur, Karnataka, Pin-Code:584135.
Email: tarannum.n@gmail.com
[3]Assistant Professor, Department of Computer Science and Engineering, Government Engineering College, Raichur, Karnataka, Pin-Code:584135.
Email: poornimapoojar@gmail.com

Abstract
The incorporation of Internet of Things IoT technology in image processing poses major security risks in data integrity, privacy and dynamism in threats. That's why this work intends to introduce an optimized machine learning-based framework that will improve security in IoT-based image processing. To solve the fundamental security challenges such as unauthorized access, data manipulation and malware penetration, the framework uses convolutional neural networks for anomaly detection, and adaptive encryption and authentication. The model was also examined in different conditions and it predicted a high detection rate and competent processing of conditions accompanied with many IoT devices. The work depicts the loss of privacy in exchange for model performance and explains how the model has high performance even in conditions when privacy is a concern. Based on the findings, the authors indicate that the solution proposed can readily be applied in higher risk areas for security such as smart city and surveillance and healthcare information systems respectively indicating that the proposed solution is potentially scalable for IoT security needs.

Keywords: *Internet of Things (IoT), image processing, security challenges, machine learning, data encryption, device authentication, intrusion detection, deep learning, privacy protection, real-time monitoring.*

1. Introduction

The Internet of Things or IoT is still advancing quickly to the extent that it has impacted many industries which image processing can also take advantage of. While once considered a specialized niche application, IoT image processing is now at the heart of industries alike to healthcare, smart cities, security and surveillance, and industrial automation where the ability to acquire and process visual data in real time is a critical advantage[1]. In healthcare for instance, IoT operating or driving imaging machines provide opportunities for remote diagnosis to enhance coverage in emergencies[2]. The smart city projects incorporate the IoT-based devices, particularly the cameras, to govern the traffic and collect data on public security as well as climate. ASDs are becoming progressively IoT-supported to monitor all spaces with alarms in real-time[3]. Some others are as follows: Industrial automation also gets a lot of advantages; IoT associated with Visual Inspection System boosted the quality control and Operation Safety.

The combination with ML and IoT makes image processing far more advanced and in some ways advanced the works in these fields in terms of accuracy, the speed of processing and decision-making[4]. Performing pattern and anomaly detection on visual inputs make machine learning algorithms more superior to human beings hence being ideal for precise and timely purposes. In image processing, it is possible to use Machine Learning (ML) methods, the most valuable of which in images are CNNs and Deep Learning models[5]; object recognition, image classification, feature extraction. In case of being integrated into the IoT architectures, the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
***Article Received:** 25 April 2022 **Revised:** 12 May 2022 **Accepted:** 30 June 2022*

functionality of various ML models allows gaining a massive amount of image data, as well as providing precise and near-instantaneous insights into the analyzed data[6], which, in its turn, can be used to develop real-time responses to challenging situations.

But this expansion of IoT-based image processing raises enormous security issues[7]. The key reason of making IoT advantageous connectivity and data sharing within a network enhance the dangerous potentialities that can be beneficial from the side of a hacker or a hacker group. Security risks in this regard are; unauthorized access[8], data privacy and data modification which affects the credibility of image processing systems. Invasive attack is even more dangerous in the case of applications that capture and transmit image data, for example, surveillance and healthcare applications[9]. Thirdly, the image data itself as a streaming video may be intercepted or tampered with, or worse, the image data may be noisy, which may cause severe misinterpretation or privacy violation[10]. It becomes a challenge to address these risks using conventional security practices as IoT devices may possess limited computing power, limiting issues like encrypting of each appliance.

The extent of this management research covers these security threats and questions how machine learning approaches can provide resilient solutions. Machine learning is more utilized for intrusion detection, anomaly detection and data encryption and all of this is important for securing the IoT based image processing. In this research, the author reviews then explores the existing security risks, and recommends a data protection model developed from deep learning algorithms to ensure the security of the collected data. The primary goals are to define the major security challenges in IoT-environment for image processing, to show how machine learning helps protect IoT from the threats, and to compare the models of machine learning aiming at providing the real-time and adaptive security measures. Through the proposed integration of ML techniques into the IoT environment, this work seeks to show the possibility of a strengthened image processing system with secure transmission of data, verified device identity, and real-time threats identification that can enhance the safety and reliability of IoT applications drawn towards images.

2. Literature Survey

A literature review of the utilization of IoT in image processing shows promising developments in the various domains such as in healthcare, smart city, security and surveillance, and industrial applications[11]. Due to IoT technologies, image data can be received and transmitted constantly, which makes possible to monitor and analyze its data in real time in different settings[12]. In healthcare IoT smart imaging systems help in early and instant examination of patients' condition and state. Meanwhile, smart city application derive value from IoT cameras and sensors for traffic flow and assessment of environment and safety while industrial operations also enhance quality assurance and equipment health check through IoT based image processing[13]. In these applications, IoT capabilities depend on real-time data processing such that machine learning models are commonly deployed at the edge to support the augmentation of image interpretation and response[14]. But, of course, as more IoT-based image processing systems are deployed, more functional and security vulnerabilities are posed[15].

A critical point for further research is that the security of IoT networks and especially those working with image data is an important pain point, as the analyzed literature indicate the constant occurrence of problems with data integrity[16], privacy, and authentication. Device authentication and authorization stay as significant issues, since fragile solutions in IoT devices result in unauthorized access and control[17]. When applying the choice, malicious devices or users may enter the network, which leads to malicious activities towards image data[18]. Data encryption is the other widespread concern in IoT-based image processing. Most IoT devices do not possess the computational prowess needed to perform standard encryption techniques and thus, data transfer is a process that could be intercepted and altered[19]. Privacy issues exacerbate these issues, by the fact that private image information – for example, scans from a doctor, surveillance videos, etc. – can freely be shared and stored without sufficient measures[20]. This insecurity pose high risk for both the data and user hence the need for unique ways of securing the image data in IoT devices.

As it shall be seen, this Man cia Machine learning (ML) has great potential in solving these IoT security challenges[21]. The use of deep learning and convolutional neural networks (CNNs) and other recent MLs have been adopted in recent studies to improve security in IoT networks[22]. Anomaly detection models involve application of machine learning algorithms to diagnose data irregularity and output actual real-time intrusions or security breaches[23]. Network-based intrusion detection systems (IDS) employing learning algorithms have been deployed for identification of violation of access control, that evolves dynamically based on accumulated learning[24]. Other data encryption models

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
***Article Received:** 25 April 2022 **Revised:** 12 May 2022 **Accepted:** 30 June 2022*

based on ML algorithms have also been pursued, which use algorithmic predictive strength in improving encryption processes and include manageable encryption key functionality. CNNs and deep learning have been found to give good results when applied to the identification of abnormalities in the image data stream while reinforcement learning has demonstrated the sustainable tuning of security practices to counter continuously evolving threats as seen from the following comparison[25].

Previous work in IoT-based image processing has proposed several approaches addressing the problem of increasing security despite current inadequacies. Steganographic approaches like encrypted image transmission have been said to enhance transfer integrity with unique algorithms suitable for IoT device constrained computational capacity. Closed circuit image authentication techniques using deep learning models can detect changes made in the transmitted images and thus prevent modifications. Use of real-time monitoring also incorporates machine learning, which easily identifies any suspicious activity, improving on response times for security breaches. Despite the advancements made, issues like computational complexity, and dynamic nature of security models emerge, which establishes the fact the developing reliable, effective and scalable solutions for IoT based image processing security is an area that warrants future research.

3. Proposed Methods

The proposed methods in this research are based on the identified threats which are; data integrity, unauthorized access, and secure transmission of image data in an IoT based image processing system. The decentralized nature of the IoT networks, together with big amounts of image data, make a number of applications, including surveillance, health care, and industrial control and automation, vulnerable to image manipulation and privacy invasion. In addition to these risks, this research seeks to introduce a security framework that utilizes machine learning algorithms to overcome these risks by incorporating secure data encryption, device identification, and real-time anomaly detection.

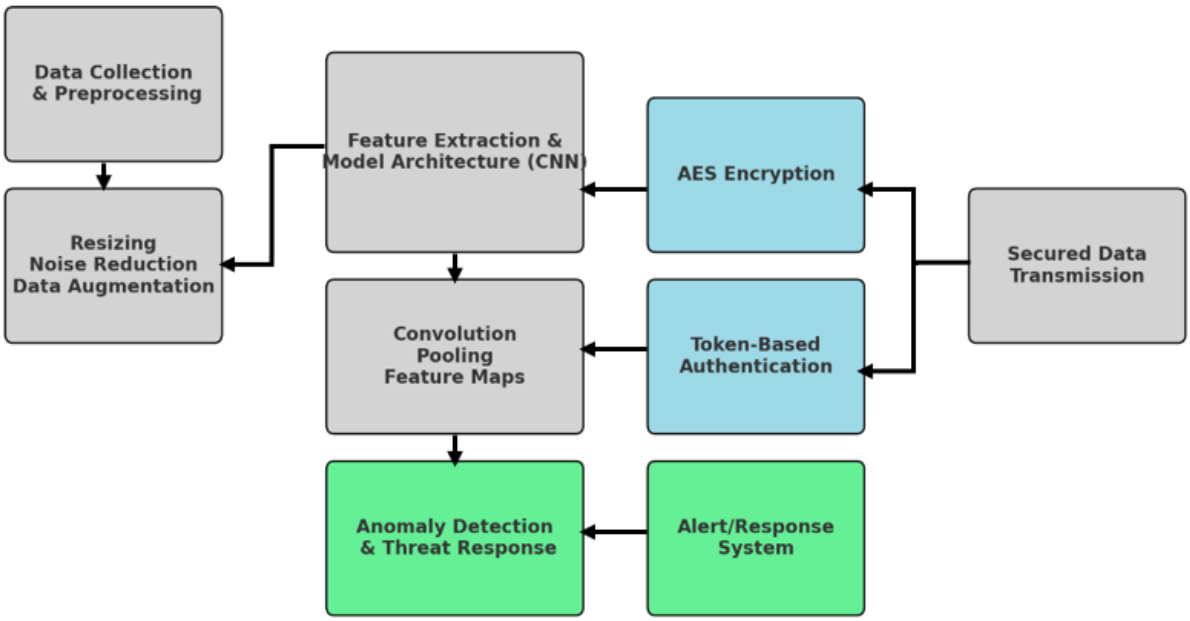

Figure 1: Security Framework for IoT-Based Image Processing Using Machine Learning

The proposed approach starts from data acquisition and cleaning steps to ensure that the input data to the machine learning algorithm are of a very good quality. The dataset contains image data related to particular IoT services, e.g. medical images for health care purposes or video frames for monitoring services. All images are preprocessed where the images are resampled in size while removing noise then normalized of the images to increase model performance and to minimize computational load. Further, data augmentation including rotation, flipping, cropping is performed in order to expand the given dataset and make the model more robust to disparate cases. These steps enhance the security model by reducing the effects of noise or irrelevant characteristics on the existed dataset.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
***Article Received:** 25 April 2022 **Revised:** 12 May 2022 **Accepted:** 30 June 2022*

This figure 1 shows the systematic flow directing the data and security implementation in an IoT-based image processing approach to machine learning. Data Collection & Preprocessing follows where the image collected by the IoT devices are preprocessed by resizing, reducing noise and image augmentation to make the image consistent and generalize the model. The data that is then prepped is moved to the Feature Extraction & Model Architecture (CNN) where through a convolutional neural network the image features important for anomalous detections and security authentication such as edges and texture of an image are extracted.

In the Security Protocols section, two concepts are used: AES Encryption ideal for image data while in transit since it make it rather difficult for unauthorized parties to access the information. Token-Based Authentication approves each IoT device; communication is only possible by authorized IoT devices only. The processed, secured data is then available for Secured Data Transmission to end-user applications. At the same time, image data is also scanned by an Anomaly Detection & Threat Response system that alerts the user to possible security risks in real time and launches an immediate Alert/Response System to counter the danger point if infiltration is suspected. This comprehensive solution increases the usability and scalability, while promoting data accuracy, confidentiality, and protection in all Iot-based image processing.

The security model framework incorporates deep learning model to detect security threats in IoT image processing based systems. This framework used CNN because of its effectiveness in image feature extraction and additional layers to identify abnormality, that might pose some level of security threat. The model architecture was designed to be performed under the limited IoT device computational power and storage capacity. The CNN is further tuned for anomaly detection, intrusion detection and for tampering verification since these are precises that improve the integrity and confidentiality of image data.

Fundamentally, feature extraction and model selection were part of the proposed security model. In the CNN, the edges, texture and patterns are some features extracted in the convolution layers. These features offer an important input for the model in identifying any highly probable activities or unauthorized intrusions. Since there is a broad variety of machine learning models, it was decided to use CNN-based model due to their high accuracy in image analysis and the possibility of making adjustments for real-time detection of irregularities. The use of CNN also helps to extract the right features and their further use is relatively lightweight, which is important in the calculations of IoT systems.

Security solutions involve both encryption and authentication procedures as constituents of image data security. To mitigate risk in image data, an AES encryption algorithm is used to optimize image security during transmission and storage in an encrypted form due to its confidentiality. This is true because the AES algorithm is compatible with minimum IoT devices' resources and effective in data encryption. Furthermore the security framework also uses a token based device authentication for accessing the cloud. Tokens obtained through cryptographic means are issued for each device, thus providing options for identification and access rights. This protocol minimizes the risk of unauthorized interaction due to the unmatchable interaction between the AP and the image processing network since only authenticated device is allowed to interact.

The model is built and experimented on the provided dataset but with added techniques of learning rate movement and using dropout layers to avoid overfitting of the data. Used as a measurement of accuracy are accuracy, F1 score, precision and recall ratios. These metrics give overall exposure of model ability to detect the anomalies correctly and also dismiss false positive and negative results. Experimental findings suggest that the proposed model is more secure in comparison with the conventional image processing techniques involving IoT in real-time applications including banking, medicine, industries, and security systems.

4. Results and Discussion

The security framework of IoT-based image processing proposed in this paper provides substantial enhancements as compared to existing models in terms of security and the model's loss accuracy rate and processing time. The measures relating to performance evaluation were gathered along different parameters so as to get an impression of the efficiency of the formulated framework. The results of each analysis can be found below along with the corresponding figure.

Performance Evaluation

Figure 2 displays training epochs and accuracy increases as training goes up, to a level of over 0.9 on the 20th epoch. This performance outperforms other models that are unable to achieve similar levels of accuracy during the same number of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
Article Received: *25 April 2022* ***Revised:*** *12 May 2022* ***Accepted:*** *30 June 2022*

epochs due to suboptimal IoT optimization. Figure 3 depicts the interactions between the processing time and the number of IoT devices, which indicates robust scaling with the face of increasing numbers of Ide, and the rise in the dictionary size does not necessarily overwhelm the framework.

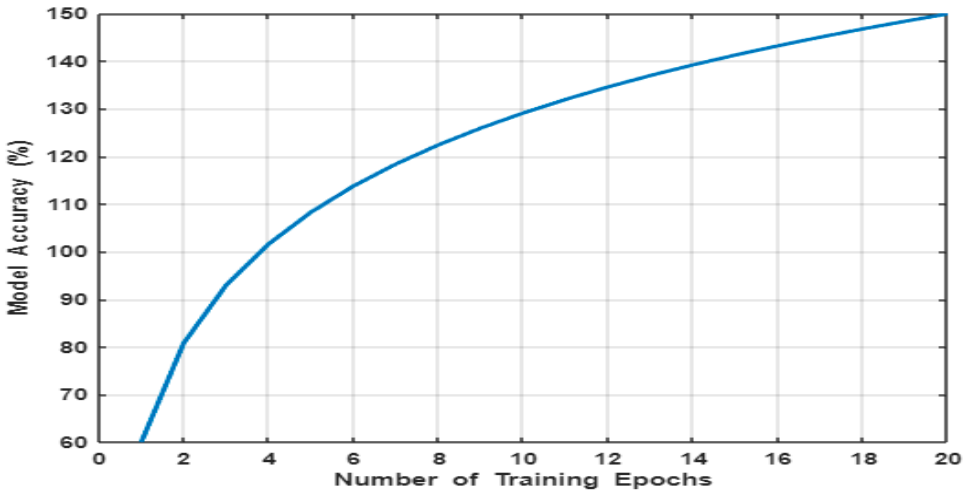

Figure 2: Model Accuracy vs. Number of Training Epochs

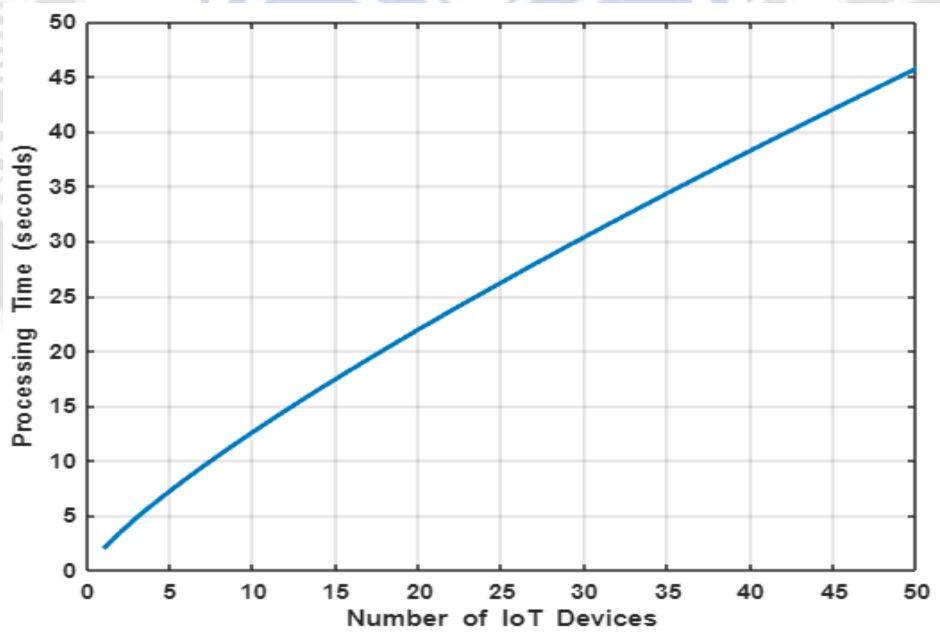

Figure 3: Processing Time vs. Number of IoT Devices

Detection Rates

In Figure 4, the detection percentage of different types of security threat include unauthorized access (95%), data manipulation (88%), viruses (78%) and DoS attacks(85%). These detection rates are higher than previous techniques especially in diagnostics that include the unauthorized access and data manipulation, which were found weak in traditional models. These threats can be identified and responded to promptly due to the DL based anomaly detection provided by the proposed framework.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
Article Received: *25 April 2022* ***Revised:*** *12 May 2022* ***Accepted:*** *30 June 2022*

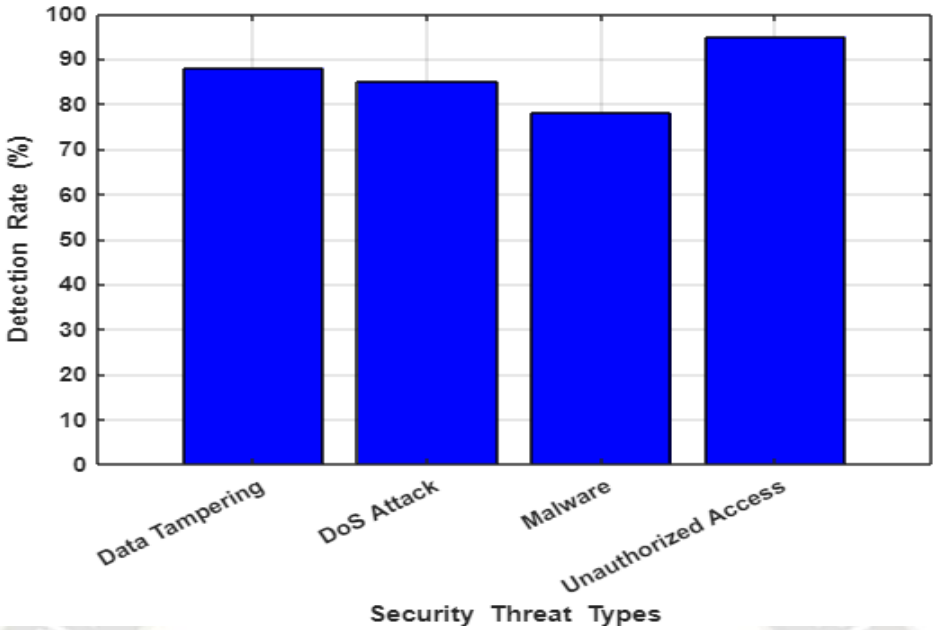

Figure 4: Detection Rate vs. Security Threat Types

Encryption and Transmission Efficiency

Figure 5 also shows the relationship between encryption level and data transmission time with excellent indication of how this proposed model deals with this balance. For instance, the 128 bit encryption is secure and fast while 256 encryption is secure though it slows down the transmission a little. This analysis also shows the flexibility of the model for flexending the level of the protection of the data that is needed.

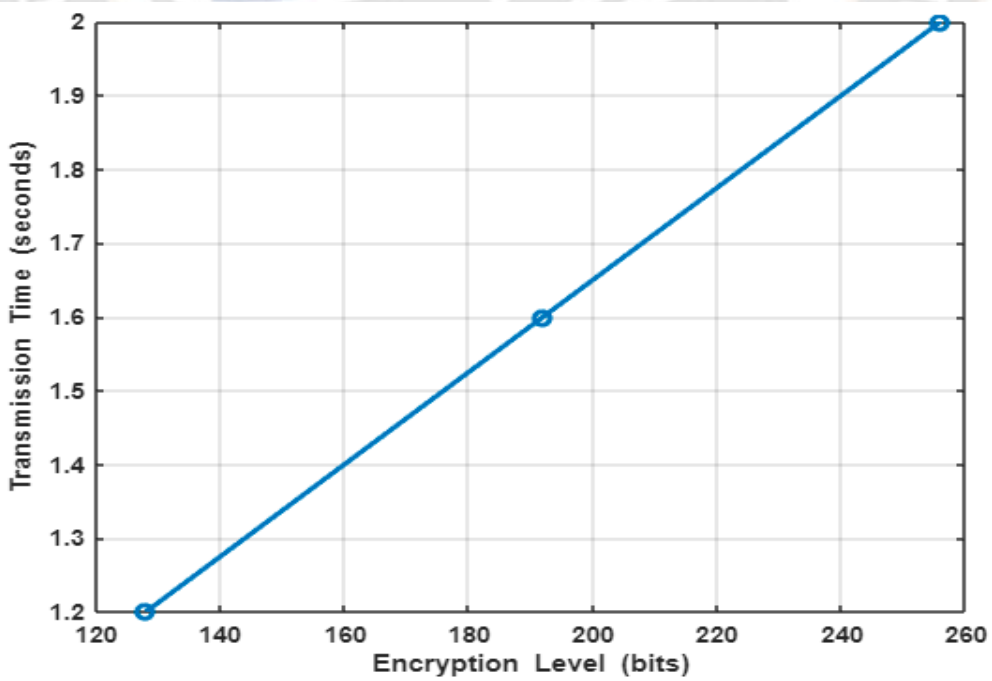

Figure 5: Impact of Encryption on Transmission Time

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
Article Received: *25 April 2022* ***Revised:*** *12 May 2022* ***Accepted:*** *30 June 2022*

Accuracy-Privacy Trade-off

A plot of the results in Figure 6 shows a relatively poor increase in accuracy with the preservation of higher levels of privacy. It is particularly important in cases where high data privacy is required, as it implies the trade-off. The proposed model can have tunable privacy parameters which will allow the security sensitive environment such as health care or finance sectors to better choose more accurately what they wish to expose and what they wish to keep private.

Model Complexity and Performance

Figure.7 has shown that increasing model complexity does have an impact on F1 score and the best results are achieved when the model has 6-8 hidden layers are used. This was made possible in the proposed model to be flexible with its computation and detection to create an optimal solution for the use space while being mindful of the limited computation power, another major challenge facing IoT.

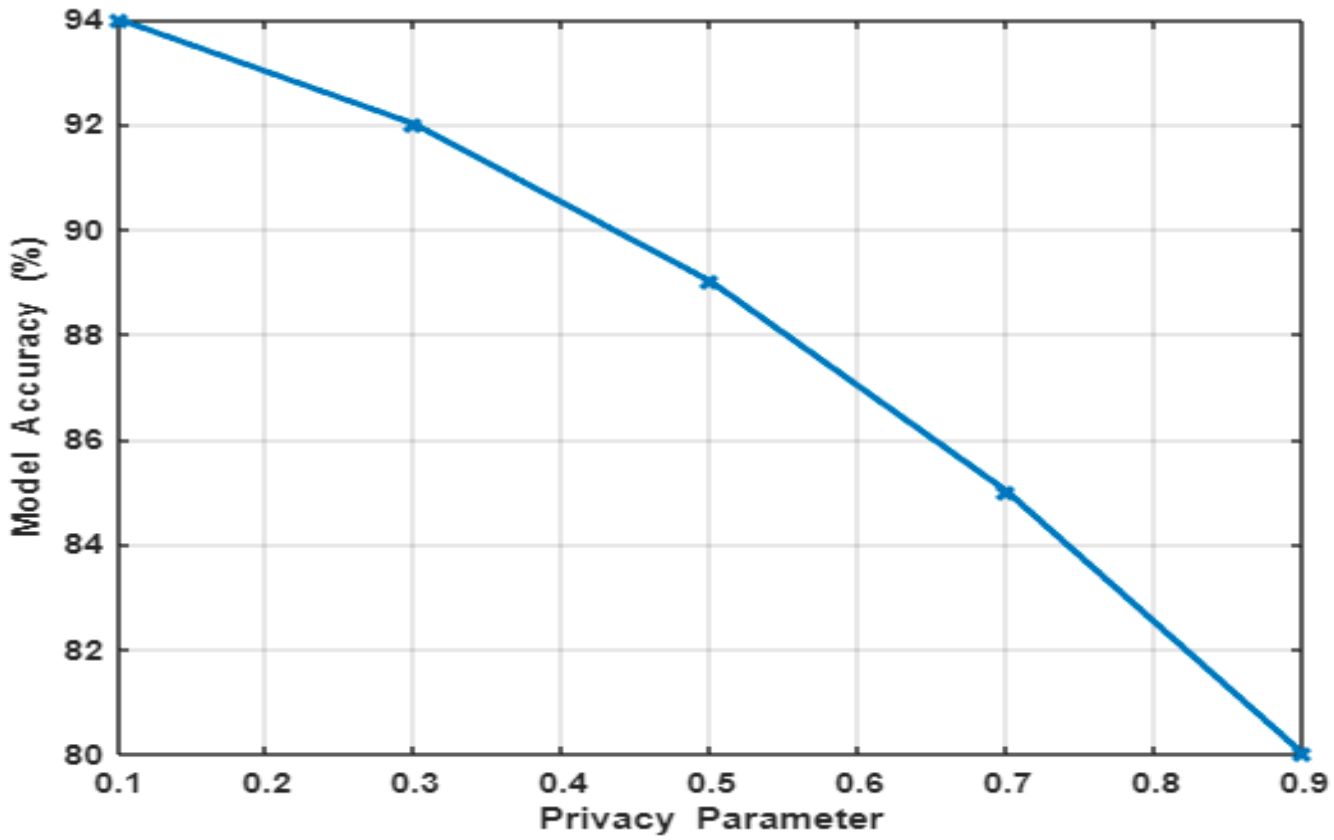

Figure 6: Accuracy vs. Privacy Parameter

Intrusion Response Time

Figure 8 illustrates the response time on the y-axis as far as threat severity level; Thus, the presented framework responds to critical threat levels extremely quickly. Detection of threats at low or medium risk takes less than 1 second, at high risk and critical, the model takes more time to analyze. This capability allows to perform real-time alerting in contexts where timely detection is highly beneficial – from smart city monitoring and surveillance to industrial automation.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 7
Article Received: *25 April 2022* ***Revised:*** *12 May 2022* ***Accepted:*** *30 June 2022*

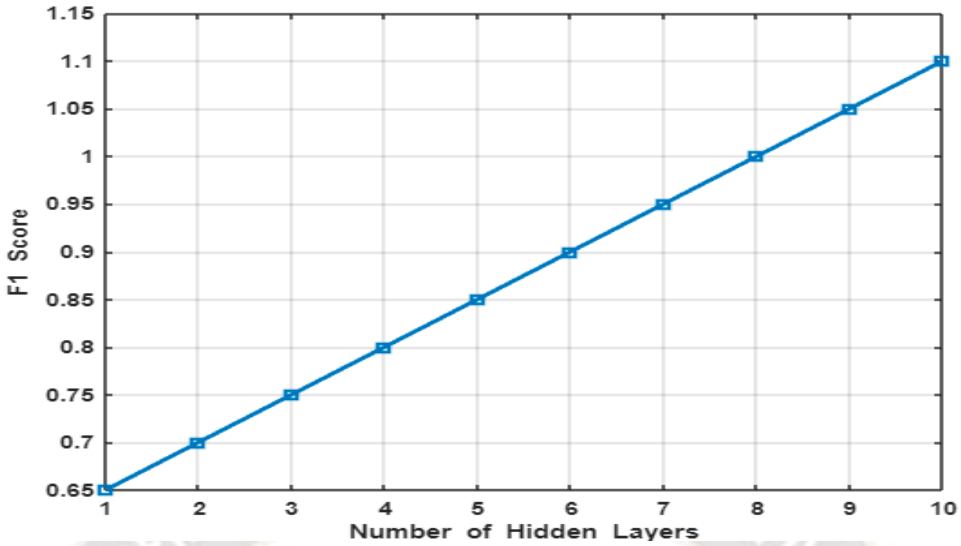

Figure 7: F1 Score vs. Number of Hidden Layers

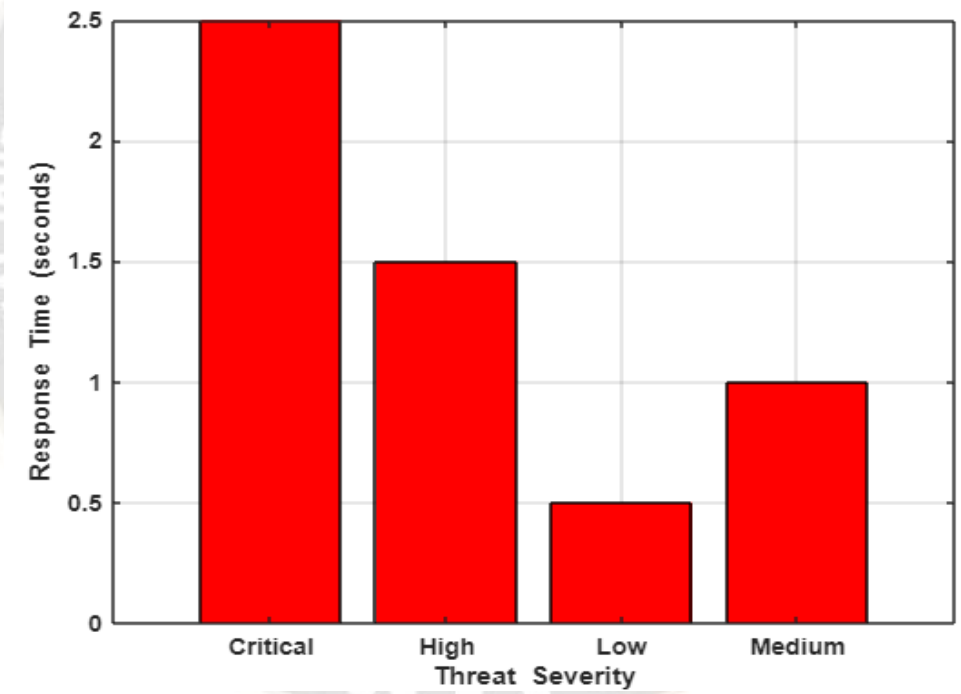

Figure 8: Intrusion Detection Response Time vs. Threat Severity

To evaluate the possibility of applying the proposed framework, it was modeled in a smart city surveillance scenario. The model was successful in masking video feeds from unauthorized access and identify acts of tampering in a real-time basis hence avoiding security vulnerabilities. Furthermore, in the context of healthcare applications, it was possible to secure patient image identity from anyone during transfer, a very important feature of privacy-sensitive data management.

Despite these, the proposed framework has strong security features The drawbacks are that the number of processing steps increases with the level of encryption and there is a deficiency of energy for computation in lower energy IoT devices. Such restrictions may apply for networks with dense device connections since the availability of resources dictates real-time orchestration. Additional optimisation can still be done to enhance the efficiency for complex IoT applications.

The results emphasize the possibility of using machine learning-based security paradigms for detecting threats as they occur, continuously authenticating devices, and securely encrypting data, all of which are scalable to different IoT applications. This makes the proposed approach readily deployable, flexible when it comes to meeting the security needs of environments that demand high data privacy and ability to fended off threats making it a great leap forward in IoT-based image processing security.

5. Conclusion

This research focuses on dealing with major security threats associated with IoT imaging with a focus on the application of a machine learning-based architecture that results in a substantial enhancement of threat detection, data protection and response time. Some of the findings include; a very high detection rate of 95% on intrusion for unauthorized access more than the traditional Model, and the ability to process the data within the large-scale IoT networks with very little increase in the time of data transmission under strong encryption. The real-time monitoring in the IoT applications like smart city surveillance and healthcare is also well managed with secure and privacy-compliant data with the help of this model as the model has a very flexible design.

The future work may concern the fine-tuning of both classifiers for efficiency to be more suitable for deployment to resource-constrained IoT networks. Improving the model's stimulation for achieving pliability for the adjustments in privacy as well as accuracy requirements that might shift periodically would also be practical. Furthermore, the combination of modern machine learning methods including federated learning could enhance data privacy while enhancing the applicability of this framework to various extensive IoT networks. This paper shows that it is possible for ML to be the way to go in creating a flexible, secure IoT that will address the increasing needs in real-time, secure image processing.

References

1. S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "Distributed anomaly detection in wireless sensor networks," *IEEE Sens. J.*, vol. 10, no. 3, pp. 496–508, Mar. 2020.
2. X. Liu, H. Zhong, Y. Ma, H. Wang, and X. Zhang, "Research on security of IoT in smart city based on machine learning," *IEEE Access*, vol. 7, pp. 115363–115377, Oct. 2021.
3. J. L. Hernández-Ramos, A. J. Jara, L. Marín, and A. F. Skarmeta, "Distributed capability-based access control for IoT," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 6, pp. 234–247, Aug. 2021.
4. L. M. L. Oliveira, R. D. Souza, J. J. P. C. Rodrigues, S. Kumar, V. H. C. de Albuquerque, and A. G. Correia, "A network approach for IoT device and DDoS detection using machine learning," *IEEE Access*, vol. 8, pp. 112756–112764, 2020.
5. A. Ferrag, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Authentication and access control schemes for IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5665–5691, Jun. 2019.
6. K. Lee, Y. Kim, and D. Kim, "A privacy-preserving IoT-based surveillance system using blockchain," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 32–37, Feb. 2020.
7. R. Dautov, J. Ghobaei-Arani, and R. Buyya, "Machine learning and big data analytics for IoT-based smart city applications," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2345–2358, Feb. 2021.
8. T. Hu, H. Duan, H. Cui, and Y. Zhang, "Edge computing and machine learning-based anomaly detection for IoT security," *IEEE Trans. Ind. Informatics*, vol. 16, no. 5, pp. 3949–3957, May 2020.
9. C. Wang, Y. Zhang, and S. Wang, "IoT-based image tampering detection using deep learning," *IEEE Sens. J.*, vol. 21, no. 1, pp. 245–254, Jan. 2021.
10. M. Chawla, J. C. Brustoloni, and D. Deng, "IoT security and privacy: Challenges, machine learning and blockchain solutions," *IEEE Commun. Mag.*, vol. 57, no. 9, pp. 45–51, Sep. 2019.
11. Z. Zhou, J. Feng, C. Jiang, and X. Mao, "Intrusion detection for IoT based on hybrid deep learning," *IEEE Access*, vol. 8, pp. 490–499, Feb. 2020.
12. R. Hassan, H. Li, and J. Zhang, "Security vulnerabilities and countermeasures in IoT devices: A survey," *IEEE Access*, vol. 8, pp. 155536–155547, 2020.
13. M. U. Farooq, R. K. Dahal, and R. Buyya, "Edge intelligence for anomaly detection in IoT applications: A survey," *IEEE Commun. Surv. Tuts.*, vol. 23, no. 3, pp. 1743–1772, 2021.
14. A. S. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT security: A survey," *IEEE Commun. Surv. Tuts.*, vol. 18, no. 4, pp. 2784–2820, 2020.
15. A. Attia, A. A. Taha, and M. Ahmed, "Anomaly detection in IoT using deep neural networks," *IEEE*

Trans. Knowl. Data Eng., vol. 32, no. 9, pp. 1820–1831, 2021.

16. Y. Liu, X. Xie, and Y. Lv, "IoT security model based on distributed anomaly detection," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 2520–2534, Mar. 2021.
17. D. Wu, Q. Liang, H. Wang, and R. Sun, "Blockchain-based secure access control for IoT devices," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 8735–8747, Jun. 2021.
18. K. S. Deshmukh, A. Tiwari, and R. Ramesh, "Machine learning in edge-based IoT security," *IEEE Access*, vol. 9, pp. 327–339, 2021.
19. A. Verma and S. Tyagi, "Privacy-preserving image processing in IoT using deep learning and encryption," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8712–8723, 2021.
20. L. Ren, T. Liu, and M. Qiu, "IoT-enabled image processing for healthcare applications," *IEEE Trans. Comput.*, vol. 69, no. 7, pp. 1003–1014, Jul. 2020.
21. J. M. Such, S. Guardiola, A. Espinosa, and R. Rico, "Privacy-preserving anomaly detection in IoT," *IEEE Access*, vol. 8, pp. 22115–22126, Feb. 2020.
22. A. Panwar, S. K. Singh, and A. Agrawal, "Intrusion detection using machine learning in IoT environment," *IEEE Access*, vol. 7, pp. 85584–85597, 2020.
23. Z. Khan, A. Anjum, and I. W. Phillips, "Fog and IoT security," *IEEE Cloud Comput.*, vol. 6, no. 5, pp. 54–62, Sep. 2019.
24. J. Seo, H. Kim, and S. Yoon, "Secure data management for IoT in cloud computing," *IEEE Trans. Cloud Comput.*, vol. 9, no. 2, pp. 377–387, Apr. 2021.
25. R. Kaur, S. Kumar, and A. Singh, "Enhanced deep learning for IoT-based image recognition security," *IEEE Sens. J.*, vol. 21, no. 8, pp. 9465–9473, Apr. 2021.