SC-IDT: SOFT COMPUTING BASED INTRUSION DETECTION TECHNOLOGY IN SMART HOME SECURITY SYSTEM

Ravi Sharma[1], Dr. Balkishan[2]

[1]*M.Tech Student, D.C.S.A., Maharshi Dayanand University, Rohtak, Haryana, India*
[2]*Assistant Professor, D.C.S.A., Maharshi Dayanand, University, Rohtak, Haryana, India*

Abstract

In this paper a theoretical model is introduced for the purpose of home security using mamdani fuzzy system in ubiquitous environment. Paper defines the architecture for such a system, in which the technological combination of ubiquitous computing and soft computing form a home security model. This model is inspired by Intrusion Detection System (IDS) and context awareness (ubicom) system. IDS categorize the normal and intrusive (malwares) data from the network traffic data and allow the normal data to be pass to the system and block the intrusive data. Ubiquitous computing is latest trend where computing can occur using any device, in any location and in any format i.e. everywhere and anywhere. By combining "ubiquitous computing, IDS, and fuzzy" technologies together a theoretical model of smart home security is introduced. Model consists of input parameters, output parameters and membership functions.

Keywords: *Ubiquitous Computing, IDS, Fuzzy Logic, Home Security.*

----------***----------

1. INTRODUCTION

Computing technologies are increasing with the speed of time corresponding to which it covers the larger area of human life. Many computer technologies are used for home securities. In this paper a theoretical model in mamdani fuzzy system for smart home security is introduced. This concept is inspired by Intrusion Detection System (IDS). Intrusion Detection System is a software or device which is used to monitor the network traffic data and categorizes the normal and intrusive data [1]. IDS only allow the normal data to be passed to the system; this decision is taken by the Fuzzy inference engine. Intrusive means data is holding some malicious activities i.e. either the attacker information or any other denial of service, IDS does not allow this type of activity to break through the system [2]. Similarly in this security model primary focus is on detecting the unauthorized entry to the homes and informs the owner of the house by various alert methods, discussed further. The whole system which is responsible for generating alerts comes under ubiquitous environment. Ubiquitous computing is the base of the smart homes. An innovative computing technology, by means of which the computing is made to appear anywhere at any time and the computing can occur using any device, in any location, and in any format, this is entitled as Ubiquitous Computing. Mark Weiser is father of Ubiquitous computing. Ubiquitous Computing origin based in Electronics and Imaging Laboratory of the Xerox Palo Alto Research Center [3]. This security aspect is implement to the lock of the doors which are equipped with the sensors connected to the fuzzy system, thus a ubiquitous environment is created as the sensors are responsible for context awareness. These sensors generate an activity output and this activity output is transferred to the mamdani fuzzy system which is responsible for generating output based on the fuzzy rules. As in IDS the generated reports are send to the management station similarly in this model the reports generated by the fuzzy systems are send to the main system which perform further tasks according to the level of intrusion. IDS system only allow the normal activity data to be passed and in fuzzy home security system similar approach is taken, activity is observed by the system, if lock is open in a single hit then the person allowed to enter but if dealing with the lock took time and some other behaviors are observed then the system does not allow unauthorized access to the home and take corresponding actions. These behaviors are discussed in next section and dealing with corresponding actions is to be discussed in section-2. In Section-2 architecture is introduced highlighting the mamdani system which completely describes the flow of the system information. Architecture includes the door lock sensors used to generate an activity output, fuzzy mamdani system responsible for categorizing the activity in normal or intrusive and main system responsible for generating alerts. Results are generated using fuzzy toolbox of MATLAB including the rule view and surface view of the fuzzy mamdani system. in Section-3 full model is described including the input parameters, output parameters and their membership functions. Section-4 shows the result of the model highlighting the attacks to the system.

2. ARCHITECTURE

The architecture is divided into two main modules i.e. ubiquitous environment and security system. Ubiquitous environment shows that the devices and computer systems are communicating with each other through sensors [4] and system take decisions rather than taking commands from the human. Security is basically performed by the Fuzzy system and main system based on the output generated by the sensors.

The architecture shows the complete home security system highlighting mamdani fuzzy security model. Architecture consists of three main systems -:

1. Door Lock System
2. Fuzzy System
3. Main System

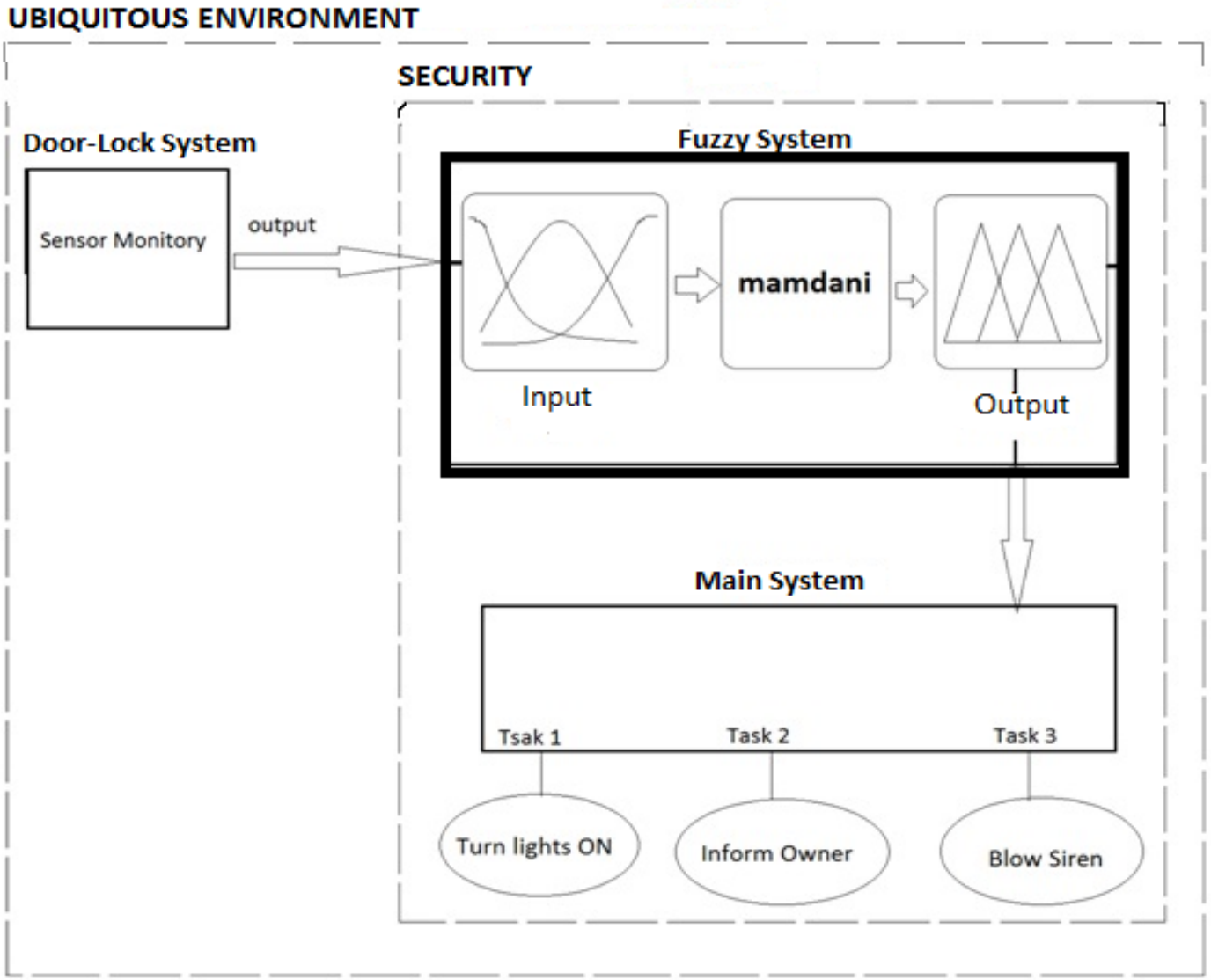

Fig 1 Architecture Highlighting mamdani Fuzzy System

Door Lock System equipped with the programmed – sensors. The sensors are used for the purpose of monitoring the environment and responsible for

Measuring the unit of all parameters and are called sensor monitory. Author took three types of parameters for this model -:

1. Temperature
2. Pressure
3. Vibration

Sensors generate output i.e. the units of temperature, pressure, and vibration showing the level of intrusion measured by membership function and send the output to the Fuzzy System. These three parameters are sensed by the sensors, whenever any intrusion is detected on the door locks whether by fire, try to break through hammer or any other heavy object or tried to cut the lock by any machine, the sensors senses these three parameters .The output of the sensor monitory system act as the input for the fuzzy system. Now fuzzy system is having the information about the units of temperature, pressure, and vibration. Input is analyzed using rules (section 5) in mamdani fuzzy system. According to the set of rules a single output is generated which shows the level of output parameters actions which is of further three types -:

1. Normal
2. Suspected
3. High Alert

The output is generated by the fuzzy system on the basis of rules (shown section 5). As the output is decided by fuzzy system, then that output report is send to the main system to take proper actions. If the output of the fuzzy system is normal then the system remains identical, if the output of the fuzzy system is suspected then main system will forward the warning message to the owner by sending information to his mobile phone and turn on the lights of the house, and if the output of fuzzy system is high_alert then the main system will generate the siren, inform the owner and also send the report to the nearest police station. Architecture hypothetically explain the full security system but paper's main focus is to build the fuzzy system model which mainly produce the single output showing the level of intrusiveness under uncertainty.

3. MODEL ANALYSIS

The security issue of houses in urban area is the major concern. In this model three types of situations are analyzed through which the unauthorized person try to violate the home security. The unauthorized access to the house could be observed by the sensors installed to the locks of the house in three forms -:

1. The outsider may try to burn the lock by any fire equipment, fire is measured in temperature , our first parameter is 'temperature'.
2. The outsider may try to break the lock by using hammer or any other heavy object, and this can be measured by 'pressure' on the lock.
3. The other situation may be arises when the outsider tries to cut the lock using any sharp metal cutter, this can be measured in form of 'vibration'.

Temperature, pressure and vibration are the three input parameters taken for this model. All these parameters are having three membership functions i.e. low, medium and high. Low and medium membership functions are of triangular type and the type of high membership function is sigmoid. An output parameter for this model is warning which gives the single activity output. Output Parameter consist of three membership functions namely, normal, suspected and high alert. Normal and suspected membership functions are of triangular type and type of high alert membership function is sigmoid shown in figure 2.

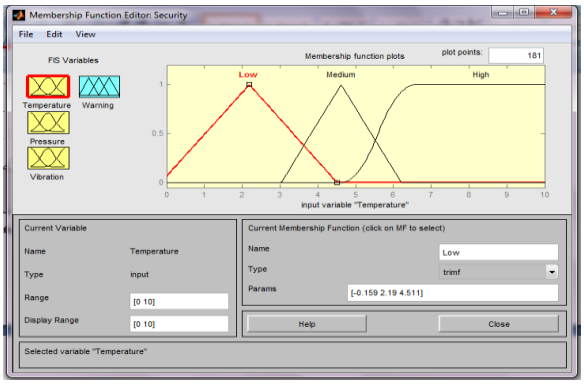

Fig 2 Membership function editor for input and output parameters

Fuzzy Sets [5] – Initially fuzzy sets are analyzed according to the real life conditions that are all three set of parameters i.e. temperature, pressure and vibration. For all these parameters three membership functions are taken low, medium and high for normal, middle-level, and high-level intrusion respectively. Fuzzy Rules - once the fuzzy input sets are defined our next step is to write the rules for each type of outsider attack. A system with input sets, rules, and output is called as fuzzy system. This model is totally implement on the Matlab in fuzzy toolbox. Rules are produced using the rule editor in fuzzy system editor presented in matlab Fuzzy Toolbox. Three Membership Functions are taken for all three parameters of security model corresponding to which rules are generated with permutation and combination of Input and Output parameters. The Fuzzy system editor in matlab is used to create the input parameters with their membership functions, for creation of rules, and the output parameter with their membership functions. The fuzzy system editor has the feature of displaying the surface view of the fuzzy system. All these three input parameter measures are observed by the sensors installed in the locks these sensors are programmed to sense the units of temperature, pressure and vibration. Now we take mamdani fuzzy system to analyze the output of sensors on the basis of fuzzy rules shown in section 5. This security model is totally rely on the Fuzzy Toolbox of the Matlab. This model is only able to detect the type of activity i.e. whether the normal behavior or intrusive [6]. The outputs of the fuzzy system generate reports and send to the main system for taking actions. Actions are considered as to stop unauthorized person to enter.

Following are some actions considered:-

1- To inform the owner of the house
2- Turning all lights ON
3- Blow the siren.

Main focus of the paper is on mamdani Fuzzy system which is responsible for produce an output in vagueness. We use Fuzzy toolbox of the Matlab software, Fuzzy System editor is used to generate the rules for the system based on the three parameters taken.

4. RESULTS

There are different conditions that may be possible to break the lock. Author took following conditions -:

1- Burning
2- Breaking
3- Cutting

For the aspect of burning, the parameter taken for fuzzy system is temperature, Pressure is to be taken in the aspect of breaking the lock, and for the aspect of cutting the lock the parameter taken is vibration. Each parameter of fuzzy system is assumed to have three membership functions, two with the triangular distribution and one of sigmoid distribution. The low and medium Membership functions are of triangular distribution and high membership function is of sigmoid distribution. All three parameters including their membership functions are shown in the Figure 3, Figure 4, and Figure 5.

Temperature Parameter is having three membership functions i.e. low, medium, and high. There may be the imprecision state occur when the state lies in normal and medium function or medium and high function. This is to be deal with the set of rules of mamdani system.

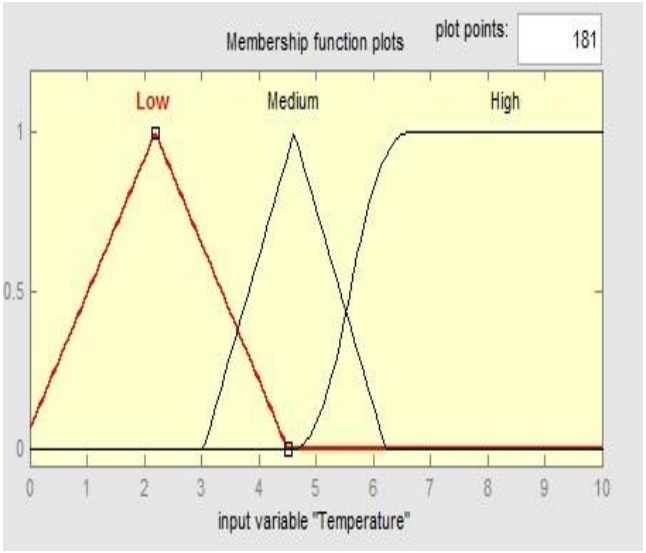

Fig 3 Membership functions for the parameter temperature

Next parameter is Pressure which is to be measure whenever a hit to the door-lock is taken place. This parameter measures how hard the intruder hit the lock and what number of times, based on this state unit decisions are taken.

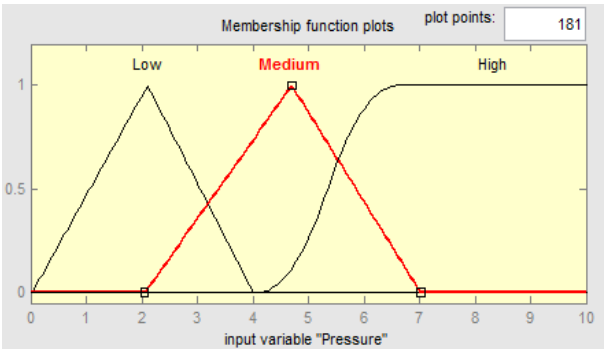

Fig 4 Membership function for the parameter pressure

After that our last parameter is Vibration, whenever metal is cutting by some tool it produces vibration. Here we take the concept of vibration, whenever any cutter is applied to the locks it generates the vibration and the unit is measured by the sensors and then the membership functions of the parameter states the level of intrusion [7].

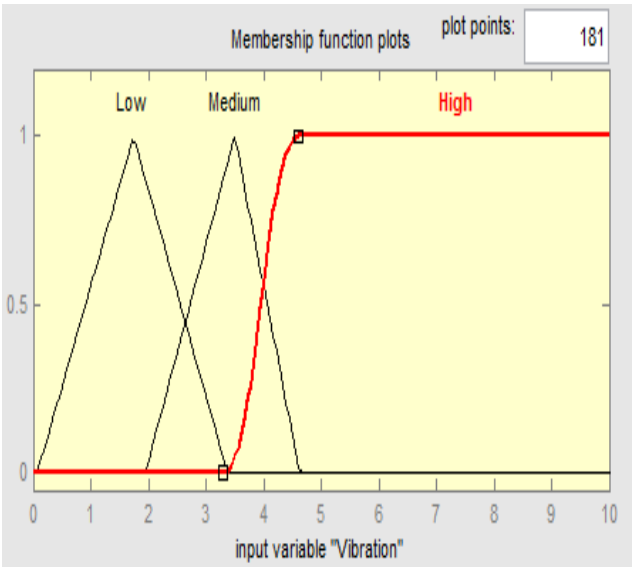

Fig 5 Membership functions for the parameter Vibration

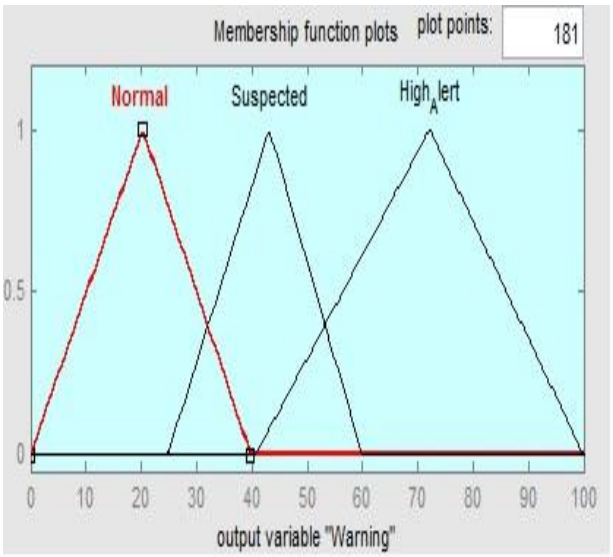

Fig 6 Membership functions for the output parameter

Now to implement the model we choose the rule viewer tool of fuzzy tool box test what will happen when the temperature, pressure, and vibration changes corresponding to time.

First we raise the temperature, whenever it raises the output unit is increased shown in figure 7.

4.1 Fire Attack

If the TEMPERATURE of Door Locks rises gradually and isHIGHAnd the Pressure of Door Lock is MEDIUMAnd the Vibration of Door Lock observed isMEDIUM-HIGHThen Warning is HIGH_Alert

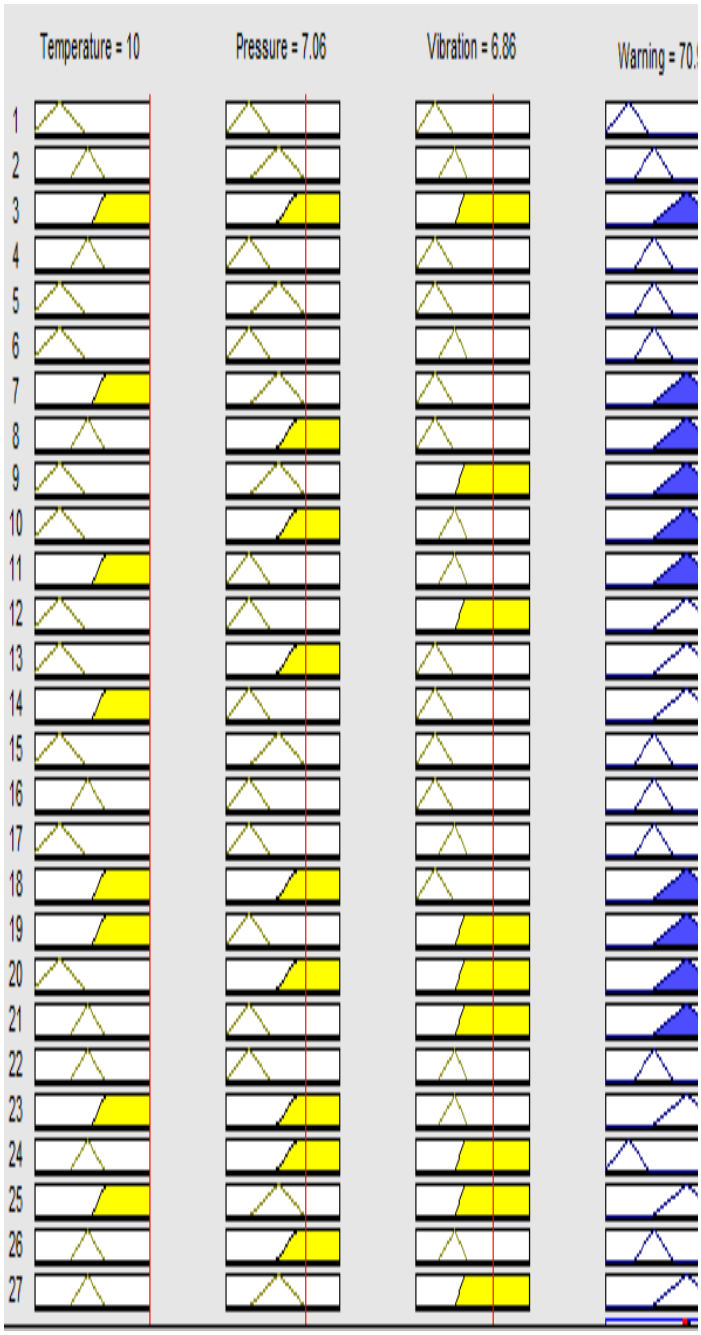

Fig 7 Fuzzy system for Temperature attack

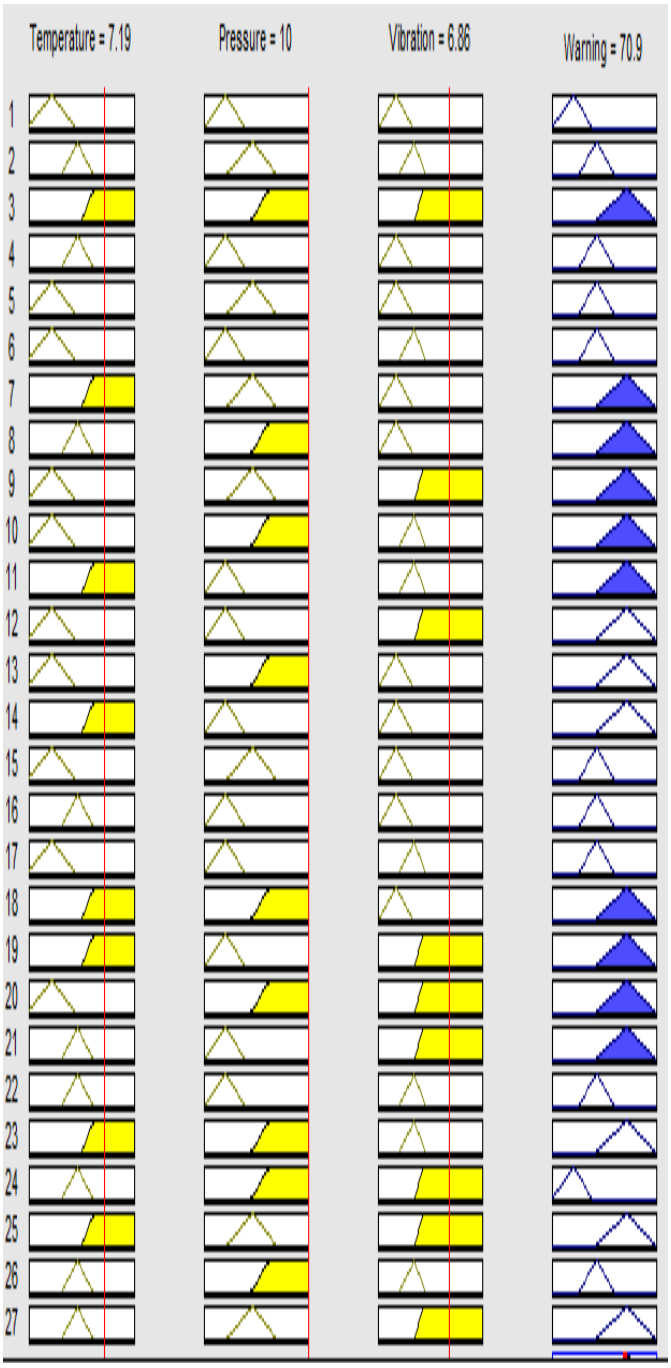

Fig 8 Fuzzy System for Pressure attack

4.2 Break _Attack

If the TEMPERATURE of Door _Locks rises gradually and is MEDIUM-HIGH And the Vibration of Door_ Lock isMEDIUMAnd the Vibration of Door _Lock observed is MEDIUM-HIGH Then Warning is HIGH_Alert

4.3 Cutter Attack

If the TEMPERATURE of Door Locks rises gradually and i MEDIUM _HIGH And the Pressure of Door _Lock is MEDIUM And the Vibration of Door Lock observed is HIGH Then Warning is HIGH_Alert

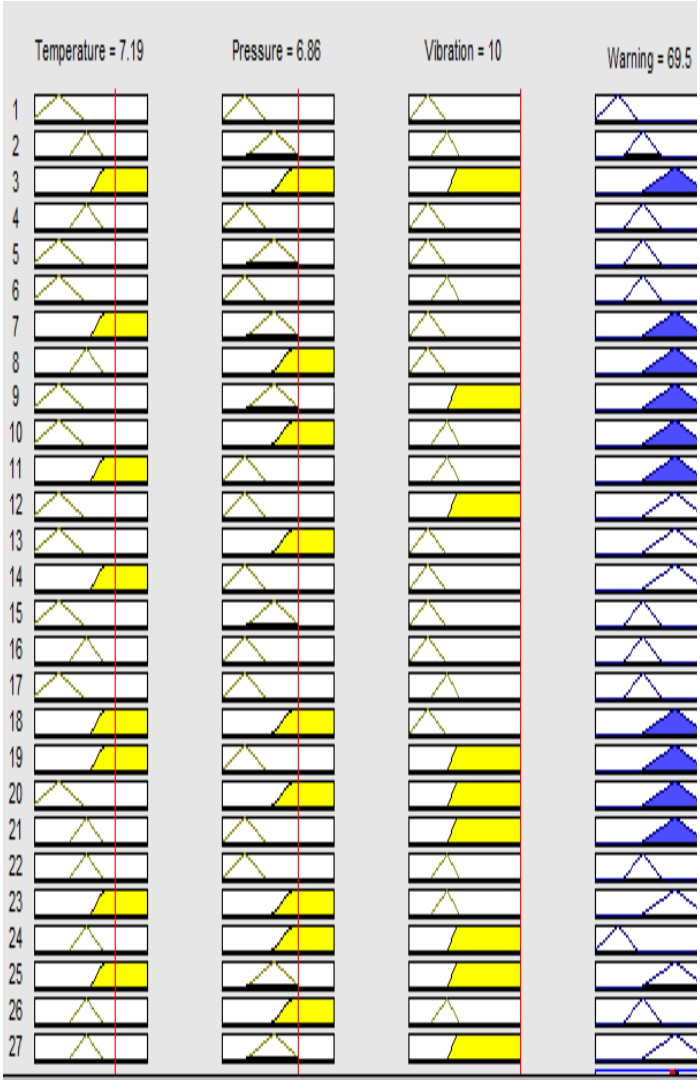

Fig 9 Fuzzy system for vibration attack

Fuzzy Toolbox in Matlab gives us the feature of having the surface view of the mamdani system which is very helpful in understanding the system.

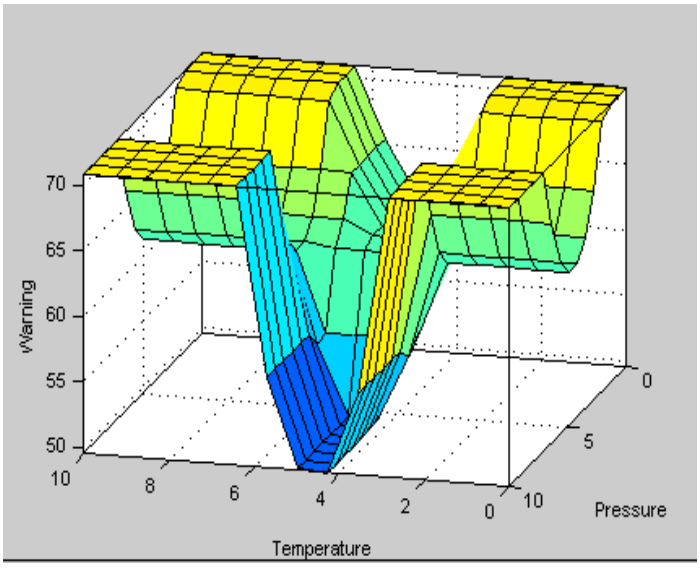

Fig 10 Surface View of system

5. FUZZY RULES

[1] If (Temperature is Low) and (Pressure is Low) and (Vibration is Low) then (Warning is Normal) (1)

[2] If (Temperature is Medium) or (Pressure is Medium) or (Vibration is Medium) then (Warning is Suspected) (1)

[3] If (Temperature is High) or (Pressure is High) or (Vibration is High) then (Warning is High_Alert) (1)

[4] If (Temperature is Medium) and (Pressure is Low) and (Vibration is Low) then (Warning is Suspected) (1)

[5] If (Temperature is Low) and (Pressure is Medium) and (Vibration is Low) then (Warning is Suspected) (1)

[6] If (Temperature is Low) and (Pressure is Low) and (Vibration is Medium) then (Warning is Suspected) (1)

[7] If (Temperature is High) or (Pressure is Medium) or (Vibration is Low) then (Warning is High Alert) (1)

[8] If (Temperature is Medium) or (Pressure is High) or (Vibration is Low) then (Warning is High Alert) (1)

[9] If (Temperature is Low) or (Pressure is Medium) or (Vibration is High) then (Warning is High Alert) (1)

[10] If (Temperature is Low) or (Pressure is High) or (Vibration is Medium) then (Warning is High Alert) (1)

[11] If (Temperature is High) or (Pressure is Low) or (Vibration is Medium) then (Warning is High Alert) (1)

[12] If (Temperature is Low) and (Pressure is Low) and (Vibration is High) then (Warning is High Alert) (1)

[13] If (Temperature is Low) and (Pressure is High) and (Vibration is Low) then (Warning is High Alert) (1)

[14] If (Temperature is High) and (Pressure is Low) and (Vibration is Low) then (Warning is High Alert) (1)

[15] If (Temperature is Low) and (Pressure is Medium) and (Vibration is Low) then (Warning is Suspected) (1)

[16] If (Temperature is Medium) and (Pressure is Low) and (Vibration is Low) then (Warning is Suspected) (1)

[17] If (Temperature is Low) and (Pressure is Low) and (Vibration is Medium) then (Warning is Suspected) (1)

[18] If (Temperature is High) or (Pressure is High) or (Vibration is Low) then (Warning is High Alert) (1)

[19] If (Temperature is High) or (Pressure is Low) or (Vibration is High) then (Warning is High Alert) (1)

[20] 20. If (Temperature is Low) or (Pressure is High) or (Vibration is High) then (Warning is High Alert) (1)

[21] If (Temperature is Medium) or (Pressure is Low) or (Vibration is High) then (Warning is High Alert) (1)
[22] If (Temperature is Medium) and (Pressure is Low) and (Vibration is Medium) then (Warning is Suspected) (1)
[23] If (Temperature is High) and (Pressure is High) and (Vibration is Medium) then (Warning is High Alert) (1)
[24] If (Temperature is Medium) and (Pressure is High) and (Vibration is High) then (Warning is Normal) (1)
[25] If (Temperature is High) and (Pressure is Medium) and (Vibration is High) then (Warning is High Alert) (1)
[26] If (Temperature is Medium) and (Pressure is High) and (Vibration is Medium) then (Warning is Suspected) (1)
[27] 27. If (Temperature is Medium) and (Pressure is Medium) and (Vibration is High) then (Warning is High Alert) (1)

6. CONCLUSIONS

We study the parameters responsible for halting the security of homes, based on which we build a fuzzy mamdani security model. Paper also describes an architecture highlighting the position of a Fuzzy model in the ubiquitous environment. The whole architecture is divided into two modules i.e. ubiquitous environment and Security system. Result shows the all three attacks with its corresponding output level of warning which satisfies the need of the security model.

REFERENCES

[1] Intrusion Detection Systems: A Survey and Taxonomy, Stefan Axelsson
[2] Intrusion Detection Systems: A Survey and Taxonomy Stefan Axels son.
[3] The origins of ubiquitous computing research at PARC in the late 1980s, M. Weiser, R. Gold, J. S. Brown.
[4] The Aware Home: A Living Laboratory for Ubiquitous Computing Research, Cory D. Kidd, Robert Orr, Gregory D. Abowd, Christopher G. Atkeson, Irfan A. Essa, Blair MacIntyre, Elizabeth Mynatt, Thad E. Starner and Wendy News letter.
[5] Fundamentals of fuzzy sets and fuzzy logic, Henrik Legind Larsen, AAUE Computer Science.
[6] Understanding Intrusion Detection Systems, Peter Mell, The EDP Audit, Control, And Security Newsletter November 2001 VOL.XXIX, NO. 5.
[7] Evolving Fuzzy Classifiers for Intrusion Detection, Jonatan Gomez and Dipankar Dasgupta, Proceedings of the 2002 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2001.