Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 2 (2024)

Advanced Spam Detection for IoT Security with Real-Time Processing

[1] Mrs. D. Archana, [2]E. Nikhita,[3] D. Sai Prasanna, [4] B. Abhishek, [5]D. Koushik

[1]Assistant Professor

Department Of Computer Science and Engineering

[2345]Department Of Computer Science and Engineering UG Scholar

Abstract-In our attempt to strengthen IoT ecosystem security, we introduce a creative improvement to spam detection within IoT data stream. Our perspective amalgamate stacked Convolutional Neural Networks (CNN), Random Forest, Logistic Regression, Support Vector Machine(SVM), and Decision Tree algorithm. While logistic regression, and SVM provide foundational analysis, stacked CNNs through complicated spatial patterns, LSTM and GRU purify intolerance by catching long-term temporal dependencies. This extensive fusion allow our model to notice delicate features and subtle dissimilarity in IoT data, improving its ability to differentiate between legitimate and spam data instance. Moreover, clustering algorithms like k-means and DBSCAN are utilized for anomaly detection, while privacy-conserving methods, such as Homomorphic Encryption and Differential Privacy safeguard the delicate data. To improve realtime responsiveness, we introduce edge computing paradigms which permits swift processing of IoT data streams and making easier to timely detection and reduction of security threats. Ensemble learning methodologies include random forests and gradient boosting increase prediction exactness and flexibility against adversarial exploit, improving robustness for our spam detection system. Updated approaches like adversarial training are united to fortify the model against to dodging trails, reducing potential suspectability. User feedback mechanism authorizes iterative clarification, permitting the model to adapt and enhance its decision-making process. In addition, the user will be notified if there is any potential spam recognized in his data. In summary, our clear methodology combine advanced machine learning approaches, Real-time processing, elasticity against adversarial threats, and techniques for iterative enhancement, authorizing organizations to fortify their IoT environments with increased security and efficiency.

Keywords- Homomorphic Encryption, Differential privacy, adversaraial exploit, gradient Boosting, User feedback mechanism, Real-Time Processing.

I. Introduction

In our search to strengthen security of IoT habitat, we introduce a developing advancement in the detection of spam in IoT data streams. Our proposed system is an enlightened combination of cutting-edge technology is of together with stacked Convolutional Neural Networks(CNNs), Random Forest, Logistic Regression, Decision tree algorithm, Support Vector Machine(SVM), LSTM and GRU.

While Constitutional analysis are provided by SVM and logistic regression, CNNs search into complicated spatial patterns, whereas LSTM and GRU purify bias by identifying long-term temporal dependencies. This comprehensive amalgamation enables our model to notice subtle dissimilarity in IoT data. Such means improving its ability to differentiate between legal and spam data cases.Moreover, We merge clustering algorithms like DBSCAN and K-means for anomaly detection, incorporated with privacy-conserving methods such as Homomorphic Encryption and Differential Privacy to protect sensitive data. Real-time responsiveness is certified through the application of edge computing patterns, making easier to swift processing of IoT data streams for cause detection and reduction of security warning.

Our work includes ensemble learning methods like gradient boosting and random forest to increase prediction correctness and flexibility against negative exploit, whereby improving the strength of our spam detection system. Moreover, enhanced methodologies like adversarial training are combined to protect the model against dodging attacks, lightening potential suspectibility.

Repeated purification is made possible through user feedback mechanisms, licensing continual adjustment and enhancement of the decision-making process. Aditionally, users are punctually informed of prospective spam detected in their data, certifying feedback estimation.

A.CONTRIBUTIONS

Based on the above discussion, Given below are the following contributions handed over in this paper.

1.The proposed procedure introduces a creative blend of machine learning approaches, which includes Random Forest, CNNs, LSTM and GRU, improving spam detection in IoT data.

2. It merges anomaly detection using DBSCAN, K-means algorithms with privacy-conserving methodologies like Homomorphic Encryption and Differential Privacy.

3. Real-time responsiveness through edge computing combined with ensemble learning and adversarial instructions, protects the model incase of intimidating remark, allowing administration to secure their IoT habitat productivity.

Figure 1.1: Block Diagram of Cybercrime Detectio

Ii. Literature Review

Recent advancements in enhancing the IoT data security and spam Machine Learning (ML) techniques. Abdullah Ayu b khan(2022) introduced a paper that label manufacturing procedure by putting forward a Hyperledger sawtooth-based blockchain framework for locked Industrial Internet of Things(IIOT). I t evaluates writings, institutes a double communication system(on-chain and off-chain), and carryout chain codes and multi-proof-of –work agreement for assests-efficient Blockchain-IIOT(B-IIOT). This framework assure trustworthiness, integrity and clearness, making it a favourable mixture for wide adoption in commercial manufacturing and production settings. P. K arthikeyyan(2019) introduced a paper which travel over the amalgamation of Blockchain Technology with IoT to label security anxiety arising from the consolidate cloud server model. Managing a systematic review, it contrast IoT and Blockchain, classify blockchain based IoT applications over sectors, and focus attention on security issues and limitations. The discovery points to lead academics and researchers in moving forward the enhancement of secure IoT applications using blockchain technology. Vinay Chamola(2019) introduced paper which drawn attention to the important need for security in the developing era of IoT, focusing on challenges and threats. It introduces labelling these concerns through progressing and existing techniques, particularly blockchain, edge computing, fog computing and machine learning. These methods are ranged over their potential to improve security, authentication, privacy and resilience against to the threats in IoT applications.

III. Problem Statement

In today’s computing environment, the increase of smart devices in IoT ecology has led to an exponential raise in data production, introducing an alarming provocation of securing data sources and volumes, the job of identifying and lightening spam in IoT data streams become important for sustaining system integrity and user trust. Existing system frequently has shortage of effiency and real-time responsiveness, failing to properly address the dynamic and complicated nature of IoT data. Additionally, the absence of alert mechanisms further intensify the weakness of IoT habitat to spam attacks. So, there is a desperate requirement for creative solutions that can efficiently detect and weaken the spam in IoT data streams while certifying real-time responsiveness and user notification abilities.

IV. Proposed System

To mark the draw backs of existing spam detection system in IoT environments, we propose a creative solution that influence advanced machine learning techniques and real-time processing capabilities. Our solution combines a varied approach that combines stacked Convolutional Neural Networks(CNNs), Random Forest, Logistic regression, Support Vector Machine(SVM), LSTMs and GRUs. Our solution aims to improve the accuracy and efficiency of spam detection in IoT data streams.

4.1 ADVANTAGES OF PROPOSED SYSTEM

1. The proposed system provides improved spam detection abilities in IoT data by exploiting a various set of enhanced machine learning techniques.

2. Real-time responsiveness by edge-computing and iterative model, Refinement through user feedback techniques additionally support the system's logicality, eventually ensuring in enhanced security for IoT ecosystems.

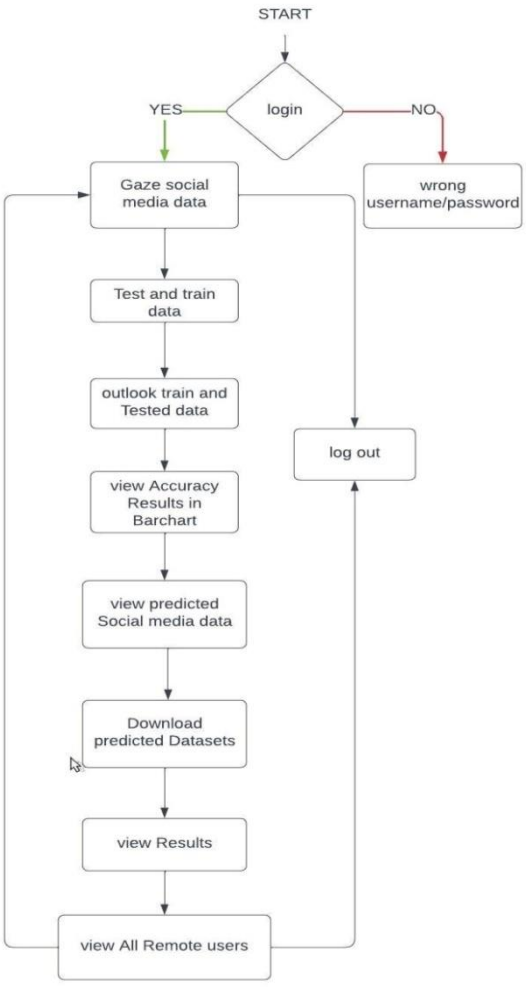


Figure 4.2 System architecture of proposed system

V. Methodology

1. Advanced Machine Learning Techniques: We engage stacked logistic regression, GRU, and LSTM to withdraw complex spatial and temporal patterns from IOT data, Additionally, SVM, Decision Trees and

Random Forest algorithms further improve classification accuracy through their identical capabilities in modelling complicated data relationships and using instance-based learning.

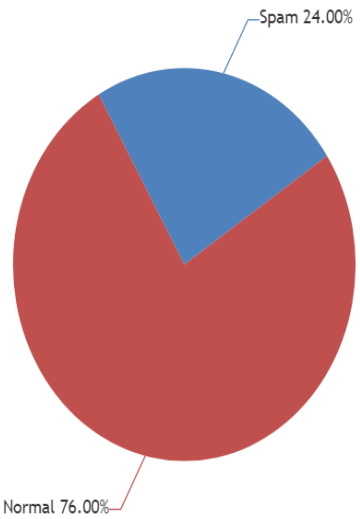
2. Real-Time Processing: Our solution organizes real-time responsiveness by using edge computing paradigms .This permits swift processing and detection of security attacks within IOT data streams, certifying punctual protection of spam attacks.

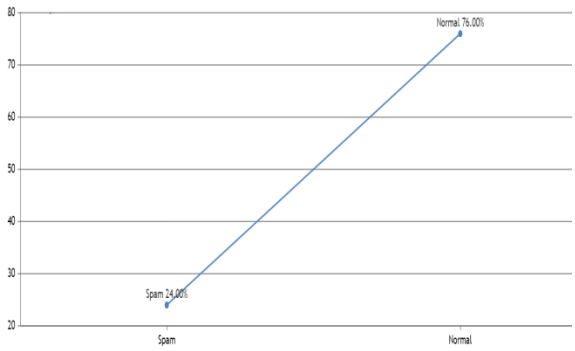
3.Ensemble Learning and Adversarial Training: To support prediction accuracy and resilience in against of adversarial exploit, we include ensemble learning techniques such as Random Forests and Gradient Boosting. Moreover advanced methods like adversarial training are introduced to fortify the model against evasion attempts and protect potential exploit.

4.User Feedback Mechanism and Privacy Preservation: continuous clarification of the spam detection ,odel is facilitated through user feedback mechanism, permitting for continual advancement of the decision- making process. User feed-back mechanism, permitting tje model to make adjustments and advance is decision-making process.

Clustering algorithms like k-means and DBSCAN are used for anomaly detection ,while privacy-preserving methods include homomorphic encryption and differential privacy ,protectthe vulnerable data. Additionally, the user is being announced if there is any potential spam recognized in his data.

Results ;





Model Type	Accuracy
SVM	94.654
Logistic Regression	98.498
CNN	91.573
Random Forest	95.642
LSTM	93.854
GRU	91.751

Conclusion

Our creative iot security approach incorporate the latest machine learning methods including stacked CNNs, Logistic Regression random forest svm decision trees LSTM and GRU certifying a exact understanding of IoT data for effective detection of fine dissimilarity. Clustering algorithms like K-means, DBSCAN, along with privacy-preserving techniques such as Homomorphic Encryption, Differential Privacy protect delicate data. Our methodology include edge computing for real-time responsiveness, employing group learning with random forests and gradient boosting to improve the accuracy predicted and flexibility against negative trails. Uninterrupted enhancement, handled by user feedback, certify elasticity and clear decision-making. Timely notifications authorize user to take punctual measures, eventually improving the efficiency and the security of IoT environment in the profile of developing computerized provocation.

V. References

[1] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, “Iot security: ongoing challenges and research opportunities,” in 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, 2014, pp. 230–234.

[2] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for iot security and privacy: The case study of a smart home,” in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, 2017, pp. 618–623.

[3] E. Bertino and N. Islam, “Botnets and internet of things security,” Computer, no. 2, pp. 76–79, 2017.

[4] C. Zhang and R. Green, “Communication security in internet of thing: preventive measure and avoid ddos attack over iot network,” in Proceedings of the 18th Symposium on Communications & Networking. Society for Computer Simulation International, 2015, pp. 8–15.

[5] W. Kim, O.-R. Jeong, C. Kim, and J. So, “The dark side of the internet: Attacks, costs and responses,” Information systems, vol. 36, no. 3, pp. 675–705, 2011.

[6] H. Eun, H. Lee, and H. Oh, “Conditional privacy preserving security protocol for nfc applications,” IEEE Transactions on Consumer Electronics, vol. 59, no. 1, pp. 153–160, 2013.

[7] R. V. Kulkarni and G. K. Venayagamoorthy, “Neural network based secure media access control protocol for wireless sensor networks,” in 2009 International Joint Conference on Neural Networks. IEEE, 2009, pp. 1680–1687.

[8] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, “Machine learning in wireless sensor networks: Algorithms, strategies, and applications,” IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996–2018, 2014.

[9] A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Communications Surveys & Tutorials, vol. 18, no.2, pp. 1153–1176, 2015.

[10] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, “Evaluation of machine learning classifiers for mobile malware detection,” Soft Computing, vol. 20, no. 1, pp. 343–357, 2016.
[11] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, “A system for denial-of-service attack detection based on multivariate correlation analysis,” IEEE transactions on parallel and distributed systems, vol. 25, no. 2, pp. 447–456, 2013
[12] V.Hassija, V.Chamola, V.Saxena. “A Survey on IoT Security:Application Areas, Security Threats, and AolutionArchitectures”,7,82743.doi:ACCESS.2924045(2020)
[13] M.Mohaammadi, A.A.Fuqaha, S.Sorour, M.Guizani. “Deep Learning for IOT Big Data and Streaming Analytics:ASurvey”,292329260.doi/COMST.2018.2844341(2018).
[14] P.Karthikeyyan, S.Velliangiri, Mr.T.Joseph. “Review Of Blockchain Based Iot Application And It's Security Issues”doi:ICICICT46008.2019.8993124.IEEE(2020).
[15] A.A.Khan, A.A.Laghari, Z.A.Shaikh. “Internet of Things(IOT) Security With BlockchainTechnology: A State-of-the-Art Review.”(2022)