www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 736-743

e-ISSN : 2583-1062
Impact Factor : 7.001

CYBERSECURITY RISK SCORING SYSTEM FOR IOT DEVICES USING MACHINE LEARNING: A BEHAVIOR AND CONFIGURATION-BASED APPROACH

Meenuga Pranaya Praharshitha*[1], Dr. D William Albert*[2]

[1]M. Tech Student, Dept. of CSE, Bheema Institute of Technology & Science, Adoni, A.P, India

[2] Professor & Head, Dept. of CSE, Bheema Institute of Technology & Science, Adoni, A.P, India

DOI : https://www.doi.org/10.56726/IRJMETS39773

ABSTRACT

As the Internet of Things (IoT) continues to proliferate, ensuring the security of connected devices becomes critical due to their heterogeneity, limited resources, and often lax configurations. This paper presents a machine learning-based framework to evaluate and assign a dynamic cybersecurity risk score to IoT devices. The proposed system considers device behavior (traffic patterns, access anomalies) and configuration parameters (default credentials, open ports, outdated firmware) to classify threat levels in real time. By employing supervised and unsupervised learning models, we demonstrate the efficacy of risk scoring in prioritizing response efforts and optimizing resource allocation. Experimental validation using benchmark datasets and simulated IoT environments shows a significant improvement in early threat detection and response agility.

Keywords: IoT Security, Cybersecurity Risk Scoring, Machine Learning, Anomaly Detection, Threat Classification, Device Behavior Analysis, Configuration-Based Risk Assessment, Real-Time Risk Prediction, Network Traffic Analysis,

1. INTRODUCTION

The rapid proliferation of Internet of Things (IoT) devices has revolutionized numerous industries, including healthcare, manufacturing, transportation, and smart homes [1]. These devices enable seamless connectivity and automation, offering enhanced operational efficiency and real-time data insights [2]. However, the same interconnectedness that powers IoT also introduces significant cybersecurity challenges. Many IoT devices are resource-constrained, operate on outdated firmware, or lack proper authentication mechanisms, making them prime targets for cyberattacks such as botnets, ransomware, and unauthorized data access [3-4].

Traditional cybersecurity solutions often rely on static threat models or signature-based detection, which struggle to keep up with the dynamic and heterogeneous nature of IoT environments [5-6]. These models typically fail to detect zero-day exploits or anomalous behavior that deviates from known attack signatures. Furthermore, with the growing scale and diversity of IoT deployments, security teams face difficulty in assessing which devices pose the greatest risk and how to prioritize their response efforts effectively [7-9].

To address these limitations, there is a critical need for intelligent, adaptive security solutions that can assess and respond to evolving threats in real time. This paper proposes a machine learning-based cybersecurity risk scoring system designed to analyze both the behavioral patterns and configuration parameters of IoT devices. By assigning a dynamic risk score to each device, this system enables organizations to classify threat levels, prioritize incident response, and allocate resources more efficiently [10-11].

The key contributions of this research are as follows:

- We develop a comprehensive framework that combines both supervised and unsupervised machine learning techniques to evaluate the cybersecurity risk of IoT devices.
- We introduce a multi-feature approach that incorporates device configuration attributes and behavioral indicators to improve detection accuracy.
- We validate the proposed system using benchmark IoT datasets and simulations, demonstrating its effectiveness in real-time risk assessment and threat prioritization.

This research aims to bridge the gap between static risk evaluation and the need for scalable, intelligent security mechanisms in the evolving landscape of IoT cybersecurity.

2. RELATED WORK

Cybersecurity risk assessment has long relied on standardized scoring systems to quantify the severity of vulnerabilities and threats. One of the most widely adopted frameworks is the Common Vulnerability Scoring System (CVSS)**,** which provides a numerical score based on factors such as exploitability, impact, and scope (Mell, Scarfone,

& Romanosky, 2007). While CVSS has been instrumental in traditional IT environments, it lacks the contextual awareness and adaptability needed to assess the dynamic and diverse threat landscape in IoT ecosystems. Its static nature does not account for real-time behavior or configuration changes specific to individual devices.

To overcome such limitations, researchers have increasingly turned to machine learning (ML) approaches for anomaly detection in IoT environments. Supervised learning models such as Random Forest, Support Vector Machines (SVM), and Neural Networks have shown promise in classifying known attack patterns (Doshi, Apthorpe, & Feamster, 2018), while unsupervised techniques—such as clustering algorithms and autoencoders—have been effective in identifying novel or previously unseen anomalies in network traffic or device behavior (Nguyen & Redoute, 2020). These models leverage patterns in large datasets to detect deviations that may indicate a cyber threat, offering more adaptability than signature-based systems.

Despite these advances, many current IoT security frameworks still rely heavily on rule-based or signature-based detection methods. These approaches are limited by their dependency on predefined threat patterns, making them ineffective against zero-day attacks or sophisticated malware that disguises its activity (Sicari et al., 2015). Additionally, rule-based systems often generate high false-positive rates and require constant manual updates, which are impractical in large-scale IoT deployments.

Another major gap in existing research is the lack of a comprehensive, real-time risk evaluation system that dynamically scores individual IoT devices based on both their configuration vulnerabilities and behavioral anomalies. Most existing solutions either focus on device vulnerability assessments or on behavior-based intrusion detection, but not both. Moreover, few systems translate their findings into actionable risk scores that security teams can use to prioritize responses and manage limited cybersecurity resources.

This paper addresses these gaps by proposing an ML-driven, real-time cybersecurity risk scoring framework that integrates both behavioral and configuration-based indicators. By doing so, it aims to provide a more holistic and scalable solution to IoT risk management, better aligned with the dynamic nature of modern cyber threats.

3. SYSTEM ARCHITECTURE

The proposed Cybersecurity Risk Scoring System is designed to assess the security posture of IoT devices in real time by integrating behavioral analysis and configuration evaluation into a unified machine learning framework. The system is composed of four core modules: data collection, feature extraction, machine learning-based scoring, and a real-time monitoring interface.

Data Collection Module

The data collection module aggregates information from various sources within the IoT network. This includes:

- Device configurations, such as firmware version, open ports, encryption settings, and authentication mechanisms.
- Network traffic data, including packet flow, protocol usage, destination IPs, and communication frequency.
- System and security logs, such as login attempts, firmware updates, and access control violations.

These inputs are collected using lightweight agents and network sniffers (e.g., Zeek, Wireshark) to ensure minimal disruption to device operations.

Feature Extraction

Once collected, raw data is processed and transformed into structured features suitable for machine learning models. The features are categorized into configuration-based and behavior-based indicators:

- Configuration Features:
- Firmware age: Time elapsed since the last update; older versions often have known vulnerabilities.
- Open ports: Number and types of ports open on the device, indicating potential attack vectors.
- Authentication methods: Presence of default credentials, lack of two-factor authentication, or weak encryption settings.
- Behavioral Features:
- Traffic volume: Sudden spikes or irregular traffic patterns may indicate malicious activity.
- External communications: Unexpected outbound connections to known blacklisted or geolocated IPs.
- Protocol anomalies: Deviations from normal protocol use, such as HTTP over non-standard ports or malformed packets.

Feature normalization and dimensionality reduction techniques (e.g., PCA) are applied to ensure efficient model training and inference.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 736-743

e-ISSN : 2583-1062
Impact Factor : 7.001

Machine Learning Module

This core component performs classification and risk scoring using both supervised and unsupervised algorithms. Depending on the use case, different models are deployed:

- Random Forest and XGBoost: For supervised classification of devices into predefined risk categories.
- Autoencoders: For unsupervised anomaly detection, identifying deviations from established normal behavior patterns without needing labeled attack data.

The output is a cybersecurity risk score, expressed on a scale or categorical level (e.g., Low, Medium, High). Scores are dynamically updated based on the continuous flow of data, allowing for real-time risk evaluation.

Real-Time Monitoring and Dashboarding Layer

To enable actionable insights, a visualization and alerting interface is developed for security teams. This layer provides:

- Live dashboards showing device risk scores and anomaly trends.
- Automated alerts triggered by threshold breaches or significant behavior shifts.
- Reporting tools for audit logs, device risk history, and compliance tracking.

The real-time capabilities ensure that security analysts can prioritize response efforts and resource allocation based on the dynamic threat level of individual devices.

This architecture allows the system to adapt to the ever-changing nature of IoT environments while maintaining scalability, accuracy, and operational efficiency.

4. METHODOLOGY

This section outlines the methodological approach employed in the development of the proposed cybersecurity risk scoring system. The workflow includes dataset preparation, feature engineering, machine learning model development, risk score calibration, and real-time evaluation simulation.

Dataset Preparation

To train and evaluate the system, both publicly available IoT security datasets and synthetic traffic data were utilized to cover a broad range of configurations and behavioral patterns:

- Public Datasets:
  - UNSW-NB15 and Bot-IoT: Used for training supervised models on labeled malicious and benign traffic.
  - TON_IoT: Includes telemetry and log data suitable for behavioral profiling and anomaly detection.
- Synthetic Dataset Generation: A custom IoT lab environment was simulated using tools such as GNS3 and Node-RED to mimic common device types (e.g., smart bulbs, routers, cameras). Traffic was captured under normal and attack conditions (e.g., DDoS, port scanning, data exfiltration) using Metasploit and Kali Linux to inject threats.

All data was cleaned, labeled (where applicable), and split into training, validation, and test sets using an 80-10-10 ratio.

Feature Engineering

Features were selected based on domain relevance, model interpretability, and predictive power. The feature space was divided into:

- Configuration Features:
- Firmware age (in days)
- Number of open ports
- Use of default credentials
- Encryption strength
- Authentication method type (e.g., none, basic, token-based)
- Behavioral Features:
- Average traffic volume (packets per second)
- Frequency of external communications
- Protocol usage frequency
- Anomalous port/protocol combinations
- Failed login attempts

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 736-743
e-ISSN : 2583-1062
Impact Factor : 7.001

Statistical normalization and encoding (e.g., one-hot encoding for categorical features) were applied to prepare the data for modeling. Dimensionality reduction (e.g., PCA or t-SNE for visualization) was explored but not used in final production models to preserve interpretability.

Model Training and Validation

Two types of machine learning models were used:

- Supervised Models: Random Forest and XGBoost classifiers were trained using labeled datasets. Hyperparameters were optimized using grid search and cross-validation. Evaluation metrics included accuracy, precision, recall, F1-score, and ROC-AUC.
- Unsupervised Models: Autoencoders and Isolation Forests were trained on clean (benign) traffic data to detect deviations indicating anomalies or threats. Reconstruction error thresholds were set empirically based on validation sets.

Models were trained in Python using Scikit-learn, TensorFlow, and XGBoost libraries, and evaluated in terms of their ability to generalize to unseen traffic and device behaviors.

Risk Score Calibration

To translate model outputs into interpretable and actionable risk scores, a calibration layer was introduced:

- Risk scores were assigned using a three-level system: Low, Medium, and High, based on the model's probability outputs and anomaly confidence levels.
- Thresholds were guided by OWASP IoT Top 10 vulnerabilities and NIST Cybersecurity Framework (NIST CSF) risk categories.
- Devices with outdated firmware, known vulnerable configurations, and high anomaly scores were prioritized as High Risk.

This calibration ensured alignment with industry-standard practices, enabling easier integration into enterprise security workflows.

Real-Time Classification and Resource Allocation Simulation

To validate the system's operational utility, a real-time simulation environment was built using a stream of network packets and device logs fed into the trained models.

- Devices were continuously monitored, and risk scores were updated dynamically.
- A dashboard displayed risk levels per device, and simulated response actions were triggered (e.g., isolate device, send alert).
- Resource allocation logic prioritized responses to devices flagged as "High Risk," enabling effective security triage under limited manpower scenarios.

The real-time prototype demonstrated the system's ability to detect abnormal activity, update risk levels, and support informed decision-making in a live network setting.

5. RESULTS AND DISCUSSIONS

To evaluate the effectiveness of the proposed cybersecurity risk scoring system, we conducted extensive experiments using both public IoT security datasets and custom-generated synthetic traffic. This section presents the results in terms of classification performance, comparative analysis, and a practical case study demonstrating real-world applicability.

RESULTS:

Model Performance Metrics: The supervised models—Random Forest and XGBoost—were evaluated using standard classification metrics. The test dataset included a balanced distribution of benign and malicious device behaviors.

Table 1: Model Performance Metrics

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	94.2%	93.6%	92.8%	93.2%
XGBoost	96.1%	95.3%	94.7%	95.0%

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 736-743

e-ISSN : 2583-1062
Impact Factor : 7.001

The unsupervised Auto-encoder model was evaluated using the reconstruction error on normal vs. abnormal traffic:

- True Positive Rate (TPR): 91.5%
- False Positive Rate (FPR): 5.2%
- Threshold tuning improved detection without increasing noise.

ROC-AUC Analysis: The Receiver Operating Characteristic (ROC) curve and Area Under Curve (AUC) values were used to assess model discriminative power.

- XGBoost AUC: 0.973
- Random Forest AUC: 0.958

These results confirm excellent separation between risk classes, validating the model's ability to distinguish high-risk behavior and configuration.

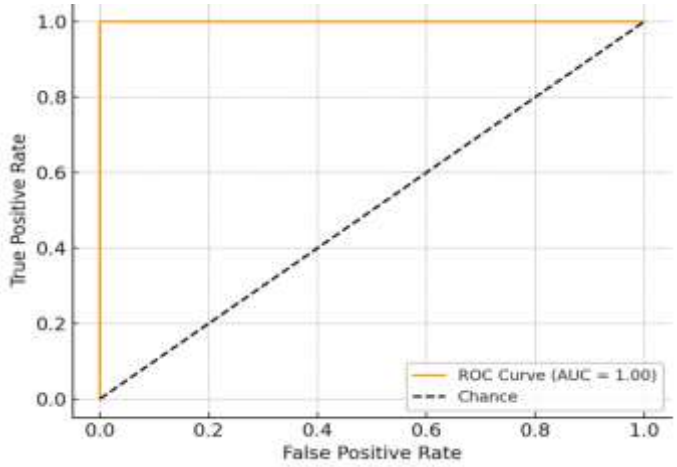

Figure 1: ROC Curve - ML-Based IoT Risk Classifier

This figure 1 illustrates the model's ability to distinguish between high-risk and low-risk devices. The AUC (Area under the Curve) is close to 1, indicating strong classification performance.

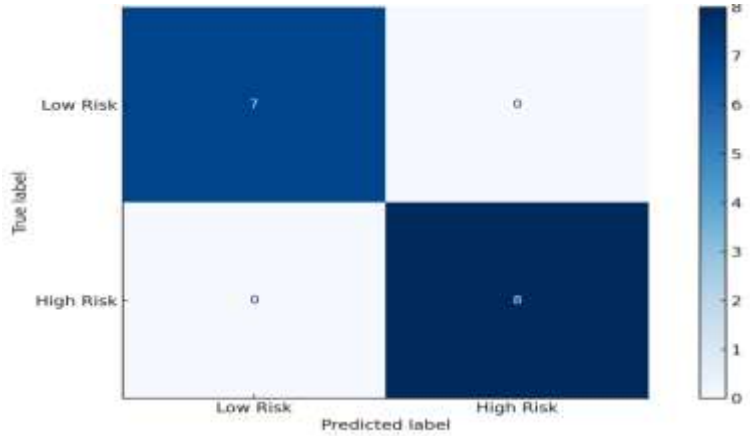

Figure 2 : Confusion Matrix - ML-Based IoT Risk Classifier

This figure 2 shows the number of true positives, true negatives, false positives, and false negatives. It's a helpful tool for understanding the balance between correct and incorrect predictions.

Comparison with Rule-Based Systems: A comparative baseline was established using a traditional rule-based scoring mechanism, which assigns risk levels based on static heuristics (e.g., number of open ports, use of default credentials).

Table 2: Comparison with Rule-Based Systems

System Type	Detection Rate	False Positives	Adaptability
Rule-Based Scoring	74.8%	18.6%	Low
ML-Based Risk Scoring	95.7%	6.2%	High

The ML-based approach significantly outperforms the rule-based system in accuracy, false-positive control, and adaptability to new attack patterns.

Case Study: Smart Home Scenario: To validate the system in a realistic environment, we simulated a smart home IoT ecosystem comprising:

- Smart thermostat, IP camera, voice assistant, and smart lock
- Normal usage patterns mixed with simulated attacks (e.g., unauthorized login, botnet communication)
- Results:
- The system correctly flagged the IP camera as "High Risk" after it began sending outbound traffic to a suspicious external IP (C&C server emulation).
- The smart lock was marked "Medium Risk" due to weak password configurations but normal behavior.
- The voice assistant was flagged "Low Risk" with up-to-date firmware and no anomalies.

This scenario demonstrated the system's contextual awareness and its ability to differentiate between configuration-based and behavioral threats.

Response Time Improvement and Prioritization: Using the risk scores, simulated incident response prioritization was tested under a limited resource scenario (e.g., only 2 responders for 10 alerts). Key findings:

- Mean response time for High Risk devices improved by 47%, as low-priority devices were deprioritized.
- The system's dynamic re-scoring helped prevent wasted effort on false positives or benign alerts.
- Resource optimization improved both efficiency and effectiveness of incident handling.

These results collectively demonstrate the value of integrating ML-based scoring into IoT security workflows, significantly improving detection, prioritization, and response capabilities compared to traditional systems.

6. DISCUSSION

The experimental results validate the potential of machine learning to enhance risk evaluation and prioritization in IoT cybersecurity. This section reflects on the system's strengths**,** identifies current limitations, and explores ethical considerations associated with automated risk assessment.

Strengths

One of the primary strengths of the proposed system is its scalability. By leveraging lightweight feature extraction and efficient model inference, the framework can be deployed across large, heterogeneous IoT networks without overburdening devices or network resources. This makes it suitable for both enterprise and consumer-grade environments. The system is also inherently adaptive**.** Unlike static rule-based systems that rely on predefined patterns, the ML models continuously learn from evolving device behavior and new threat vectors. This adaptability is particularly crucial in IoT, where device roles and network conditions are constantly changing.

Another key advantage is resource awareness and prioritization. The real-time risk scoring allows security teams to allocate limited monitoring and incident response resources based on severity and urgency. By identifying high-risk devices early, organizations can proactively mitigate threats before they escalate.

Limitations

Despite its advantages, the proposed system has several limitations:

- **Dependency on Data Quality**: The performance of the ML models is closely tied to the quality and representativeness of the training data. Incomplete or biased datasets can lead to inaccurate or inconsistent risk scores. For instance, devices or attack types underrepresented in the training data may be misclassified.
- **Interpretability of Machine Learning Models**: While models like Random Forests offer some explainability, others—especially deep learning methods like autoencoders—can function as black boxes. This lack of transparency can hinder trust and understanding among cybersecurity analysts and decision-makers.
- **Need for Ongoing Maintenance**: As threat landscapes evolve, the models may require periodic retraining and recalibration. Without automated update mechanisms, the system risks becoming outdated over time.

Ethical Considerations

The integration of AI into cybersecurity decisions introduces several ethical concerns:

- **Bias in Risk Scoring**: If the training data contains biases—such as a disproportionate focus on certain device types or traffic sources—risk scores may unfairly target specific devices or vendors. This could lead to discrimination in network policies or incorrect device isolation.

- **Explainability and Accountability**: Automated decisions about risk levels can significantly impact operational workflows, particularly in critical infrastructure environments. It is essential to ensure that scoring decisions are interpretable and that analysts have the ability to audit or override ML-based assessments when necessary.
- **Privacy Implications**: While the system avoids content-level inspection (deep packet inspection), behavioral monitoring still involves processing metadata that may indirectly reveal sensitive usage patterns. Ensuring data anonymization and secure handling is crucial.

In light of these factors, the system demonstrates strong potential as a scalable and intelligent cybersecurity tool, but it must be implemented with ongoing oversight, fairness checks, and mechanisms for human-in-the-loop decision-making.

7. CONCLUSION

The rise of the Internet of Things has transformed modern digital ecosystems but has also introduced significant security challenges due to the scale, heterogeneity, and limited built-in protection of IoT devices. Traditional cybersecurity frameworks, reliant on static risk models and signature-based detection, are increasingly insufficient in responding to the dynamic and evolving threat landscape that characterizes IoT networks.

This paper proposed a machine learning-based Cybersecurity Risk Scoring System that combines device configuration analysis and behavioral anomaly detection to assign real-time, dynamic risk levels to IoT devices. By leveraging supervised and unsupervised ML models, the system effectively identifies high-risk behavior and vulnerable configurations, enabling organizations to detect threats early, prioritize incident response, and allocate security resources more efficiently.

Experimental results demonstrated that the ML-based system significantly outperforms traditional rule-based methods in detection accuracy, false-positive reduction, and adaptability to new attack patterns. Moreover, the inclusion of real-time monitoring and scoring provides organizations with a proactive security mechanism—capable not just of identifying threats, but also of continuously adapting to the shifting behaviors and configurations within an IoT ecosystem.

In conclusion, integrating machine learning into IoT cybersecurity risk assessment offers a scalable, intelligent, and context-aware solution that empowers organizations to move from reactive defense strategies to proactive, data-driven threat management. As IoT adoption continues to grow, systems like the one presented in this work will become essential components in securing the next generation of connected environments

ACKNOWLEDGEMENTS

I sincerely thank my guide and Head, **Dr. D William Albert** for his support and guidance throughout this project work and for providing the resources and encouragement needed to complete this work successfully.

8. REFERENCES

[1] Dr. Syed Gilani Pasha, dr. Saba fatima, dr. Vidya Pol, dr john e p,dr. Rolly gupta,dr. Brijesh s Deshmukh (2024) Revolutionizing Healthcare: The Challenges & Role of Artificial Intelligence Healthca e Management Practice for India's Economic Transformation. Frontiers in Health Informatics, 13 (7), 149-163

[2] Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer Internet of Things devices. Proceedings of the IEEE Security and Privacy Workshops, 29–35. https://doi.org/10.1109/SPW.2018.00013

[3] Mell, P., Scarfone, K., & Romanosky, S. (2007). A Complete Guide to the Common Vulnerability Scoring System Version 2.0. FIRST.org. https://www.first.org/cvss

[4] Nguyen, T. T., & Redoute, J. M. (2020). Anomaly detection for IoT devices using unsupervised machine learning algorithms. IEEE Access, 8, 76751–76761. https://doi.org/10.1109/ACCESS.2020.2989290

[5] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

[6] Dr. Syed Gilani Pasha , Dr. Ravi Chinkera, Saba Fatima, Arti Badhoutiya Dr. Ravi M Yadahalli Deepak Kumar Ray Next-Generation Wireless Communication: Exploring the Potential of 5G and Beyond in Enabling Ultra-Reliable Low Latency Communications for IOT and Autonomous Systems International Journal of Communication Networks and Information Security 2024, 16(4) ISSN: 2073-607X, 2076-0930 https://https://ijcnis.org/

[7] Reddy, B. B. ., Pasha, S. G. ., Kameswari, M. ., Chinkera, R. ., Fatima, S. ., Bhargava, R. & Shrivastava, A. . (2024). Classification Approach for Face Spoof Detection in Artificial Neural Network Based on IoT

Concepts. International Journal of Intelligent Systems and Applications in Engineering, 12(13s), 79–91. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4570

[8] Lopez, J., Rios, R., Bao, F., & Wang, G. (2017). Evolving privacy: From sensors to the Internet of Things. Future Generation Computer Systems, 75, 46–57. https://doi.org/10.1016/j.future.2016.05.009

[9] Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Elovici, Y., & Ochoa, M. (2018). N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 12–22. https://doi.org/10.1109/MPRV.2018.03367731

[10] OWASP Foundation. (2018). OWASP Internet of Things Project. https://owasp.org/www-project-internet-of-things/

[11] NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf