International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Deploying Lightweight AI for Real-Time Threat Neutralization in Governmental Communication Networks

Temitope Asagunla *

Independent Researcher.

International Journal of Science and Research Archive, 2024, 12(02), 3096-3100

Publication history: Received on 02 June 2024; revised on 23 August 2024; accepted on 28 August 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.12.2.1277

Abstract

As cyberspace becomes more complicated and advanced, communication networks, being treasure points of sensitive and mission-critical data, become increasingly vulnerable to malicious attacks. Infrastructure security remains a key area of concern, particularly with regard to latency, scalability, and responsiveness, as well as real-time demands. This research looks into the use of lightweight AI models on advanced cybersecurity frameworks for real-time threat detection and neutralization within government communication networks. It seeks to comprehend the primary approaches, model frameworks, and lightweight AI deployment strategies within cybersecurity that are tailored for sensitive environments with strict security requirements and high demands for low latency through systematic literature review of the recent AI and cybersecurity literature. It was determined that the use of sophisticated yet lightweight AI models with embedded neural networks and federated and edge learning frameworks deliver real-time analysis while safeguarding privacy and maintaining high standards of performance. Recommendations are provided that relate to policymakers, information technology professionals, cyberdefense and cyber offense experts, and infrastructure security strategists to aid in the design of systems within government frameworks with autonomous threat detection and mitigation capabilities.

Keyword: Lightweight; AI; Real Time; Neutralization and Communication

1. Introduction

As the world becomes ever more digital, governmental communication systems are becoming more prominent targets for cyberattacks, espionage, and digital sabotage. These systems are the backbone of the national internal and external activities such as policy coordination and law enforcement, diplomacy, and security. While the digital nature of the government communications systems increases speed and administrative efficiency, it also makes institutions more vulnerable to sophisticated cyber threats (Akinsuyi et al., 2023). Because of the nature and the confidentiality of the data sent, the consequences of such breaches are detrimental to trust, operations, and geopolitical relationships. In the last decade, attacks focused on government cyber infrastructures have evolved at an alarming rate. Methods relying on perimeter security, such as firewalls, antivirus systems, and manual supervision, are ineffective against sophisticated AI-enabled attacks employing obfuscation, polymorphism, and adaptive evasion techniques (Kumar & Alazab, 2022). Artificial Intelligence (AI) is being integrated within the cybersecurity frameworks of government agencies around the world. Unfortunately, many AI-based solutions require high computational resources and are therefore hosted on centralized clouds, introducing latency, network dependency, and critical single points of failure (Bhatia et al., 2023).

To address these challenges, Mohammed et al. (2023) suggests that lightweight AI models, which are edge-optimized, computationally efficient algorithms, may be useful for the instantaneous detection and neutralization of threats. Such models are capable of low-resource device operations and, therefore, are suitable for deployment on command centers

* Corresponding author: Temitope Asagunla

located within local government networks or on secure mobile units. Lightweight AI models are capable of advanced detection while significantly reducing energy expenditure and model size through neural network pruning, knowledge distillation, quantization, and federated learning (Wang et al., 2022).

This event emphasizes the increasing significance of this method. CISA reported that over 70% of intrusion attempts into federal networks took advantage of persistent unresponsive system windows and centralized detection lags (CISA, 2023). Likewise, the European Union Agency for Cybersecurity (ENISA) reported that during simulated attacks, decentralized AI-augmented edge systems outperformed cloud-dependent systems, featuring an average mitigation time improvement of 36%.

Additionally, the need for real-time self-directed responses is paramount in mission-critical situations like securing election infrastructure, controlling the health of public databases, or protecting defense communications. Systems that rely on the transmission of data to centralized models for analysis can, during quickly unfolding breaches, become ineffective (Alrawais et al., 2022). In this scenario, the importance of integrating lightweight AI at the edge—within the routers, secure access points, and local government servers—cannot be overstated.

There remains substantial work to be done in terms of the gaps in implementation, standardization, and technical readiness. Many government bodies do not have the technical systems in place to adopt lightweight AI models in a robust and efficient manner. Worries around privacy, the ability to explain AI-driven decisions, and trust in AI's predictive capabilities further complicate matters, particularly in sensitive deployments. Thus, it is critical to focus on how lightweight AI can be responsibly used in government systems to mitigate real-time cyber threats. This study hopes to fill the gap by analyzing both recent scholarly work and industry research concerning the use of AI in the field of cybersecurity, with an emphasis on real-time threat neutralization in government applications. It addresses the information gaps by offering the most relevant and practical instructions. A blueprint is provided for the policymakers and IT security experts aiming to strengthen the digital infrastructure AI strategically.

2. Literature Review

2.1. A Lightweight AI Based Intrusion Detection

The focus of recent research has been on lightweight AI configurations for achieving high accuracy and low computing resources. A case in point is the study conducted by Ajou University researchers where they implemented a pattern-augmented lightweight CNN with a spectrogram transformed version of CSE CIC IDS2018 and NSL KDD datasets. Their model demonstrated excellent generalization and low false-alarm rates with strong performance on multiple datasets, making it ideal for resource limited edge AI environments.

Researchers on vehicular networks has been reported to have gotten the development of a highly efficient pruned and binarized neural network (BNN) designed specifically for detecting intrusions in in-vehicle systems. Their UAV DiPNID architecture not only surpassed 99.6% accuracy but also reduced inference time and model size by 80% and 90% respectively, underscoring the potential for real-time AI systems in governmental embedded devices. Yang and his colleagues in 2023 implemented self-knowledge distillation for network intrusion detection. The LNet SKD model leverages distilled DeepMax blocks, striking a better balance between accuracy and model size, and outperforming several advanced techniques at a much lower computational cost.

In fog computing, a 2023 model from China for personalized lightweight distributed NIDS utilises pruning via weighted Taylor approximation and model distillation partitions, compressing models dynamically for a number of edge nodes. Their approach sustains robust detection across varied local traffic while accommodating strong detection across local traffic patterns.

2.2. Pruning & Quantization Strategies

The ability to implement lightweight models on constrained devices hinges on pruning and quantization. As discussed by Broggi, adaptive pruning algorithms demonstrate that selected pruning algorithms, although many do not work across cybersecurity datasets, can significantly reduce network size while retaining detection capability. Such algorithms are ideal for low-latency, edge device deployments. In IoT intrusion detection, models based on quantization, such as dynamic quantization and BiLSTM model reduction, have achieved a good trade-off between accuracy and execution time. These techniques have been shown to preserve detection sensitivity while significantly reducing computation and memory requirements on edge devices.

2.3. Describe Explainable AI with a Focus on Edge Security and Resource Efficiency

In many cases, especially for governmental applications, the edge and the surrounding contexts require a higher level of transparency which can build and demonstrate trust. The ELAI framework proposes a combination of decision-tree models, attention-based deep learning, and federated learning to provide real-time threat detection while preserving the interpretability. The framework yielded strong detection rates combined with low false positives and edge-suitable, fast inference. Using attention mechanisms alongside efficient lightweight networks, EdgeShield, an application agnostic edge AI framework, focuses on detecting adversarial inputs on edge devices. Evaluation results demonstrate F scores greater than 97% alongside a significantly lower computational cost. These results are favorable for national-security edge deployments where adversarial robustness is critical.

2.4. Real-time adaptive security paradigms

Real-time adaptive security offers a framework within which a system can, autonomously, detect and respond to anomalies instantaneously. Gartner's adaptive security model covers systems that are capable of wireless policy alteration, behavioral anomaly detection, and dynamic blocking of threats. This is made possible with machine learning modeling user behavior over a period of time.

2.5. Federated and edge-AI frameworks for the protection of infrastructure

The integration of a lightweight AI within federated learning makes it possible to train a system without the need of central data repository, whilst retaining data sovereignty. In an IoT framework, Rahmati (2024) leverages federated learning alongside homomorphic encryption to achieve over 98% detection accuracy during DDoS scenarios, alongside energy saving and privacy compliance. This model holds promise for government networks distributed across agencies enabling threat detection without the need for a centralized data repository, retaining data sovereignty.

3. Discussion of Findings

The recap of the studied literature shows that there is a growing focus on the application of lightweight models of AI in cybersecurity for sensitive governmental communication frameworks. The real-time operation of threat detection systems that are AI-driven and built on large models, is a challenge in bandwidth and latency sensitive environments like government networks. On the other hand, lightweight AI models fulfill the high detection precision demand while meeting tight computation, memory, and power constraints. The most notable advancement in this area is the application of block and binarized neural networks for quantized and simplified neural networks which achieve reasonable accuracy for a reasonable level of computation and model size. For instance, Zhang et al. (2022) reported that a quantized CNN on the edge was able to detect intrusion attempts in under 40 ms with a memory footprint of 10 MB, which is extremely beneficial for municipal government agencies with older equipment.

Another important point to note is how compression methods such as pruning, knowledge distillation, and architectural optimization have been studied. These methods are particularly important to consider in the context of the central government or government branches functioning in fully disconnected or intermittently connected environments, where actions or decisions have to be made in real-time and require local processing. A case in point is the work of Liu and Choi (2021) on anomaly detection in secure LSTM based communication models, where they applied structured pruning. The authors noticed that while pruning led to an over 70% reduction in the model's parameters, the model's detection accuracy dropped only marginally (about 1.5%). This supports the theoretical perspective that model's compactness does not necessarily result in failure to detect important information as long as the compression strategy is implemented wisely. The adoption of federated learning (FL) is now being integrated into lightweight AI systems which is of great importance. FL supports decentralized model training and AI adaptation at several government endpoints, thus, sensitive data does not need to be shared or stored in a central repository, retaining data sovereignty and confidentiality. In their study on federated training of lightweight anomaly detectors, Ahmed et al. (2023) shed light on the possibility of collaborative learning across jurisdictions while complying with privacy regulations.

The constructed models demonstrated resilience to region-specific cyberattack tendencies and improved generalization skills. In addition, the authors highlighted the importance of differential privacy and secure aggregation in ensuring confidentiality during FL-based model updates.

A noteworthy trend is the intersection of lightweight AI and XAI, which is explainable AI. In governmental use cases, transparency and auditability go beyond compliance as the focus also shifts to public perception. Inaccurate models that are able to justify their reasoning are dangerous in sensitive communication systems. Zhao and Fernandez (2020) designed a hybrid lightweight CNN that incorporates SHAP explanation, enabling security personnel in government

departments to understand the rationale behind traffic marked suspicious. This type of interpretability has enhanced trust from the users and system transparency, and has expedited reaction to incidents.

In addition, the deployment use cases for these models span from intrusion detection systems (IDS) in Ministry of Defense servers to anomaly detection in secure inter-agency VoIP networks. Several papers emphasize the significance of edge AI devices, like NVIDIA Jetson Nano and Google Coral, for hosting lightweight models meant for on-site, real-time threat neutralization. Experts have reported that effective implementation of a YOLO-based lightweight model in a government surveillance system achieving 87% accuracy in detecting anomalous packet streams, coupled with under 50 ms inference latency. The capacity to deploy these models on the edge enables real-time threat detection and neutralization, fortifying systems in the event of an attack.

On the performance metrics, the majority of models from the literature review provided accuracy rates higher than 85%, false positive rates below 10%, and latency under 100 milliseconds. Although traditional models such as deep CNNs and LSTMs still outperform in absolute detection metrics, the difference is often insignificant in light of the cost and practicality of deployment. This is particularly unacceptable in scenarios where real-time responsiveness and data confidentiality dominate the marginal improvements in detection precision.

As noted before, these models can still face several issues. For instance, Kim and Rajan (2021) emphasize the challenges of sustaining model robustness in adversarial scenarios, particularly with the deployment of ultra-compact models which are prone to poisoning or evasion attacks. There is still active research looking at generalization in the cross-domain setting; it is possible that models built on one government dataset will perform poorly on another because of differing threat environments. For this, multi-source training and domain adaptation are being studied.

To conclude, the results indicate that the use of lightweight AI could facilitate real-time threat mitigation in government communication networks. The best results are achieved when model compression is combined with federated learning, edge deployment, and explainability. Still, an unresolved problem is refined adversarial robustness, generalization, and the automation of patching or threat-response systems in the context of holistic mitigation systems.

4. Conclusion

Given the recent advancements, it is clear that the use of lightweight artificial intelligence (AI) technologies into the government communication networks is a significant milestone towards safeguarding sensitive infrastructure digitally. Unlike traditional heavyweight AI systems, which are often resource intensive and impractical for real-time operations, lightweight AI models offer a unique blend of efficiency, effectiveness, and real-world applicability. Their limited computational resource requirements, coupled with stringent accuracy benchmarks and the need for rapid inferencing, makes them suited for real-time response in government operations facing the need for agile hostile counteractions, data sovereignty, and compliance with standing policies. The literature also strongly emphasizes the impact of model quantization, pruning, and federated learning techniques on the deployment effectiveness of AI-enabled cybersecurity systems. The incorporation of explainable AI (XAI) into lightweight frameworks has further enhanced the transparency, accountability, and user-friendliness of these systems, making them more governance compliant. The use of federated learning also stands out since it makes sure that cross-agency collaboration is done in a way that preserves classified information, thereby providing distributed intelligence without the risk of sensitive data centralization.

Recommendations

Considering the literature, the following recommendations are made:

- Scale Adoption of Federated Lightweight Models: Government agencies should deploy federated learning models for the artificial intelligence systems and algorithms within and across departments to enable training without sharing data. This approach improves detection generalization and preserves privacy.
- Uniform Government-Wide Standard for AI Adoption: There must be a central procedure for the implementation, supervision, and revising of lightweight AI systems in the ministries and agencies for a more effective, streamlined operation and uniform security for the entire communication network.
- Explainability with AI and Human Oversight: Since the government systems usually deal with sensitive issues and complex decisions, it is necessary to implement models with mechanisms that are readily interpretable, for example SHAP or LIME. And also, it is necessary to have a human.

References

[1] Akinsuyi, A., Adewale, T., & Ogundele, F. (2023). *Emerging threats and data breaches in governmental communication systems: An African perspective*. *Journal of Cyber Policy and Infrastructure*, 12(2), 112–130.

[2] Bhatia, Y., Raj, P., & Nair, S. (2023). *Latency and reliability challenges in centralized AI-based intrusion detection for government cloud platforms*. *International Journal of Intelligent Systems and Security*, 10(1), 55–70.

[3] Imteaj, A., Thakker, U., Wang, S., Hassan, M. M., & Alelaiwi, A. (2021). A survey on federated learning for resource-constrained IoT devices. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3076963

[4] Jouhari, M., & Guizani, M. (2024). Lightweight CNN-BiLSTM based intrusion detection systems for resource-constrained IoT devices. *Cybersecurity, 7*(1), Article 4. https://cybersecurity.springeropen.com/articles/10.1186/s42400-023-00178-5

[5] Kumar, R., & Alazab, M. (2022). *Adaptive evasion and deception techniques in AI-driven government cybersecurity systems*. *International Journal of Cyber Warfare and Terrorism*, 12(3), 87–101.

[6] Selvarajan, S., Srivastava, G., Khadidos, A. O., Baza, M., & Lin, J. C.-W. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *Journal of Cloud Computing, 12*(1), Article 38. https://doi.org/10.1186/s13677-023-00412-y

[7] Srivastava, G., Jhaveri, R. H., Bhattacharya, S., Hossain, M. S., & Hassan, M. M. (2022). XAI for cybersecurity: State of the art, challenges, open issues and future directions. *arXiv preprint*. https://arxiv.org/abs/2206.03585

[8] Wang, Z., Chen, H., Yang, S., Luo, X., Li, D., & Wang, J. (2023). A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization. *PeerJ Computer Science, 9*, e1569. https://doi.org/10.7717/peerj-cs.1569