

Detecting Cybersecurity Attacks in IoT Using AI Methods

SEMINAR

ANTONY CYRIAC THEKKEDATH

SJC22MCA-2010

Under the guidance of Mr. Anish Augustine

Associate Professor

Department of Computer Applications

SJCET, Palai

CONTENT

- ▶ **Introduction to IoT Cybersecurity**
- ▶ **Metasurvey on AI Techniques for Cybersecurity in IoT**
- ▶ **Survey Methodology**
- ▶ Major Findings Based on the Research Questions
- ▶ **Artificial Intelligence Roadmap for Detecting Cybersecurity Attacks in IoT Systems**
- ▶ **DiscussionReferences**

Introduction to IoT Cybersecurity

Overview of IoT's rapid growth and its impact on various domains.

- Increase in cybersecurity attacks across smart homes, healthcare, energy, etc.
- Transition from traditional security methods to AI-based techniques for improved protection.

Review of Studies:

- Importance of AI methods in detecting cybersecurity threats in IoT devices and networks.
- Examples of AI approaches such as DL and ML used for anomaly detection and attack prevention.
- Integration of IoT with cyber-physical systems (CPS) and Industry 4.0 for innovative applications.
- Mention of research works proposing distributed service frameworks and hybrid intelligent control approaches.
- Utilization of AI-enhanced encryption algorithms for IoT security and privacy preservation.

Recent Advances:

- Studies highlighting the role of AI in reducing human effort and improving cybersecurity in IoT.
- Introduction of ML-based cyberattack and defense strategies using reinforcement learning algorithms.
- Application of semi-supervised learning and DL methods for wireless intrusion detection in IoT.



Challenges and Limitations:

- Concerns regarding the exposure of IoT devices and networks to cybersecurity risks due to AI implementation.
- Need for scalable and distributed attack detection mechanisms to meet IoT device requirements.

Lack of comprehensive IoT security guidelines and evaluation methods.




Research Contribution:

- Formulation and analysis of research questions on AI methods for IoT cybersecurity.
- Review of empirical studies using AI techniques for threat detection in IoT.
- Classification of studies based on ML and DL algorithms, model performance, and types of threats.
- Discussion on study limitations and recommendations for future researchs.

Metasurvey on AI Techniques for Cybersecurity in IoT

- Overview of existing literature on AI-based techniques for detecting cyberattacks and anomalies in IoT.
- Emphasis on the importance of developing smart and secure IoT infrastructure.
- Utilization of AI algorithms, particularly ML and DL, for improved cybersecurity in IoT.
- Mention of studies analyzing DL models like CNN, RNN, LSTM for anomaly detection using IoT-Botnet 2020 dataset.
- Comprehensive review on AI techniques for distributed smart grids to support renewable energy integration.

- 
- Survey of ML-based solutions addressing various types of IoT security attacks.
 - Analysis of anomaly-based intrusion detection systems in IoT using DL techniques.
 - Investigation of cybersecurity models based on hardening processes to secure IoT infrastructure.

Recent Concerns are:

- Rising cybersecurity issues in IoT infrastructure highlighted.
- Critical analysis of cybersecurity issues for IoT-based critical infrastructures.

Survey Methodology

- Conducted according to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines.
- Utilized standard guidelines by Kitchenham for systematic reviews.
- Figure 2 illustrates the study screening and selection process.
- Table 2 outlines the SLR method based on the PRISMA protocol.



Research Motivations:

- Aimed to explore effective AI methods for detecting cybersecurity attacks and threats in IoT systems.
- Investigated available practices to reduce cybersecurity attacks using AI techniques.
- Provided insights into IoT security using AI for both traditional and DL techniques.

Research Questions:

- RQ1: Identification of existing cybersecurity attacks and threats in the IoT environment.
- RQ2: Examination of common AI methods employed for detecting cybersecurity attacks in the IoT.
- RQ3: Exploration of available practices to reduce cybersecurity attacks in IoT using AI approaches.

Information Sources and Database:

- Utilized SCOPUS, Science Direct, IEEE Xplore, Web of Science, ACM, and MDPI databases.
- Developed a search strategy based on PRISMA guidelines.
- Two authors assessed the article screening and selection processes.

Search Strategy and Key Terms:

- Customized search terms included variations of AI, ML, DL, cybersecurity, IoT, and detection.
- Covered articles published from database inception until 2021.
- Limited search to articles published in English.

Eligibility Criteria:

- Included original and review articles from peer-reviewed journals and conference proceedings.
- Covered articles published from January 2016 to 2021.
- Excluded non-English articles, theses, white papers, reports, and editorials.

Quality Assessment:

- Evaluated the quality and relevance of abstracts and full-text articles.
- Ensured no duplicate records and excluded non-English articles.
- Thoroughly checked the abstracts and filtered for quality and relevance.

Data Extraction:

- Utilized Microsoft Excel 2019 for data extraction.
- Extracted data included author(s), year, AI type, algorithm used, performance focus, model performance, predictive features, cybersecurity attacks, and data sources.
- Data extraction performed by two authors for accuracy and consistency.

Characteristics of the Selected Studies:

- **Yearly Distribution:** The number of studies has increased over the years, indicating growing interest in cybersecurity and IoT.
- **Journal Sources:** Studies were obtained from respected scholarly journals, including IEEE Access, IEEE Internet of Things Journal, and others.
- **Subject Areas:** Computer science had the highest percentage of studies, followed by decision science and engineering.

Classification of Selected Studies:

- ML Algorithms: SVM, SVR, DT, RF, NB classifier, LR, KNN, and fuzzy algorithms were commonly used to address cybersecurity-related issues.
- DL Algorithms: Deep autoencoders (DA), recurrent neural networks (RNN), convolutional neural networks (CNN), and others were used to detect threats in IoT systems.

Major Findings Based on the Research Questions:

- Existing Cybersecurity Attacks: Identified attacks include DoS, DDoS, ransomware, reconnaissance, and more, affecting IoT environments.
- Practices to Reduce Cybersecurity Attacks: AI approaches such as smart intrusion detection systems and anomaly detection techniques are employed to mitigate cybersecurity threats in IoT systems.



Discussion Points

- The increasing number of studies reflects the growing importance of cybersecurity in IoT.
- ML and DL algorithms play a crucial role in detecting and mitigating cybersecurity threats in IoT environments.
- Combination of AI models and updated datasets from real-world IoT systems can enhance detection techniques and performance.

Artificial Intelligence Roadmap for Detecting Cybersecurity Attacks in IoT Systems

AI for Detecting Probe Attack

Objective: Obtain data from external network sources (e.g., portsweep, IPsweep).

Methods:

- Zhang et al. [86]: Proposed an IDS model using genetic algorithm (GA) and deep belief network (DBN).
- Hybrid AI techniques (e.g., RF, Naïve Bayes, C4.5, REPTree) used for fast intrusion detection

AI for Detecting U2R Attack

- **Objective:** Gain access into systems using normal accounts (e.g., perl, xterm).
- **Methods:**
 - Bagaa et al. [88]: Introduced a novel SVM model within a security framework for mitigating U2R threats.
 - Genetic algorithm (GA) used for rule generation to detect U2R threats .

AI for Detecting R2L Attack

- Objective: Send packets to systems without legal access (e.g., xclock, guest password).
- Methods:
 - Chatterjee and Hanawal [90]: Proposed a federated learning IDS based on probabilistic hybrid ensemble classifier (PHEC) using KNN and RF.
 - GA employed for rule generation to detect R2L attacks .

AI for Detecting DoS Attack

- Objective: Disturb network traffic to make system resources busy (e.g., DDoS, UDP storm).
- Methods:
 - Various ML/DL techniques (e.g., CNN, RNN, SVM) used for detection in IoT Botnets datasets.

Discussion

- AI methods play a critical role in detecting various cybersecurity threats in IoT systems.
- Different attack types require tailored detection approaches, ranging from genetic algorithms to federated learning IDS.
- ML/DL techniques such as CNN and RNN show promise in detecting DoS attacks in IoT environments.

References

1. Singh, S.; Sheng, Q.Z.; Benkhelifa, E.; Lloret, J. Guest Editorial: Energy Management, Protocols, and Security for the NextGeneration Networks and Internet of Things. *IEEE Trans. Ind. Inform.* 2020, 16, 3515–3520. [CrossRef]
2. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. *Simul. Model. Pract. Theory* 2020, 101, 102031. [CrossRef]
3. Hong, Z.; Hong, M.; Wang, N.; Ma, Y.; Zhou, X.; Wang, W. A wearable-based posture recognition system with AI-assisted approach for healthcare IoT. *Futur. Gener. Comput. Syst.* 2022, 127, 286–296. [CrossRef]
4. Adil, M.; Khan, M.K. Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions. *Sustain. Cities Soc.* 2021, 75, 103311. [CrossRef] [PubMed]
5. Kurte, R.; Salcic, Z.; Wang, K.I.K. A Distributed Service Framework for the Internet of Things. *IEEE Trans. Ind. Inform.* 2020, 16, 4166–4176. [CrossRef]