Quest Journals
Journal of Software Engineering and Simulation
Volume 8 ~ Issue 5 (2022) pp: 01-08
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Intrusion Detection and Classification of Anomalies in Smart Homes Using Deep Learning Approach

[#1] UGAVAH BLESSING
Department of Computer Science, Rivers State University, Nigeria

[#2] Dr. O.E Taylor
Department of Computer Science, Rivers State University, Nigeria.

[#3] Dr. Daniel Matthias
Department of Computer Science, Rivers State University, Nigeria.

ABSTRACT
In recent years, due to the emergence of an unlimited communication paradigm and the increased number of networked digital devices such as smart homes technology, there is a growing concern about cybersecurity which tries to preserve either the information or the communication technology against an intruder. Intruders discover new attack methods every day, and to prevent these attacks first, they need to be identified correctly, and then proper responses should be given. This paper is centered on optimizing the security of smart home intrusion detection and anomalies classifications using a deep learning approach. This technique helped to independently identify and classify an intrusion as either brute force, dictionary, or an unknown attack. The model is trained and tested with several test cases. Network security laboratory NSL coupled with Knowledge discovery databases KDD (NSL-KDD) dataset is used in this paper which is more in line with the data characteristics of the new era than the traditional dataset. NSL-KDD is used to train and test intrusion and detection from internet network traffic. Our choice for an Anomaly-based intrusion detection system is because, it is a better option than a signature-based system since it does not require prior knowledge of the attack signature before it can be used to detect an intrusion. The developed system was tested on the public domain and with NSL-KDD dataset, the result obtained was significantly satisfactory, the output results show that the accuracy of using deep learning model for IDS are better than those of other comparison methods, reaching 94% accuracy. Finally,we suggest the future work should add biometrics such as fingerprints as a means of smart home user authentication and authorization. This will reduce an intrusion from a stranger which in turn keeps smart home safe and secured.

Keywords: Intrusion detection, anomaly classification, Deep Learning, Smart home.

***R**eceived 25 Apr, 2022; **R**evised 05 May, 2022; **A**ccepted 07 May, 2022 © The author(s) 2022.*
P**ublished with open access at **www.questjournals.org

I. INTRODUCTION

Home has been a reliable haven of rest after all human activities of the day since the dawn of time. A house is defined as a secure location that is safe from intruders and provides a conducive atmosphere for human habitation". Home security has been a problem as a result of human greed; this has put the human race in risk and resulted in the loss of property and lives. Due to technological advancement in recent times, aero planes, ocean liners, ships, cars etc. are designed and built to respond to certain human immediate needs automatically. The term "smart home" refers to a home that is controlled by smart devices. In agreement with one of the most important later definitions by [1] "a smart home is a home which is smart enough to assist the inhabitants to live independently and comfortably with the help of technology: "All mechanical and digital components in a smart home are connected to form a network that can communicate with one another and with the user to create an interactive environment. The savvy domestic, according [2], is an application that can automate or assist clients through various forms such as surrounding insights, further domestic control, or domestic mechanization frameworks.It will not be wrong to say living in an unautomated home posed a lot of challenges. Some of the problems that the occupants faced are wastage of energy such as light and other resources, forgetting to turn off the air conditioner or perhaps a micro wave or an oven etc. Despite, numerous advantages of living in smart homes, people are still skeptical to adopt this technology due to security challenges that comes with it. Thus, the effort to effectively secure a smart home is still a topic of discussion that needs to be explored if this newest and evolving technology are to be taken seriously. The smart home attacks are vast, and they're only becoming bigger and better. Therefore, Analyzing and strengthening cybersecurity posture is no longer a challenge that can be solved on a human scale. As a result of this unprecedented challenge, Artificial Intelligence (AI)-based cybersecurity tools have evolved to assist information security teams in reducing breach risk and improving their security posture quickly and effectively. This paper work will be centered on developing a secured smart homes instruction detection and classification of anomalies using deep learning approach. Some of the issues or problems in existing system are:Identity theft, Password exploitation, Ineffective management of appliances in homes leading to energy wastage.We decided to use deep learning algorithm to find solution to the aforementioned problems because it has the capability to learn optimal feature representation by itself and more robust in an adversarial environment compared to classical machine learning algorithms.

II. RELATED WORK

Zhao [3] presented a comprehensive review of deep learning research on machine health monitoring. The goal of health-monitoring systems based on deep learning (MHMS) is to extract hierarchical signals from input data by using deep neural networks with distinct layers of nonlinear changes.

Petersen [4] presented an internet of things application for home automation using Rasberry Pi and Wi-Fi as a communication protocol for controlling home devices using Smartphones.

Gerfriedcebrat [5] developed an IoT application that controls heating, air conditioning, and ventilation in the home using an embedded programmable logic controller. In addition, a home security system is being developed that ensures the security of user data.

Mohamed [6] proposed a novel way to build an economical environmental monitoring device using raspberry pi. Environmental information such as temperature, humidity, light intensity and concentration of carbon monoxide is taken through sensors and uploaded to the internet where it can be accessed anywhere and anytime. It can also detect tectonic disturbances like earthquakes with the help of seismic sensors.

Cenedese [7] proposed an urban smart city system in which advanced communication technologies are used to support value-added services for the administration of the city and for its citizens. This paper has been implemented in the Padova Smart City project Italy in collaboration with the city municipality.

Mubashir [8] worked on the use of Survey on prediction algorithms in smart homes. They defined smart homes as a living or working space that interacts in a natural way and adapts to the occupant. Adaptation refers to the ability of the system to learns to recognize and change itself depending on the identity and activity undertaken by the occupant with minimal intervention from the occupant. Hence, a Smart Home predicts the mobility patterns and device usages of the inhabitants.

The study done by Sleman [9] discussed the main stumbling blocks in modern home computerization systems: the high overall cost of the system, inflexibility due to integration of different devices into the home computerization system, lack of reliable devices at home, complex user interfaces, and reliance on skilled consultants. All these factors cause poor manageability and lack of adequate security.

Thati [10] proposed an internet of things application for home automation system for Controlling of home appliances through internet in which Wi-Fi is used as a communication protocol. Home appliances like lights, fans and door lock are easily and remotely controlled and monitored using a webpage. The server which is connected to the appliances through relay hardware circuits allows the user to access the various appliances.

Cebrat [11] proposed an IoT application which uses an embedded programmable logic controller to control heating, air conditioning and ventilation in home. Also, a home security system is designed which maintains the integrity of user data.

Soliman [12] proposed a smart home using Internet of Things application that is a combination of portable devices, cloud computing, wireless sensor nodes that allows the user to control appliances within the house like lights, fans, door locks etc

III. METHODOLOGY

We adopted a Research Methodology called SCRUM for this paper. Scrum is an agile methodology for guiding teams through the iterative and incremental delivery of a product. Its focus is on the use of an empirical approach that allows teams to adjust quickly, efficiently, and effectively to change, and it is sometimes referred to as an agile project management framework

3.1 SYSTEM DESIGN

The system will be integrating Deep learning to secure smart homes. The system will detect the anomalies and classify the type of the attack.This is done to enhance security in the home. The architecture specification is a precise description and illustration of our system, which is constructed in such a way that assists understanding with respect to the structures and actions of the system.

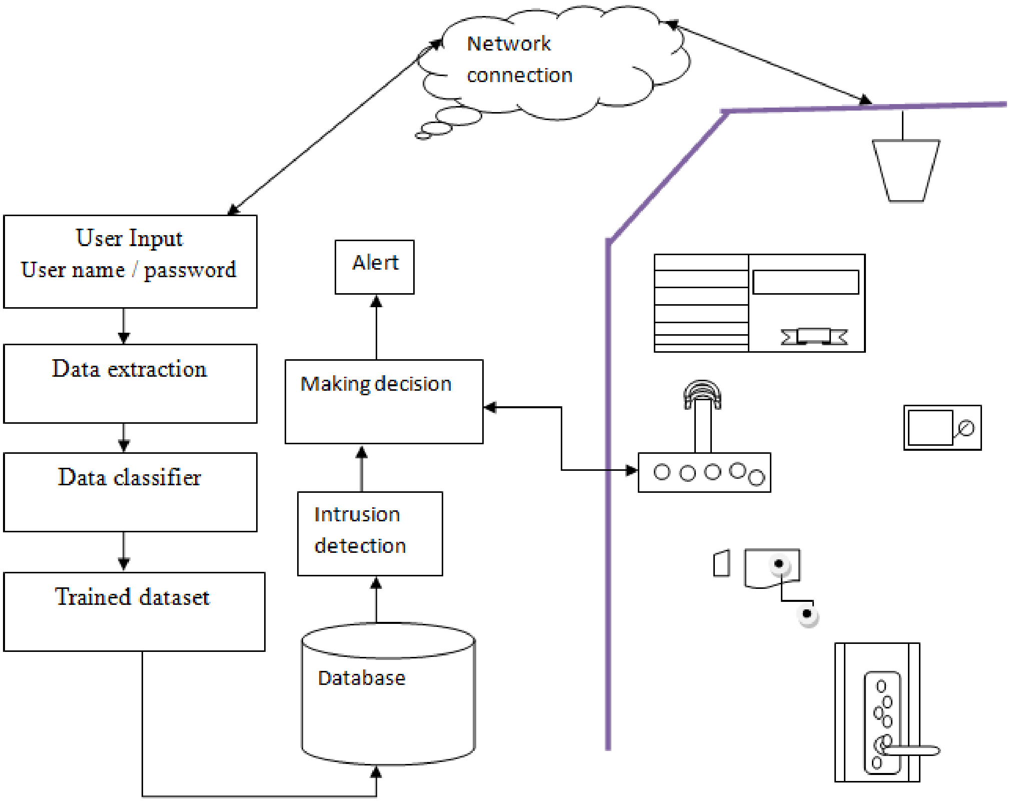

Figure 3.1: System Diagram for Smart Home

The main component of are smart home, the cloud, and the end application. These components depend on each other, so they are interconnected. The smart home is the main gateway, consists of all the smart home appliances ranging from wifi, the door lock, the television, wired and wireless sensors, lights, etc. The cloud platform handles the Smart app, access control mechanism, as well as smart devices. This architecture controls the internal function of Smart home behavior and shows the connections made by each component to attract each other. IDS and classification will be handled by a deep learning approach, that will help to protect and prevent unwanted users from gaining access to a smart home. It must be noted that the system must be trained to be able to detect instruction and classify anomalies from an intruder independently. It must be noted that, the system must be trained to be able to sense and predict the occupants’ mobility habits and their use of electrical appliances and detect an anomaly and classify it appropriately.

It must be noted that the system must be trained to be able to detect instruction and classify anomalies from an intruder independently.

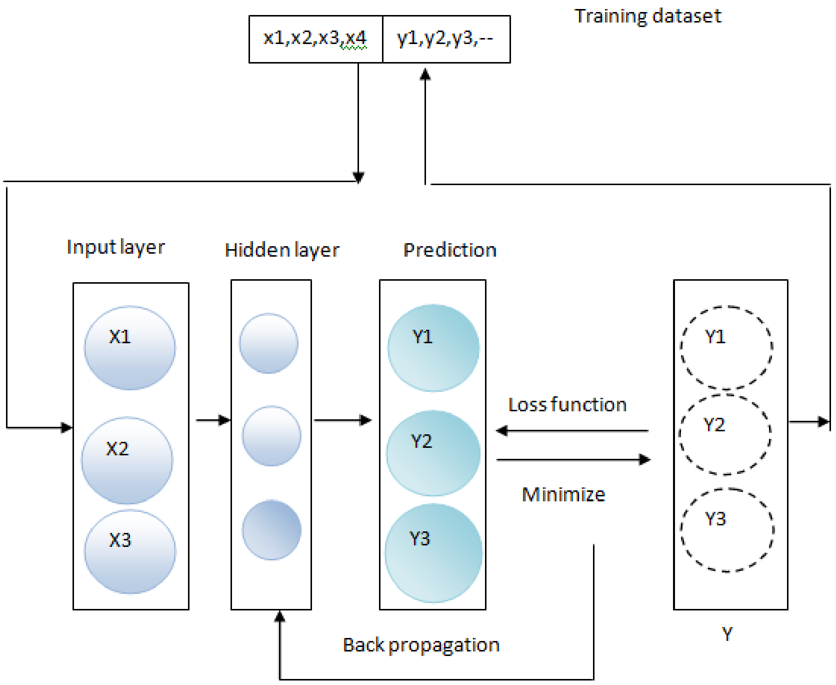

Figure. 3.2: Deep Learning model

Deep learning algorithms are actually Deep architectures of consecutive layers. Each layer applies a nonlinear transformation on its input and provides a representation in its output. The input levels (x1, x2, x3) which in this case is username, or email and password. Also, for the home users' appliance predictions the x-series are marked as TV, AC and so on. These inputs are connected to a neural where weights of connections between neurons are set using a supervised learning method. The hidden layer is to store the dataset form the input layer classifier the feature converts them into the normalized range –1 to 1 and outputs a standard deep learning model. From diagram above the training phase, the input layer assigns (usually randomly) weights to the input training data and outputs it to the next layer. Each subsequent layer also assigns weights to their input and passes their output (y1, y2, y3) outcome of the input, which serves as the input for the following layer. At the last layer, the final output representing the prediction of the model will be produced. A loss function helps to specify how right or wrong is this prediction by computing the error rate between the prediction and true value. The error rate is recycled back across the network to the input layer. The network at that point rehashes this training cycle, subsequent to adjusting the weights on every neuron in each cycle, until the blunder rate falls under an ideal limit. At this point, the Deep Neural Network (DNN) is trained and is ready for inference.

3.2 Intrusion Detection and Anomalies Classification Using Deep Learning

IDS is a piece of software that uses machine learning methods to detect network intrusion. IDS protects a computer network from unwanted access by monitoring it for malicious behavior. IDS ensures speedy and effective detection of known anomalies while minimizing the danger of false alarms by utilizing the signature database. It examines various sorts of attacks, detects dangerous content patterns, and assists administrators in tuning, organizing, and implementing effective restrictions. In this paper we have decided to only focus on Brute force and Dictionary attack because the are common attacks among smart home user.

3.2.1 Brute-Force Attack

Brute Force is a hacking technique used to find out the user credentials by trying various possible credentials. It is a kind of intrusion with aim of guessing the credential, use a trial-and-error approach on the username and password list of the targeted domain.

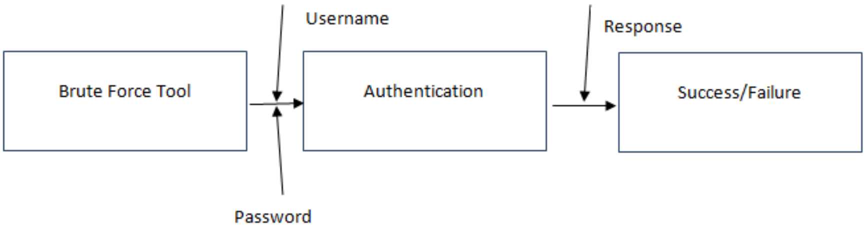

Fig 3.2 Brute Force Attack

First there a brute force tool to which you feed username and password; this could be one username and a list of passwords. This brute force tool will send these username and password or the combination of the username and password to the web application or to the application in general where the username and password is checked it is authentication and depending on the response of the application tool. It will decide the status of tried credential whether they are right or wrong. If the login is successful the n the username and password is considered to be right, otherwise the combination of username and password will be considered wrong. This is how a typical force attack works.

3.3.3 Dictionary Attack Detection System

The security architecture we implored to detect dictionary attacks within the smart home was designed like decision tree. the choice tree helped the safety system classify data supported the conditions we set for key security variables. We got common dictionary key phrases that attackers use to attack password systems. the info was accustomed filter user credentials in other to detect dictionary attacks within the smart home.

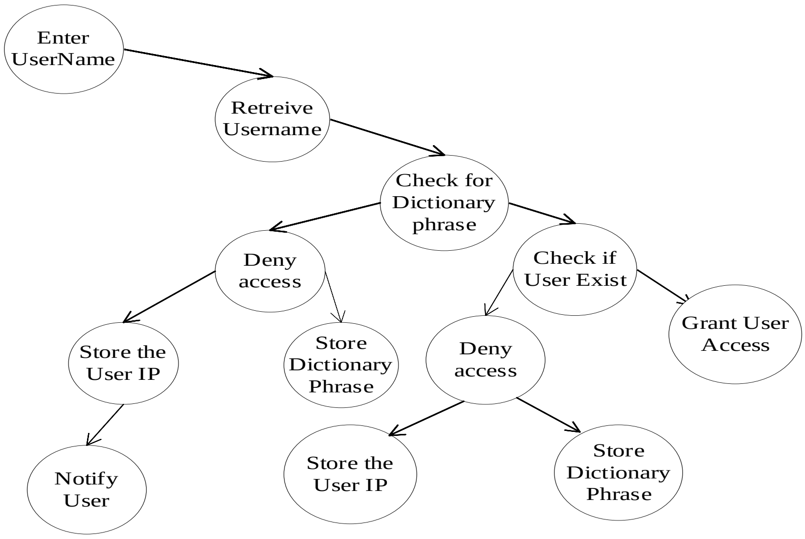

Fig. 3.3: System Diagram of the Dictionary Detection Decision Tree

The Dictionary Detection Decision two-dimensional figure shows the way the system detects dictionary attacks within the system and therefore the decisions being made by the system to mitigate dictionary attacks. the choice tree depends on input from the user which the system uses to create a choice. the choice tree allows the safety system to be dynamic by reacting to dictionary checks done at two levels a call tree the primary level is when the user enters the username and also the second level occurs when the user enters the password. The system features a dictionary dataset which is employed to validate username and password made during authentication.

3.4 Intrusion Detection and Anomalies Classification Using Deep Learning

From figure 3.3 the input is fed via internet enable device and data verification and authentication is carried out. The purpose of Data aggregation is to helps the collected data to be searched, gathered, and presented in a report-based, a summarized format which in turn aid human analysis. The application of a deep learning algorithm is to work independently to detect anomaly detection and if an anomaly is found. It will be classified into different categories of threat/attack and this will swiftly notify the system administrator.

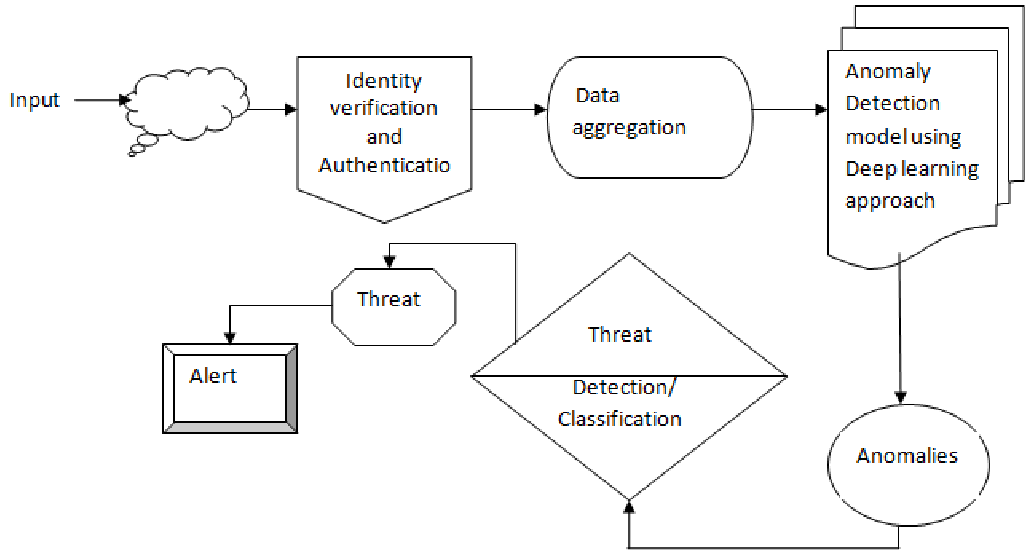
Input
Identity verification and Authenticatio
Data aggregation
Anomaly Detection model using Deep learning approach
Threat
Alert
Threat
Detection/ Classification
Anomalies

Figure 3.3: Intrusion Detection and Anomalies Classification Using Deep Learning

IV. RESULTS AND DISCUSSION

Table 4.1: Dictionary Attack Detection Table

Date	User Name	Attempts	Dictionary detected	IP Address Detected	Security Action
1/10/2021	bb2700	3	2	3.13.192.206	Block & notify
15/10/2021	uche2100	1	1	204.11.58.46	Notify
1/11/2021	Uguah41	3	2	129.168.58.47	Block & notify
5/11/2021	Elon74	2	1	192.20.76.48	Notify
20/11/2021	kaka	2	1	192.20.58.50	Notify

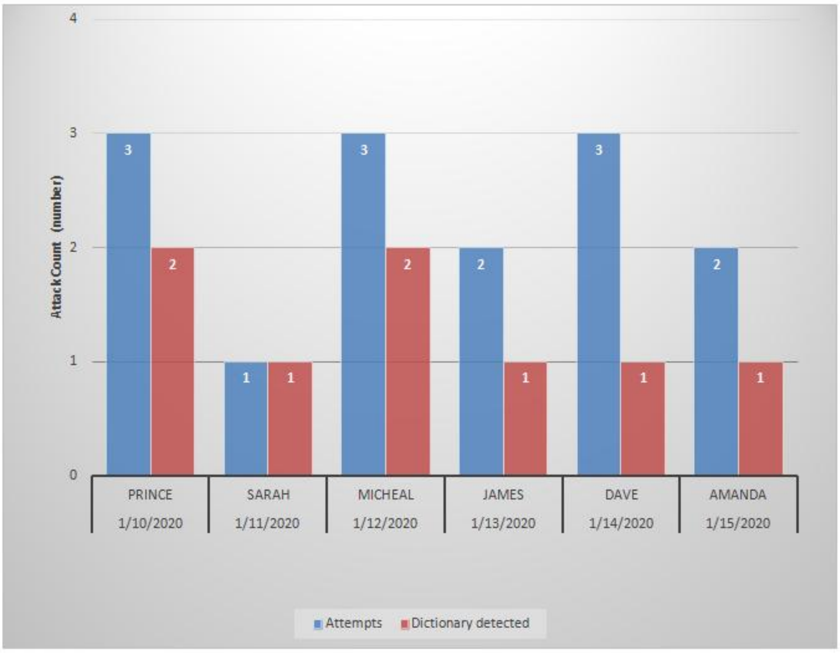

Fig. 4.1: Dictionary Attack Detection Graph

Figure 4.1 shows the attempted attacked on his smart home user's account.

Table 4.2. Classification of attack to brute force and dictionary

Month	Brute-Force	Dictionary Attack
Oct	10	4
Nov	6	7
Dec	22	16
Jan	7	10
Feb	33	20
March	5	10

Table 4.2 show attempts by hacker between Oct 2021– March 2022. These attacked were successfully classified to either brute force and dictionary attack. The figure 4.2 below show the visualization of these attack on line graphs.

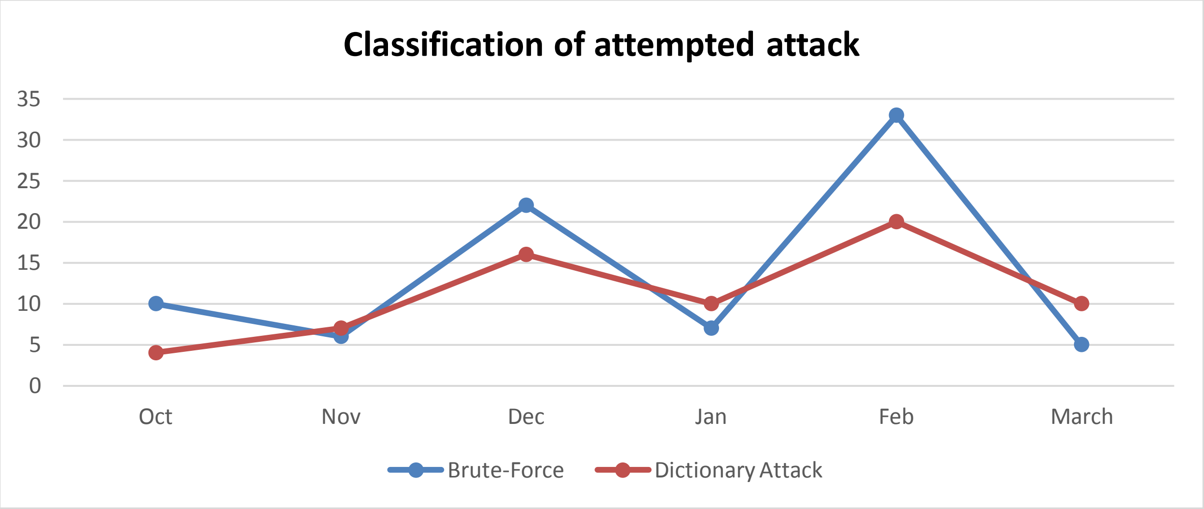

Fig 4.2 Intrusion classification.

Fig 4.2 displayed the visualized chat of the numbers of attempted an intruders made between Oct 2021 – March 2022 and it was successfully identified and classified to brute-force or dictionary attack as shown in table 4.2

V. DISCUSSIONS OF RESULTS

In Table 4.1 we showed user and number of attempts to gain access to smart home control panel. The developed model only triggers against an un-authorized user that has made three failed attempts to access smart home. Immediately after the third attempts is made, the access button will be disabled for 15 seconds. During the interval, a message will be sent to administrator about the malicious attempt. This message will contain the IP address of an intruder, the date and classifications of the intrusion. The model also has capacity to learn from historical dataset. This enabled the model to classified the intrusion to either dictionary, brute-brute force or un-known. "We used deep neural network (DNN), a type of deep learning model, because it enables us to develop a flexible and effective IDS to detect and classify unforeseen and unpredictable cyber-attacks. The DNN model learns the abstract and high dimensional feature representation of the IDS data by passing them into many hidden layers. Through a rigorous experimental testing it is confirmed that DNNs perform well in comparison to the classical machine learning classifiers. This developed model monitors a network or system for malicious activity and protects smart home network from unauthorized access from users. This Model ensures quick analyzes of different types of attacks, identifies patterns of malicious content and help the smart home owner to tune, organize and implement effective controls over suspicious users. We made use of NSL-KDD dataset. The KDD data set is a well-known benchmark in the research of Intrusion Detection techniques. The analysis is done with respect to two prominent evaluation metrics, Detection Rate (DR) and False Alarm Rate (FAR) for an Intrusion Detection System (IDS) and anomaly classifications Finally, our implemented IDS model is highly scalable which can be used in real time to effectively monitor the network traffic and host-level events to proactively alert possible cyber-attacks. The experiment started with training the system where we used one hidden layer and one hidden unit. This turned out to be a binary classification problem where the classifier classifies the intrusion anomalies. Hence, we used the evaluation metrics for classification like accuracy, precision, recall, false positive rate. In order to use this application a user must be registered in the system before he/she can have access to the smart home. The information to be provided by the users are email, phone number, first name, last name and username. A new user that has been registered and tried to access the home has to input his login details. It is evident that an attacker will have lower success rate in our implemented System. The attack attempts and possible intrusion can be visualized from fig 4.1. From fig 4.2 it can be seen that there are more brute-force attack on the smart users than dictionary attack.

VI. CONCLUSION AND RECOMMENDATION

In recent years, due to the emergence of unlimited communication paradigm and increased number of networked digital devices such as smart homes technology, there is a growing concern about cybersecurity which tries to preserve either the information or the communication technology of the system. Intruders discover new attack types day by day, therefore to prevent these attacks firstly they need to be identified correctly, and then proper responses should be given. This research work was centered on optimizing security of smart home intrusion detection and anomalies classifications using deep learning. We have implemented an improved intrusion detection and anomaly classification using deep learning algorithm. The model is trained and tested with NSL-KDD dataset which is more in line with the data characteristics of the new era than the traditional dataset. The experimental results show that the implemented intrusion detection model has achieved remarkable results in improving the accuracy, performance, and efficiency of intrusion detection. We settled for Anomaly based intrusion detection system because is better option than signature-based system since it does not require prior knowledge of attack signature before it can be used to detect an intrusion. And this model has been proved to avoid security gaps and optimize user’s confidentiality by providing an extra level of protection in smart home. With positive result obtained after tested the developed model, we are recommending that, this secured smart home intrusion detection and classification of anomalies using deep learning approach be deployed as a user reminder, energy management and security measure in smart homes so as to optimize overall smart home system. Software needs to be constantly upgrading to meet new challenges. Thus, we are encouraging the future works to add biometrics such as fingerprints as a means of smart home user authentication and authorization. This will reduce an intrusion from a stranger which in turn keeps smart home safe.

REFERENCES

[1]. Satpathy, L. Smart Housing: Technology to Aid Aging in Place. New Opportunities and Challenges. Master’s Thesis, Mississippi State University, Starkville, MS, USA, 2006.

[2]. Alam M.R., Reaz M.B.I., Ali M.A.M. 2012. A Review of Smart Homes Past, Present and Future. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews. 42(6): 1190-1203.

[3]. Zhao Alam and Ali (2017) "A living laboratory for the design and evaluation of ubiquitous computing On the use of Pattern Matching for rapid Anomaly Detection in SmartGrid

[4]. Petersen, J., Larimer, N., Kaye, J. A., Pavel, M. and Hayes, T. L. (2012). “SVM to detect the Issues and Challenges for Cyber Physical System. In Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on Int'l Conference on Cyber, Physical and Social Computing (CPSCom), 733

[5]. GerfriedCebrat Aditi Dixit and Anjali Naik (2014) “work on the use of Prediction Algorithms Smart Homes”.*IEEE Trans. Syst., Man, Cybern. C, Appl. Review*, 39, 240 – 245

[6]. Mohannad, E., Helal, H. A., Abdulrazak, B. and Jansen, E. (2015). Self-sensing spaces: smart plugs for smart environments. In: Proceedings of the third international conference on smart homes and health telematicSherbrooke, Canada

[7]. Cenedese, A., Zanella, A., Vangelista, L., &Zorzi, M. (2014). Padova smart city: An urban Internet of things experimentation. Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014.

[8]. Mubashir, M., Shao, L. and Seed, L. (2013). “A survey on fall detection: Principles and on videobasedhuman activity recognition,” *Computers*, 2 (2), 88–131

[9]. Sleman, A., & Moeller, R. (2011). SOA distributed operating system for managing embedded devices in home and building automation. 2011 IEEE International Conference on Consumer Electronics (ICCE).

[10]. Thati, J., Kumari, P. V., & Narayana, Y. (2017). Controlling of home appliances through internet. 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS).

[11]. Cebrat, G. (2014). Secure web-based home automation: Application layer-based security using embedded programmable logic controller. 2014 2nd International Conference on Information and Communication Technology (ICoICT).

[12]. Soliman, M., Abiodun, T., Hamouda, T., Zhou, J., & Lung, C. (2013). Smart home: Integrating Internet of things with web services and cloud computing. 2013 IEEE 5th International Conference on Cloud Computing Technology and Science.