GUARDING AGRICULTURE'S IOT REALM: DETECTING MALWARE AND STRENGTHENING CYBERSECURITY

PAPER ID #G20DA0564
ANUSHKA RAWAT

INTRODUCTION

The agriculture sector is undergoing a digital revolution through widespread IoT adoption, transforming farming practices, monitoring and consumer-farmer interactions. Yet, this shift from traditional to wireless, sensor-based systems poses cybersecurity challenges.

OBJECTIVE

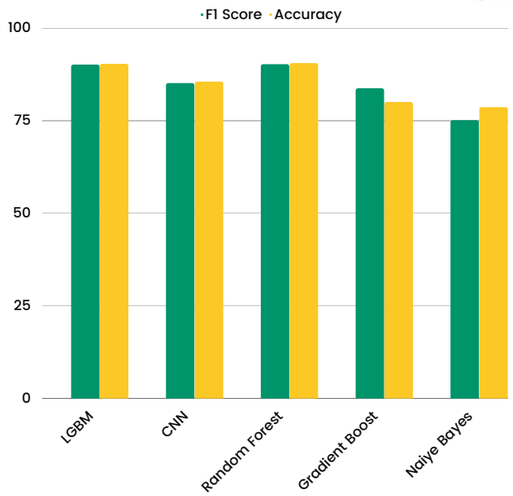
This research aims to address the emerging cybersecurity challenges in agriculture's digital transformation driven by IoT adoption by developing a model for IoT malware detection and classification.

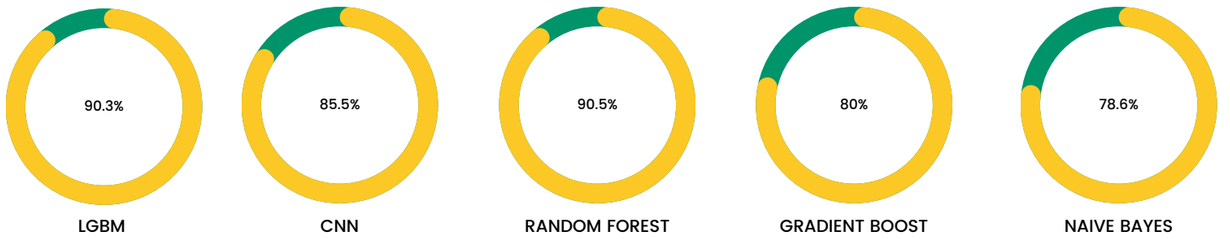
METHODOLOGY

In the proposed model, IoT malware from the MQTT dataset has been detected and classified with the help of different machine learning algorithms such as Random Forest, CNN, Gradient Boost, Light GBM, and Naive Bayes which are then compared on the basis of their accuracy, F1 score, and confusion matrix.

RESULT

The research demonstrated that the Random Forest algorithm outperformed other machine learning algorithms in accurately detecting and classifying IoT malware from the MQTT dataset, achieving an impressive accuracy rate of 90.5%. This robust detection capability offers a promising foundation for enhancing the cybersecurity of IoT-enabled agricultural systems, contributing to their resilience in the face of evolving digital threats.





ANALYSIS

ACTUAL \ PREDICTED	Bruteforce	DoS	Flood	Legitimate	Malformed	SlowITe
Bruteforce	3558	536	0	9	248	0
DoS	225	35554	0	3263	35	0
Flood	1	4	88	90	1	0
Legitimate	0	3171	0	46468	0	0
Malformed	1087	281	24	457	1429	0
SlowITe	0	0	0	0	0	2761

CONCLUSION

This research highlights the critical importance of addressing cybersecurity challenges as agriculture undergoes a digital transformation through IoT adoption. The study successfully developed an effective IoT malware detection and classification model, with Random Forest achieving a high accuracy of 90.5%. As agriculture ventures into the digital era, this research serves as a foundational step in securing IoT-enabled farming systems.

Future studies in digital agriculture should prioritize IoT security enhancements, threat intelligence systems, and secure communication protocols. To fortify digital agriculture against cyber threats, future measures must encompass regulatory frameworks, security audits, collaborative threat sharing, secure supply chains, and continuous monitoring. These efforts will establish a robust cybersecurity foundation, ensuring the secure adoption and operation of digital agriculture technologies in the face of evolving cyber risks.