IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June, 2019 E-ISSN: 2347-2693

Security of Smart Home Intrusion Detection Systems using Data Mining Technique

Queen .U. Agunya[1*], N.D. Nwiabu[2]

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

Corresponding Author: queenywilly87@gmail.com, Tel.: +234-9090275327

DOI: https://doi.org/10.26438/ijcse/v7i6.11691176 | Available online at: www.ijcseonline.org

Accepted: 23/Jun/2019, Published: 30/Jun/2019

Abstract— Poor security of Smart homes resulting from compromised system password and IP address has been on the increase as a result of hackers' access to system. For this reason, there is need to introduce tertiary security feature. This work presents comprehensive survey of security challenges in smart home intrusion detection systems using qualitative research methodology. The researcher provided design of tertiary security parameter- Soft token along side IP address and password that serve as primary and secondary parameters to optimize system. Object oriented analysis and design plan was similarly embraced to help indicate the relationship between object and its class. K-means algorithm as data mining clustering technique was used to aid intrusion detection and prevention in smart home i.e. the system was able to differentiate between authorized from unauthorized access and simultaneously, send security warning to the framework administrator's email whenever there is an intrusion. The development stage was done using some sets of software tools: PHP, HTML, JavaScript, and MySQL database system. Xampp server was used to test-run the system during the development process. Experimental result shows that soft token alongside IP address and password to check for an intrusion was able to optimize security.

Keywords— Smart Home, Intrusion Detection systems, K-Means algorithm, Password, Security, Soft token.

I. INTRODUCTION

Security of intrusion detection system is a mitigation strategy to prevent unauthorized access to smart home in view of lives/asset protection. In the present day, security frameworks assume a significant role in the assurance of lives and investments. This is accomplished by fusing various sub frameworks into the security framework with a solitary controller, for instance, observation, attacker regulator, flame discovery, and so on. As innovation progressed with time, electronic gadgets and web turned out to be increasingly prevalent and reasonable, so the concept of shrewd residence with individual's expectation from it has changed dramatically. The researchers concentrated on functions that smart home can offer for detection, prevention and response to safety hazards. Normal challenge emerges when smart home abilities are undermined. In this case, the residence may turn into a liability for the inhabitant(s) as opposed to a benefit [1]. Smart home applications range from promoting independent lifestyle for elderly users, energy efficiency, provide comfort, entertainment, and security [2], but the researcher has limited the work to security by deploying the use of IP address (primary security), password (secondary security) and software token (tertiary security) as the intrusion detection security variables to enhance security of smart homes intrusion detection systems using data mining technique. Internet protocol (IP) address is seen as a primary security because it is a unique arithmetical label allotted to every linked gadget on the web using network protocol for interaction [3]. Therefore, since our smart home is a web based system, the legitimate user's system automatically has an IP address while connected to the web (internet), so, intruders using their system to hack into the smart home is checked first for their IP address if it corresponds with the one the trained system already knows as normal. Password is seen as a secondary security tool because even if the system is in another person's possession, wrong password entry can also be used to check for intrusion. Software token as a tertiary security tool or parameter is configured in such a way that just few random digital codes are trained and given to the legitimate user or administrator and this can serve also as an enhanced security check for intrusion.

Data mining technique helps to detect patterns in the dataset and use them to detect forthcoming intrusions. It uses historical data to make future prediction i.e. in real life, we take the things we've seen previously & try to make future predictions. In this research, clustering technique is used in intrusion detection as malicious activities are clustered

together separating itself from non-malicious activities. To achieve this K-means clustering algorithm is proposed. This research aims at providing optimized security in smart home intrusion detection systems using data mining clustering technique.

The purpose of the contribution statement

This research aims at providing optimized security in smart home intrusion detection systems using data mining clustering technique. The objectives are:

1. To collect reliable data on the present security challenges in smart home using qualitative research method.
2. Using K-means algorithm as the data mining clustering technique to aid intrusion detection and prevention.
3. To provide, design, and develop tertiary security parameter – Soft token to enhance security of the system along side with IP address and password that serve as primary and secondary security features.
4. To provide security detection and notification whenever there is an intrusion.
5. To test and evaluate developed system efficiency.

The rest of the paper is organized as followed: section I contains introduction of smart home intrusion detection system, Section II contains the Related Work of the proposed systems, section III explains the methodologies and class diagram of the system, section IV contains the system design involving the architectural design and the essential steps taken for the intrusion detection system security, section V describes the result and discussion of the system are presented, section VI concludes the research work.

II. RELATED WORK

Utilization of infrared lattice in context aware smart home security framework to perfectly guess the position of users in their homes was suggested [4]. They also adopted static object check. It recognizes the position of an occupant by checking if he or she is close to a static object. This strategy is limited by environment's adaptability, for instance, if someone moves or changes the location of these static objects, the system becomes extremely confused, making recognition of home occupants difficult. Home security system on Intelligent Network (HSSIN) framework was described. The framework utilized a centralized control security methodology by consolidating numerous homes into security network with a control or chief hub committed to each zone depending on user quantity [5]. Centralized control framework has its special difficulties in that most homes in the area need to join for the approach to be more affordable and operative.

A conventional Bluetooth software design stack known as Smart home application protocol (HAP) was fabricated to make interaction between devices conceivable [6]. Gadgets in the home are linked to the host controller's phone with Bluetooth communication connectors for interaction. They have limited interaction range of 100m in an ideal situation. The work of [7] displayed a remote control system design and implementation by methods of worldwide system for mobile communication net and applied residence security framework utilizing microcontroller and Sony Ericsson GM-47 global system for mobile communication element. His work showed how two home applications were tentatively tested by means of computer-based condition. The rule task of the Machine to Machine (M2M) structure is checked and the secret key or PIN for the entry lock and home lighting framework is also given.

The researchers [8] proposed a framework for home security utilizing Radio service for general packets (GPRS). They used web camera to transmit home videos and photos from the legitimate user's phone via GPRS. In their work, video streaming was carried out using home web connection.

Researcher [9] work enables legitimate user to peruse and alter the status of gadgets at home utilizing pre-registered phone number with Radio service for general packets. Exactly when a genuine gadget with the correct phone number attempts to interface with the home environment, connection is set up between the simulated home mirroring the current state of the home contraptions and user. The researchers identified in their proposed framework that experienced attacker could trick the phone number of a legitimate user, such that he could control home gadgets or know its status.

The effort of [10] depicted the Double tone multi-recurrence (DTMR) based smart home framework design and execution. Here, the legitimate owner calls home phone number while controlling the gadgets of the home by producing DTMR tone. This tone is obtained, and then decrypted at home using a DTMR decoder via GSM module. Researchers [11] executed web based smart home framework for aiding remote access and electromagnetic innovation for gadget interaction in the home. The researchers used PC to execute duty of interface, web server, and database. They utilized RS 232 module as interaction interface. Interface of user was created and made available through the web by these researchers. They proposed utilization of secure socket layer (SSL) certificates that guarantees web server authenticity. Decentralized based smart home framework was proposed [12], by incorporating actuators into the home's network of wireless sensor (WSN). Researchers proposed distributed control or process design where sensor data is obtained and prepared by at least one control hubs, which in this way begins to modify or control the setting as formally indicated by the legitimate user. Major issue in decentralized based smart home security framework: sophisticated intruder(s)

having prior knowledge about the network data and actuator position can easily detach them because no notification mechanism is actualized to provoke the legitimate user about the attack(s).

III. METHODOLOGY

The researcher adopted qualitative research method and the system was designed using Object oriented methodology (OOM). Qualitative research method aims to gather in depth account of human behavior and belief within the settings they occur in. It seeks to describe the 'quality' and 'nature' of how people behave, experience and understand [13]. Object oriented methodology is a fresh method for framework growth by facilitating reuse of software modules. OOM requires that object oriented methods be utilized during analysis, design and execution of the framework [14].

The proposed system is a system that will secure the smart home intrusion detection systems using data mining technique; it is an optimized security system that doesn't only detect intrusion but also prevent intruder(s) from gaining access into a smart home and also makes use of software token to make the system more secured. Using K-means algorithm of clustering data mining technique [15], the system is trained to store the activities of only legitimate user. For the proposed system; combination of username, password and software token serves as input to the system but to check for intrusion, parameters used are ip address password and software token. Normal behavior of legitimate user stored in the historical database helps during extraction of features such that any information received as input are matched with behaviors stored in the database, if they match, access is granted otherwise access is denied following Anomaly-based detection approach which is based on a supposition that intruder's behavior is different from normal users' behavior [16]. This approach flags anomalous observed activities that behave differently than the defined normal behaviour of the system. This system basically works by detecting the processes deviating from the expected behaviour or the nodes behaving abnormally. The process of modelling the normal behaviour of network nodes is known as training [17].

A. Class diagram

Figure 1 depicts the structure of the proposed system which comprises of its classes, attributes, operations (or methods), and the relationships among objects. The framework process starts with identification process which extracts features of the legitimate user's (username, password, soft token). Subsequently, these features are used to authenticate or verify the users before access is allowed for them to perform various tasks in the smart home, which are stored in database.

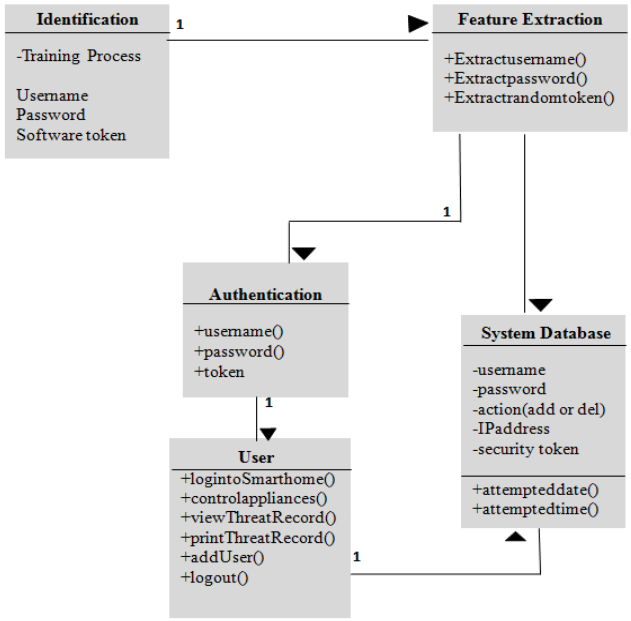

Figure 1 Class diagram of the proposed system

B. Data Set

In order to properly develop the proposed system, proper information was gathered through interview.

Intrusion Detection Security parameters

Password: Users should change their default password to a stronger one consisting of combination of symbols, numbers, uppercase and lowercase letters and system shall reject incompatible password orientation e.g. starting with two wrong letters or numbers. Peradventure, the legitimate user accessing device is stolen and that intruder wants to access the smart home, the system should block after two times wrong password entry.

System IP Address: Since every system has a unique IP address, a particular device the legitimate user uses to login has its unique IP Address, therefore this can be one major criteria to check for intrusion i.e. if the intruder uses different device to intrude, it means the IP address is different hence the system should consider this as an intrusion and an alert should be sent to the legitimate user.

Software token: In addition to password, random software tokens e.g. up to 4 to 5 different digital codes already trained is given to the legitimate user therefore even if a password is cracked because of the random nature of digital codes of software token used here, the security is stronger and thereby enhanced.

C. System Architecture

When user wants to gain entry to the home via web as seen in Figure 2, the system requests the user to supply the log

in credentials such as username, password and soft token. The Smart home controller (smartphones) takes the input data from the user, sends it to data mining. Data mining will capture the source address (IP address) and the password of the sender; it then compares it with normal behavior of the right user stored in the historical database. If correct, access is granted otherwise access is denied.

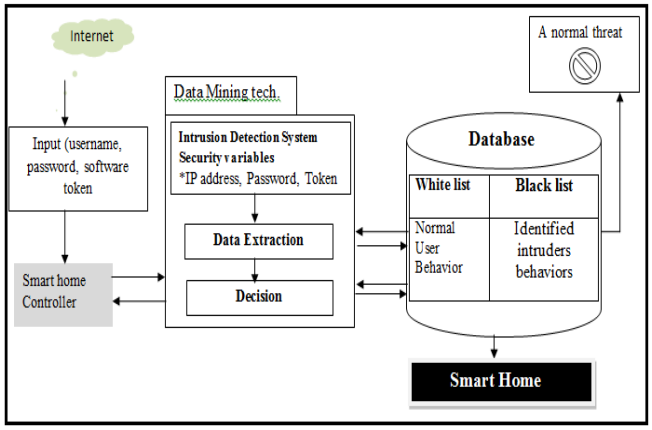

Figure 2 Architecture of proposed system

D. Data Mining clustering technique: K-means Algorithm

K-means clustering is a type of unsupervised learning used to identify groups of patterns in a collection of unlabeled data (i.e., data without defined categories) that behave similarly and dissimilarly. Those that behave similarly from the first stage and stands over time, for example, a particular ip address of a device, username, password, and software token is trained for a legitimate user, so, whenever that user wants to access the home with his/her login details, the information received or input is compared with the trained data, if similar, it is seen as normal or non-malicious entry/activity, access is granted but if dissimilar after comparison with the trained data, it is considered a malicious entry/activity, thus, access is denied. K-Means data mining clustering techniques used will help the admin filter his information based on the type of record he wants to retrieve.

Input:

Given $T_1, T_2, \ldots\ldots T_i$ // set of elements
k // number of desired clusters
Output:
K //set of clusters

K-means Algorithm:
randomly initialize values for mean $c_1, c_2, \ldots . c_k$;
repeat
assign each element T_i to centroid with the closest mean;
recalculate to find new mean to each cluster;
process is repeated;
until merging target is met;

Example : Suppose we have the following set of elements (user behaviors)

T_i = 2 5 6 8 12 15 18 28 30

And we want to divide them (elements or data point) into 3 clusters i.e. k=3 where k is the number of clusters

Step 1: Randomly initialize values for mean i.e. Select K no. of centroid farthest apart from each other i.e.
C1=2, C2= 12 and C3 = 30.

2	**5**	**6**	**8**	**12**	**15**	**18**	**28**	**30**
C1				**C2**				**C3**

Step 2: Assign each element T_i to centroid with the closest mean by utilizing Euclidean distance.

2	**5**	**6**	**8**	**12**	**15**	**18**	**28**	**30**
C1	c1	c1	c2	**C2**	c2	c2	c3	**C3**

Step 3: Recalculate centroids by finding mean of data points belonging to that same centroid.

Mean for C1 = 4.3 (New C1 centroid)
Mean for C2 = 13.25 (New C2 centroid)
Mean for C3 = 29 (New C3 centroid)

Step 4: Repeat steps 2&3 until merging target is met.

This algorithm works repeatedly to assign each data point to one of K partitions based on the similarity features that are provided such that k < n. K-means clustering intends to partition T elements into k clusters with each element belonging to centroid with the nearest mean. The aim of this algorithm is to minimize total intra-cluster variance, or the squared error function, which may be expressed as:

$$J = \sum_{i=1}^{k} \sum_{j=1}^{T} || T_i - c_k ||^2 \quad \ldots\ldots\ldots\ldots (1)$$

J = objective function,
k = number of clusters,
T = number of elements,
T_i = element i,
c_k = centroid for cluster k.
$|| T_i - c_k ||$ = Euclidean distance (selected space measure two point T_i and centroid c_k,) iterated over all k points in the i^{th} cluster, for all T elements.

Note: the squared error function prevents mean calculation to result in negative value(s).

V. RESULTS AND DISCUSSION

A. Results

Password-Soft token-based Security (Model 2)

This model uses the combination of IP address, password and soft token to optimize security. The use of soft token as a security model in addition to password has gained a lot of traction. So even if the password is lost, stolen or hacked, the second layer of security model will prevent any unauthorized individuals from gaining access thereby optimizing its security. For this system, random soft tokens e.g. up to 4 to 5 different digital codes are trained and given to the legitimate user to use interchangeably before the validity for a particular token expires.

Figure 3 shows where the entire intruder's information is kept during log in. This table captures the IP addresses, username, password, token, country, city, date and time of the attempted intrusions. The Action column shows where the admin confirms or deletes record of attempted intrusions. If admin clicks delete (x) button, record is deleted and when he clicks the other button, a dialogue box will ask to confirm or cancel and if he confirm access will be given at the next attempt, that means a user is added (not important).

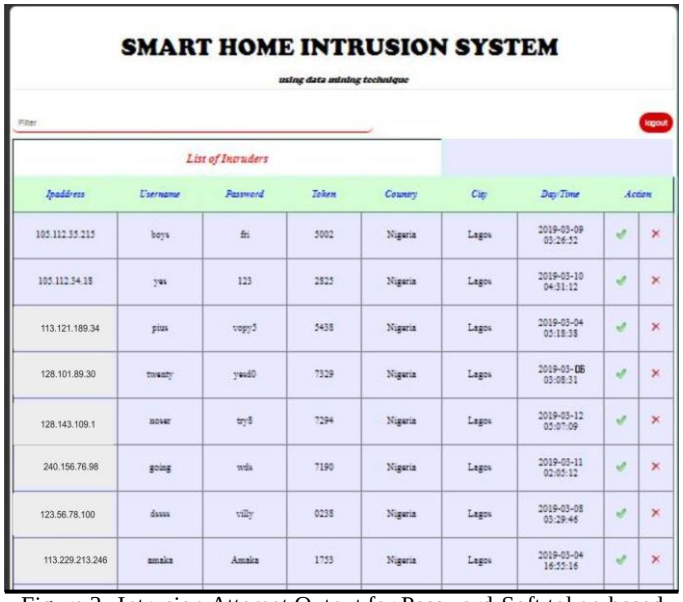

Figure 3 Intrusion Attempt Output for Password-Soft token-based security (Model 2)

Table 1 shows all attributes of the intruder(s) as shown above as well as the system intrusion frequency depicting the number of times intrusion occurred in the system. Zero (0) frequency indicates that intrusion was unsuccessful but details of intruder (s) where captured during attempt to log in with the model hence; there was "No Access". Intrusion was unsuccessful because one of the security variables must have been incorrect. For example, when there is an attempt to login to the system with IP address that is out of the range of the set IP address trained, also with incorrect password and soft token. One (1) frequency indicates that intrusion occurred just once on that particular day after database has been checked. For example, suppose a user is permitted access to the system by the administrator with all security variables correct, the database will still capture his/her details as an intruder for the administrator to know how frequent he accessed the system as to be able to track harmful intrusion.

Table 1 Result presentation Table for Model 2

DATE (March 2019)	TIME(HRS)	IP ADDRESS	USERNAME	PASSWORD	SOFT TOKEN	SYSTEM INTRUSION FREQUENCY	INTRUSION LEVELS
12th	1707	128.143.107.1	Noser	Try8	7294	0	0
11th	1405	240.156.76.98	Going	Uvdx	7190	0	0
10th	1631	105.112.34.18	Yes	1234	2825	1	2
9th	1526	105.112.35.215	boys	Fri	5002	0	1
8th	1529	123.56.78.100	Dssss	Villy	238	0	0
6th	1508	128.101.89.30	Twenty	Yard0	7329	0	0
4th	1718	113.121.189.34	Pius	vopy5	5438	0	0
4th	1655	111.229.213.246	Amaka	Amaka	1753	0	0
					TOTAL FREQUENCY	1	

Table 1.1 Intrusion Levels

System status	Conditions	Intrusion Levels
Intrusion detected/No Access	Incorrect IP address, Incorrect Password, Incorrect Token	0
Minor intrusion attempt/ No Access	Incorrect IP address, correct password, Incorrect token or Correct IP address, Incorrect password, incorrect token	1
Major Intrusion attempt/No Access (Access can be granted by administrator)	Correct IP address, Correct password, Incorrect token	2

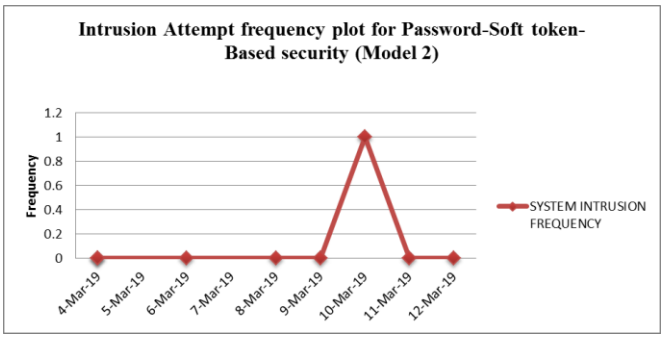

Figure 4 Intrusion Attempt plot for Password-Soft token-based security model

Password-based Security (Model 1)

Table 2 shows date, time, username, password, and login frequency or the number of times user (s) login into the system.

Table 2 Result presentation Table for Model 1

Date (March 2019)	**Time(Hrs)**	**Username**	**Password**	**System Intrusion Frequency 0=No access**
12th	1707	Noser	Try8	1
11th	1405	Going	Uvdx	1
10th	1631	Yes	1234	2
9th	1526	Boys	Fri	1
8th	1529	dssss(hacked via unsecured Wi-Fi network, phishing emails)	Villy	2
6th	1508	Twenty	Yard0	0
4th	1718	Pius	vopy5	0
4th	1655	Amaka	Amaka	0
			Total frequency	**7**

Comparison of Password-based Security (Model 1) with Password-Soft Token-based Security (Model 2)

For comparing the above two models in terms of optimization to security, we consider the intrusion frequency of the systems i.e. we measure how vulnerable a particular model is by taking the total of the occurrences of malicious system logins.

Table 3 Comparison Table for Model 1 and Model 2

Time (Hrs)	**Date**	**Model 1 System Intrusion Frequency**	**Model 2 System Intrusion requency**
1707	12-Mar-19	1	0
1405	11-Mar-19	1	0
1631	10-Mar-19	2	1
1526	9-Mar-19	1	0
1529	8-Mar-19	2	0
1508	6-Mar-19	0	0
1718	4-Mar-19	0	0
1655	4-Mar-19	0	0
	TOTAL FREQ.	**7**	**1**

Table 3 shows the comparison between the Password-based security model 1 and Password-Soft token security model 2. On 4-Mar-19 and 6-Mar-19, during testing of the both system models with IP address 111.229.213.246 and 113.121.189.34 at the same time (in hours), the systems were stable (No access). But on 8-Mar-19, Model 1 system was rendered unstable after being hacked; the system became very vulnerable to any type of security variables used. Model 2 system was able to detect the intrusion at that same date/time and access was denied based on incorrect security variable (s) used but even if some security variables like ip address, password are correct, because of the dynamic nature of soft token, it will be difficult to guess the codes hence they can't penetrate.

Model 2 as compared to Model 1 has shown great ability to detect and prevent intrusion based on the less frequency of intrusion occurrences. Thus, this has assured a higher or optimized level of security and reliability as compared to password-based security model.

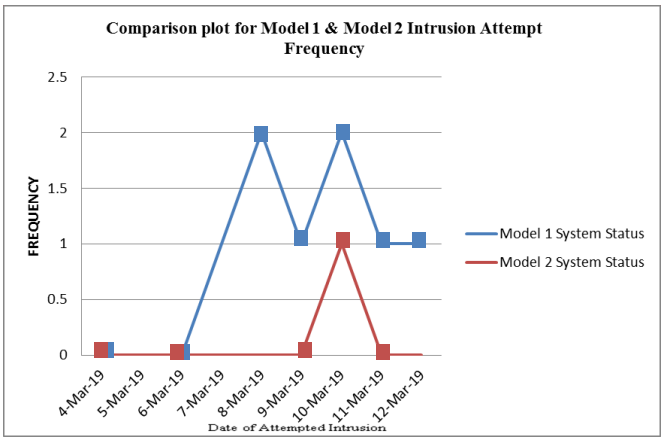

Figure 5 Comparison plot for Model 1& Model 2 Intrusion Attempt frequency

Figure 5 is an attempted intrusion frequency graph plotted against dates of intrusion captured during testing of the system. Firstly, the blue line indicates the number of times corresponding with dates of malicious logins (intrusions) for Model 1 (Password-based security model) while the red line indicates the number of times corresponding with dates of intrusions for Model 2 (Password-Soft token-based security model).

A. Discussion

This research focused on optimizing security of smart home intrusion detection systems using data mining. IP address, password, and software token are the primary, secondary and tertiary system security parameters used to checking for an intrusion. In other words, the proposed system is trained to be able to extract the IP address, username, password and software token of any user (legitimate or intruder) and then compares it to the real stored variables in the historical database prior to system access. Password-Soft token based security model is highly confidential but in addition, access to system also depends on allowable system IP addresses.

The results in this research work shows how the optimized security system was able to detect and prevent intrusions using the above stated model. However, to enjoy the privacy of a smart home, an anti intrusion system needs to be built to stop intruders from access to your smart home. It works in way when the intruder try to gain access to your smart home, notification is sent to the owner's email stating that an intruder or unknown person is trying to log in to her home and at the same time the system will retrieve the information of the intruder such as the IP address, Username, password, soft token, date, time as well as the location for proper identification of the intruder. The application of K-means algorithm filters or group information based on similarities during feature extraction and decision making with the help of a search bar.

The graphical result as shown in Figure 5 is an attempted intrusion frequency graph plotted against dates of intrusion captured during testing of the system. Firstly, the blue line indicates the number of times corresponding with dates of malicious logins (intrusions) for Model 1 (Password-based security model) while the red line indicates the number of times corresponding with dates of intrusions for Model 2 (Password-Soft token-based security model). Zero (0) frequency indicates that intrusion was unsuccessful but details of intruder (s) where captured during attempt to log in with the model hence; there was "No Access". Intrusion was unsuccessful because one of the security variables must have been incorrect. The number of times (frequency) intrusion occurred in Model 2 is extremely less as compared to Model 1. Hence, the Model 2 system is considered an optimized system.

VI. CONCLUSION

Smart homes are not common in Nigeria precisely in Rivers State and the few ones available are facing challenges of security of the intrusion detection system installed. Up until a few years back, user id and password combination (Password-based security model) has been the most common model used to secure these systems and networks. Nevertheless, with development of complex technologies, passwords can no longer be considered secured. In view of research data/information obtained locally in Port Harcourt, there were several cases of intrusion in smart home as a result of compromised username, password. Utilizing password model only has in fact proven to be the weakest link in smart home security framework. Hence, this model cannot guarantee maximum safety of the smart home intrusion detection framework. This work developed an optimized security system model which has additional form of security variable to authenticate user's identity. Therefore, this model has been proven to avoid security gaps and optimize user's confidentiality by providing an extra level of protection.

In light of the knowledge acquired from this research, the tremendous value contribution to academic research and to the security organizations even to smart home users, the researcher is recommending that this soft token be deployed as tertiary security parameter in smart home security as well as private/corporate web mail and website log on to optimize system security.

REFERENCES

[1] S. Chitnis, N. Deshpande & A. Shaligram, "*An Investigative Study for Smart home security: Issues, challenges and countermeasures"*, Wireless Sensor Network, 8(04), 61, 2016.

[2] C. Badica, & M. Brezovan, "*A Review on Vision surveillance techniques in smart home environments",* 19th International

Conference on Control Systems and Computer Science, pp. 471-478, 2013.
[3] M. Kumar & K. Shinde, "*Technical Report on Intruder Detection and Alert System"*, arXiv preprint arXiv:1509.09138, 2015.
[4] B. N. Schilit & M. M. Theimer, "*Disseminating Active Mop Infonncition to Mobile Hosts"*, IEEE network, 1994.
[5] S. M. Tsai, P. C. Yang, S. S. Wu, & S. S. Sun, "*A Service of Home security system on Intelligent network"*, IEEE Transactions on Consumer Electronics, 44(4), 1360-1366, 1998.
[6] N. Sriskanthan, F. Tan & A. Karande, "*Bluetooth Based smart home system.* Microprocessors and Microsystems", 26(6), 281-289, 2002.
[7] A. Alheraish, "*Design and Implementation of Smart home system*", IEEE Transactions on Consumer Electronics, 50(4), 1087-1092, 2004.
[8] M. Danaher & D. Nguyen, "*Mobile Home Security with GPRS*", ISI, 2002, 377-380, 2002.
[9] L. Yang, S. H. Yang, & F. Yao, "*Safety and Security of Remote Monitoring and control of intelligent home environments",* IEEE International Conference on Systems, Man and Cybernetics Vol. 2, pp. 1149-1153, 2006.
[10] L. Muhury & A. A. Habib, "*Device control by using GSM network",* 15th International Conference on Computer and Information Technology (ICCIT) IEEE pp. 271-274, 2012.
[11] A. Z. Alkar & U. Buhur, "*A Web based Wireless smart home system for multifunctional devices*", IEEE Transactions on Consumer Electronics, 51(4), 1169-1174, 2005.
[12] M. Gauger, D. Minder, P. J. Marron, A. Wacker & A. Lachenmann, "*Prototyping Sensor-Actuator Networks for Smart home"*, In Proceedings of the workshop on Real-world wireless sensor networks pp. 56-60, 2008.
[13] N.K Denzin & Y.S. Lincoln, "*The Sage Handbook of Qualitative Research",* Sage Publications 2017.
[14] E. Colbert, "*Requirement Analysis with the Object Oriented Software Development Method"*, 1998.
[15] N. Rehman, "*Data Mining techniques methods Algorithms and Tools",* International Journal of Computer Sciences and Mobile Computing, Vol. 6 Issue 7, pg 227-231, 2017.
[16] P. Rutravigneshwaran, "*A Study of Intrusion Detection System using Efficient Data Mining Techniques*", International Journal of Scientific Research in Network security and Communication, Vol. 5, Issue 6, 2017.
[17] P. Pareta, M. Rai & M. Gangwar, "*An Integrated Approach for effective Intrusion Detection with ElasticSearch*", International Journal of Scientific Research in Computer Sciences and Engineering, Vol. 6, Issue 3, pp.13-17, 2018.

Authors Profile

Queen .U. Agunya pursed her Bachelor of Technology from Sharda University, Greater Noida, New Delhi, India in 2010 and currently pursuing her Master of Science from Rivers State University in year 2016. She is a Redhat Certified System Administrator and Cisco Certified Network associate since 2012 and 2014 respectively. Her main research focuses on Network Security, Cloud Security and Privacy, Data Mining, IoT. She has 3 years of working experience in Oil and gas company and a year research experience.

Dr N. D Nwiabu pursed Bachelor of Science from Kwame Nkrumah University of Science & Technology, Kumasi, Ghana in 2002, and Master of Science from University of Port Harcourt, Nigeria in year 2006. He also obtained PgCert in Research Methods and PhD from Robert Gordon University, Aberdeen, UK in 2009. He is currently working as a lecturer in Department of Computer Science, Rivers State University, Nigeria since 2012. He is a member of IEEE computer society since 2011, a member of the NCS since 2005 and CPN since 2005. He has numerous publications and conference papers in reputed international journals including IEEE and it's also available online. His main research work focuses on Situation-aware systems, Pipeline monitoring, Decision support system, prediction system, etc. His work won awards in the North Sea, IEEE, MIT and EIM. His work has also got an application area in sociology to monitor crime. He has 16 years of teaching experience and over 10 years of Research Experience.

