IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 6, June 2021

DOI 10.17148/IJARCCE.2021.10602

Predicting Home User Activities in a Secured Smart home Using Internet of Things and Deep Learning

Chidera Okara[1], N.D Nwiabu[2], V.I.E Anireh[3]

Department of Computer Science, Rivers State University, Port Harcourt, Nigeria[1,2,3]

Abstract: The innovation Smart home is a home where appliances can be remotely controlled and monitored with the help of a network connection. Despite the numerous advantages of smart home, the security of smart homes has been a concern to home users also, smart home can improve in predicting user activities in the home. In this research work, we were able to predict home user activities in a secured smart home. A software interface was provided for One Time Password (OTP) authentication and for controlling home appliances. The use of deep learning model enables us to predict accurately, when appliances homes should be ON or OFF. The prediction was made from previous appliances historical dataset. The home security was enhanced with one time password and decision tree to detect dictionary attacks. The result gotten from the prediction system showed series of predictions made by the system at different time interval. The security result shows how effective the smart home security system is in mitigating attacks in the home.

Keywords: Smart home, Security, One Time Password, Internet of Things, Machine Learning.

1. INTRODUCTION

As technology is still evolving, there is not a specific standard to define a ‘smart home’ nor a distinctive feature to classify ‘smart home’ [1] In relation to various related terms used and from similar other systems, we can say a smart home is a convenient home setup where appliances and devices such as lighting and heaters can be automatically controlled remotely from anywhere with an internet connection using a mobile or other networked device (Jam, 2020). The advent of Internet of Things (IOT) has made it possible to interconnect home devices in order to provide remote management for devices in a smart home. It is not just connecting things, devices, appliances and machines to the internet but to allow these things to execute while achieving common user and machine goals. Smart homes have to meet certain goals for communicating and exchanging data with surroundings [2]. We have from machine to corresponding environment, machine to machine, machine to human and human to machine. Security has become a major concern in smart homes. Smart home users suffer from identity theft where an attacker infiltrates the database of a smart home which allows the attacker to steal personal user data that could be used by the attacker. Smart home also suffers property damage where an attacker gains access into the home and intentionally uses the home appliance to facilitate a disaster like a fire outbreak [3].

Machine Learning (ML) is not a new concept. ML is closely related to Artificial Intelligence (AI). AI becomes feasible via ML. Through ML, computer systems learn how to carryout tasks such as classification, clustering, predictions, pattern recognition, etc. Machine Learning systems need to undergo a learning phase that is why the systems are trained using various algorithms and statistical models to analyse sample data. The data used to train the system are usually characterized by measurable characteristics called features and an ML algorithm attempts to find a correlation between the features and some output values called labels. The data obtained during the training process is used to help the system identify patterns or make decisions based on new information gotten by the system. ML is ideal solution for problems such as classification, regression, clustering, and association rules determination. The learning mechanism of ML system vary and can be grouped into Supervised learning, Unsupervised learning, Semi-supervised Learning and Reinforcement Learning. Supervised learning is an ideal solution for problems involving regression such as estimating life experience, weather forecasting, and population growth forecasting, by using algorithms like Linear Regression or Random Forest. Additionally, supervised learning addresses classification problems such as digit recognition, speech recognition, diagnostics, and identity fraud detection, by using algorithms such as Support Vector Machines, Nearest Neighbour, Random Forest, and others. There are two phases in supervised learning. The training phase and testing phase. The data sets used to train the system requires known labels on them. The algorithms learn the relationship between the input values and labels and try to predict the output values of the testing data [5].

DOI 10.17148/IJARCCE.2021.10602

We propose a smart home system that will predict home user's activities by using integrating Deep Learning and Internet of Things. The system will utilize decision tree to detect dictionary attacks in the Smart Home. The use of a One Time Password (OTP) can help mitigate security flaws in smart homes where the user is sent a unique password when they access the smart home [7]. The research work will help change the security perspective people have on smart homes which has been a limitation to its general acceptance [8]. The project predicts home user's activity and upgrades the security of current smart homes.

2. RELATED WORKS

A review of related relevant research work in smart home and Internet of things are included in this section. Gerfried Cebrat [9] 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 [10] 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.

Thati [12] 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.

Mohamed [13] 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 [11] 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.

Wu [14] 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.

In 2015, Ghazal [15] proposed a Smart home automation system for elderly, and handicapped people using XBee and a smart multi- sensor system based on advanced telecommunication. The system made it possible for disabled and elderly people to control appliances in the home with a remote control. The system monitors IoT devices of the home using the smart sensors in real time.

The work of Ghazal [15] discussed some of the early challenges faced by home computerization systems. These include high manufacturing costs, high development costs, high installation costs, additional service and support costs, lack of home computerization standards, consumer unfamiliarity with technology, and complex user interfaces. With the advancement of time, we saw an exponential development in technology and processing power which leads to a reduction in device cost and size. All of these factors have contributed to the popularity of electronic devices today, so people are no longer confused or unsure about the use of computers, mobiles, or tablets. A lot of home automation protocols, communication and interface standards were defined overtime [16]. All these factors contributed to addressing the challenges and concerns of early home automation systems, which lead to the popularity and wide acceptance of computerized homes.

The study done by Sleman [17] 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.

3. METHODOLOGY

We adopted a Research Methodology called Structured System Analysis and Design Methodology (SSADM) in this project because it involves the application of a sequence of analysis, documentation and design tasks concerned. SSADM divides an application development cycle into modules, stages, steps, and tasks, and provides a framework for describing projects in a fashion suited to managing the project. SSADM's objectives are to:

1. Improve project management and control,
2. Make more effective use of experienced and inexperienced development staff
3. Develop better quality systems.

4. Make projects resilient to the loss of staff.
5. Enable projects to be supported by computer-based tools such as computer-aided software engineering systems.
6. Establish a framework for good communications between participants in a project.

3.1 SYSTEM DESIGN

The system will be integrating Internet of things (IoT) and Deep learning to secure smart homes. The system will use OTP 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.

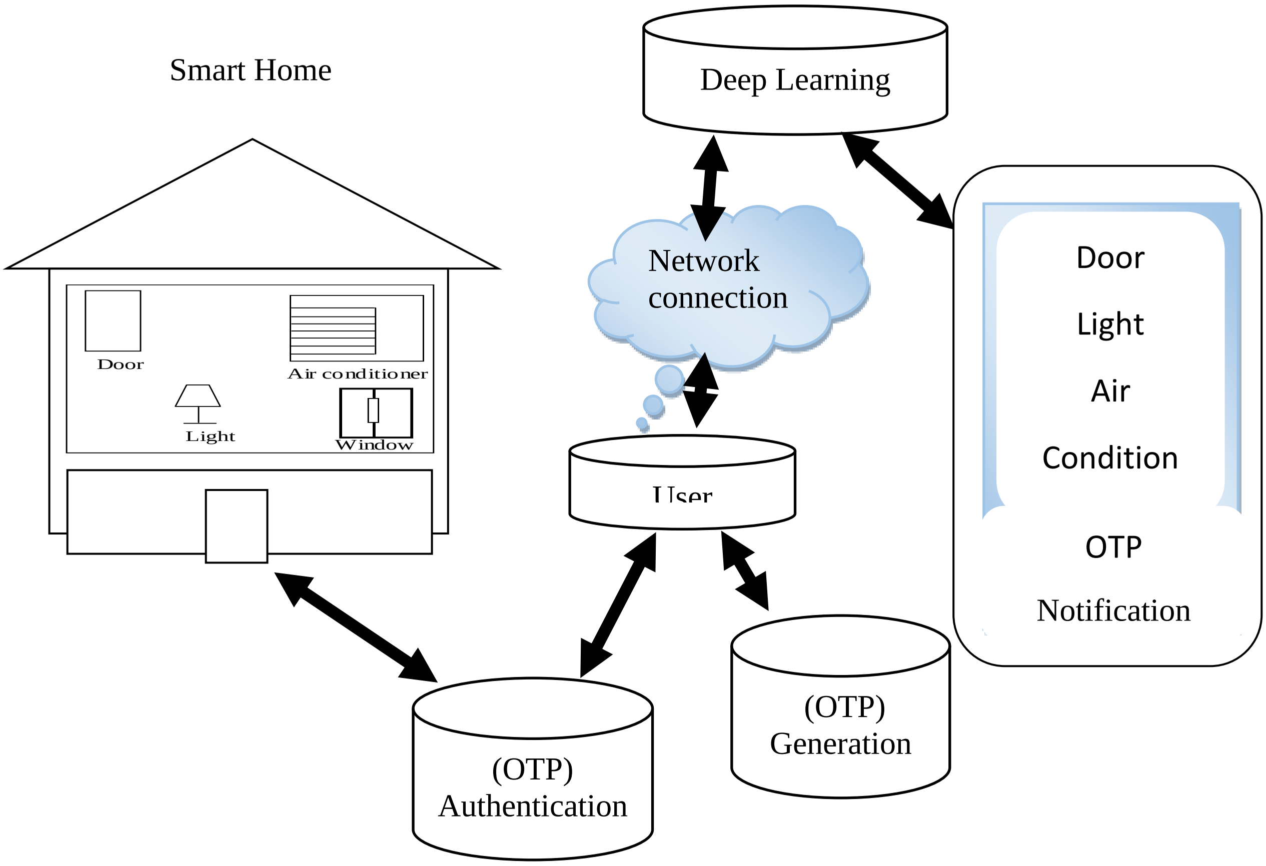

Figure 3.1: System Diagram Users Activity Prediction System for Smart Home

The system Integrate Internet of Things (IoT) and deep learning to secure smart homes using One Time Password (OTP). It is a smart home system that is based on its learning on the user's regular activities. This project was aimed at creating a smart home as a rational agent, monitoring the state of the home through sensors and acting in response to the environment to maximize the comfort and security of its residents while minimizing the operation costs. In order to achieve this objective, the system must be trained to be able to sense and predict the occupants' mobility habits and their use of electrical appliances and utilize email notification to send the One Time Password (OTP).

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 6, June 2021

DOI 10.17148/IJARCCE.2021.10602

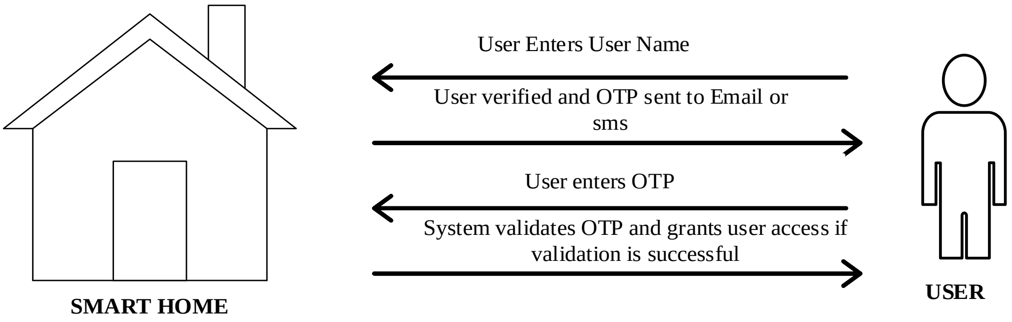
User Enters User Name
User verified and OTP sent to Email or sms
User enters OTP
System validates OTP and grants user access if validation is successful
SMART HOME
USER

Figure 3.2: System Diagram of the OTP Security System

The diagram in fig 3.5 shows the interaction between the user and the home during authentication. The user initially provides his username as a way of identifying a home user. The system then checks if the user exists before sending an OTP which the user will need to enter within a 10minutes timeframe before he is given access to the home. Failure to provide the correct OTP or providing the OTP after 10minute will lead to authentication failure.

3.1 DICTIONARY ATTACK DETECTION SYSTEM

The security architecture used to detect dictionary attacks in the smart home was designed using decision tree. The decision tree helped the security system classify data based on the conditions we set for key security variables. We got common dictionary key phrase that attackers use to attack password systems. The data was used to filter user credentials in other to detect dictionary attacks within the smart home.

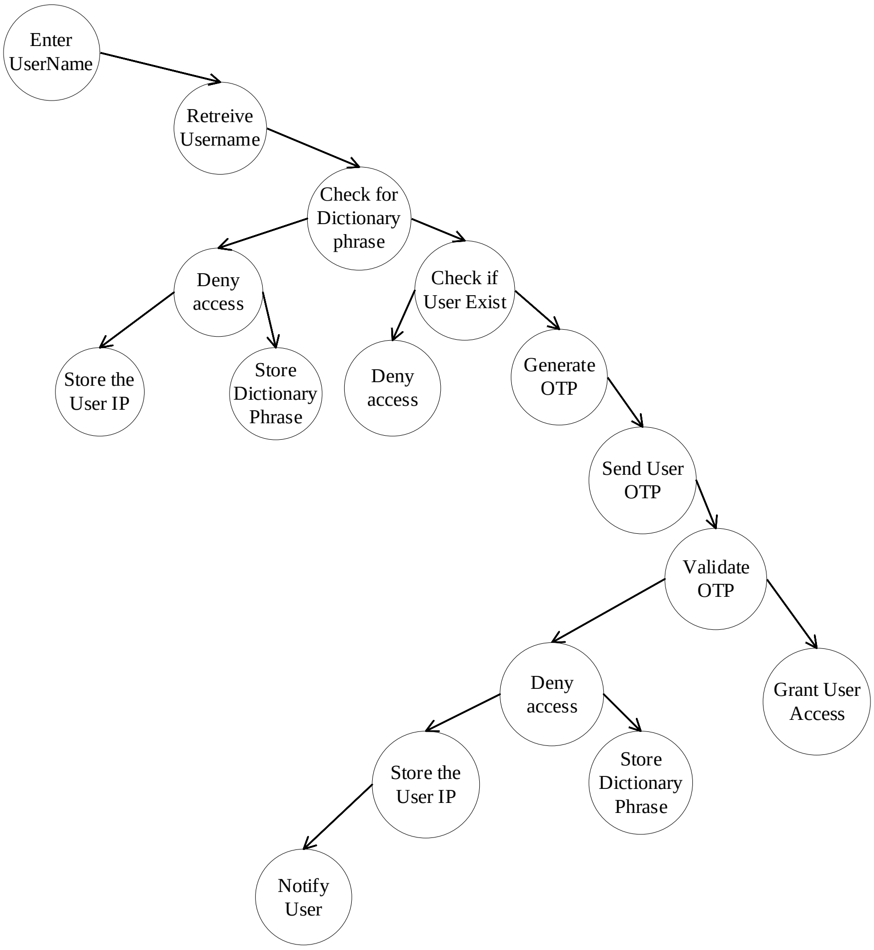

Figure 3.3: System Diagram of the Dictionary Detection Decision Tree

DOI 10.17148/IJARCCE.2021.10602

The Dictionary Detection Decision Tree diagram shows the way the system detects dictionary attacks in the system and the decisions being made by the system to mitigate dictionary attack. The decision tree depends on input from the user which the system uses to make a decision. Decision tree allow the security system to be dynamic by reacting to dictionary check is done at two levels a decision tree the first level is when the user enters the username and second level occurs when the user enters the one-time password. The system has a dictionary dataset which is used to validate username and password made during authentication.

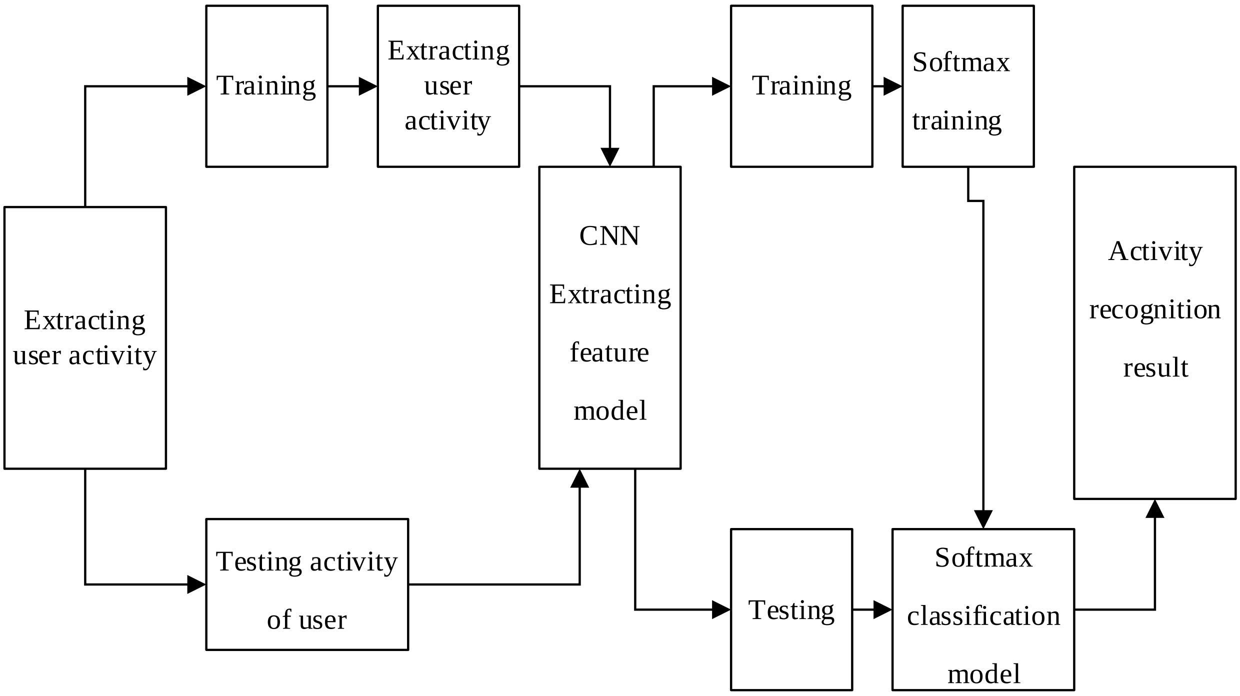

Fig 4.3: The overall block diagram for deep learning training Algorithm

In the deep learning algorithm Kinect was used to obtain the position of activity of the user, and the activity recognition instructions of various households were defined. The Convolutional neural network (CNN) model was established, the sample activity will be captured and labelled, and each kind of activity training illustration was input into CNN to train the model, which helps in adjusting the model until it turns to be astringency; the output layer was transformed into a soft Max classifier. Input test activities to identify the accuracy of validation results. Through this model, the behaviour of human was recognized accurately and efficiently, and finally the desired results were achieved.

4. EXPERIMENT

The result includes the dataset used to train and test the performance of the system Necessary results obtained from the test will be given. The result representation for the security feature in the project includes the dictionary detection table for simulated attacks in the smart home it shows how the system was able to detect dictionary attack and store information of the attacker.

Table 5.1: OTP Generation Table (Model 2)

User name	One Time Password	Generation Date	Expiration Date	Actual Date	STATUS
Chidera	Jmw&G9	2021-04-16 06:40:49	2021-04-16 06:50:49	2021-04-16 06:40:49	Valid
Mike	rHs3t#	2021-04-16 06:30:40	2021-04-16 06:40:40	2021-04-16 07:40:40	Expired
Sarah	HsF3p!	2021-04-16 07:40:00	2021-04-16 07:50:00	2021-04-16 07:44:00	Valid
Peter	V8O!UQ	2021-04-16 06:40:00	2021-04-16 06:50:00	2021-04-16 07:40:40	Expired

Table 5.1 shows an OTP generation for users in the Smart Home security system. The result shows the different time a one-time password was generated by users and the status of the OTP at the time the user uses it. The one-time password

is set to expire in 10 minutes. The system compares the time the user keys in the password with the expiration time if the actual time exceeds the expiration time, then password is classified Expired. Expiration time is derived from generation time plus 10 minutes.

Table 5.2: Dictionary Attack Detection Table (Model 2)

Date	User Name	Attempts	Dictionary detected	IP Address Detected	Security Action
1/10/2020	prince	3	2	3.13.192.206	Block & notify
1/11/2020	Sarah	1	1	204.11.58.46	Notify
1/12/2020	micheal	3	2	129.168.58.47	Block & notify
1/13/2020	james	2	1	192.20.76.48	Notify
1/14/2020	dave	3	1	224.11.58.49	Block & notify
1/15/2020	amanda	2	1	192.20.58.50	Notify

Table 5.2 shows a Dictionary attacks detected by the Smart Home security system. The result shows the number of dictionary attacks that the system was able to detect and the decision the system was able to take. The security actions carried out by the system are Block and Notify. Notification action is taken the immediately the system detects a dictionary attack. Block action on the user account occurs when the user incorrect password exceeds 2 times.

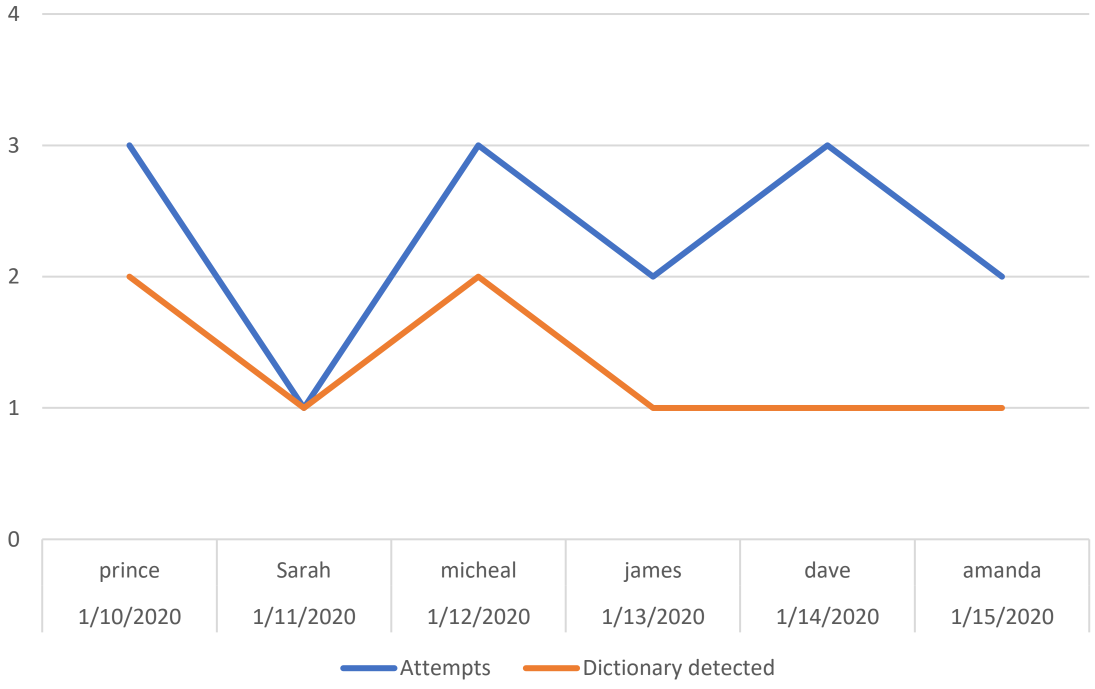

Fig 5.1: Dictionary Attack Detection Graph

The graph in fig 5.1 shows the frequency of attempts an attacker had on the system and the number of times the system detected a dictionary attack.

Table 5.3: Result Presentation Table for User Activities

Date	Device	Status	Actual Time	Predicted Time	Standard Deviation
1/1/2020	Light	on	17.00	17.00	0
1/1/2020	Light	off	6.50	6.50	0
2/1/2020	Refrigerator	on	18.30	18.30	0

2/1/2020	Refrigerator	off	7.30	7.30	0
1/1/2020	Television	on	18.45	18.45	0
1/1/2020	Television	off	8.00	8.00	0
2/1/2020	Television	on	18.47	18.46	0.00
2/1/2020	Television	off	8.45	8.23	0.0253125
2/1/2020	Light	on	17.30	17.15	0.075
2/1/2020	Light	off	6.30	6.40	0.05
3/1/2020	Refrigerator	on	18.40	18.35	0.024
3/1/2020	Refrigerator	off	7.50	7.40	0.05
3/1/2020	television	on	18.49	18.47	0.0002
3/1/2020	television	off	8.56	8.34	0.024938889
4/1/2020	television	on	19.40	18.70	0.243253125
4/1/2020	television	off	7.50	8.13	0.196878125

Table 5.3 shows over 48 hours home activities of a user mike with respect to time. The result captures the time activities was carried. The result also captures the deviation between the predicted activity time made the system and the actual time the activity occurred.

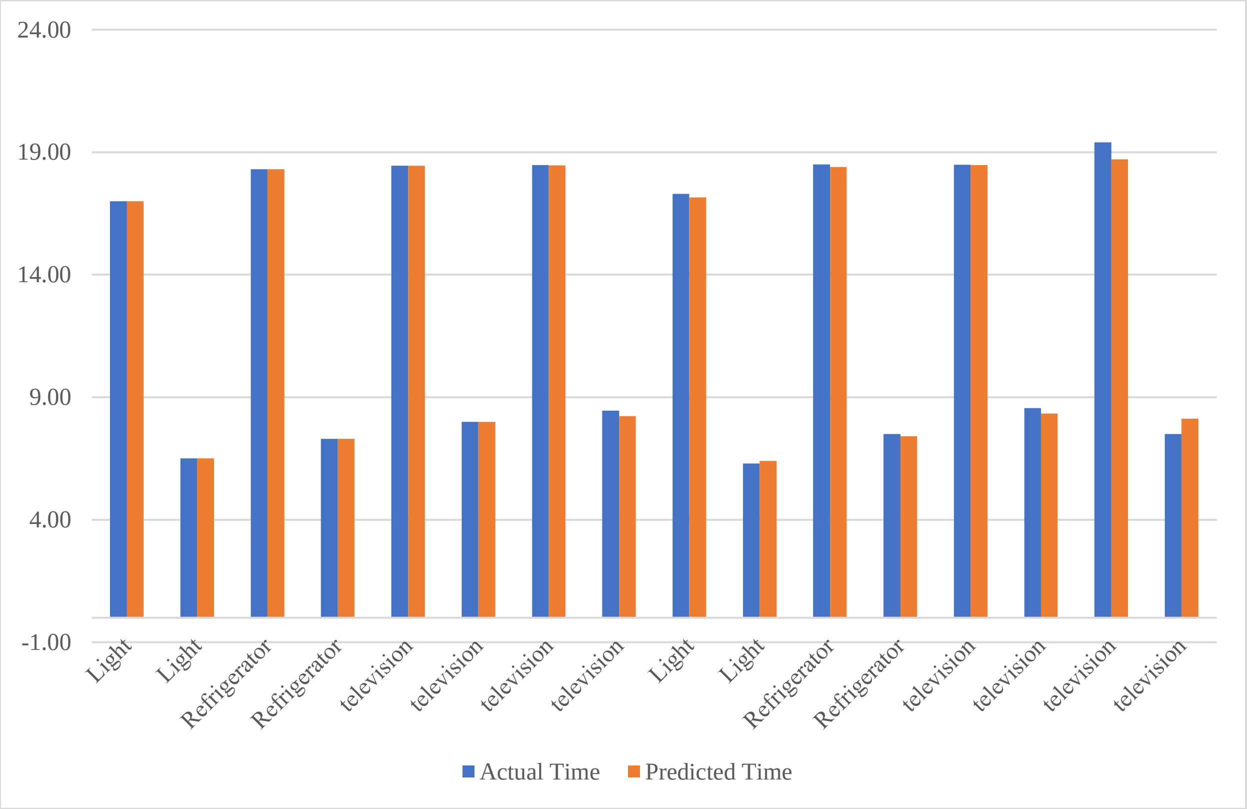

Fig 5.2: Home Devices Actual Time Prediction Deviation

The graph in fig 5.2 is a representation of the result captured in table 5.3. The graph compares the actual time with predicted time.

5. DISCUSSION OF RESULTS

In this paper, we provide the results of the system that predicts home user activities in a secured smart home using deep learning. 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 each sample as on/off. Hence, we used the evaluation metrics for classification like accuracy, precision, recall, false positive rate.

In this experiment section, we adopted deep learning as our algorithm for predicting user behaviour within the system. The algorithm has three layers the input layer, the hidden layer and the prediction layer. Data must pass through these three layers in order for the system to learn from the activities. The system also mitigated security challenge in the home with the one-time password. 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 was registered and tried to access the home using his username. A one-time password was sent to his email which expires in 10 minutes. We simulated dictionary attacks on the OTP smart home security. This was to determine the efficiency of the smart home security and to know the chance of success a hacker will have if a dictionary attack is carried out on the smart home. We simulated this security penetration test several times in other to get accurate result on the smart home security system. It was evident that an attacker will have lower success rate in our OTP password System. A test was carried out on prediction of user activity in the home. We were able to ascertain the level of accuracy predictions have by plotting graphs to show the deviation between the predicted time and the actual time the activity occurred.

6. CONCLUSION & RECOMMENDATION

This paper was centered on predicting human activity in a secured smart home using deep learning. The IoT device industry is undergoing rapid changes in only a few short years. The market has now grown to encompass enterprise players working together to create ecosystems, tailored for mobile technology, which allows IoT devices to become interconnected. This thesis was developed to optimize the efficiency of home appliances and learning the regular behavior of smart home users. Therefore, this model has been proved to avoid energy waste, bridge hazardous security gaps and optimize users' interaction with appliances by adequately providing an efficient smart appliances operational management.

In light of the knowledge acquired from this research, the tremendous value contribution to academic research and to the smart home in general even to smart home users, the researcher is recommending that this Internet of Things based smart home deep learning mechanism be deployed as a user reminder, energy management and security measure in smart homes as well as community energy management and to optimize overall smart home system. I encourage researchers to consider the entire home automation network, and improve voice attribute with advanced deep learning neural network scheme that will help identify and deter sophisticated, experienced and professional intruders and energy waste.

REFERENCES

[1] Batov, E. I. (2015). The distinctive features of "Smart" buildings. *Procedia Engineering*, *111*, 103-107.

[2] Jin, Z. (2018). Requirements and requirements engineering ∗ ∗This chapter serves to deliver general background knowledge about requirements and requirements engineering. *Environment Modeling-Based Requirements Engineering for Software Intensive Systems*, 3-11.

[3] A. Zandamela, A. (2017). An approach to smart home security system using Ardunio. Electrical Engineering: An International Journal, 01-18.

[4] Alaa, M., Zaidan, A., Zaidan, B., Talal, M., & Kiah, M. (2017). A review of smart home applications based on Internet of things. Journal of Network and Computer Applications, 97, 48-65.

[5] Al-Mashhad, A. S., Al-Arifi, S. A., Al-Kadem, M. S., Al-Dabbous, M. S., & Buhulaigah, A. (2016). Multilateral wells evaluation utilizing artificial intelligence.

[6] Kubat, M. (2017). Reinforcement learning. An Introduction to Machine Learning, 331-339.

[7] Kubat, M. (2017). Unsupervised learning. An Introduction to Machine Learning, 273-295.

[8] Geneiatakis, D., Medentzidis, C., Kounelis, I., Steri, G., & Nai Fovino, I. (2017). Android applications privacy risk assessment. Intrusion Detection and Prevention for Mobile Ecosystems, 99-116.

[9] Hajjej, F., Hamdi, M., Ejbali, R., & Zaied, M. (2019). A new optimal deployment model of Internet of things based on wireless sensor networks. 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC).

[10] 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).

[11] 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.

[12] 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.

[13] 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).

DOI 10.17148/IJARCCE.2021.10602

[14] Ibrahim, M., Elgamri, A., Babiker, S., & Mohamed, A. (2015). Internet of things based smart environmental monitoring using the Raspberry-Pi computer. 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC).

[15] Wu, S., Rendall, J. B., Smith, M. J., Zhu, S., Xu, J., Wang, H., Yang, Q., & Qin, P. (2017). Survey on prediction algorithms in smart homes. IEEE Internet of Things Journal, 4(3), 636-644.

[16] Ghazal, B., & Al-Khatib, K. (2015). Smart home automation system for elderly, and handicapped people using XBee. International Journal of Smart Home, 9(4), 203-210.

[17] Edden. (1990). Modelling cebus home automation with knowledge-based tools. IEEE International Conference on Consumer Electronics.

[18] 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).