RESEARCH ARTICLE

SAMRIDDHI Volume 12, Issue 2, 2020 Print ISSN: 2229-7111 Online ISSN: 2454–5767

Protecting Smart Home Environment using Machine Learning Algorithm Based on Internet of Things

Chanchal Singh[1], Piyush Rai[2], Nidhi Prashad[3]

[1]Student, Computer science, Institute of Engineering and Technology, Faizabad, Ayodhya, India

[2]Assistant Professor, Computer science, Institute of Engineering and Technology, Faizabad, Ayodhya, India

[3]Assistant Professor, Computer science, Institute of Engineering and Technology, Faizabad, Ayodhya, India

Abstract

In today's information technology-driven society, automation systems make people's lives easier and comfortable than ever before. We call the proposed system IoT-Home Advanced Security System or internet of things (IoT) -Home Advance Security (HAS) for short. IoT-Home Advance Security System was established using Python 3 and can be executed in two modes of operation. The in-line mode allows the IoT-Home Advance Security System to be installed in-line with the traffic inside a Raspberry Pi or a Router. In the in-line mode, IoT-HAS System acts as an IPS that can detect and block threats as well as alert the user. The second mode is the passive mode, where IoT-HAS System in not connected in-line with the traffic and can act as an IDS that passively monitors the traffic, detecting threats and alerting the user, but not blocking the attack. IoT-HAS System was evaluated via four testing scenarios.

Keywords: Internet of Things, Smart Homes, Intelligent Homes, Building Automation, Smart Buildings, Security Risk Assessment, Security Recommendations, Security Threats, Security Countermeasures.

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology (2020); DOI: 10.18090/samriddhi.v12i02.6

Introduction

The list above includes most of the widely used IOT devices among consumers. However, since this market is very volatile and new devices are being developed or released daily, this list is anticipated to grow dramatically.

Internet of things (IOT) is probably the most revolutionary invention since the invention of the internet. IOT brought about a tremendous amount of data that the world has never seen before. With the huge amount of data, one of the challenges with the Internet of Things is the ability to secure the data while it is at rest, in transit, and during processing. Many sectors, such as Healthcare, Manufacturing, and Retail, widely use IOT technology, taking advantage of its ease. However, our interest is in the Home IOT sector. It is expected that by the year 2021 the average number of IOT devices in a smart home will reach thirteen devices in North America, nine in Western Europe, four in Central and Eastern Europe, three in Latin America, three in Asia, and one in both the Middle East and Africa (Martin, 2017).

Methodology

1. Intrusion Detection Evaluation Dataset

An intrusion detection dataset is a dataset that is intended to test the strength of an intrusion detection system. Such a dataset is normally lled with various cyberattacks that target networks. Attacks such as DoS, DDoS, Port Scanning, and Brute Force are among those found in an intrusion detection dataset. These datasets are normally created by researchers in laboratories under a speci c set of requirements and conditions. Several intrusion detection system datasets are available today. However, some are very old and include outdated attacks that do not reflect today's real-world attacks. When choosing an intrusion detection dataset, a researcher should select one that has the most current attacks resembling or identical to real-world ones.

2. Choosing the Right Dataset

There are two ways to choose the dataset:

1. Creating a dataset from scratch satis es the purpose of

Corresponding Author: Chanchal Singh, Student, Computer science, Institute of Engineering and Technology, Faizabad, Ayodhya, India , e-mail: chanchalsinghh36@gmail.com

How to cite his article: Singh, C., Rai, P., & Prashad, N. (2020). Protecting smart home Environment using machine learning Algorithm Based on Internet of Things. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology,* 12(2), 89-92.

Source of support: Nil

Con ict of interest: None

the experiment, which is to train our model to recognize di erent attack types. Yet preparing a good intrusion detection dataset for an IoT is not an easy task. The researcher should have the time and capabilities to run, capture, and label di erent types of attacks. The process of developing an accurate dataset can take days. This method is preferred if the researcher has the right tools to do it.

2. The other method is to use one of the existing intrusion detection datasets. If choosing this route, the researcher must ensure that the dataset has a variety of attacks that

3. The CICIDS2017 Dataset

The CICIDS2017 dataset was created to overcome problems that accompanied the eleven datasets created prior to its creation. Prior datasets such as DARPA98, KDD99, ISC2012, and ADFA13 are mostly out of date and su er from a lack of diversity and volume of attacks. The CICIDS2017, on the other hand, includes benign data and a variety of most attack types that are available in the real world today. The dataset includes more than eighty features created with a network ow generator tool called CIC Flow Meter.

Litrature Survey

Nikam and Ambawade (2018) proposed an opinion metrics lightweight intrusion detection approach in IoT networks to detect new threats. Opinion Metrics are based on nding each node's Believe, Disbelieve, and Uncertainty values concerning other nodes in the network. Malicious nodes in the network are then detected by identifying nodes with a high degree of disbelieving values.

Roux *et al*. (2018) presented an approach for intrusion detection systems in IoT networks that uses radio communication signals to monitor whether detected signals match the legitimate ones from a saved pro le. This approach is designed to be independent of large and heterogeneous networks. A case study was presented to show the system's feasibility with the proposed intrusion detection system implemented in a smart home environment (Roux et al., 2018).

Aldaej (2019) proposed an intrusion detection and prevention system for IoT devices that prevent DDoS attack types. DDoS attacks are known to ood the network with a huge number of requests originating from several computers to overwhelm the network and prevent legitimate users from accessing the network and using services (Aldaej, 2019).

Choi and Choi (2019) studied vulnerabilities in the power system in a cloud-based environment and de ned a set of security inference rules. Furthermore, a security framework that protects power systems hosted in a cloud environment was proposed. A smart meter was used to verify the feasibility of the proposed framework by creating attacks against it. The inference rules were found e ective in detecting those attacks (Choi & Choi, 2019).

Modeling and Analysis

There are a few limitations to this research. The rst limitation is that the evaluation and testing were conducted in a virtual environment. This is because the experiment was conducted in a regular home network where only one network was available. We needed two di erent networks, one external network for the attacker and one internal network for the victim device, and a router with IoT-HASS installed to execute the experiment. The only available environment to design this setting was the virtual environment as a home network has only one network. The second limitation is that the Raspberry Pi has limited resources and capabilities compared to a regular router, and thus a ects the performance of IoT-HASS. We used the latest version of Raspberry Pi 4 with enhanced functionality and 4 GB of RAM, yet it is still less e cient compared to a typical average router. IoT-HASS would perform better if installed in a more powerful device. The third limitation in this research is that IoT-HASS still needs to be trained on an updated dataset to be able to predict new attacks. Otherwise, it will likely result in more false positives as the system becomes older. Frequent training of the system with an updated training dataset will reduce the number

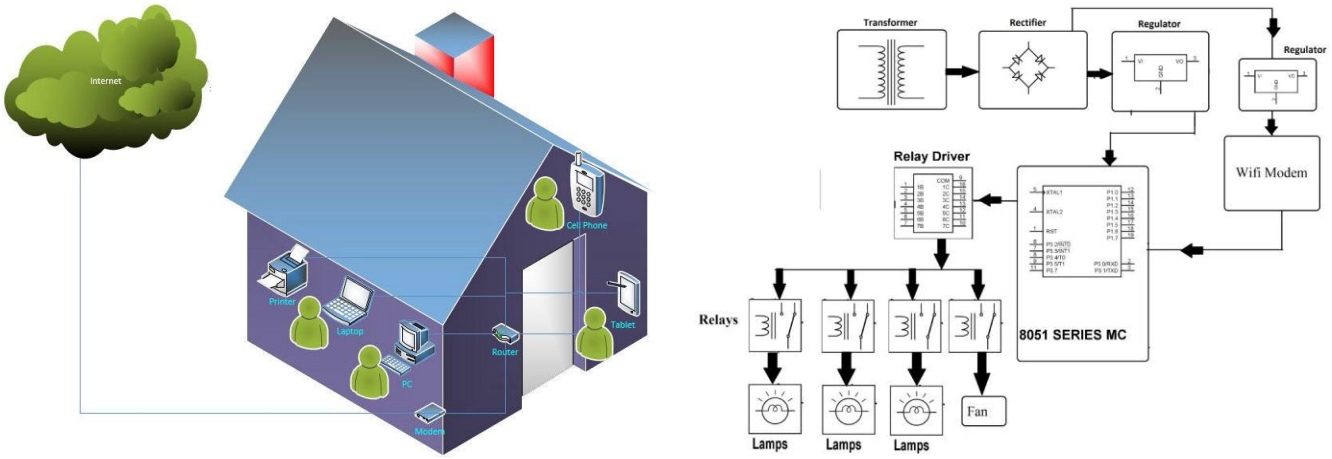

Figure : Block Diagram

Figure 1: 3D view of building.

of false positives, resulting in a more accurate system. Of course, frequent training of the system with updated training datasets cannot be performed by non-technical smart home users, which is a further limitation.

Results and Discussion

This chapter discussed di erent methods used to validate the strength of IoT-HASS. We started with evaluating IoT-HASS by comparing it to other similar solutions. We chose four other solutions to perform the comparison. The solutions selected for the comparison include the GA-SVM model, the WFS-IDS model, the A-IDS model, and the Beget model. The comparison was performed using the CICIDS2017 DDoS dataset. The IoT-HASS outperformed all the other models, as illustrated in the results. IoT-HASS was then evaluated by running a series of simulation attacks inside a virtual environment. The attacks included DDoS attacks, Brute Force attacks, and XSS attacks. Those three attacks represent some of the major attacks that target the Home IoT environment. IoT-HASS was evaluated in two modes when running those attacks: the in-line mode and the passive mode. Finally, IoT-HASS was evaluated on the Raspberry Pi when running in passive mode. Simulation attacks were executed. The results showed that IoT-HASS detected di erent attacks successfully. In all the evaluation scenarios above, IoT-HASS showed a high prediction accuracy, and thus it can be a valuable tool for protecting the smart home environment.

Conclusion

This research aimed to close some of the gaps that exist in the security of smart home environments. Unlike Industrial IoT, Corporate IoT, Retail IoT, or Healthcare IoT environments where tighter security measures are enforced on IoT devices, a lack of security mechanisms exist in the Home IoT environment. Home IoT devices have fewer security measures and guidelines when compared to other IoT sectors. Some home IoT devices have very little to no security, putting their users and their users' information at great risk. IoT-HASS was evaluated through four testing scenarios. In the rst scenario, we compared it to similar systems. As shown in the evaluation and testing chapter, IoT-HASS outperformed the GA-SVM, WFS-IDS, A-IDS, and Beget models. IoT-HASS was also evaluated by executing simulation attacks and checking its performance. Simulation attacks were executed in a controlled virtual environment. Inside the virtual environment, simulation attacks were executed with IoT-HASS installed and running in both in-line mode and passive mode. Three major attacks were simulated, including DDoS Attacks, Brute Force Attacks, and Cross-Site Scripting Attacks. DDoS attacks were simulated using the Low Orbit Ian Cannon (LOIC) attack simulator tool, and the results showed that IoT-HASS captured attacks with a very high accuracy detection. Similarly, Brute Force attacks were simulated using the Medusa simulation tool from Kali, and results showed that IoT-HASS attained an outstanding detection accuracy.

References

[1] Sirsath N. S, Dhole P. S, Mohire N. P, Naik S. C &Ratnaparkhi N.S Department of Computer Engineering, 44, Vidyanagari, Parvati, Pune-411009, India University of Pune, "Home Automation using Cloud Network and Mobe Devices".

[2] CharithPerera, Student Member, IEEE, ArkadyZaslavsky, Member, IEEE, Peter Christen,andDimitriosGeorgakopoulos, Member, IEEE "Context Aware Computing for The Internet of Things: A Survey". IEEE COMMUNICATIONS SURVEYS & TUTORIAL.

[3] Charith Perera_y, ArkadyZaslavskyy, Peter Christen_ and DimitriosGeorgakopoulosy Research School of Computer Science, The Australian National University, Canberra, ACT 0200, Australia yCSIRO ICT Center, Canberra, ACT 2601, Australia" CA4IOT: Context Awareness for Internet of Things".

[4] Bl N. Schit, Norman Adams, and Roy Want, "Context-Aware Computing Applications".

[5] JayavardhanaGubbi, ,RajkumarBuyya, SlavenMarusic,aMarimut huPalaniswamia, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions".

[6] S.P. Pande, Prof. PravinSen, "Review On: Home Automation System For Disabled People Using BCI" in IOSR Journal of Computer Science (IOSR-JCE) e- ISSN: 2278-0661, p-ISSN: 2278-8727 PP 76-80.

[7] Bas Hamed, "Design & Implementation of Smart House Control Using LabVIEW" at International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, January 2012.

[8] Basma M. Mohammad El-Basioni1, Sherine M. Abd El-kader2 and Mahmoud Abdelmonim Fakhreldin3, "Smart Home Design using Wireless Sensor Network and Biometric Technologies" at Volume 2, Issue 3, March 2013.

[9] Inderpreet Kaur, "Microcontroller Based Home Automation System With Security" at IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 1, No. 6, December 2010.

[10] Rosslin John Robles and Tai-hoon Kim, "Review: Context Aware Tools for Smart Home Development", International Journal of Smart Home, Vol.4, No.1, January 2010.

[11] Hitendra Rawat, Ashish Kushwah, Khyati Asthana, AkankshaShivhare, "LPG Gas Leakage Detection & Control System", National Conference on Synergetic Trends in engineering and Technology (STET-2014) International Journal of Engineeringand Technical Research ISSN: 2321-0869, Special Issue.

[12] Nicholas D., Darrell B., Somsak S., "Home Automation using Cloud Network and Mobe Devices," IEEE Southeastcon 2012, Proceedings of IEEE.

[13] Nalluri, S. K., & Parasaram, V. K. B. (2016). Early Approaches to Robotic Process Automation in Enterprise Systems. International Journal of Humanities and Information Technology, 1(01), 12-28. https://doi.org/10.21590/ijhit.01.01.06

[14] Parasaram, V. K. B., & Nalluri, S. K. (2016). A Comparative Analysis of Risk Management Frameworks in Enterprise IT Projects. SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, 8(02), 147-155. https://doi.org/10.18090/samriddhi.v8i2.7149

[15] Chan, M., Campo, E., Esteve, D., Fourniols, J.Y., "Smart homes-current features and future perspectives," Maturitas, vol. 64, issue 2, pp. 90-97, 2009.