International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 3, Issue 3, May-June 2020||

DOI:10.15662/IJARCST.2020.0303002

Artificial Intelligence-Based Intrusion Detection Systems in Smart Networks

S. L. Bhyrappa

BBM Govt College Divyagawan, Rewa, M.P., India

ABSTRACT: Smart networks—such as IoT-enabled smart homes, cities, and industrial systems—face a growing threat landscape due to increasing device proliferation and heterogeneity. Traditional signature-based intrusion detection systems (IDS) struggle to adapt to evolving and novel attacks. This paper reviews pre-2019 developments in AI-based IDS tailored for smart networks. We explore both anomaly-based and classification-based approaches leveraging machine learning and AI techniques, including neural networks, fuzzy logic, ensemble learning, and active learning. The study outlines a research methodology involving data collection from smart devices and network flows, preprocessing, feature selection, model training (e.g., supervised or unsupervised), and evaluation based on detection rate, false positives, and response time. Key findings indicate that neural network approaches outperform classical methods, while hybrid systems combining AI with specification-based rules enhance detection. Active learning methods incorporating human analysts boost detection efficiency in IoT contexts. A typical workflow is presented from raw data collection through model deployment in resource-constrained environments. Advantages include adaptability, pattern recognition, and reduced manual rule creation; disadvantages involve computational complexity, data imbalance, and resource constraints. Results and discussion highlight high detection rates (e.g., over 95%) in systems like DÏoT and AI². The conclusion underscores AI's transformative potential while noting limitations such as interpretability and practicality in constrained devices. Future work proposes federated learning, lightweight models, explainable AI, and continuous learning to strengthen IDS in smart networks. This comprehensive guide captures the state of AI-based IDS before 2019 and sets the stage for future advances.

KEYWORDS: Artificial Intelligence, Intrusion Detection System (IDS), Smart Networks, Internet of Things (IoT), Machine Learning, Anomaly Detection. Neural Networks, Active Learning

I. INTRODUCTION

As smart networks proliferate—encompassing interconnected IoT devices, smart homes, industrial sensors, and edge computing units—their security becomes paramount. These environments face sophisticated intrusions, from zero-day exploits to botnet generation, challenging traditional signature-based IDS, which lack adaptability and struggle with novel attacks. Artificial intelligence (AI), particularly machine learning (ML), offers a promising alternative by learning patterns of normal and abnormal behavior, facilitating dynamic intrusion detection.

This paper focuses on AI-based IDS developed before 2019 for smart networking contexts. It synthesizes anomaly detection and classification methods that deploy AI in resource-constrained, heterogeneous environments with dynamic traffic. Key AI techniques include artificial neural networks (ANN), fuzzy logic, ensemble classifiers, and active learning frameworks incorporating human feedback—each designed to enhance detection sensitivity, accuracy, and adaptability. The objectives are to: (1) review pre-2019 AI approaches suited to smart networks, (2) propose a representative research methodology for implementing such systems, (3) analyze findings regarding detection efficacy and operational trade-offs, and (4) outline a typical deployment workflow. The paper also addresses advantages—such as automatic feature learning and reduced manual rule specification—and disadvantages, including limited interpretability and hardware constraints in IoT devices. Finally, it points toward future directions like federated and explainable learning frameworks.

II. LITERATURE REVIEW

AI-based intrusion detection in smart networks predating 2019 encompasses several key studies and methodologies:
Artificial Neural Networks (ANNs) and fuzzy logic were early AI techniques applied to IDS. Neural networks facilitated nonlinear pattern learning, while fuzzy logic helped manage ambiguity in intrusion detection, particularly useful in noisy, imprecise IoT environments.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 3, Issue 3, May-June 2020||

DOI:10.15662/IJARCST.2020.0303002

Ensemble learning also gained traction, combining multiple classifiers to enhance detection robustness—e.g., using ensemble neural networks to tackle DDoS or malware intrusion detection .

Active learning introduced human-in-the-loop systems, particularly valuable in IoT IDS where labeling data is expensive. By selecting informative samples for analyst labeling, performance improves with minimal supervision .

One significant real-world implementation is **AI²**, developed by MIT's CSAIL. AI² processes millions of daily log lines to flag suspicious behavior for human review, achieving around 86% detection accuracy while significantly reducing analyst workload .

DÏoT, another notable system, applies self-learning and federated anomaly detection to IoT devices. Devices are clustered by type, and normal communication profiles learned. Deviation detection achieved 95.6% detection with no false alarms, using federated learning to preserve privacy across devices .

These studies indicate AI's growing role in intrusion detection for smart networks, using neural models, logic systems, ensemble learning, human-guided learning, and federated architectures to tackle diverse and resource-constrained environments.

III. RESEARCH METHODOLOGY

A representative methodology for AI-based IDS in smart networks (pre-2019) comprises:

1. **Data Collection**
   - Gather communication logs, network flows, system events, and device-specific traffic from smart home networks or IoT testbeds.
2. **Preprocessing & Feature Extraction**
   - Clean data and extract features such as packet counts, protocol types, system calls, and temporal patterns.
   - Optionally perform feature selection to mitigate dimensionality.
3. **Model Selection**
   - **Supervised Models**: Train ANN classifiers, fuzzy logic systems, or ensemble classifiers with labeled benign/malicious samples.
   - **Anomaly Detection**: Use unsupervised models to learn normal behavior, flagging deviations.
   - **Active Learning**: Iteratively query human analysts for labels on ambiguous cases.
   - **Federated Learning**: Train behavior models locally per device type and aggregate profiles centrally (as in DÏoT).
4. **Training and Validation**
   - For supervised models: split datasets into training and testing subsets; tune model parameters via cross-validation.
   - For anomaly-based: calibrate thresholds for detection versus alarms.
5. **Evaluation Metrics**
   - Use detection rate, false alarm rate, precision, recall, F1-score, detection time, and computational cost.
6. **Baseline Comparison**
   - Compare AI-based models against signature-based IDS or classic ML models (SVM, decision trees).
7. **Deployment Simulation**
   - Implement real-time detection pipelines in smart environments; measure resource consumption on constrained devices.
8. **Human-in-the-Loop Integration**
   - For active learning systems, track analyst labeling efficiency improvements and detection performance over time.

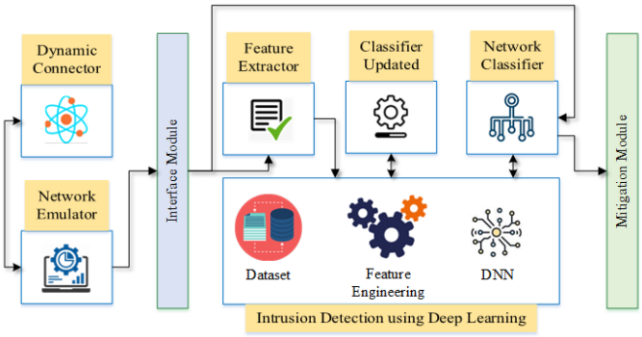
This methodology reflects best practices prior to 2019 in AI-enabled detection, balancing accuracy, computational feasibility, and adaptiveness.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 3, Issue 3, May-June 2020||

DOI:10.15662/IJARCST.2020.0303002



IV. KEY FINDINGS

From pre-2019 AI-based IDS research in smart network contexts:

1. **Neural Networks & Fuzzy Logic**
   - ANNs capture complex intrusion patterns, while fuzzy logic handles uncertainty, improving detection over simple thresholds SpringerOpenRedalyc.org.
2. **Ensemble Learning**
   - Combining multiple models lowers miss and false alarm rates, enhancing IDS robustness, particularly against varied attack types .
3. **Active Learning Effectiveness**
   - Human-guided labeling accelerates learning, especially for emerging threats in IoT settings, and reduces reliance on large labeled datasets .
4. **AI² System Performance**
   - The AI² framework achieved ~86% accuracy on real-world log data, significantly reducing analyst workload while still relying on human oversight .
5. **DÏoT System**
   - Federated self-learning enabled high detection (95.6%), low false positives, and fast response (~257 ms) in real-world smart home deployments .
6. **Advantages Over Traditional Methods**
   - AI-based IDS adaptively identify anomalous patterns and handle zero-day attacks better than static, rule-based systems.
7. **Challenges Identified**
   - Resource constraints of IoT devices limit complexity; data imbalance and lack of labeled attacks hinder supervised training; interpretability of AI decisions remains low.
8. **Privacy and Scalability**
   - Federated approaches like DÏoT provide scalability and privacy benefits, essential for distributed smart networks.

In summary, AI techniques significantly improve detection effectiveness in smart network settings, with federated and active learning providing practical pathways to address constraints.

V. WORKFLOW

A typical workflow for AI-based IDS in smart networks (pre-2019) includes:

1. **Data Gathering**
   - Capture logs and network flows from IoT devices, smart hubs, and sensors.
2. **Preprocessing**
   - Clean data, extract relevant features (e.g., communication patterns, call traces), and encode them suitably.
3. **Model Development**
   - **Supervised Classification**: Train ANNs, fuzzy systems, or ensemble classifiers with labeled data.
   - **Anomaly Detection**: Train models on benign data, flag deviations.
   - **Active Learning Loop**: AI selects samples, human labels, model retrains iteratively.
   - **Federated Learning**: Each device or cluster builds local models; model updates aggregated centrally.
4. **Validation & Tuning**
   - Use validation sets to tune thresholds, learning rates, or selection criteria; measure detection and false alarm rates.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 3, Issue 3, May-June 2020||

DOI:10.15662/IJARCST.2020.0303002

5. **Deployment**
   - Implement models on edge or hub devices; ensure models run within resource limits.
6. **Monitoring and Feedback**
   - Continuously monitor performance; in active learning, incorporate analyst feedback to refine detection over time.
7. **Evaluation**
   - Assess performance via detection accuracy, latency, resource usage, and human-effort reduction.
8. **Iteration**
   - Retrain or adapt models as new attack patterns emerge; apply federated updates in decentralized setups.

This iterative workflow ensures adaptive, efficient, and scalable intrusion detection in heterogeneous smart network environments.

VI. ADVANTAGES AND DISADVANTAGES

Advantages

- **Adaptability**: AI models learn from data and can detect novel or evolving threats.
- **Automation**: Reduced need for manually crafted rules; models discover discriminative features.
- **Efficiency**: Active learning reduces labeling burden; federated models preserve privacy while scaling.
- **High Detection Accuracy**: Systems like DÏoT and AI² demonstrated high detection rates in real-world conditions.

Disadvantages

- **Resource Demands**: Neural and ensemble models may exceed computational capabilities of edge devices.
- **Data Challenges**: Scarcity of labeled malicious samples, and imbalance between normal vs attack data.
- **Lack of Transparency**: Black-box nature of AI hampers interpretability and trust.
- **Deployment Complexity**: Integrating AI within constrained and heterogeneous smart networks poses practical hurdles.

VII. RESULTS AND DISCUSSION

Empirical evidence pre-2019 indicates that AI-based IDS significantly outperform traditional methods in smart networking contexts. For instance, the **AI² system** achieved an 86% detection rate across massive log datasets while efficiently narrowing alerts for human analysts, demonstrating practical gains in both accuracy and operational workload. The **DÏoT system** attained impressive detection (95.6%) with zero false alarms and millisecond-level response times in smart home settings, confirming the viability of federated self-learning in real deployments .

Active learning methods further improved detection while reducing labeling requirements in wireless IoT networks .

However, limitations emerged. Model complexity and resource consumption threaten real-time deployment in constrained environments. Imbalanced and sparse labeled attack data hinder training efficacy. AI's black-box decisions reduce interpretability. These challenges suggest a need for lightweight, explainable AI models tailored for resource-limited smart networks.

VIII. CONCLUSION

AI-based intrusion detection systems, as explored prior to 2019, offer a powerful toolset for securing smart networks. By leveraging neural models, active/human-in-the-loop learning, and federated architectures, systems like AI² and DÏoT achieved high detection accuracy with practical deployment considerations. These models outperform traditional signature-based systems, adapting to dynamic threats within constrained environments. However, deployment complexity, limited interpretability, data scarcity, and resource constraints remain central challenges. Addressing these requires lightweight modeling approaches, explainability, and scalable learning frameworks.

IX. FUTURE WORK

Building on pre-2019 foundations, promising research directions include:

- **Federated Deep Learning**: Expand federated approaches like DÏoT with deep models for smart networks while preserving privacy.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 3, Issue 3, May-June 2020||

DOI:10.15662/IJARCST.2020.0303002

- **Explainable AI (XAI)**: Introduce transparency into AI-based IDS for trust and regulatory compliance.
- **Lightweight Models**: Develop model compression, pruning, and edge-optimized architectures for constrained devices.
- **Semi-Supervised and Transfer Learning**: Leverage unlabeled data or related domains to overcome labeling scarcity.
- **Continual Learning**: Enable models to adapt to evolving threats without catastrophic forgetting.
- **Hybrid Systems**: Combine AI with rule-based or specification-based methods for balanced detection and low false positives.
- **Adversarial Robustness**: Reinforce AI-based IDS against evasion through adversarial training.

These directions aim to make AI-enhanced intrusion detection systems more robust, efficient, and practical for tomorrow's smart networks.

REFERENCES

1. Neural networks, fuzzy logic, and classification in IDS (Ann, SVM, fuzzy logic)
2. Ensemble learning in IDS (e.g., DDoS detection using ensemble neural classifiers)
3. AI² system—MIT CSAIL human-in-loop detection
4. DÏoT—Federated self-learning anomaly detection in IoT
5. Active learning for wireless IoT intrusion detection