Scientific Research Publishing

Advances in Internet of Things, 2021, 11, 10-25
https://www.scirp.org/journal/ait
ISSN Online: 2161-6825
ISSN Print: 2161-6817

A Hybrid Intrusion Detection System for Smart Home Security Based on Machine Learning and User Behavior

Faisal Alghayadh, Debatosh Debnath

Department of Computer Science and Engineering, Oakland University, Rochester, Michigan, USA
Email: falghayadh@oakland.edu, debnath@oakland.edu

How to cite this paper: Alghayadh, F. and Debnath, D. (2021) A Hybrid Intrusion Detection System for Smart Home Security Based on Machine Learning and User Behavior. *Advances in Internet of Things*, **11**, 10-25.
https://doi.org/10.4236/ait.2021.111002

Received: December 8, 2020
Accepted: January 25, 2021
Published: January 28, 2021

Abstract

With technology constantly becoming present in people's lives, smart homes are increasing in popularity. A smart home system controls lighting, temperature, security camera systems, and appliances. These devices and sensors are connected to the internet, and these devices can easily become the target of attacks. To mitigate the risk of using smart home devices, the security and privacy thereof must be artificially smart so they can adapt based on user behavior and environments. The security and privacy systems must accurately analyze all actions and predict future actions to protect the smart home system. We propose a Hybrid Intrusion Detection (HID) system using machine learning algorithms, including random forest, Xgboost, decision tree, K-nearest neighbors, and misuse detection technique.

Keywords

Anomaly Detection, Smart Home Systems, Behavioral Patterns, Security, Threats

1. Introduction

The Internet of Things (IoT) is a commonly used term for a concept that incorporates technology and devices for networking. This idea encompasses creations such as Machine-to-Machine (M2M), Wireless Sensor Networks (WSN), Low Power Wireless Personal Area Networks (LoWPAN) communications, or technologies such as Radio-Frequency Identification (RFID) [1] [2]. Ultimately, the goal of the IoT is to develop capabilities for making these devices communicate with other devices using Internet communication protocols. However, despite having limited resources most developers of IoT devices such as smart TVs, smart watches, and smart lights attempt to add additional capabilities such as

audio and visual sensors [1] [3].

IoT technology has quickly been incorporated into the development of smart home systems. Smart home systems are designed using sensor technologies; several devices are linked to a specific network where they can be easily operated and monitored [1]. In addition to personal computers and smartphones, objects such as coffee makers and air conditioners, have recently begun linking to the internet, hence the term IoT. Customers can access relevant data from embedded applications while using a smartphone, tablet, or AI speaker to start operating IoT devices. One major example is Google Home [4]. The possibility of these products being the object of cyber attacks is growing as the variety of devices connected to the network increases [5] [6]. In fact, direct attacks and viruses attacking IoT devices have already been identified [4] [7]. These threats may be detected utilizing techniques based on an analysis of hacking behavior as compared with valid use [8].

The fact that smart home systems allow various electronic devices, such as security cameras, to be remotely accessed through the internet means that attackers can take advantage of their faults to steal personal information and breach the privacy of smart home users. These security violations include eavesdropping on communication inside and out of the house through the involved wireless and Internet technologies, while the security cameras may be compromised to expose the activities of a smart home user [9]. Such violations of security and privacy can threaten the protection of a smart home customer and such data can be used to commit serious crimes.

The majority of mainstream attacks targeting connected technologies are intended to undermine the growth of IoT systems [10]. However, because IoT devices are intertwined with everyday life, attacks can have an immediate and direct effect on users [11]. For example, hacking into commercial air conditioning units could result in the ability to change the temperature range in medical centers thereby compromising the safety of the healthcare environment. Tools to detect and eradicate attacker-initiated activities are also essential. Traditionally, cyber threats, safety tools, and intrusion prevention systems are also used to identify attackers. Using pattern recognition, these tools normally recognize threats by comparing the packets with a set of rules.

The conventional IDS is not very accurate when detecting anomalous trends since it operates on the basis of standard laws. In smart homes, these laws cannot be changed with new anomalous patterns [12]. In a smart home environment, modern wireless networks, computers, and sensors face various security threats, and machine learning is seen as an ideal solution to this problem. Using different learning algorithms train sensors, and computers without any explicit programming, machine learning technology takes advantage of artificial intelligence using various learning algorithms train sensors, and devices without any explicit programming [13] [14] [15].

This paper aims to introduce the use of a Hybrid Intrusion Detection System

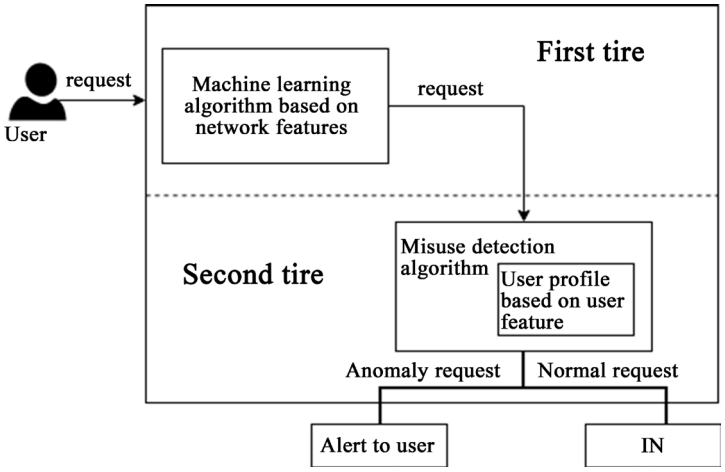

Figure 1. System model of HID.

(HID) with a two-tiered intrusion detection system as shown in Figure 1. The first tier contains the machine learning technique. This technique has been studied by the smart home's network traffic. The second tier will examine all requests that are being sent to the system based on patterns of user behavior profile. The reason for having a two-tiered intrusion detection system is to increase the system security and restrain the error rate since there will be more than one user who can control and monitor a smart home [1] [13].

The remainder of this paper is organized as follows: Section 2 briefly discusses the smart home technology. Sections 3 presents the problem statement. Next, the evaluation is demonstrated in Section 4. Section 5 shows the result. Finally, Section 6 contains the conclusion.

2. Smart Home Technology

The design of smart homes architecture consists of four main layers: the physical layer, communications layer, information layer, and decision layer [16]. The physical layer contains the essential hardware of the smart home such as devices, sensors, routers, and any devices that can be involved in the smart home network. The communications layer is comprised of the software that is mainly used to format and route data between users, agents, and the house. The information layer in a smart home's network is used to capture and store information which is later used to produce information to identify patterns used in decision-making. The decision layer is structured to determine the type of behavior obtained or stored in the information layer. As such, all four layers work closely together in the sense that the activities associated with one layer support the others [13] [17].

2.1. Devices

Smart home devices consist of hardware such as sensors, actuators, gateways, and smart objects. These connected devices can communicate with various devices and smart home equipment to different network devices [1] [18]. Actua-

tors are used to manipulate a physical component; these are devices that are given a specific input upon the information on which to act and a specific motion. A physical feature, such as a temperature control valve mounted in smart homes, is manipulated by actuators [1] [19]. A sensor gathers and distributes information about the physical environment and sends it to systems and devices for action. Sensors detect, measure, and indicate physical quantities such as light, motion, heat, pressure, and moisture, among others by converting them into electrical signals [1] [20]. Gateways serve as the bridge between the actuator and the sensor. Gateways collect data from the sensors and send the processed data for action to the actuator. Gateways are technically the control centers to provide access to the users to their smart home device [1] [21].

2.2. Communication

There are several communication protocols available that are used in smart homes. Wired, wireless, or radio communication protocols are common communication forms. Routers such as Zigbee or Z-Wave, which are automation protocols, interact with most sensors that operate in smart homes. Network protocols such as Wi-Fi, Bluetooth, 6LoWPAN, or IEEE 802.15.4 are also available for these sensors [1] [22].

2.3. Services

The service is a software program that has two methods to operate in a smart home system. A cloud provider that takes the responsibility of maintaining the program hosts is the first method, and the second method is to provide the service within the home environment. However, having the service inside the home setting means that users are responsible for tracking and upgrading any components of the software themselves [1] [22].

3. Problem Statement

Today, architects are incorporating smart home technology into new construction designs by adopting wired and wireless network infrastructures, paving the way for a seamless transition to this technology in the future. Many users are unaware of the threats to their privacy and security that exist from the potential breach of information collected by smart home devices (**Figure 2**). Every year the sophistication and number of cyber threats increase with millions of identities and billions of dollars being stolen.

There are hardware limitations on smart home devices presenting a major issue for IoT devices. These hardware limitations also lead to difficulty in adapting security features to any IoT devices over time. Since encryption and decryption are complex operations that involve a lot of computations, security approaches that rely heavily on encryption are not a good match for applying these resource-constrained devices. Most researchers agree that there are two major drawbacks to smart home devices: battery power and hardware computing [1]

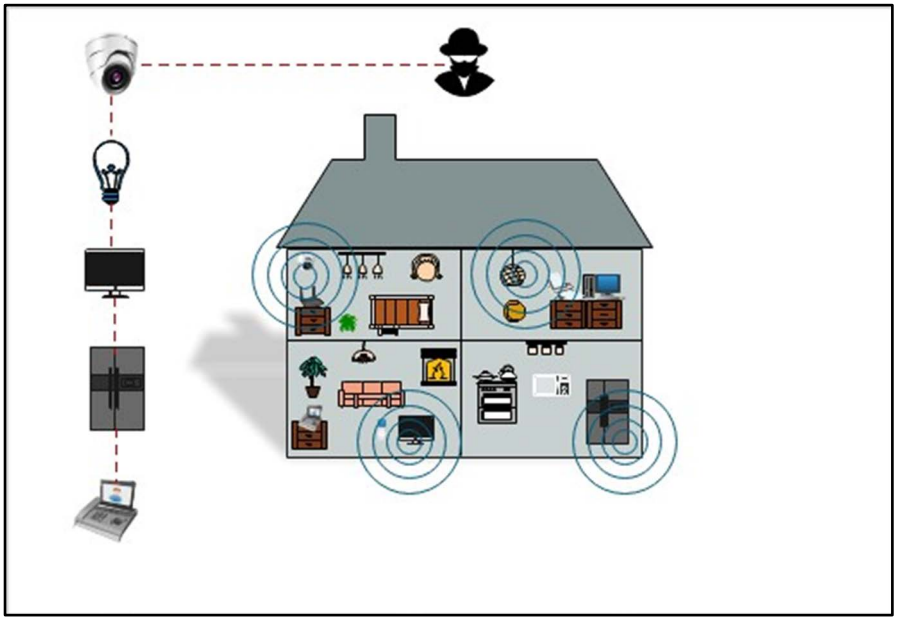

Figure 2. Threaten the privacy and security of smart home.

[23] [24]. The second major dilemma is heterogeneous protocols and weak encryption schemes can also affect dynamic features of smart home devices. Both heterogeneous protocols and weak encryption schemes lead the smart home network to face a lot of security problems [1] [22]. Smart home providers often try to deploy secure services by reaching the essential security and privacy requirements, which include confidentiality, integrity, and availability. All these implementations will depend on factors such as device capabilities, mode of operation, and the manufacturer [1] [22].

Such network attacks that can occur at any given time might be detectable by applying a technique to study smart home network traffic. However, because smart home devices are closely employed by the user every day, there would be a risk of attack coming from the user behavior tier [25]. For example, if the request is legitimate, and passes the network tier, the only method to determine if this request comes from the legitimate user is to have a known set of patterns. Therefore, user-behavior needs to be studied and identified, selecting the right user who sends the proper request at the right time while receiving the sensors correct request.

3.1. System Description

In the context of a sensor network, the smart home as a distributed environment shows the generic features of unreliability, which creates problems for behavior prediction. Security methods that rely heavily on encryption are not standard on these resource-constrained devices because encryption and decryption are complicated operations that require several computations [1] [26]. Even if activated correctly, the malfunctioning condition of sensors may not produce a trigger event. Currently, using only one IDS will not be enough to secure and determine

all requests that might occur in the smart home. We propose a HID in order to detect such attacks based on a profile of user behavior by using a two-tiered IDS.

The first tier is for intrusion detection systems using machine learning algorithm. The machine learning algorithm is an efficient data mining algorithm that can be used for real-time network intrusion detection [1] [26]. The second tier is the misuse detection technique that applies a known set of user activity patterns. The user behavior profile will ask questions to determine the normal behavior of a user, thereby allowing anomalies to be identified [1].

In this paper, there are two experiments using two sorts of datasets. The first one is CSE-CIC-IDS2018 and the second one is NSL-KDD as shown in Table 1. This experiment was done using Jupyter Notebook and, Python. The libraries that we used are panada, and sklean. The operating system is Windows with Intel core i7 processor.

3.2. System Model

Figure 3 provides an overview of the first tier of the HID smart home system which will scan the network requests that come from the user side. This phase aims to examine all requests coming to the smart home system using machine learning. We used and compared four types of machine learning algorithms [26]. They are random forest, Xgboost, decision tree, and K-nearest neighbors on

Table 1. Datasets.

Dataset	Attacks type	Attacks name	Labels	Public
NSL-KDD	4	DoS, U2R, R2L, Probe	Yes	Yes
CSE-CIC-IDS2018	6	Bot, brute force, DoS infiltration, SQL injection	Yes	Yes

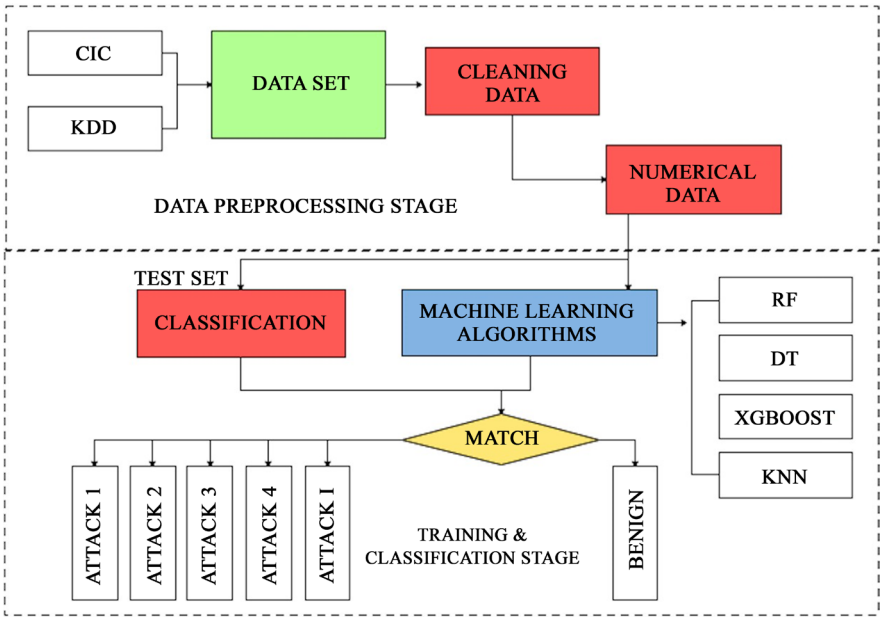

Figure 3. Machine learning technique.

two kinds of datasets. We randomly selected three samples from each dataset. The results show that our models for each algorithm can effectively achieve seemingly satisfactory classification accuracy with the lowest false positive [26].

Before starting the training model, we applied preprocessing the CSE-CIC-IDS2018 and, NSL-KDD datasets the following steps:

1) Preparing the dataset by clearing noisy, and missing data.

2) Replacing the data frame with pandas library.

3) Deleting features which do not affect the performance of the model, such as the Time Stamp column.

4) Transform all categorical features into binary features by using One-Hot-Encoding.

5) Dealing with "Infinity" and "NaN" values with the mean value for each column by replacing them.

6) Formatting data into a standard datatype.

7) Unbalancing and balancing data by using two methods, down and up sampling.

Figure 4 illustrates the model with static user behaviors. Misuse detection is usually related to signature-based detection since alerts are created based on unique signatures. The misuse is also a misinterpretation of illegal device access or use of the sensor at an inappropriate time for an event. This concept is an analysis of the variety of misuse detection techniques to identify device attacks by implementing profile pattern matching. This model is illustrated by the conditions and the stored user behaviors for each sensor. The conditions will be defined as a combination of time of day and the number of requests that will be sent to the sensor, such as how many times the user will operate his sensor from

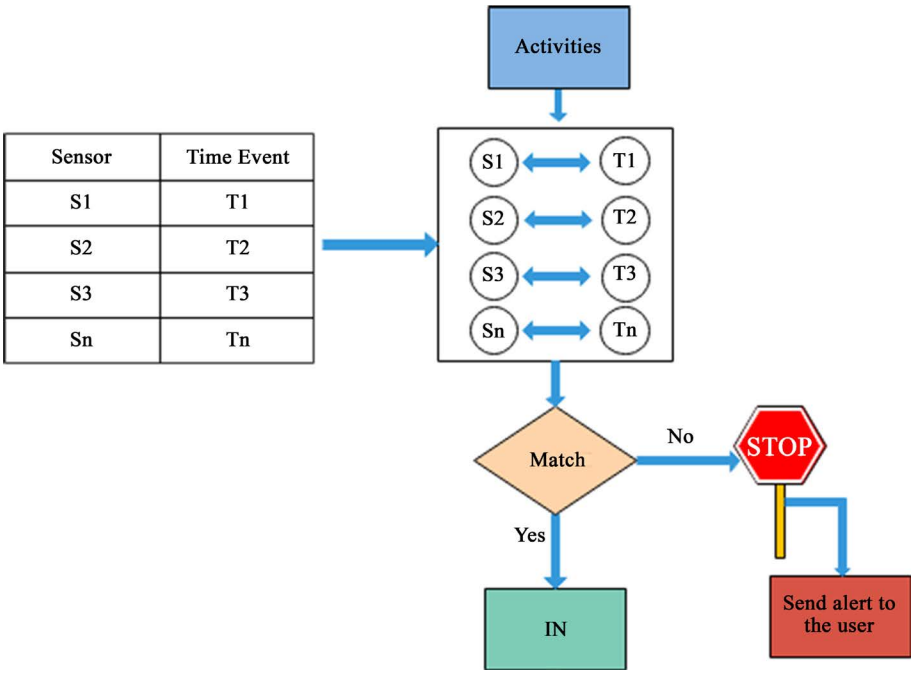

Figure 4. Misuses detection technique.

his phone. This table will be stored on the user behavior side. The steps below show how the user behavior tier works:

1) Sensors do not exist for all users, which may lead to error reports.

2) When users are not sending requests to sensors, the system is in static or fixed mode.

3) Each sensor is programmed to expect requests from certain users during predetermined times each day.

4) If requests are made outside of these given times, it implies the request may have been made by an intruder.

5) There is an access policy for all users, and based on this policy we have safe use resources and safe normal use.

6) There are exit access policies for all users. Based on this policy, we can determine if the request is unsafe and abnormal.

4. Evaluation

Most of the similar research work was executed by doing one tier of IDS. This tier could be focused on network behavior or user behavior. To summarize these methods, Table 2 presents the current IDSs for the IoT network tier. Consequently, current IDS ideas on the IoT environment are still at an early stage of growth. Some experiments have used data from network simulations or datasets that might dramatically decrease from a realistic setting.

Amouri *et al.* [27] incubated IDS for IoT networks by using machine learning. Their idea was to create list of the benign behavior of each sensor and detect any irregularities in network traffic. However, the experiment was evaluated by using a simulated network and not a real testbed. Doshi *et al.* [28] also developed machine learning algorithms in IoT networks to detect a particular attack, Distributed Denial of Service (DDoS) attacks. However, the studies rely exclusively on learning one attack behavior. In a study conducted by Lotfi *et al.* [29], with the intention of identifying any unusual short term and long term activities happening in a smart home environment by using neural networks. The results demonstrate that the system was showing the many false positives that can occur when analyzing the security of a given network. Yamauchi [4] developed an IDS for the smart home system by applying method learned sequences of events for a

Table 2. Similar to exist work on IDS for IoT.

Work	Security Threat	Detection Method	Strategy
Amouri *et al.* [27]	Identifies Malicious Nodes	Machine learning	Using one tier
Doshi *et al.* [28]	DDoS	Machine learning	Using one tier
Lotfi *et al.* [29]	Identifying any unusual short term and long term activities	Machine learning	Using one tier
Yamauchi *et al.* [4]	Unusual sequences of events	Machine learning	Using one tier
Novak *et al.* [30]	Identify unusual short/long activities	Machine learning	Using one tier
Proposed system	Identifies anomalies requests/unusual activities	Machine learning	Using two-tier

predefined set of conditions. Yamauchi detected attacks by comparing the sequences of the events, including the current operation with the learned sequences. This approach was just focused on user behavior and although the outcome of this system may provide a good evaluation result, it has not been applied against other network attacks. Novak *et al.* [30] outlined a technique for anomaly detection in user behaviors for a smart home. The main aspect of their work was to identify unusual short/long activities that occurred in a home environment. They used neural network self-organizing maps to identify various anomalous activities. Furthermore, their detection technique was based on the duration of activities, which can lead to many false positives.

Parameter Setting

In this paper, we attempted different parameters to achieve accuracy in all the implemented algorithms. The chosen training and test data were divided into 80% to 20%. We used a random forest classifier, Xgboost, decision tree, and K-nearest neighbors. The accuracy shows the percentage of data normality and attack data that are true to classify. The metric used to detect attacks can be calculated using the following Equation (1), where True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN).

The other metrics, such as precision and recall, can be calculated using the following Equation (2) and (3). Precision is indicated as a positive predictive value that means the precision of exposed attacks behaviors was correct [13] [26]. Recall indicates the true positive rate or sensitivity, meaning how many anomalies requests the model exposes. Accuracy, recall, and precision is the most distinguished metrics used for comparing the performance of the algorithms used in intrusion detection systems. Other metrics, such as F1, should also be considered. F1 values refer to how discriminative the model is. It can be calculated by using Equation (4):

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{2}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{3}$$

$$\text{F1-Score} = \frac{2 * TP}{2 * TP + FP + FN} \tag{4}$$

5. Result

5.1. Network Behavior

The results demonstrate that the system, for the first tier experiment CSE-CIC-IDS2018 in **Figure 5**, the K-nearest neighbors was recognized as the most successful algorithm with an average accuracy rate of 95.9% [26]. Random forest was identified as the second most accurate with an average rate of 95.7% [26]. Other

algorithms also earned strong accuracy relative to K-nearest neighbors and random forest. For the second experiment, NSL-KDD in Figure 6, random forest was the most successful algorithm with an average accuracy rate of 98.6%. Xgboost was the second most accurate with an average of 98.5%. The other algorithms also fulfilled strong accuracies likewise to random forest and Xgboost [26].

5.2. User Behavior

In several matching pattern methods, pattern matching algorithms are a crucial

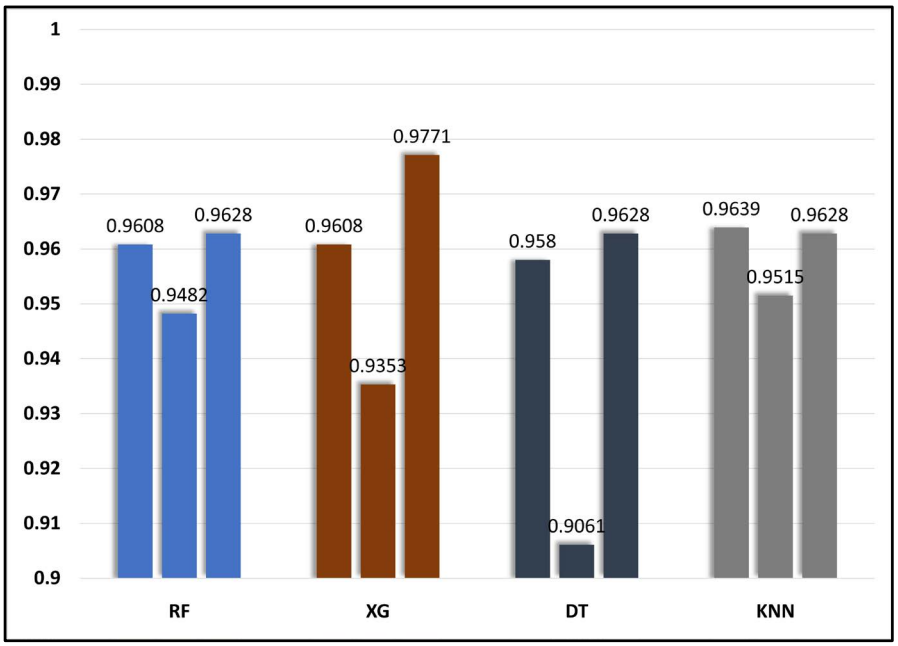

Figure 5. Accuracy rate for CSE-CIC-IDS dataset.

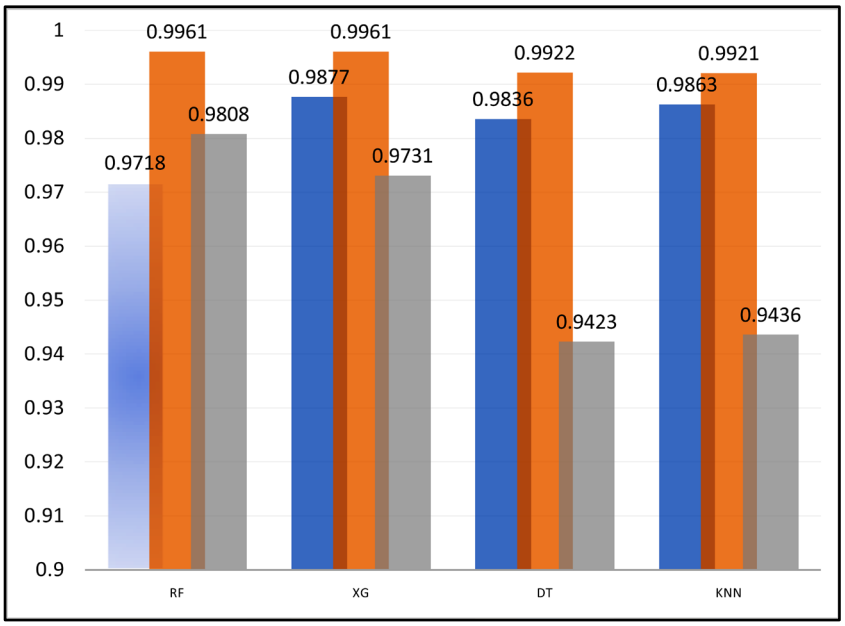

Figure 6. Accuracy rate for NSL-KDD dataset.

factor. For some patterns, the term relates to the procedure of matching, represented within a body of information as tree frameworks. The matching pattern method is most commonly used to examine and detect any request for concern that arrives at the smart home and does not correspond with the pattern model. Based on our previous work [1] [13] about the smart home network and using machine learning as an overarching framework, we added the patterns of user behavior profile based smart connected home described as **Algorithm 1**, S: is the sensor number which will be in a different location, t: is the time, u: user.

We used a dataset that belongs to the CASAS project [31]. The CASAS is a project for creating real smart homes for researchers in this field. A simple and lightweight toolkit called "smart home in a box" has been developed. To be able to provide smart tasks, the components of this toolkit are packaged in a single small box and conveniently mounted in a home. The toolkit was installed in 32 smart homes and created several datasets [31]. We employed one of the CASAS datasets for this study. The file that we employed has three features: date, time, sensor number, and status. We used the time column and sensor number column to create a scenario, as we mentioned in the case study part.

To improve user protection, Human behavior is various and hard to incorporate into one lifestyle. This means that each person can differ from one person to another. Therefore, to implement a data-driven approach for human behavior dealing with smart home sensors, feature extraction is one of the most important steps. This refers to the process of learning how many times a user will send a request to the smart home system using his smart devices such as a smartphone or smart tablet information from the sensor data. To conceptualize static user behavior to a normal level that is applicable to more than one individual, static user behavior will be usefully represented as a stable use of smart home sensors.

We created a scenario that considered an example to highlight the pattern task-related in user behavior. The task model of this use case starts from the early morning routine of a user awakening around 5:00 AM. The User always turns on the light, runs the water, and turns the coffee machine on to get ready before leaving to work. The User also turns on the TV and watches it while eating

Algorithm 1: Pseudocode for misuses detection algorithm

Result: Detect every request that comes from network tier
Input: Monitor user behavior;
Output: Defined user behavior
Normal or Abnormal ;
while *Not null* **do**
  A request will be sent by user;
  The request will be checked based on condition current date and time;
  $\forall_u \nexists_s$ Reports(Erorre);
  $\forall_s \nexists_u$ static case;
  $\forall_u \forall_{(t)} \forall_{(s)}$ Handles(t,s) $\rightarrow Receiptor$
  $\forall_u \forall_t$ Generates(conditions) $\rightarrow Affector$
  $\forall_u \exists\ Access\ Policy\ Safe\ Access(resource) \rightarrow SafeNormal$;
  $\forall_u \exists\ Access\ Policy\ Check\ Access(resource) \rightarrow SafeAbnormal$;
end

breakfast. Then, the user leaves for work, and around 2:00 PM the user checks his refrigerator to see what type of groceries are therein. Also, the user usually, double-checks some sort of smart home sensors during the user's time spent outside the home. Table 3 shows the time that each sensor can be received a request from the user side. Table 4 shows the anomaly event, which included routine attacks that may cause immediate and personal harm to users.

In this experiment, we create 8 types of sensors listed that connect it to a smart home. We assume these smart home devices can be connected to the Internet, users can command these devices.

We analyzed the packets from/to for a period of time. The result showed us the deployed electronics when the user controls the devices and shows the system has ability to clarify the status of the sensor when devices are operated. Figure 7 shows how the system can determine and accurately classify all requests that come to the smart home. To prove the efficacy of the user behavior system, we tested the system by generating a random request with a time and ran it through the system to see how the system determined the request, Figure 8 shows the random result. The evaluation shows that the system can detect the type of request if it is legitimate and match it with the user behavior profile. We

Table 3. User behavior table.

Sensor	Static event
Sensor 1	5:00:00 AM to 6:00:00 AM and 5:00:00 PM to 6:00:00 PM
Sensor 2	5:00:00 AM to 6:00:00 AM and 5:00:00 PM to 6:00:00 PM
Sensor 3	5:00:00 AM to 6:00:00 AM
Sensor 4	1:00:00 PM to 2:00:00 PM
Sensor 5	2:00:00 AM to 3:00:00 AM
Sensor 6	4:00:00 AM to 5:00:00 AM and 5:00:00 PM to 6:00:00 PM
Sensor 7	2:00:00 PM to 4:00:00 PM
Sensor 8	7:00:00 AM to 8:00:00 AM and 4:00:00 PM to 6:00:00 PM

Table 4. Attempt attack scenario.

Sensor	Anomaly event
Sensor 7	3:00:00 AM to 6:00:00 AM and 3:00:00 PM to 4:00:00 PM
Sensor 8	1:00:00 AM to 6:00:00 AM and 3:00:00 PM to 4:00:00 PM

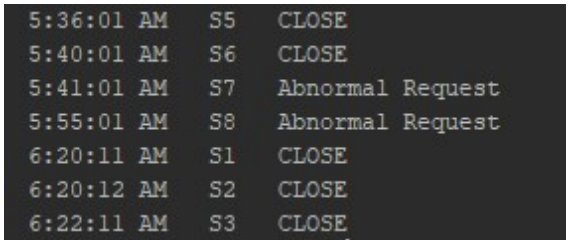

Figure 7. User behavior data analysis.

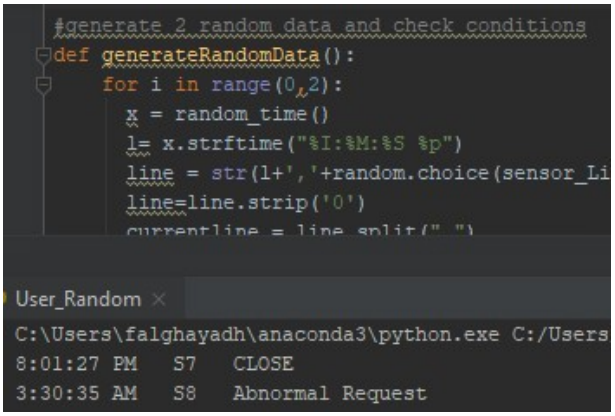

Figure 8. Random test data analysis.

observe that there are a limited number of legitimate requests that the user input into the user behavior profile. We added 2 anomalous requests that resembled legitimate request of turning on each sensor into data and attempted to detect them. The evaluation shows that the system can detect the type of request if it is legitimate and match it with the user behavior profile.

6. Conclusions

Theoretically, the smart home system would be a part of overall smart living, such as entire smart cities, and connect to various networks at any time and anywhere. The smart home system has two divisions, including network behavior and user behavior. However, this two-part design makes the system more vulnerable. This paper proposed a novel hybrid model based on intrusion detection methods tailored for smart homes, a machine learning-based prevention technique, and misuse detection methods based on user behavior profile patterns.

For the first tier, the proposed approach can be used for controlling data and monitoring systems that have specifications for individual smart home devices. The method is a scalable model that is cohesive with big data. We analyzed the model with CSE-CIC-IDS2018, and NSL-KDD datasets can still be applied on relatively minimal datasets with a low ratio of anomalies request. For the second tier, we focused on adding the detect anomalies method that offers more protection to smart home systems and supports the network tier. This approach examines all requests that come from the network tier and detects anomalies from user profiles. Anomalies will be identified and analyzed by monitoring the number of requests for specific events and the time duration of an activity. By doing this, the system will be most effective and secure [1].

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Alghayadh, F. and Debnath, D. (2020) Hid-Smart: Hybrid Intrusion Detection

Model for Smart Home. 2020 10*th Annual Computing and Communication Workshop and Conference*, Las Vegas, 6-8 January 2020, 384-389. https://doi.org/10.1109/CCWC47524.2020.9031177

[2] Granjal, J., Monteiro, E. and Silva, J.S. (2015) Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, **17**, 1294-1312. https://doi.org/10.1109/COMST.2015.2388550

[3] Lee, K., Kim, D., Ha, D., Rajput, U. and Oh, H. (2015) On Security and Privacy Issues of Fog Computing Supported Internet of Things Environment. 2015 6*th International Conference on the Network of the Future*, Montreal, 30 September-2 October 2015, 1-3. https://doi.org/10.1109/NOF.2015.7333287

[4] Yamauchi, M., Ohsita, Y., Murata, M., Ueda, K. and Kato, Y. (2019) Anomaly Detection for Smart Home Based on User behavior. 2019 *IEEE International Conference on Consumer Electronics*, Las Vegas, 11-13 January 2019, 1-6. https://doi.org/10.1109/ICCE.2019.8661976

[5] Lee, I. and Lee, K. (2015) The Internet of Things (IoT): Applications, Investments, and Challenges for Enterprises. *Business Horizons*, **58**, 431-440. https://doi.org/10.1016/j.bushor.2015.03.008

[6] Capellupo, M., Liranzo, J., Bhuiyan, M.Z.A., Hayajneh, T. and Wang, G. (2017) Security and Attack Vector Analysis of IoT Devices. *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Guangzhou, 12-15 December 2017, 593-606. https://doi.org/10.1007/978-3-319-72395-2_54

[7] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M., *et al.* (2017) Understanding the Mirai Botnet. 26*th USENIX Security Symposium*, Vancouver, 16-18 August 2017, 1093-1110.

[8] Shirali-Shahreza, S. and Ganjali, Y. (2018) Protecting Home User Devices with An SDN-Based Firewall. *IEEE Transactions on Consumer Electronics*, **64**, 92-100. https://doi.org/10.1109/TCE.2018.2811261

[9] Kim, B.-K., Hong, S.-K., Jeong, Y.-S. and Eom, D.-S. (2008) The Study of Applying Sensor Networks to a Smart Home. 2008 *Fourth International Conference on Networked Computing and Advanced Information Management*, Gyeongju, 2-4 September 2008, 676-681. https://doi.org/10.1109/NCM.2008.221

[10] Xu, K., Wang, F., Egli, R., Fives, A., Howell, R. and Mcintyre, O. (2014) Object-Oriented Big Data Security Analytics: A Case Study on Home Network Traffic. *International Conference on Wireless Algorithms, Systems, and Applications*, Harbin, 23-25 June 2014, 313-323. https://doi.org/10.1007/978-3-319-07782-6_29

[11] Komninos, N., Philippou, E. and Pitsillides, A. (2014) Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *IEEE Communications Surveys & Tutorials*, **16**, 1933-1954. https://doi.org/10.1109/COMST.2014.2320093

[12] Chase, J. (2013) The Evolution of the Internet of Things. *Texas Instruments*, **1**, 1-7.

[13] Alghayadh, F. and Debnath, D. (2020) A Hybrid Intrusion Detection System for Smart Home Security. 2020 *IEEE International Conference on Electro Information Technology*, Chicago, 31 July-1 August 2020, 319-323. https://doi.org/10.1109/EIT48999.2020.9208296

[14] Mamdouh, M., Elrukhsi, M.A. and Khattab, A. (2018) Securing the Internet of Things and Wireless Sensor Networks via Machine Learning: A Survey. 2018 *International Conference on Computer and Applications*, Beirut, 25-26 August 2018,

215-218. https://doi.org/10.1109/COMAPP.2018.8460440

[15] Perlich, C. (2010) Learning Curves in Machine Learning. In: Sammut, C. and Webb, G.I., Eds., *Encyclopedia of Machine Learning*, Springer, Boston, 10-50. https://doi.org/10.1007/978-0-387-30164-8

[16] Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G. and Baldini, G. (2017) Security and Privacy Issues for an IoT Based Smart Home.2017 40*th International Convention on Information and Communication Technology, Electronics and Microelectronics*, Opatija, 22-26 May 2017, 1292-1297. https://doi.org/10.23919/MIPRO.2017.7973622

[17] Dixit, A. and Naik, A. (2014) Use of Prediction Algorithms in Smart Homes. *International Journal of Machine Learning and Computing*, **4**, 157-162. https://doi.org/10.7763/IJMLC.2014.V4.405

[18] Samuel, S.S.I. (2016) A Review of Connectivity Challenges in IoT-Smart Home. 2016 3*rd MEC International Conference on Big Data and Smart City*, Muscat, 15-16 March 2016, 1-4. https://doi.org/10.1109/ICBDSC.2016.7460395

[19] Altolini, D., Lakkundi, V., Bui, N., Tapparello, C. and Rossi, M. (2013) Low Power Link Layer Security for IoT: Implementation and Performance Analysis. 2013 9*th International Wireless Communications and Mobile Computing Conference*, Sardinia, 1-5 July 2013, 919-925. https://doi.org/10.1109/IWCMC.2013.6583680

[20] Giri, A., Dutta, S., Neogy, S., Dahal, K. and Pervez, Z. (2017) Internet of Things (IoT): A Survey on Architecture, Enabling technologies, Applications and Challenges. *Proceedings of the* 1*st International Conference on Internet of Things and Machine Learning*, Liverpool, October 2017, Article No. 7. https://doi.org/10.1145/3109761.3109768

[21] Dey, S., Roy, A. and Das, S. (2016) Home Automation Using Internet of Thing. 2016 *IEEE* 7*th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*, New York, 20-22 October 2016, 1-6. https://doi.org/10.1109/UEMCON.2016.7777826

[22] Bugeja, J., Jacobsson, A. and Davidsson, P. (2016) On Privacy and Security Challenges in Smart Connected Homes. 2016 *European Intelligence and Security Informatics Conference*, Uppsala, 17-19 August 2016, 172-175. https://doi.org/10.1109/EISIC.2016.044

[23] Karimi, K. and Krit, S. (2019) Smart Home-Smartphone Systems: Threats, Security Requirements and Open Research Challenges. 2019 *International Conference of Computer Science and Renewable Energies*, Agadir, 22-24 July 2019, 1-5. https://doi.org/10.1109/ICCSRE.2019.8807756

[24] Yang, Y., Wu, L., Yin, G., Li, L. and Zhao, H. (2017) A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, **4**, 1250-1258. https://doi.org/10.1109/JIOT.2017.2694844

[25] Brdiczka, O., Langet, M., Maisonnasse, J. and Crowley, J.L. (2008) Detecting Human Behavior Models from Multimodal Observation in a Smart Home. *IEEE Transactions on Automation Science and Engineering*, **6**, 588-597. https://doi.org/10.1109/TASE.2008.2004965

[26] Alghayadh, F. and Debnath, D. (2020) Performance Evaluation of Machine Learning for Prediction of Network Traffic in a Smart Home. 2020 11*th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*, New York, 28-31 October 2020, 837-842. https://doi.org/10.1109/UEMCON51285.2020.9298134

[27] Amouri, A., Alaparthy, V.T. and Morgera, S.D. (2018) Cross Layer-Based Intrusion

Detection Based on Network Behavior for IoT. 2018 *IEEE* 19*th Wireless and Microwave Technology Conference*, Sand Key, 9-10 April 2018, 1-4. https://doi.org/10.1109/WAMICON.2018.8363921

[28] Doshi, R., Apthorpe, N. and Feamster, N. (2018) Machine Learning ddos Detection for Consumer Internet of Things Devices. 2018 *IEEE Security and Privacy Workshops*, San Francisco, 24 May 2018, 29-35. https://doi.org/10.1109/SPW.2018.00013

[29] Shahreza, M.L., Moazzami, D., Moshiri, B. and Delavar, M. (2011) Anomaly Detection Using a Self-Organizing Map and Particle Swarm Optimization. *Scientia Iranica*, **18**, 1460-1468. https://doi.org/10.1016/j.scient.2011.08.025

[30] Novák, M., Jakab, F. and Lain, L. (2013) Anomaly Detection in User Daily Patterns in Smart-Home Environment. *Journal of Selected Areas in Health Informatics*, **3**, 1-11.

[31] Cook, D.J., Crandall, A.S., Thomas, B.L. and Krishnan, N.C. (2012) CASAS: A Smart Home in a Box. *Computer*, **46**, 62-69. https://doi.org/10.1109/MC.2012.328