A Project Report on

Home Automation System

Submitted in partial ful llment of the requirements for the award of the degree of

Bachelor of Engineering

in

COMPUTER ENGINEEING

by

ASHISH C KOTHARI (16102045)
SNEHAL SURVE (17202013)
ADESH THOSANI (17202001)

Under the Guidance of

Prof. Archana Kotangane

Department of Branch Name A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615
UNIVERSITY OF MUMBAI

Academic Year 2018-2019

Approval Sheet

This Project Report entitled HOME AUTOMATION SYSTEM Submitted by Ashish Kothari(16102045),Snehal.Surve"(17202013),Adesh.Thosani(17202001),is approved for the par-tial ful llment of the requirenment for the award of the degree of Bachelor of Engineering in Branch Name from University of Mumbai.

(Name)
Co-Guide

( )
Guide

Prof. Sachin Malve
Head Department of Information Technology

Place:A.P.Shah Institute of Technology,
Thane Date:

CERTIFICATE

This is to certify that the project entitled Home Automation system submitted by Ashish Kothari (16102045),Snehal Surve (17202013),Adesh Thosani (17202001), for the partial ful llment of the requirement for award of a degree Bachelor of Engineering in Computer Engineering. To the University of Mumbai, is a bona de work carried out during academic year 2018-2019.

( ) ( )

Co-Guide Guide

Prof. Sachin Malve
Head Department of Computer Engineering

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Place:A.P.Shah Institute of Technology,
Thane Date:

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, We have adequately cited and referenced the orig-inal sources. We also declare that We have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsi ed any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

(Signature)

(Ashish Kothari -16102045)
(Snehal Surve -17202013)
(Adesh Thosani -17202001)

Date:

Abstract

This project presents the overall design of Home Automation System (HAS) with low cost and wireless system . This system is designed to assist and provide support in order to fulfill the needs of elderly and disabled in home . Also, the smart home concept in the system improves the standard living at home. The main control system implements wireless technology to provide remote access from smart phone .As home energy use is increasing and renewable energy systems are deployed, home energy management system (HEMS) needs to consider both energy consumption and generation simultaneously to minimize the energy cost. This paper explains the evolution of device fingerprinting concept over time, and discusses various pitfalls in existing device fingerprinting approaches. In this paper, we propose a two-stage verification process for smart homes, using device fingerprints and login credentials, which verifies the user device as well as the user accessing the home over the Internet. The main control system implements wireless technology to provide remote access from smart phone.

Contents

List of Figures

List of Abbreviations

IDS:	Intrusion Detection System
WSN:	Wireless Sensor Network
MANET:	Mobile Ad-Hoc Network
AODV:	Ad-Hoc On-demand Distance Vector Routing
DSR:	Dynamic Source Routing Protocol
NS2:	Network Simulator 2
ACK:	Acknowledgement
AGT:	Agent
RTR:	Router

Chapter 1

Introduction

This project aims to enhance the home automation experience by collecting usage data from the user and applying prediction algorithms on it to predict the next step the user may take. Furthermore, external data will also be collected and correlated with the usage data in order to determine what external conditions may influence the user's behaviour. This involves data like weather data and traffic data. Most present-day smart homes use simple reflex agents for automation. Simple reflex agents are non-flexible and can work with limited perceptions and hard-coded actuation rules.
This could be established by limiting access to a home over the internet; Access should be limited to a fixed number of trusted people using a fixed number of trusted electronic devices. To achieve this, we have to identify the user as well as the device accessing the home over the internet

Challenges in Home Automation Security

In this section, we discuss why home automation systems are such an attractive target for an attacker, and the Challenges faced by a home automation system from the point of view of the homeowner and security engineer.

■ **Why Home Automation Systems are Such Attractive Targets for an Attacker**

- Data, information, video or audio feeds available from home are almost always personal.
- Almost all smart homes are connected to the Internet 24/7. This allows an attacker to be anywhere in the World and can still be targeting the home. Moreover, an attacker can cherry pick the moment of attack.
- Home automation systems don't have a dedicated system administrator, unlike a traditional network, which means that attackers can do their "foot printing" efficiently with comparatively less monitoring. When the network is compromised, there is also very little chance of detection.
- A homeowner who is also the system administrator may be reluctant to do the upgrades or patches necessary, like a homeowner's reluctance to do the plumbing. In addition to this, home automation systems could look very complicated to an ordinary non tech-savvy homeowner.
- Home automation systems usually consist of devices belonging to different manufacturers. Each comes with its own vulnerabilities. Moreover, home inhabitants who are not experts on networking or security do the Upgrade or reconfiguration of their own home networks, unlike researchers do in the labs, which brings in its Own set of vulnerabilities.
- An attacker always has the choice to scan the Internet for a specific vulnerability belonging to a specific home automation device from a particular manufacturer. An attacker can keep up the scanning process until finding the specific vulnerability they are looking to exploit.

1.1 Objectives of our work:

• Successfully identify a device accessing the home over the internet using Device Fingerprinting. Successfully identify a user accessing the home over the internet using his/her login credentials

. • Identify legitimate user even when there are changes in location, browser or other browser specific features, which happens over time.

• Identify malicious devices and create a ‘blacklist’ consisting of fingerprints of those devices that will not be allowed access to home. Identify legitimate devices and develop a ‘whitelist’ consisting of fingerprints of devices that are allowed access to the home

Chapter 2

Literature Review

In current situation home automation system is developed using many technology like IoT and cloud etc.
This survey of existing automation systems and coming up with improvements over them would not have been possible without help from some very respectable people and resources

For future work in the field of home automation security, we encourage the researchers to consider a home automation system as a whole and develop behaviour prediction and advanced sensing parameters that can help to identify and prevent skilled and sophisticated intruders.

2.1 Sensor Based Home Automation and Security System.

This is a web based home automation system in which user can interact with the system through a webbased user interface over the Internet. The system connected to home appliances. The main processor interacts with external components, viz. sensors, appliances and devices

.

Chapter 3

MACHINE LEARNING IN HOME AUTOMATION

3.1 Introduction

This Topic aims to enhance the home automation experience by collecting usage data from the user and applying prediction algorithms on it to predict the next step the user may take. Furthermore, external data will also be collected and correlated with the usage data in order to determine what external conditions may influence the user's behaviour. This involves data like weather data and traffic data. Most present-day smart homes use simple reflex agents for automation. Simple reflex agents are non-flexible and can work with limited perceptions and hard-coded actuation rules.

These rules may not suit all people. This rigidity in usability of present consumer automation systems forms the core of our problem. We intend to develop a software solution to this problem, which is centred on machine learning. This solution will be in the form of a learning agent that learns user habits by observation and anomaly detection.

3.2. EXISTING TECHNIQUES

Most modern home automation systems in the consumer market have evolved into one the following two categories, or some combination of these:

3.2.1Centralized Electronic Control Based

These are the systems where all conventionally electrical switching and regulating mechanisms are integrated into a single “smart” electronic device. In simpler terms, the electrical components are hidden behind electronic hardware that provides a simplified, compact, and often mobile control interface to the user. An example of this can be found in contemporary smart home systems where the user needs to install purposefully designed smart switchboards and smart appliances that can be controlled wirelessly by a central interface in the form of a smartphone application.

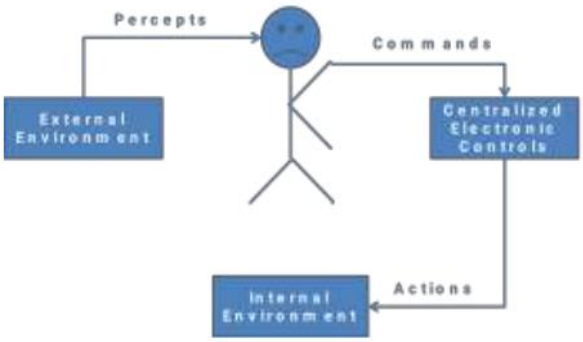
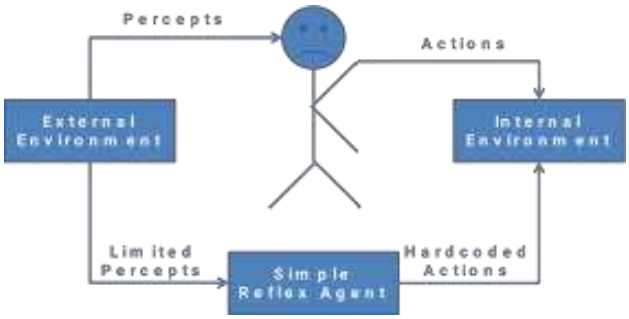


Figure 1: Type-I Automation System

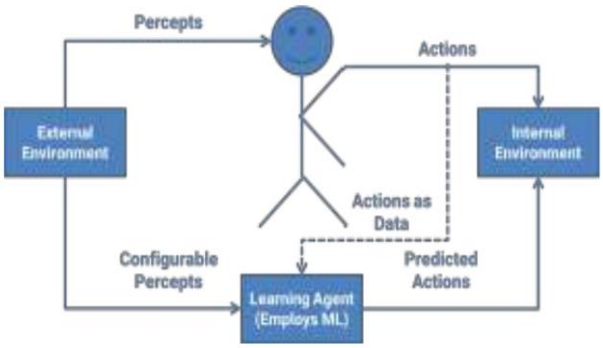
These controls also provide some low level automation in the form of time-based planning by the user; the user may design and save plans to turn specific appliances on or off at specific times, and keep them so for a specific length of time.

3.2.2: Simple Reflex Agent Based



These are the more autonomous type of systems. A reflex agent is employed in these systems to sense some parameters from the external environment. These parameters are then used to decide the value of a corresponding internal parameter of the smart home. The correlation between the external and internal parameters has to be configured manually by the manufacturer or the user. This also means that these systems are very rigid, and extreme variations in the external factors may not have a configured corresponding reflex and the system may report a failure or choose a non-optimal default reflex – depending on its design.

3.2.3 Machine Learning Based Automation System



Taking the limitations and inefficiencies of the above mentioned types into consideration, we came up with a novel solution – a Machine Learning Based automation system. Such a system will act autonomously by reading external parameters and behaviour patterns of the user in real time and correlating the two to create a behaviour model of the user. This model will help the system make a more educated guess about the user's next action which it will perform on encountering similar external parameters again.

It will thus give the user a sense of true automation by mimicking the user's habits.

This represents the functioning of the learning agent within the home environment. The agent will sense the external environment using it's sensors,

These actions are then Correlated to the state of the external parameters, which help the agent learn the user's habit given a set of external state parameters. It is pertinent to note the similarity between the functioning of the agent and the actions of the agent. Just like the user gets influenced by the environment to act in a certain way, so does the agent – once it learns to mimic the user.

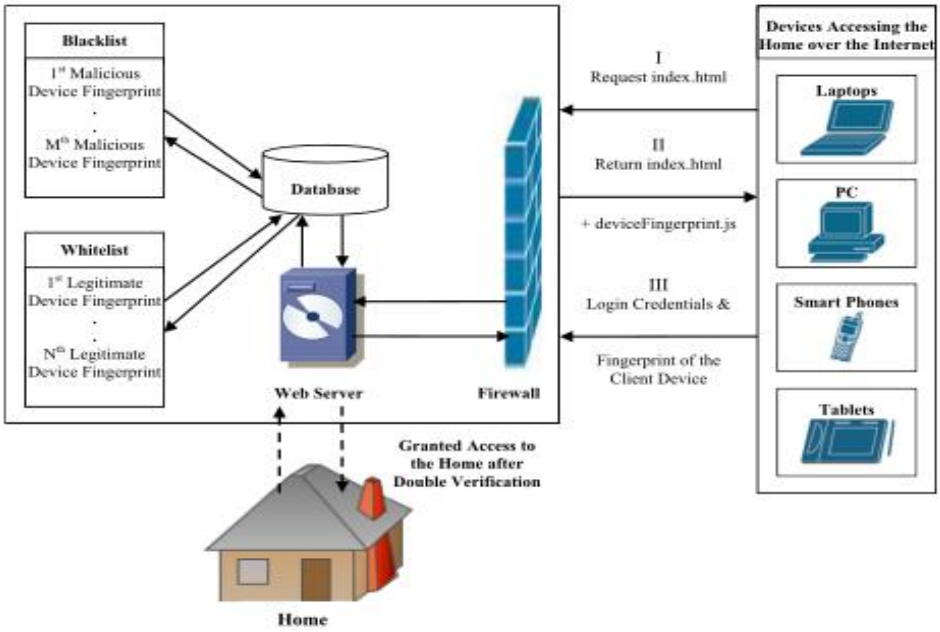
Chapter 4

FINGERPRINTING PROCESS

4.1 IMPLEMENTATION

The figure given below, Fig. shows the Device Finger-printing process in the proposed system. When a user wishes to access the home over the internet, he requests the login page from the server, the server then returns the login page along with the fingerprint java script. The user provides the login credentials along with the fingerprint of the device he is using. The login credentials are verified, if the verification is passed, then the gathered device fingerprint is analysed to see if there are enough device fingerprinting parameters available to provide a comprehensive fingerprint of the user device. If not, the client is requested to enable his Flash, JavaScript and Geo-location for accurate fingerprinting at the login page again.

There are two fingerprint lists in our database, whose entries are accumulated over time. The 'whitelist' is a list of approved or authorized device fingerprints belonging to legit-inmate users. Client devices with fingerprints in the whitelist are allowed access to the home after login credential verification. The 'blacklist' is a list of unauthorized or malicious device fingerprints belonging to potential attackers who tried to gain access to the home. Client devices with fingerprints in the blacklist are denied access to the home even if their login credentials are correct.



If the login credential are matched and there are sufficient fingerprinting parameters and the Device Fingerprint is not in our 'whitelist' and 'blacklist', then the client should be verified by some other more direct method in order to assure legitimacy. A simple and safe method would be make contact with the client using a phone call to the registered mobile number of the client and verify it is him trying to login to his home. Another alternative is, the server

generates a One Time Password (OTP) and sent it to the legitimate user's registered mobile number via Short Message Service (SMS), which the user enters in the website and thus the legitimacy of the user is verified. When a new device's legitimacy is verified, user is asked, if he wants to add the device's fingerprint into the whitelist. A user adds a device's fingerprint to the whitelist, if that device is his own or it is a trusted third party device which is often used to access the home like the clients office computer. Irrespective of the user's choice to add/not add a fingerprint into the database, he is allowed access to the home after direct verification. During direct verification via phone or OTP, if the verifi- cation fails it means the user trying to access the home is not a legitimate user. So that device's fingerprint is added to the blacklist. It also means the login credentials of a legitimate user are compromised, so he is also asked to change them. User devices with continuous and repeated failed login attempts are also added to the blacklist as they are trying to guess the login credentials. When a device tries to access the home whose fingerprint is in the blacklist, it is immediately denied access to the home even if the login credential is correct. This way our proposed system identifies an attacker's device and denies access to the home without bothering the user. The flow chart of the two stage verification process is given in Fig

4.2. FEATURES OF OUR WORK

The device fingerprinting technique discussed in this paper was designed for home automation systems with security as the primary objective. Our work attempts to identify the person operating the device as well as the device used to access the home; this is achieved through a two stage verification process .Comparing and verifying different parameters like OS name in UA string, and screen maximum width and height in Screen parameter, with those from flash, helps us to establish the legitimacy of UA and Screen parameters. Moreover, getting the country name from Google API by utilizing the latitude and longitude obtained from Geo-Location and comparing the country name with the country name in the date object helps us to determine the validity of the date object and time zone. These validations safeguard against parameter spoofing and enhance security. Hash function can be used to encrypt the device fingerprinting parameters (with a few exception where version number has to be checked) to protect against eavesdropping attack or man in the middle attack attempts. The proposed system gives clients accessing the home a reason to enable Flash, JavaScript and Geo-Location and encourage device fingerprinting

Praposed Algorithm For finger print

Step 1: Begin

Step 2: Obtain the device fingerprint from the client using java script, flash and geo-location.

Step 3: If (at least 7 out of the 9 device fingerprinting parameters are available), then, Step 4 else, Step 10.

Step 4: Analyse and compare each device fingerprinting parameter with the fingerprints in the whitelist and generate the parameter score corresponding to each of the available parameters.

Step 5: Compute the probabilities corresponding to each of the parameters based on the parameter score from Step 4.

Step 6: Analyse each probability score and compute the total probability score corresponding to the client's fingerprint.

Step 7: If (total probability score >= threshold probability) then, Step 8 else, Step 9.

Step 8: Device Fingerprint match found. Do Step 11.

Step 9: No Device Fingerprint match found, check the blacklist for malicious device's fingerprint match. Contact the user if fingerprint not in the blacklist. Do Step 11.

Step 10: Ask user to enabled JavaScript, Flash and Geo-Location so that parameters for device fingerprinting can be gathered and return to login page.

Step 11: End

4.3. MATHEMATICAL MODELLING

The information contained in a device fingerprint can be calculated using Entropy; Shannon entropy H(X) of a discrete variable with possible values{x1, x2 .....xn} is given by the equation: where P (xi) is the probability of each value and I(xi) is the information content and 'b' is the base of the logarithm; Shannon Entropy is calculated with logarithm to the base 2.

Chapter 5

Result

- Remotely on/off the electric appliances.
- Check the Status of electrical devices in home
- If user found electrical appliances is ON then user can operate or OFF appliances using Android application from outside the home.
- Using this system we can successfully saves Electrical energy.
- Using Machine Learning we can Predict the energy usage .
- By Machine learning we can Automatically complete some tasks before the user returns the home, For example if the user arrives to parking the Home automation system can on AC , lights, etc,.

Chapter 6

Conclusions and Future Scope

- The device fingerprint along with username/password based security proposed in this paper, enables the verification of user as well as the device used to access the home, which significantly improves home security when they are accessed over the internet. In our work, the device fingerprinting algorithm was able to uniquely identify 97.93% of devices accessing our test website with an entropy of over 22 bits. Unlike any previous approaches to device fingerprinting, we use geolocation data in our algorithm which improves the fingerprint accuracy. The UA verification, screen parameter verification and client's date object verification proposed in our work drastically improves the legitimacy of the fingerprints generated.
- With the rise of Internet of Things and more powerful computers, we will be able to achieve Utopian homes using Smart Automation powered by Machine Learning Algorithms of higher complexity than Temporal Difference based Reinforcement Learning running on current data. More data will lead to better prediction of potential user action which will help us lead more comfortable lives.
- Physically challenged people can also benefit from such systems which will eventually make them more independent, as more and more data gets collected to predict such users' habits. The impact of this technology on human lives will be deep and possibly every human-machine interface in the future will have some form of machine learning powered intelligent assistance. Changes in user habits can also be used to predict a lot of other things about the user such as the user's physical and mental health. In fact, many current technologies aim to provide basic level medical assistance using machine learning systems

Bibliography

1. . Bluetooth Remote Home Automation System Using Android Application. http://www.theijes.com/papers/v2-i1/X021014 901 53. pdf.

2. Android Controlled Home Automation. http://www. researchgate.net/publication/266373446_Android_countrolled_ Home_Automation

3. Zigbee Technology and its application in wireless home automation system.

4. Giannetsos Athanasios, \Intrusion Detection in Wireless Sensor Networks", Master THE-SIS, Carnegie Mellon University, April 8, 2008.

5. https://ieeexplore.ieee.org/document/7563403

Appendices

Detailed information, lengthy derivations, raw experimental observations etc. are to be presented in the separate appendices, which shall be numbered in Roman Capitals (e.g. Appendix I). Since reference can be drawn to published/unpublished literature in the ap-pendices these should precede the Literature Cited section.

Appendix-A: NS2 Download and Installation

1. Download ns-allinone-2.35.tar.gz from http://sourceforge.net/projects/nsnam/

2. Place ns-allinone-2.35.tar in your desired directory; like /home/vishal.

3. Go to terminal and do as following commands
sudo apt-get update
sudo apt-get install automake autoconf libxmu-dev build-essential

4. Extract ns-allinone-2.35 and after extracting go to folder ns-allinone-2.35 from Terminal as
$cd ns-allinone-2.35
$./install

5. Path Setting
$ gedit .bashrc

This command will open an existing le in editor. Just put the following path which is given bellow. [Remember that our ns-allinone path is /home/vishal. we will change this path according to our ns-allinone folder's path]

export PATH=$PATH:/home/vishal/ns-allinone-2.35/bin:/home/vishal/ns-allinone-2.35/tcl8.5.10/unix/home/vishal/ns-allinone-2.35/tk8.5.10/unix

export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/home/vishal/ns-allinone- 2.35/otcl-1.14:/home/vishal/ns-allinone-2.35/lib

export TCL_LIRARY PATH=$TCL LIBRARY PATH:/home/vishal/ns-allinone-2.35/tcl8.5.10/library

After this save and exit.

6. Now type in terminal to check that, is all command we entered in .bashrc is correct or not? And To take the e ect immediately
$source .bashrc

7. Then perform the validation test using this command.
$ ./validate

8. Run ns2 using this command $ns

We will get % prompt in our terminal. Now ns2 has been installed.

Acknowledgement

We have great pleasure in presenting the report on Home Automation System. We take this opportunity to express our sincere thanks towards our guide Prof Archana Kotangane Department of CE, APSIT thane for providing the technical guidelines and suggestions regarding line of work. We would like to express our gratitude towards his constant encouragement, support and guidance through the development of project.

We thank Prof. Sachin Malve Head of Department, CE, APSIT for his encouragement during progress meeting and providing guidelines to write this report.

We thank Prof Amol Kalugade BE project co-ordinator, Department of CE, APSIT for being encouraging throughout the course and for guidance.

We also thank the entire sta of APSIT for their invaluable help rendered during the course of this work. We wish to express our deep gratitude towards all our colleagues of APSIT for their encouragement.

Ashish Kothari:
16102045:

Snehal Surve:
17202013:

Adesh Thosani:
17202001:

Publication

Paper entitled \Paper Title" is presented at \International Conference/Journal Name" by \Author Name".