DOI: 10.5748/20CONTECSI/PSE/SEC/7233

eLocator: e207233

ENHANCING CYBERSECURITY IN SMART HOMES: A SYSTEMATIC REVIEW OF AIDRIVEN TRENDS AND CHALLENGES

Mauro Cesar Dos Santos Leite – https://orcid.org/0000-0003-0264-403X
Instituto De Pesquisas Tecnológicas - Ipt

Adriano Galindo Leal – https://orcid.org/0000-0001-7114-6830
Instituto De Pesquisas Tecnológicas - Ipt

Otavio Kiyatake Nicesio – https://orcid.org/0000-0002-3975-1261
Instituto De Pesquisas Tecnológicas - Ipt

ENHANCING CYBERSECURITY IN SMART HOMES: A SYSTEMATIC REVIEW OF AI-DRIVEN TRENDS AND CHALLENGES

ABSTRACT

The onset of the COVID-19 pandemic has accelerated the adoption of digital solutions and smart devices, fundamentally altering daily activities like online shopping, e-government services, and home automation. This transition, while beneficial, has introduced new cybersecurity challenges, particularly in the domestic environment where smart home technologies are prevalent. Previously, severe internet connectivity vulnerabilities were a concern for large corporations and internet-based businesses. However, the scenario has shifted dramatically with the ubiquitous use of smart devices, leading to heightened vulnerabilities due to inadequate security measures in these devices and the complex architecture of modern digital ecosystems.

This systematic literature review addresses the critical role of Artificial Intelligence (AI) in enhancing cybersecurity measures within smart home environments. It aims to demonstrate the efficacy of existing AI-based cybersecurity frameworks in detecting, preventing, and precisely responding to intrusion attempts in smart homes. By examining various frameworks and their methodologies, this study highlights the evolution and effectiveness of AI applications in mitigating cyber threats in residential settings. The review not only underscores the advancements in the field but also identifies existing gaps and proposes directions for future research. Through this comprehensive analysis, the Paper contributes to understanding AI's potential to fortifyCybersecurity in smart homes, an area of increasing importance in the current digital age.

Keywords: Artificial Intelligence, Cybersecurity, Smart Home, Digital Transformation, Vulnerability Assessment.

I. INTRODUCTION

The need to rely on artificial intelligence as an ally against cyber threats stems from the increased use of intelligent devices without any control within the residential and domestic environment. As stated by (Bordel, Alcarria, Robles, & Sánchez-Picot, 2018), home automation was restricted to technology enthusiasts, and the security concern was zero as there were no cyber threats. Still, when we look at the present day, this is no longer the case.

This increase in the use of devices brings an increase in data generation. The inhabitants can benefit from this situation by adopting solutions with artificial intelligence, whereby, by learning their behaviors, AI can detect threats by identifying unusual situations, improving the protection and monitoring of the environment (Singhal, Som, & Ahuja, 2021).

One of the obstacles in cyber threat mitigation is the low computational capacity of intelligent devices, such as memory, energy, and other resources, to perform the complete analysis in situ (Soltani, Rahmani, Bohlouli, & Hosseinzadeh, 2022).

Even if there were an increase in computational power, it would not solve the security problem, as they would act in isolation. This fact is highlighted by (Alzahrani & Alsaade, 2022), where a single compromised device can affect the entire network, being the gateway to attacks such as DDoS (denial of service), ransomware, and packet forwarding, among many others, violating the inhabitants' privacy. They also reinforce that even the use of a security system in Smart Homes would not be enough as it would depend a lot on the skill and technical knowledge of the administrator, and even then, it would only be possible to foresee some situations.

From these reflections, one of the biggest challenges of Cybersecurity in intelligent environments is clear: the detection and prevention of intrusions in the various connected devices and with unstructured data. This is the biggest challenge due to the complexity of the network structure, the absence of a controlled environment, the diversity of directly or indirectly connected devices, the massive flow of data generated, and the impact on performance in processing devices and current software solutions. (Heartfield R. , et al., 2018).

According to (Bordel, Alcarria, Robles, & Sánchez-Picot, 2018), Ambient Intelligence (AmI) is susceptible to a new type of attack, i.e., attacks on Cyber-Physical Systems (CPS), which, from the logical environment, interfere directly with the physical environment. Therefore, a way to prevent and mitigate this type of attack is essential to ensure Smart Home residents' security against malicious actors. Since 2008, the number of studies seeking a solution to this problem has consistently increased yearly, as noted by (Wiafe, et al., 2020).

Within this context, the following research question will be answered: Are intrusion detection and prevention models capable of autonomously ensuring the Cybersecurity of Smart Homes?

This Paper is organized into the following sections: primary literature on cyber threats and the application of AI for Cybersecurity in Smart Homes in Section 2. Section 3 presents the methodology of the systematic literature review. The results and discussion of the solutions described in this review are conducted in section 4, while section 5 presents the conclusions of this study.

We gratefully acknowledge the financial support from"There."

II.BACKGROUND LITERATURE

A.AI and Cybersecurity

Constructing our reasoning from the fundamentals: An algorithm is a well-defined computational procedure that inputs a value or set of values and produces an output value or set of values (Cormen, Leiserson, Rivest, & Stein, 2009). An algorithm is a step-by-step procedure for performing a task with a finite set of inputs and outputs and is guaranteed to terminate after a limited number of steps. Algorithms are used in various fields, including computer science, mathematics, and engineering, to solve problems and perform tasks efficiently and accurately. Machine learning algorithms are a type of algorithm that allows a computer to learn and adapt to new data without being explicitly programmed. These algorithms are trained using substantial amounts of data and statistical techniques and can be used to make predictions, classify data, and perform other tasks(Géron, 2019).

Thus, there are three significant ways in which machine learning algorithms can be used in Cybersecurity, including:

- Intrusion detection: Machine learning algorithms can be used to identify and prevent unauthorized access to a computer system or network. These algorithms can analyze network traffic, system logs, and user activity to identify patterns or anomalies indicating an attempted intrusion (Soltani, Rahmani, Bohlouli, & Hosseinzadeh, 2022).
- Malware detection: Machine learning algorithms can be used to identify and classify malware, such as viruses and ransomware, based on patterns in the code or behavior of the malware. These algorithms can be trained on a dataset of known malware to recognize a previously unseen(Wiafe, et al., 2020).
- Phishing detection: Machine learning algorithms can identify and prevent phishing attacks, which are fraudulent attempts to obtain sensitive information, such as login credentials or financial information, by disguising it as a legitimate entity. These algorithms can analyze emails and websites to identify patterns indicating a phishing attempt (Alzahrani & Alsaade, 2022).

Overall, using machine learning algorithms in Cybersecurity can help improve the effectiveness and efficiency of security systems by automating the detection and prevention of threats (Halder & Ozdemir, 2018). However, it is essential to ensure that these algorithms are trained on a diverse and representative dataset to avoid biases and ensure accurate performance.

B.Cybersecurity for Smart Homes

Cyberattacks occur constantly and daily, as observed in several tools made available by cyber security companies like Kaspersky, NetSol, and CheckPoint.

These attacks have been increasing yearly and are related to the increase in devices connected to the internet due to the adoption of the remote work culture and the popularization of intelligent devices for the home environment. This environment contributes to the concentration of attacks directed at Smart Homes precisely because of the low or complete lack of cybersecurity layers. Also, several of those Smart Devices force weak passwords in Wi-Fi Networks since they can only work with letters and numbers, not allowing the full range of special characters.

Residents and owners of Smart Homes live under diverse types of threats in the current scenario, as shown in the following examples:

- Damage to the devices: Changes in the sensors' configurations may lead to overload or uselessness.
- Denial of service: Unavailability in data collection and transfer that causes service errors or total failure.
- Theft of information: Attackers gain possession of data transmitted in the environment and may use this information illicitly. (Mitre Att&ck. Link: https://attack.mitre.org/).

In some cases, the risks can go beyond technological damage, expanding into personal life and affecting their relationships, physical and psychological health, and finances.

III.SYSTEMATIC LITERATURE REVIEW METHODOLOGY

Following a methodology described by (Kitchenham & Charters, 2007), the present study proposes a systematic literature review on the state-of-the-art algorithms and techniques applied in cybersecurity frameworks that focus on behavioral learning for intelligent homes. These solutions learn the standard behavior of smart devices in the environment. Considering savvy home residents' routines, any anomaly within the expected behavior is promptly detected by the AI-enhanced system responsible for monitoring, and protective measures are then taken autonomously.

The methodology divides the systematic literature review into planning, conduction, and synthesis phases. The planning phase was divided into twelve stages described in this section.

A. Research Objective

To build a systematic review that presents current promising frameworks and their integration with the protocols used in smart home devices.

B. Research Question

Are there intrusion detection and prevention models capable of autonomously ensuring the Cybersecurity of Smart Homes?

The research question was decomposed using the PICO framework (Kitchenham & Charters, 2007).

- Population (P): Research in Cybersecurity for Intelligent Homes.
- Intervention (I): Frameworks or techniques for detecting and preventing cyber threats.
- Control (C): List of references obtained through exploratory research on the topic, serving as a basis for the selection of keywords and sources, such as (Chong,

Sandberg, & Teixeira, 2019) and (Heartfield R. , Loukas, Bezemskij, & Panaousis, 2021).

- Results (O): Security against cyber threats in the domestic environment.

C. Database Selection Criteria

The bases used were chosen because of their worldwide recognition and for including the leading papers and journals in AI for Cybersecurity (Table 1).

Tabela 1 - Database List

Database	Web Address
ACM *DigitalLibrary*	dl.acm.org/
IEEE *Xplore*	ieeexplore.ieee.org/xplore/
Scopus *DigitalLibrary*	www.scopus.com/
ISI Web of Science	www.webofscience.com/

D. Query String

framework AND Cybersecurity AND artificial intelligence AND smart home

E. Inclusion Criteria:

- I1) Papers or study materials available in full text demonstrate cybersecurity frameworks applied to smart homes.
- I2) Studies focusing on threat detection and prevention in intelligent home environments.

F. Exclusion Criteria:

- E1) Study materials in languages other than English.
- E2) Model accuracy less than 90%.
- E3) Materials unrelated to residents' behavioral learning for risk prevention.
- E4) Materials that have no applicability in intelligent homes.
- E5) Duplicate studies.

G. Studies Search Strategy

The automatic string search method was used for the metadata in the four chosen databases, restricting the year of publication to 2018-2022.

H. Studies Selection Strategy

The evaluations were conducted in 3 stages:

- 1st Stage: Reading the papers' metadata identified by the initial search in the selected databases.
- 2nd Stage: Reading the introduction and conclusion of the papers included in the 1st Phase. The included papers were documented for the third evaluation phase.
- 3rd Stage: Full-text reading of the papers included in the 2nd Phase. A final list was generated with the papers for the Synthesis of the Systematic Literature Review.

I. Data Extraction and Synthesis Strategy

We extracted and synthesized the following data from the papers:

- Description of the framework recommended by the study.
- Threats and Vulnerabilities presented.
- Machine learning model used in the framework.
- Results and conclusions of the study.
- Summary of studies according to the extracted data.

J. Data Analysis Strategy and Results

We used the following strategy for displaying and analyzing the results:

- Comparative summary of the frameworks found.
- Answer the research question with the extracted data.

IV.SYSTEMATIC LITERATURE REVIEW RESULTS

A. Conduction of the Systematic Literature Review

The systematic review conduction occurred in November 2022. The three stages of the conduction were summarized as follows:

In the first stage, we identified keywords in specific areas of the 200 or so papers located in the databases. These stepsincluded reading the Paper's Title, Abstract, and Keywords.

The next step consisted of reading the Introduction and Conclusion of the papers that passed the first stage and contained the searched keywords.

The selection criteria sought to help answer the research question, which is to identify the applicability of AI in the domestic environment, so we observe criteria such as accuracy, practical tests conducted in domestic settings, focus on threat detection and prevention, learning from the routine and behaviors of the inhabitants.

We arrived at the papers that met the research requirements in the third and final stage. In this way, we started with a complete and thorough reading to investigate how the frameworks presented by the authors behave in natural environments.

Figure 1 - Studies Selected in the Synthesis of the Systematic Review

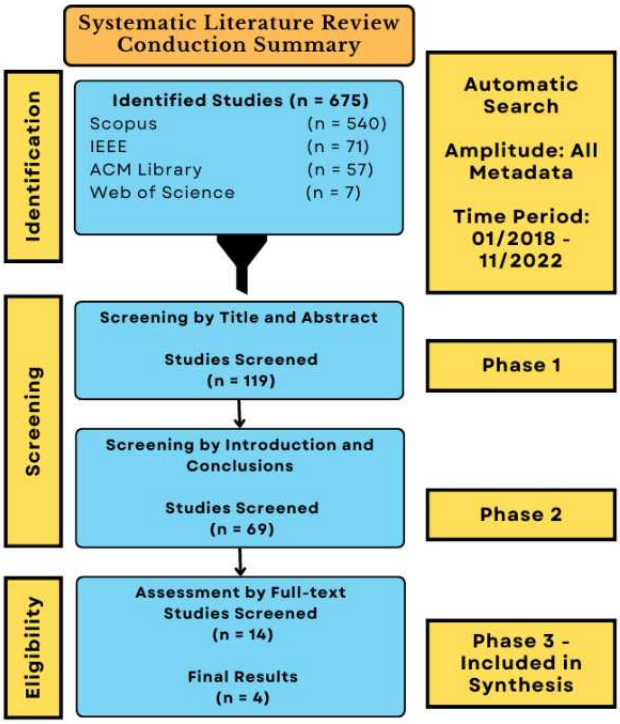

Figure 2 - Results of the Systematic Literature Review Conduction (the complete version with previous phases is available online)

#	Title	Author	Year	Selection Criteria	Status
1	Aegis+: A Context-aware Platform-independent Security Framework for Smart Home Systems (Sikder, Babun, & Uluagac, 2021)	Sikder et al.	2021	I1	Accepted
2	Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning (Heartfield R. , Loukas, Bezemskij, & Panaousis, 2021)	Heartfield et al.	2021	I2	Accepted
3	Jarvis: Moving Towards a Smarter Internet of Things (Mudgerikar & Bertino, 2020)	Mudgerikar and Bertino	2020	I1	Accepted
4	Haunted House: Physical Smart Home Event	Birnbach et al.	2022	I1	Accepted

	Verification in the Presence of Compromised Sensors (Birnbach, Eberz, & Martinovic, 2022)				

B.Synthesis of the Systematic Literature Review

Before discussing the articles that met the research criteria, the works selected up to phase 3 are worth mentioning. Even though they do not meet all the eligibility criteria, they demonstrate potential for evolution, making it possible to apply them in Cybersecurity in domestic environments and leading to reflection on new possibilities for the field of research.

Paper (Iwendi, Rehman, Javed, Khan, & Srivastava, 2021),

Synthesis: The model seeks to improve threat detection (Port Scanning, HTTP and SSH Brute Force, and Synchronize (SYN) Flood attacks) given the presence of sensors and smart devices in a specific product or environment.

Features: The study is focused on preventing DDoS attacks but presents conditions to mitigate other threats.

ML Model: Long Short-Term Networks (LSTM) classifier

Threats and Vulnerabilities detected or mitigated: Port Scanning, HTTP and SSH Brute Force, and Synchronize (SYN) Flood attacks.

Study Results and Conclusions: The study seeks to show that during tests in a controlled environment, the results are promising and superior to other methods. The next step is to scale the research and simulate real-life situations of smart cities, using the Croncolic test algorithm for real-time analysis and exploring the use of blockchain.

Paper (Spanos, et al., 2020),

Synthesis: The methodology aims to use the implementation of an IDS in the so-called edge computing.

Features: The methodology leverages the combination of machine learning, time series, and statistical techniques, and the results obtained will be used for an ECHO cross-sector prototype using the GHOST defense infrastructure.

ML Model: The methodology combines statistical and machine learning methods, such as the Principal Components Analysis (PCA) and the Clustering.

Threats and Vulnerabilities detected or mitigated: Simulations of physical access attacks to capture the impact on network behavior.

Study Results and Conclusions: Despite reasonable accuracy rates, the number of devices on which the tests are performed is low compared to the highlighted materials.

Paper (Diallo & Patras, 2021),

Synthesis: This Paper proposes a new intrusion detection method based on adaptive clustering (ACID) that can be deployed at the network edge with a 20-year dataset.

Features: The Adaptive Clustering Intrusion Detection System (ACID) incorporates an original neural model based on multiple kernels that allows it to generalize well regardless of any minor changes incurred by small groups of packets or the unbalanced nature of the training dataset.

ML Model: Adaptive Clustering (AC).

Threats and Vulnerabilities detected or mitigated: bfssh, DDoS, HttpDoS, Infiltration.

Study Results and Conclusions: The research presents consistent numbers if you consider the size of the databases used and the different metrics used to validate the effectiveness, but I felt a lack of results in the field.

Paper (Moustafa, Turnbull, & Choo, 2019),

Synthesis: The authors propose new features based on network packet flows, MQTT, DNS, and HTTP information to identify malicious activities that exploit IoT applications within these protocols.
Features: They assess the impact of these features using statistical and machine learning techniques on various datasets, including the UNSW-NB15 and NIMS botnet datasets.
ML Model: Decision Tree, Naive Bayes, and Neural Network.
Threats and Vulnerabilities detected or mitigated: Backdoor, DoS, Exploit, Fuzzers, Worm, and Reconnaissance.
Study Results and Conclusions: The methodology presented superior results and demonstrated, with clear graphs and well-defined metrics, the behavior of malicious traffic from the analyzed network protocols. However, it is left out of the results because it still does not present tests in real situations with the impact of human actions.

Paper (Al-Hawawreh, Moustafa, Garg, & Hossain, 2021).
Synthesis: Threat Intelligence (TI) has become a powerful security technique to understand cyberattacks using artificial intelligence models that can automatically protect SAGS networks.
Features: The proposed method contains three modules: a deep pattern extractor, IT-driven detection, and an IT attack-type identification technique.
ML Model: Deep sparse auto-encoder, Gated Recurrent Neural Network (GRNN), and Deep GRNN.
Threats and Vulnerabilities detected or mitigated: Denial of Service (DoS), wormhole, and bluejacking are some examples.
Study Results and Conclusions: In the tests presented, data processing may be delayed, and the existing base may not be sufficient due to the recent use of IoT devices. There is also the fact that the method has not been applied in an actual situation.

Paper (Protogerou, et al., 2022),
Synthesis: The proposed system is a robust and user-friendly platform that can detect and mitigate cybersecurity threats in IoT networks. The platform is based on AI and uses algorithms to monitor the network, detect anomalies, and generate mitigation strategies.
Features: The system also includes visualization and analysis capabilities to help security operators understand network status and make informed decisions.
ML Model: graph neural network (GNN).
Threats and Vulnerabilities detected or mitigated: DoS, UDP Flood, and port scanning.
Study Results and Conclusions: The article mentions that the framework was evaluated in real situations but does not make the scenarios clear, specifically in the context of smart homes, the objective of this research, but reinforces that it can be applied in different situations.

Paper (Wan, Xu, Wang, & Xue, 2022),
Synthesis: The IoTMosaic system can infer different user activities from IoT network traffic in smart homes.
Features: Recognizes and generates user activity signatures, characterizing each user activity with an ordered sequence of IoT device events.
ML Model: The article does not highlight the use of an ML.
Threats and Vulnerabilities detected or mitigated: Detection of physical threats such as open locks and fire.
Study Results and Conclusions: The system presents superior resultsin identifyingabnormal behaviors based on the residents' activities, making it possible to improve its use in determining cyber threats.

Paper (Khamesi, Shin, & Silvestri, 2020),

Synthesis: The article discusses the importance of considering user behavior when applying ML in intelligent environments. Results show that this can significantly improve accuracy and reduce model training time.
Features: Recognition of appliances from smart plugs and use of the user's legitimate voice as a security layer. From this approach, they achieved an increase of up to 55.38% in anomaly detection accuracy and a reduction in the training period.
ML Model: stream-based active learning (SAL), Random Sampling (RS), and User Aware Sampling (UAS).
Threats and Vulnerabilities detected or mitigated: Not shown.
Study Results and Conclusions: The study demonstrates that machine learning has better chances of results when it focuses on the user interacting with the Cyber-Physical environment; that is, it is an approach focused on the user itself and not on patterns of network behavior, for example.

Papers (Siddharthan, Deepa, & Chandhar, 2022)(Vaccari, Chiola, Aiello, Mongelli, & Cambiaso, 2020),
Synthesis: Experimental analysis using a lightweight Message Queue Telemetry Transport (MQTT) protocol.
Features: Evaluation of datasets using ML algorithms.
ML Model: Logistic Regression, K-Nearest Neighbor, Random Forest, Naive Bias, Support Vector Machine, Gradient Boosting, Neural Network, Multilayer perceptron, and Decision Tree.
Threats and Vulnerabilities detected or mitigated: DoS, MQTT Publish flood, SlowITe, malformed data, brute force authentication.
Study Results and Conclusions: The study is limited to a single protocol, which reduces its effectiveness in an environment with diverse devices and multiple protocols working.

Based on the eligibility criteria, the articles presented below demonstrate satisfactory results for protection and safety in domestic environments.

Paper (Sikder, Babun, & Uluagac, 2021)
Synthesis: Demonstrates how Aegis+ correlates the residents' actions with the events that occurred with smart devices in the smart home environment (SHS), thus performing the training and learning of the patterns.
Features: it has an architecture composed of an event logging system, a log parser, a security policy learning model, an intelligent reward function, a reinforcement learning environment, an optimizer, and a model of practical DL.
ML Model: uses Markov Chain to train the context matrices generated in the second module to detect anomalous and malicious activities.
Threats and Vulnerabilities detected or mitigated: Fake Data Injection, Side Channel Attack, Impersonation Attack, Denial of Service, Malicious Application Injection.
Study Results and Conclusions: The study demonstrated an accuracy above 95% when correlating the device events with the behavior of the residents in different scenarios and types of layouts of the domestic environment without impairing or overloading the performance of the devices.

Paper (Heartfield R. , Loukas, Bezemskij, & Panaousis, 2021)
Synthesis: MAGPIE proposes a framework adaptable to the characteristics of each smart home and its inhabitants. It first collects all the events of the devices and starts to classify them. In the second stage, it performs reinforcement learning, adapting to different scenarios and characteristics.
Features: MAGPIE was designed to operate in 3 phases, described as the collection, where it captures and decodes data from physical or cybernetic means. Moving on to the

transcription stage, MAGPIE uses metadata because it is more consistent, regardless of the environment, and represents greater privacy security. Finally, there is the reasoning phase, where the learning techniques are applied, and the solution for the analyzed events is presented.
ML Model: In the first learning block, events are collected individually from each device and are classified as normal or abnormal. The second block is an adaptation based on reinforcement learning. It is assumed that no smart home is the same as another, and each has particularities, whether of devices or residents' habits.
Threats and Vulnerabilities detected or mitigated: Denial attacks, spoofing, malware injection, device compromise, and automation.
Study Results and Conclusions: The study proved that there are changes in the accuracy rates when there is a human presence in the environment and demonstrated the differences and advantages when using two reinforcement learning methods. Even so, the accuracy rates were below those of the other studies surveyed. Still, the work presents good possibilities for evolution, and the material is made available by the researchers on GitHub for anyone who wants to contribute to the research.

Paper (Mudgerikar & Bertino, 2020)
Synthesis: Features a framework called Jarvis, based on reinforcement learning for IoT environments. Jarvis was instantiated in a smart home environment to evaluate its performance using actual and simulated data.
Features: it has an architecture composed of an event logging system, a log parser, a security policy learning model, an intelligent reward function, a reinforcement learning environment, an optimizer, and a model of practical DL.
ML Model: It uses a Deep-Q reinforcement learning network model to determine the highest-quality actions for each environment state, performing agent training with a deep neural network (DNN).
Threats and Vulnerabilities detected or mitigated: T/A (trigger-action) security violations, integrity or access control violations, general security, conflicting actions, security violations by malicious applications, and insider attacks.
Study Results and Conclusions: Jarvis detected 100% of manually created security breaches in the study and correctly filtered out 99.2% of benign user-defined anomalies and malfunctioning security breaches.

Paper (Birnbach, Eberz, & Martinovic, 2022)
Synthesis: Peeves is a system capable of learning the behavior of the inhabitants of a smart home by collecting data from smart devices when they interact with them and through sensors spread throughout the house that identify everyday events.
Features: Data collection is done through sensors and smart devices in the experiment presented. After that, the data is labeled, thus receiving identifications based on the time point in which they were recorded. Next, the division of the dataset for the development, training, and testing of the framework is done.
ML Model: two decision-making processes were used and compared. The first process was a monolithic classifier, and the second was a set of classifiers trained on individual sensors. For both processes, a binary linear support machine (SVM) was used as a classifier.
Threats and Vulnerabilities detected or mitigated: spoofing attacks, masking, opportunistic attackers spoofing events, sensor compromise.
Study Results and Conclusions: The experiments showed accuracy rates greater than 90% in each attack case evaluated. It was also found that using a single data classifier compromises the accuracy of the detections, and having another set of classifiers strengthens the results.

V.DISCUSSION

Our RSL showed that the number of papers on using Artificial Intelligence to detect and prevent intrusions has increased since 2018. This result is consistent with the need for modern society to address Cybersecurity seriously in smart devices.
Nonetheless, we realize as we advance in research and apply the criteria to analyze the applicability of AI in everyday life deeply that there are still many technical and cultural issues to be resolved before it can be said that we can make effective use of AI, especially in the context of smart homes, where little research focused on this environment has been noticed.
The work by (Heartfield R. , Loukas, Bezemskij, & Panaousis, 2021) presents an issue that should be considered in smart homes: human inference in the environment and the machine learning model that adapts to the conditions of the domestic scenario. Among the researched papers, this is the one that is in the most embryonic Phase and presented lower accuracy rates than what this research proposed. However, they consistently identify that more than one learning method is required, using a second technique that reinforces the system's precision and concludes that each environment is unique. It is not possible to replicate the same configurations.
Aegis+, by(Sikder, Babun, & Uluagac, 2021), presents a solution for human inference in the domestic environment by creating event signatures. These events are stored in matrices, where the Markov chain technique is applied to identify abnormal patterns. Through its operating method, the framework collects various events, classifies them in matrices, analyzes and decides based on the results, and then meets the need to correlate the events of the domestic environment with the actions of its inhabitants and the interaction between them and the various devices installed.
Following the same line, Peeves (Birnbach, Eberz, & Martinovic, 2022) relates the events generated by the sensors with the users' habits, thus identifying attackers based on anomalous usage signatures. This same association is made in Jarvis by (Mudgerikar & Bertino, 2020), both at distinct stages of the learning process. However, Peeves differs from the others by highlighting and solving ethical problems that can arise with this framework category, as these systems can, theoretically, monitor user behavior (door sensors, for example, tracking user movement). For a microphone, for instance, only sound level data is recorded.
Regarding the algorithm model, Jarvis differs by using a reinforcement learning strategy, determining an optimal state for each possible smart home environment to be mapped.

VI.CONCLUSIONS AND FUTURE WORK

Our exploration into the application of Artificial Intelligence (AI) in Cybersecurity, specifically within the smart home domain, has revealed promising developments and notable challenges. The research landscape highlights an array of sophisticated AI methodologies aimed at fortifying the Cybersecurity of smart homes. Nevertheless, a recurring theme in our findings is the disparity between theoretical AI models and their practical, real-life applications in domestic settings.

One of the key insights from this review is the underrepresentation of real-world testing and human-centric considerations in current AI-based cybersecurity solutions for smart homes. This observation points to a pivotal avenue for future research: the development and validation of AI models that are not only technically sound but also attuned to the behavioral patterns of residents in smart homes. The involvement of AI researchers, cybersecurity experts, and smart home device manufacturers is crucial in crafting robust and user-friendly solutions.

The review also highlights the necessity of incorporating human behavior into the design of AI-driven cybersecurity systems. This perspective is treasuredby smart device

manufacturers, suggesting a shift towards more intuitive and responsive Cybersecurity features that align with daily user interactions.

VII.ACKNOWLEDGMENT

We want to express our most profound gratitude and appreciation to ZZZZZZZZ.

VIII. REFERENCES

Al-Hawawreh, M., Moustafa, N., Garg, S., & Hossain, M. S. (2021, October). Deep Learning-Enabled Threat Intelligence Scheme in the Internet of Things Networks. *IEEE Transactions on Network Science and Engineering, 8*, 2968–2981. doi:10.1109/tnse.2020.3032415

Alzahrani, M. S., & Alsaade, F. W. (2022). Computational Intelligence Approaches in Developing Cyberattack Detection System. *Computational Intelligence and Neuroscience, 2022*. doi:10.1155/2022/4705325

Birnbach, S., Eberz, S., & Martinovic, I. (2022, April). Haunted House: Physical Smart Home Event Verification in the Presence of Compromised Sensors. *ACM Trans. Internet Things, 3*. doi:10.1145/3506859

Bordel, B., Alcarria, R., Robles, T., & Sánchez-Picot, Á. (2018). Stochastic and Information Theory Techniques to Reduce Large Datasets and Detect Cyberattacks in Ambient Intelligence Environments. *IEEE Access, 6*, 34896-34910. doi:10.1109/ACCESS.2018.2848100

Chong, M. S., Sandberg, H., & Teixeira, A. M. (2019, June). A Tutorial Introduction to Security and Privacy for Cyber-Physical Systems. *2019 18th European Control Conference (ECC).* IEEE. doi:10.23919/ecc.2019.8795652

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). *Introduction to Algorithms.* The MIT Press.

Diallo, A. F., & Patras, P. (2021, May). Adaptive Clustering-based Malicious Traffic Classification at the Network Edge. *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications.* IEEE. doi:10.1109/infocom42981.2021.9488690

Géron, A. (2019). *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow.* Alta Books.

Halder, S., & Ozdemir, S. (2018). *Hands-On Machine Learning for Cybersecurity: safeguard your system by making your machines intelligent using the python ecosystem.* Packt.

Heartfield, R., Loukas, G., Bezemskij, A., & Panaousis, E. (2021). Self-Configurable Cyber-Physical Intrusion Detection for Smart Homes Using Reinforcement Learning. *IEEE Transactions on Information Forensics and Security, 16*, 1720-1735. doi:10.1109/TIFS.2020.3042049

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J. R., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers and Security, 78*, 398-428. doi:10.1016/j.cose.2018.07.011

Iwendi, C., Rehman, S. U., Javed, A. R., Khan, S., & Srivastava, G. (2021, June). Sustainable Security for the Internet of Things Using Artificial Intelligence Architectures. *ACM Transactions on Internet Technology, 21*, 1–22. doi:10.1145/3448614

Khamesi, A. R., Shin, E., & Silvestri, S. (2020, January). Machine Learning in the Wild: The Case of User-Centered Learning in Cyber Physical Systems. *2020 International Conference on {COMmunication} Systems {\&}amp$\mathsemicolon$ {NETworkS} ({COMSNETS}).* IEEE. doi:10.1109/comsnets48256.2020.9027329

Kitchenham, B., & Charters, S. (2007, January). Guidelines for performing Systematic Literature Reviews in Software Engineering. *2*. Retrieved from https://www.researchgate.net/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering

Moustafa, N., Turnbull, B., & Choo, K.-K. R. (2019, June). An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things. *IEEE Internet of Things Journal, 6*, 4815–4830. doi:10.1109/jiot.2018.2871719

Mudgerikar, A., & Bertino, E. (2020). Jarvis: Moving towards a smarter internet of things., *2020-November*, pp. 122-134. doi:10.1109/ICDCS47774.2020.00020

Protogerou, A., Kopsacheilis, E. V., Mpatziakas, A., Papachristou, K., Theodorou, T. I., Papadopoulos, S., . . . Tzovaras, D. (2022, February). Time Series Network Data Enabling Distributed Intelligence—A Holistic IoT Security Platform Solution. *Electronics, 11*, 529. doi:10.3390/electronics11040529

Siddharthan, H., Deepa, T., & Chandhar, P. (2022). SENMQTT-SET: An Intelligent Intrusion Detection in IoT-MQTT Networks Using Ensemble Multi Cascade Features. *IEEE Access, 10*, 33095–33110. doi:10.1109/access.2022.3161566

Sikder, A. K., Babun, L., & Uluagac, A. S. (2021, February). Aegis+: A Context-Aware Platform-Independent Security Framework for Smart Home Systems. *Digital Threats, 2*. doi:10.1145/3428026

Singhal, D., Som, S., & Ahuja, L. (2021). A Review: IoT Based Smart Grid. doi:10.1109/ICRITO51393.2021.9596157

Soltani, N., Rahmani, A. M., Bohlouli, M., & Hosseinzadeh, M. (2022). Artificial intelligence empowered threat detection in the Internet of Things: A systematic review. *Concurrency and Computation: Practice and Experience*. doi:10.1002/cpe.6894

Spanos, G., Giannoutakis, K. M., Votis, K., Viano, B., Augusto-Gonzalez, J., Aivatoglou, G., & Tzovaras, D. (2020, August). A Lightweight Cyber-Security Defense Framework for Smart Homes. *2020 International Conference on INnovations in Intelligent SysTems and Applications (INISTA).*IEEE. doi:10.1109/inista49547.2020.9194689

Vaccari, I., Chiola, G., Aiello, M., Mongelli, M., & Cambiaso, E. (2020, November). MQTTset, a New Dataset for Machine Learning Techniques on MQTT. *Sensors, 20*, 6578. doi:10.3390/s20226578

Wan, Y., Xu, K., Wang, F., & Xue, G. (2022, May). IoTMosaic: Inferring User Activities from IoT Network Traffic in Smart Homes. *IEEE INFOCOM 2022 - IEEE Conference on Computer Communications.* IEEE. doi:10.1109/infocom48880.2022.9796908

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access, 8*, 146598-146612. doi:10.1109/ACCESS.2020.3013145