Re-engineering Real-time Intrusion and Burglary Detection using Fuzzy Technique

Isah Mohammed M.
National Institute for Educational Planning and Administration (NIEPA-NIGERIA)
KM4 Laje Road, Off Ondo-Ore Road,
Ondo City

Charles Ikerionwu
Department of Software Eng
School of Information and Communication Technology
Federal University of Technology, Owerri

Chinenye C. Opara
Department of Computer Science, Faculty of Natural Sciences and Environmental Studies, Godfrey Okoye University, Enugu

ABSTRACT

The alarming rate of burglary and theft across the country, which has drawn societal security concerns, increased individual and government spending in protection of lives and properties, necessitated the urgent need to design and implement an automated building intrusion and theft detection system. In this paper, a burglary and theft detection system using Fuzzy Logic and Short Message Service (SMS) system that will detect intruders and report this crime on a real-time was realized. The design approach combines the acquisition of vibration signal obtained from the burgles/intruder(s) by microcontroller-based accelerometer, intrusion detection logic built on the Fuzzy Inference System installed and configured on a cloud infrastructure with an alerting system which communicates on a real time basis to the appropriate authorities of an intrusion/burglary. This phenomenal innovation and breakthrough in intrusion detection systems will bring about the detection and prosecution of intruders/burglars and thieves in the society – thus reducing the level of crime.

Keywords

Fuzzy Inference System, Burglary Detection system, Intrusion detection system, Theft detection system, Short Message Service (SMS) system

1. INTRODUCTION

Buildings serve several needs for the society, primarily as shelter from weather, security, living space, privacy, to storage of belongings, for a comfortable live and work, a physical division of human inhabitant [14]. As building plays increasingly vital roles in our modern society, they have become the targets of intrusion by enemies and criminals. It is important to note that increasing population and crime rate will thus increase the rate of building intrusion and theft. Thieves and vandals/burglars can directly have a negative effect on the security of lives and properties, thereby posing considerable problem in our society today [6]. The security of lives and properties is considered the most important in any society. Anon [2] described security as the protection of people and things, such as buildings, properties from harm, theft or sabotage and encompasses several components such as physical, personal, investigations using automated gadget, awareness and information. Crime prevention on buildings and properties has become a major concern due to the importance of buildings in our society. Therefore, there is need to urgently design and implement an automated building intrusion and theft detection system that will detect intruders and report this crime on a real-time. Appropriate strategies currently used to curb and manage building intrusion and theft is implementing security plans according to the rate of occurrence. Fitzgerald and Poynton [8] suggest that firms, government and individuals, should relate history of reoccurrence of theft and building intrusion problems so as to adopt the best security plan required to reduce the problem. Nancy, Samantha, Allison and Joshua A [11] suggested a surveillance system which is monitored by a security staff operator. The system is attached to security cameras that captures all activities that are happening within the perimeter of the building, where it has been installed. Then, through live streaming video, the staff /operator sees exactly what is happening within the building and its environment, which is not secure enough in monitoring and detecting theft as well as building vandalism.

Intrusion in buildings is a crime that needs urgent attention due to the importance of building to humanity. Current systems used in detecting theft and burglary/intrusion in buildings, only capture video stream but do not report the crime in real-time. The systems also require human input to detect crimes. Therefore, the need for an automated fuzzy based theft and building intrusion detection system is essential, thus the system will alert residential owners, the police and other security agencies of intrusion into buildings the crime was committed via SMS. This will accelerate the authorities in combating crimes.

2. RELATED WORK

2.1 Related Work on Building Burglary and Theft Detection

Eseosa and Promise [7] proposed the intruder alarm detection system, the study demonstrated the intruder alarm systems and detectors, while giving special focus on the several technologies applied. The technologies include wireless transmission and reception of alarm messages, and commands through GPRS and TCP/IP, which involves development of web-based intruder alarm monitoring and control hardware and software using distributed networks (“grid”). The distributed network intelligence allows an intruder alarm system to react to multi-signalization intrusion situations in much efficient ways, being also able to distinguish more accurately real security violation adverted operations.

Jordal Robert [9] in his work designed an intelligent automated home smoke detection system using the conventional security systems, which are the most common form of protection to lives and properties but the limitation is the lack of real-time monitoring of intruders activities. The study by Zurich [15] suggested video surveillance equipment which can help capture details of theft and intrusion in building and can provide police department with important evidence that can be used to apprehend criminals only at the exterior part of the building because the surveillance camera only monitors and records the activities within the perimeter of the building. It is also limited in streaming video clips that capture the act of intrusion but not detect and report theft and building intrusion. Ahn, Jung, Lee, and Yoo [1] on the other hand, provided a high-level overview of security requirements for network CCTV in the context of u-City services. These requirements relate to the confidentiality, the integrity, the system protection and the content privacy. Moreover, Costin, A.[5] summarized a subset of threats posed to network and IP based CCTV systems. Subsequently, they propose two enhanced security protocols for user registration and authentication in order to increase the security of such networked systems. Coole, Woodward and Valli [4] described a subset of the security issues related to networked, and especially Wi-Fi based surveillance devices. Their work also discuss the significance of vulnerability exploitation of such devices in the context of confidentiality, integrity, availability. They conclude with a framework for implementing controls to reduce risk associated with Wi-Fi based CCTV systems. Recently, in a research by Obermaier and Hutle [12] provided a practical analysis of the security and privacy of four major cloud-based video surveillance systems. They reverse-engineered the security implementation and discovered several vulnerabilities in every of the tested systems. The authors considered two attacker models, namely local network attacker and remote network attacker. They demonstrated how these attackers can exploit vulnerabilities to blackmail users and companies by DoS attacks, by injecting forged video streams, and by eavesdropping private video data, even without physical access to the systems. Their main findings, however, relate to classical weaknesses such as fallback to unsecured function, proprietary security protocols, weak passwords, and insecure authentication.

2.2 Related Work on Fire Detection System Using Fuzzy Logic

In a research by Khanna and Cheema [10], the researchers designed a fire detection system in buildings using fuzzy logic. The designed system is based on the principles of implementing Fuzzy Logic on the information collected by sensors. In their system design, enhancement is done within the system which has high accuracy with low alarm rate and also the simulation was done in MATLAB using event detection mechanism. Also in a work by Chaudhary, Tiwari, and Kumar [3], fuzzy logic based intrusion detection systems in mobile ad hoc networks was designed using fuzzy logic which can detect black hole attack on MANETs.

3. SYSTEM ANALYSIS AND DESIGN

The current and proposed systems employed in detecting theft and intrusions in building is analyzed based on the flow and schematic diagram as illustrated in figure 1 & 2. The flowchart in figure 1 shows the systemic steps involved in intrusion detection, while the schematic diagram in figure 2 shows how the system acquires vibration signals from the vibrating object, converts the signals into crisp for onward transmission to the cloud infrastructure via internet for processing and the building owner and appropriate authorities alerted once the vibration is above the set threshold

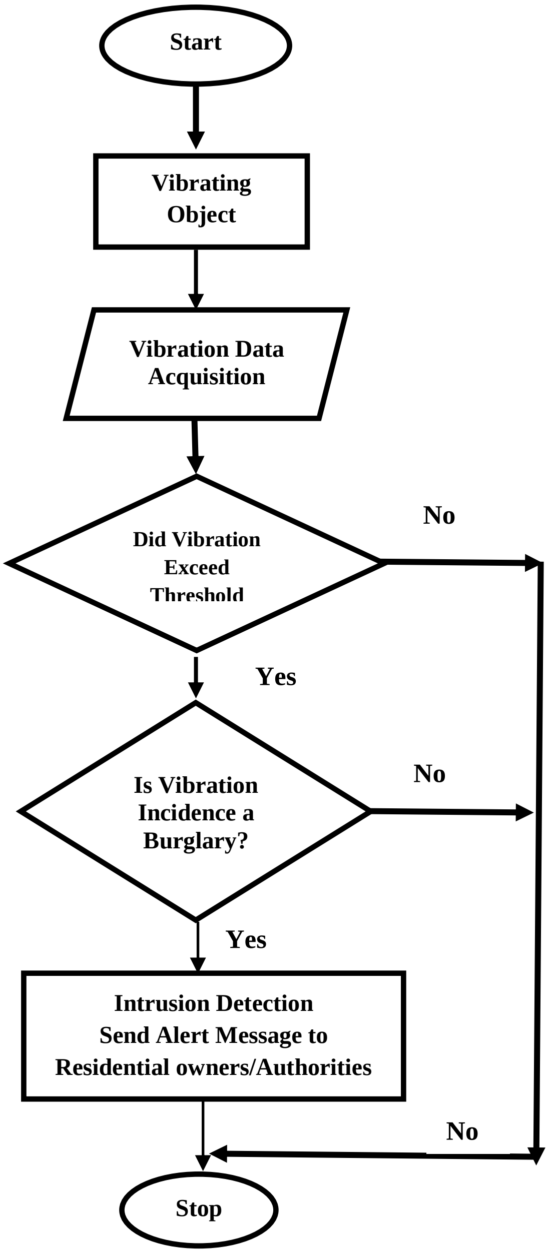

Start
Vibrating Object
Vibration Data Acquisition
Did Vibration Exceed Threshold
No
Yes
Is Vibration Incidence a Burglary?
No
Yes
Intrusion Detection Send Alert Message to Residential owners/Authorities
No
Stop

Fig 1: Flow Diagram of the Proposed System

The proposed system is divided into two functional units which are; Microcontroller based Accelerator and the Cloud Infrastructure. These are described as follows:

a. Microcontroller Based Accelerator

The microcontroller based accelerometer is a configuration of the accelerometer sensor and the microcontroller. The accelerometer sensor is an electromechanical device used to measure acceleration forces such as continuous force of gravity and to sense movement or vibrations. It senses the vibrations signal from the building or its premises and converts these signals to velocity spectrum (m/s) and route it to the microcontroller.

A microcontroller is a compact integrated circuit designed to govern a specific operation in an embedded system. The microcontroller processes these signals by digitalizing it into a readable form (crisp) and sends it to the cloud via a specific IP address as shown in figure 2.

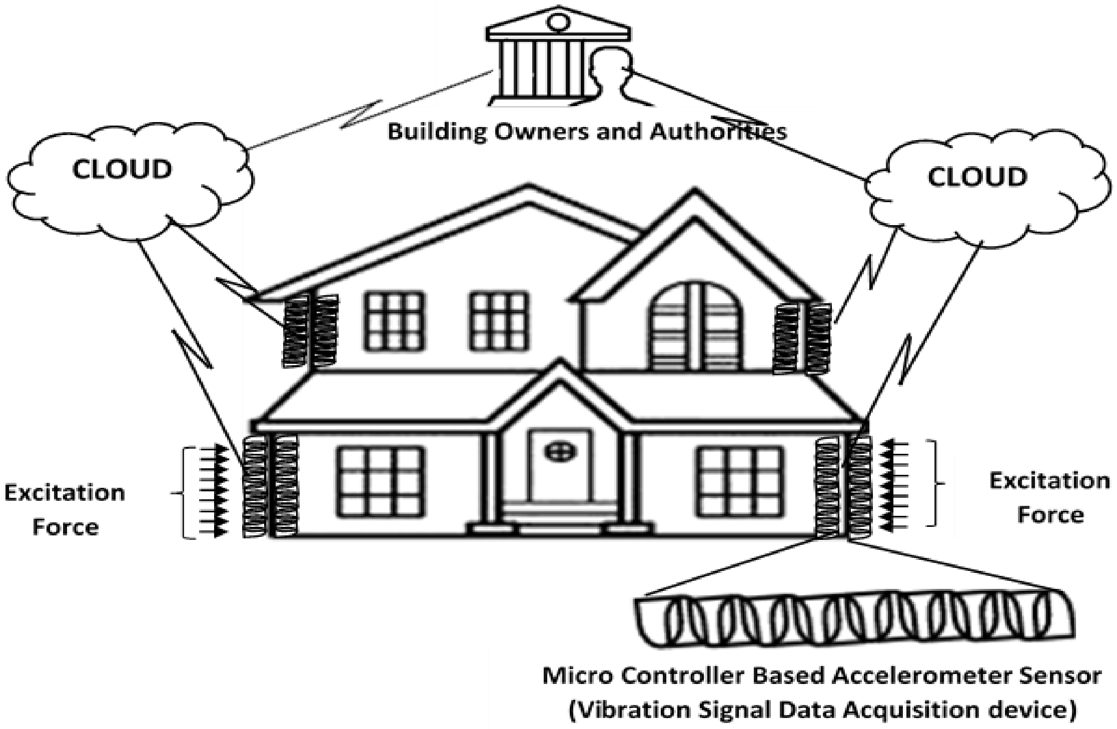

Building Owners and Authorities
CLOUD
CLOUD
Excitation Force
Excitation Force
Micro Controller Based Accelerometer Sensor (Vibration Signal Data Acquisition device)

Fig 2: Schematic Diagram of the Proposed System

b. The Cloud Infrastructure

Cloud is a general term used to describe network or Internet. The Cloud architecture comprises of many cloud components which includes servers, applications, infrastructures, database, storage etc, each of them is loosely coupled. Messages are sent from the cloud to targeted individuals or appropriate authorities notifying them about intrusion when the sensed vibration signals exceed certain threshold.

3.1 The Fuzzy-Based System Model

The model of fuzzy logic system consists of fuzzification, fuzzy rules, and fuzzy inference system and defuzzification process. The system process/operation flow as shown in figure 3.

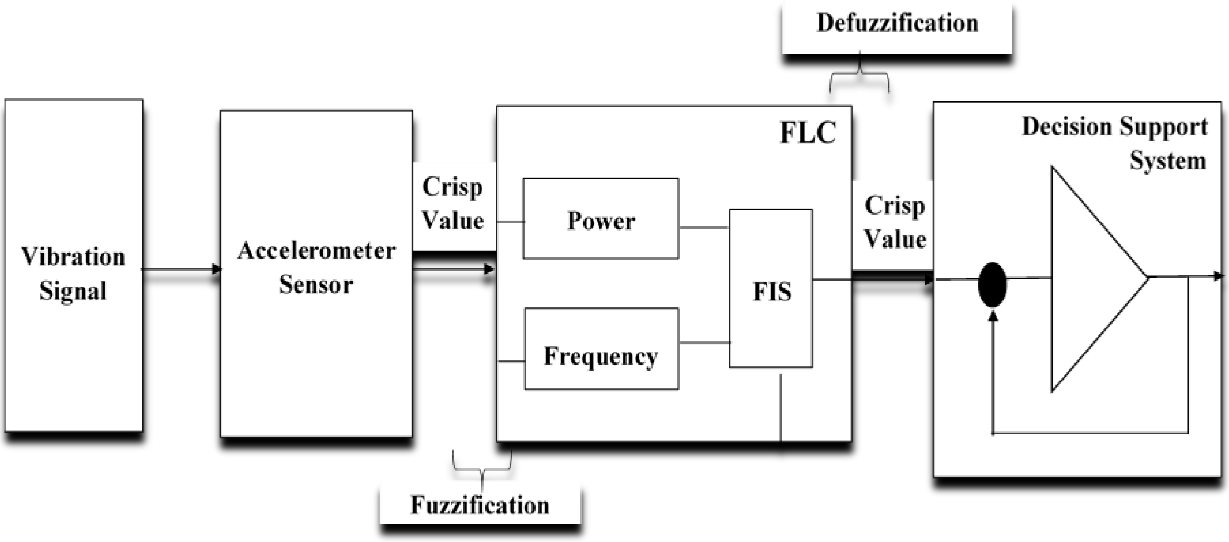
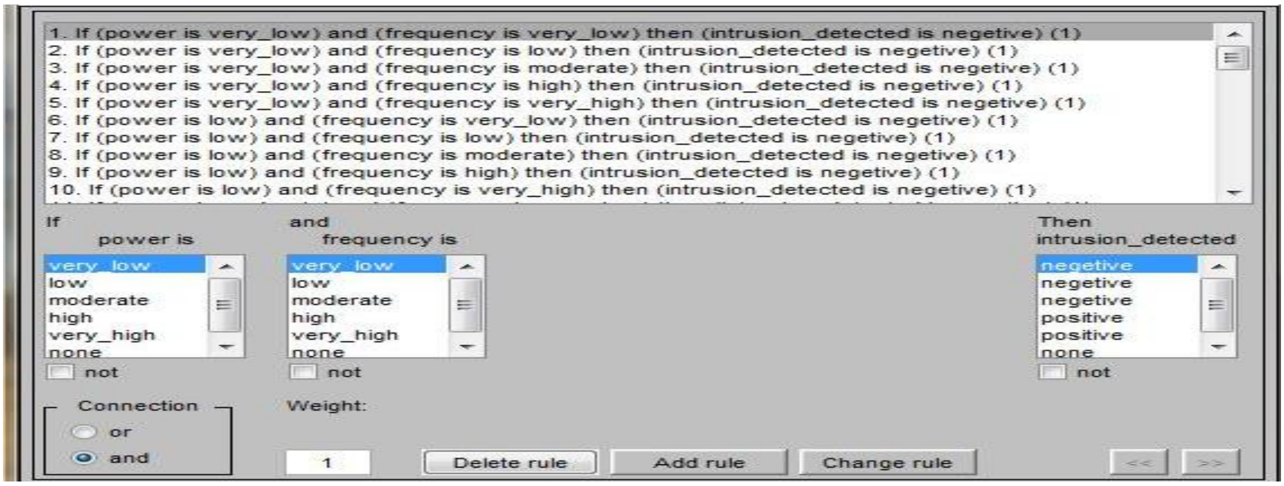


Fig 3: The Fuzzy-Based System Model

The accelerometer converts real time vibration signal from the vibration object into crisp, the process of transforming crisp values (ie the digitalized signals) into fuzzy linguistic variables is called fuzzification. The membership function is used to associate a grade to each linguistic variable.

The fuzzy inference system consists of fuzzy rules as shown in Figure 4 (IF antecedent THEN consequent) that are devised by an expert knowledge base or through system input-output learning, the transformation from a fuzzy set to a crisp value is called defuzzification.



1. If (power is very_low) and (frequency is very_low) then (intrusion_detected is negetive) (1)
2. If (power is very_low) and (frequency is low) then (intrusion_detected is negetive) (1)
3. If (power is very_low) and (frequency is moderate) then (intrusion_detected is negetive) (1)
4. If (power is very_low) and (frequency is high) then (intrusion_detected is negetive) (1)
5. If (power is very_low) and (frequency is very_high) then (intrusion_detected is negetive) (1)
6. If (power is low) and (frequency is very_low) then (intrusion_detected is negetive) (1)
7. If (power is low) and (frequency is low) then (intrusion_detected is negetive) (1)
8. If (power is low) and (frequency is moderate) then (intrusion_detected is negetive) (1)
9. If (power is low) and (frequency is high) then (intrusion_detected is negetive) (1)
10. If (power is low) and (frequency is very_high) then (intrusion_detected is negetive) (1)

If power is: very_low, low, moderate, high, very_high, none; ☐ not

and frequency is: very_low, low, moderate, high, very_high, none; ☐ not

Then intrusion_detected: negetive, negetive, negetive, positive, positive, none; ☐ not

Connection: ○ or ● and

Weight: 1

Fig 4: Rule Editor in MATLAB

The fuzzy logic tool (MATLAB) is a software tool that resides in the cloud, it runs as part of software infrastructure for the realization of this implementation. Digitized vibration signals are the crisp input (fuzzy variable) of the proposed intrusion detection system generated by Micro-Controller-Based-Accelerometer while the system's crisp output variables are formed by fuzzification of the intensity of the crisp input signals decoded by the Micro-Controller-Based-Accelerometer. The membership functions VERY LOW, LOW, MODERATE, HIGH and VERY HIGH are defined by intensity of vibration as shown in figure 5, whereas the vibration signals is classified as very low when the intensity of the vibration signals is 0 to 15m/s, low when it is from is 16 m/s to 25m/s, it is classified as medium when the m/s vibration signals intensity ranges from 26m/s to 55m/s, it is classified as high when the vibration signals intensity is 56m/s to 59m/s and it is classified as very high when the vibration signal is 60 and above

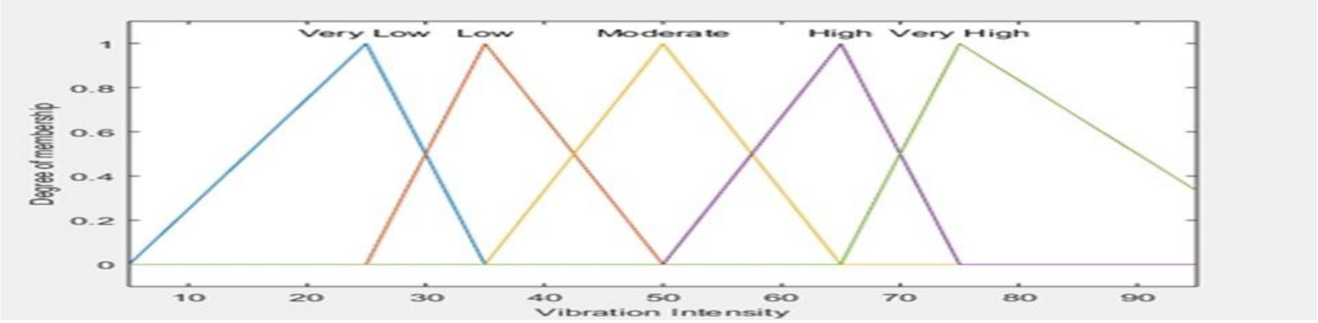


Fig 5: Degree of Membership Function for Member Function

3.2 Input and Output Model for the Proposed System

The input power: for a very low signal is low between 0 and 30; for a low signal is between 14 and 40; for a moderate signal is between 28 and 55; for a high signal is between 42 and 69; and for a very high signal is between 56 and 100 as shown in figure 6, likewise the input frequency: for a very low signal is low between 0 and 30; for a low signal is between 14 and 40; for a moderate signal is between 28 and 55; for a high signal is between 42 and 69; and for a very high signal is between 56 and 100 as shown in figure 7. The output membership function is shown in figure 8, when the input signal is very low, low and moderate, the output membership function (ie between 0 and 55) is negative and when input signal is high and very high the output membership function becomes positive (ie between 56 and 100).

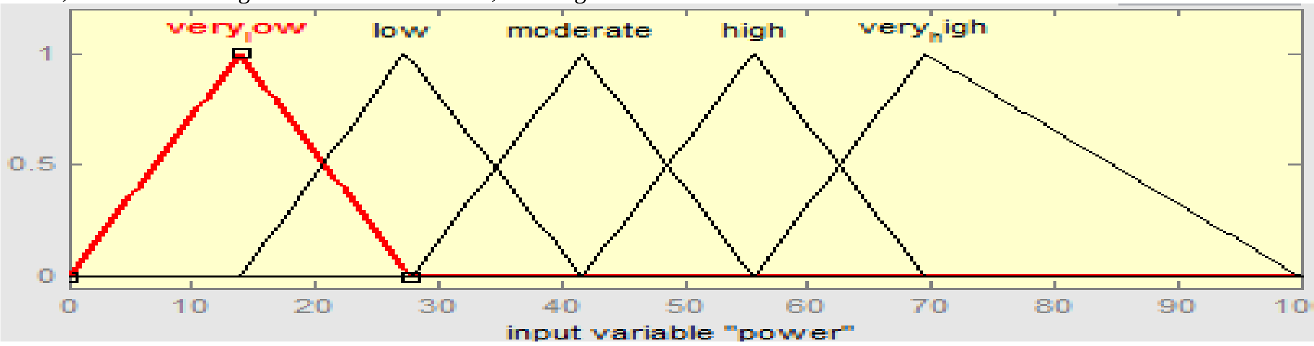


Fig 6: Input Variable Power

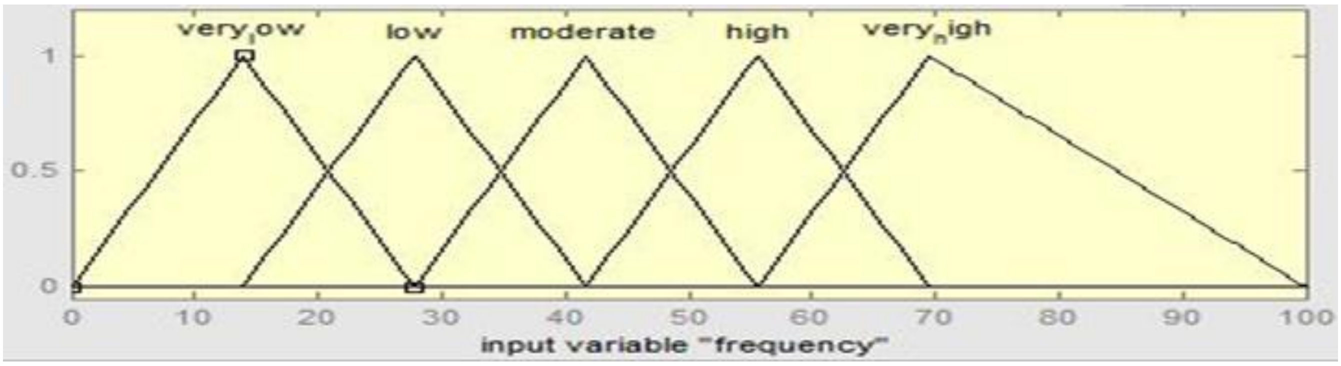


Fig 7: Input Variable Frequency

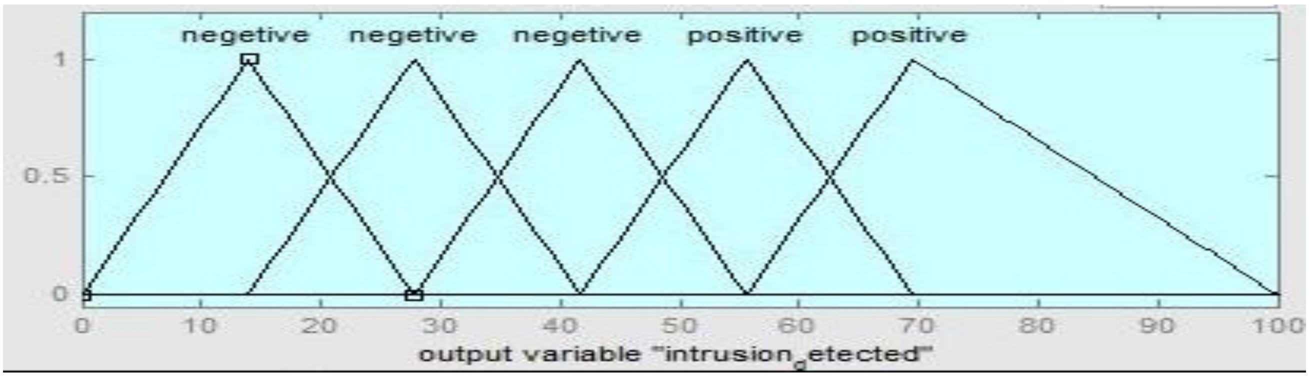


Fig 8: System Output; Intrusion Detected Positive and Not Detected Negative

When the membership function is very low and low the probability of an intrusion is 0 and the system will not send an alert message. When the membership function is moderate, the probability of an intrusion is less than 0.5, no alert message would be sent owing to the fact that both 0 and 0.5 are within manageable intrusion level. When the membership function is high and very high, the probability of an intrusion is greater than 0.5 and the system will send and alert message to the appropriate individuals or authorities whose phone numbers have been stored in the system. The surface view a graph that combine the membership function of the input variable power and frequency against the membership function of the output variable is illustrated in figure 9

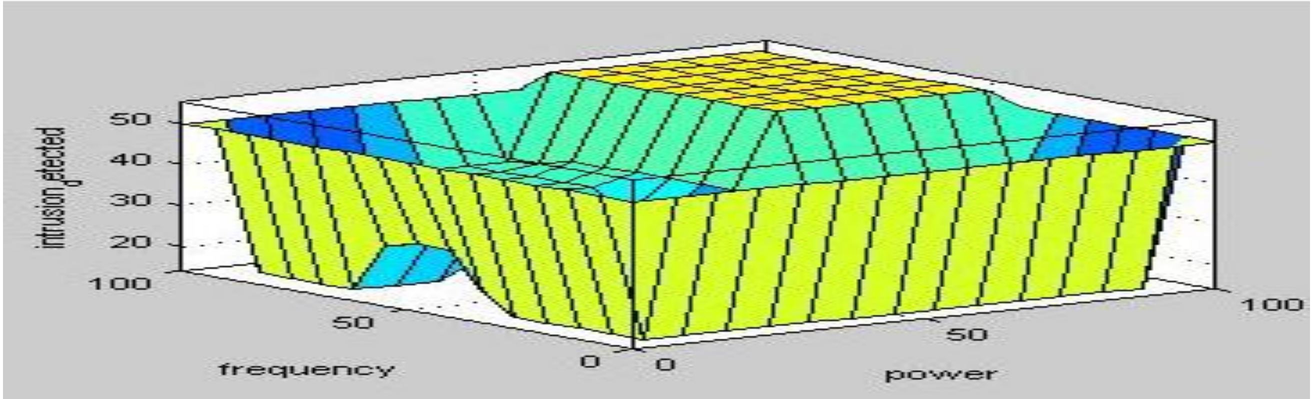


Fig 9: Surface View

3.3 Fuzzy design Inference Rules

The fuzzy inference rules used in achieving the system design are as follows(see figure 4):

1. If (power is very_low) and (frequency is very_low) then (intrusion_detected is negative) (1)
2. If (power is very_low) and (frequency is low) then (intrusion_detected is negative) (1)
3. If (power is very_low) and (frequency is moderate) then (intrusion_detected is negative) (1)
4. If (power is very_low) and (frequency is high) then (intrusion_detected is negative) (1)
5. If (power is very_low) and (frequency is very_high) then (intrusion_detected is negative) (1)
6. If (power is low) and (frequency is very_low) then (intrusion_detected is negative) (1)
7. If (power is low) and (frequency is low) then (intrusion_detected is negative) (1)
8. If (power is low) and (frequency is moderate) then (intrusion_detected is negative) (1)
9. If (power is low) and (frequency is high) then (intrusion_detected is negative) (1)

10. If (power is low) and (frequency is very_high) then (intrusion_detected is negative) (1)
11. If (power is moderate) and (frequency is very_low) then (intrusion_detected is negative) (1)
12. If (power is moderate) and (frequency is low) then (intrusion_detected is negative) (1)
13. If (power is moderate) and (frequency is moderate) then (intrusion_detected is negative) (1)
14. If (power is moderate) and (frequency is moderate) then (intrusion_detected is positive) (2)
15. If (power is moderate) and (frequency is high) then (intrusion_detected is positive) (2)
16. If (power is moderate) and (frequency is very_high) then (intrusion_detected is positive) (2)
17. If (power is high) and (frequency is very_low) then (intrusion_detected is negative) (1)
18. If (power is high) and (frequency is very_low) then (intrusion_detected is positive) (2)
19. If (power is high) and (frequency is low) then (intrusion_detected is positive) (2)
20. If (power is high) and (frequency is moderate) then (intrusion_detected is positive) (2)
21. If (power is high) and (frequency is high) then (intrusion_detected is positive) (2)
22. If (power is m high) and (frequency is very_high) then (intrusion_detected is positive) (2)
23. If (power is very_high) and (frequency is very_low) then (intrusion_detected is positive) (2)
24. If (power is very_high) and (frequency is low) then (intrusion_detected is positive) (2)
25. If (power is very_high) and (frequency is moderate) then (intrusion_detected is positive) (2)
26. If (power is very_high) and (frequency is high) then (intrusion_detected is positive) (2)
27. If (power is very_high) and (frequency is very_high) then (intrusion_detected is positive) (2)

3.4 Database Specification Model

The research model has five tables in the database and these tables describe the fields and data types that are stored in the database. The database is built in My Structured Query Language (MySQL) database management system whose schemas this section describes holistically. The first table in the system database is **User Intrusion table** which has six fields; the first field being user **id** that stores details of the user or owner of the building whose phone number is to store in the system and the expected data type is **integer** which length is 11 characters. The second field is **FullName** of the users, this stores the name of the user/users, and the expected data type is **variable character** with length of 65 characters. The third field is **ContactAddress** of users which corresponds to the address of the build where our system has been installed to detect intrusion the field stores the contact address information and the expected data type is **variable character** with 200 character length. The fourth field is the **phoneNumber** of users that is needed to be stored in the database; these are the numbers that will receive an alert message when the system detects intrusion in the building. The user(s)/owener(s) and appropriate authorities maybe more than one individual as the phone number stored may also be more than one. The fields' stores the phone numbers of users; the expected data type is **integer** with length of 11 characters. The fifth field is the EmailAddress of the users; it stores the users email address information, the data type expected is **variable character** which length is 50 characters and the sixth field is MsgBody which holds the content of the message that is sent to the users and appropriate authorities' cell phones and their emails, the data type is **variable character** with 256 character length while the seventh field is MsgDate which holds the date and time the intrusion was detected, the data type is date. The structure of this table gives access to users from the front end and stores information of the users. The structure of user intrusion table is shown in table 1.

Table 1. Structure of User Intrusion table

Field	Type
id	int(11)
FullName	varchar(65)
ContactAddress	varchar(200)
PhoneNumber	varchar(11)
EmailAddress	varchar(50)
MsgBody	Text(256)
MsgDate	Date

The admin table gives rights to an admin to access the back end and stores the admin's information. **Username** is the first field, it store the user name of the admin and the expected data type is **variable character** which is 50 characters in length. Password is the second field in the database table, it stores the admin password, and the data type stored in this field is **variable character** which length is 50 character. Fullname is the third field in the admin table, the table stores the admin full name and the expected data type is **variable character** which length is 50 characters. The fourth field in table is EmailAddress of the admin which stores the email address information of the admin and **variable character** is the expected data type which can hold up to 50 characters. The structure of the admin table is showed in table 2 :

Table 2. Structure of Admin Login Table

Field	Type
TableName	varchar(50)
GroupID	int(11)
AccessMask	varchar(10)

The user group database table enables the admin to group users and the table stores the information of the group of users. It comprises of two fields, GroupID and GroupName. GroupID stores the GroupID number and the expected data type is **integer** which length is 11 characters while GroupName store the name of the group, the expected data type is **variable character** whose length is 50 characters. Table 3 represents the users' Group Member Structure.

Table 3. Structure of Group Member Table

Field	Type
GroupName	varchar(50)
GroupID	int(11)

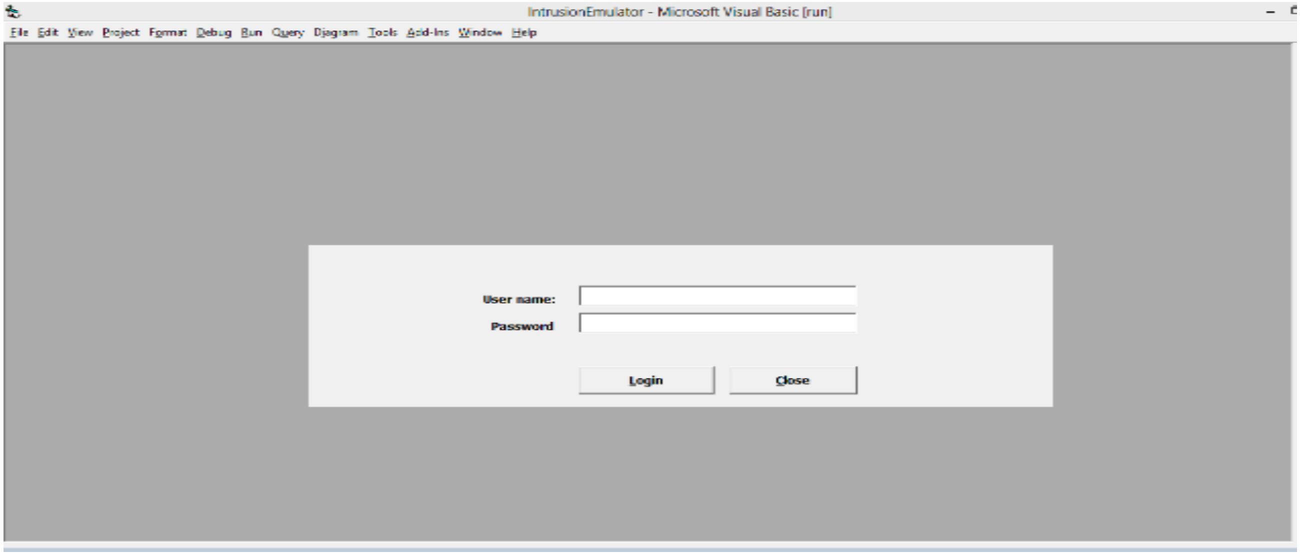
Table 4. Structure of Member's Rights Table

Field	Type
Username	varchar(50)
Password	varchar(50)
Fullname	varchar(50)
EmailAddress	varchar(50)

The structured of membership right table stores information of the privileges or rights given to group members in a particular group created, which is right to perform any operation in the admin table. The table comprises three fields; TableName, GroupID and AccessMask. TableName stores the name of the table and the expected data type is **variable character** which length is 50. GroupID stores the Group ID number and the expected data type is integer with length of 11 character. AccessMask stores Access Mark information and the expected data type is **variable character** which is 10 character in length.

3.5 Design Interface Model

Once a user login, its takes the user to the main page. Its shows the user how the system work. The main page was used to captures the building model where the system has been installed, the cloud and user' cell phone. Figure 10 shows the main page.


IntrusionEmulator - Microsoft Visual Basic [run]
File Edit View Project Format Debug Run Query Diagram Tools Add-Ins Window Help

User name:

Password

Fig 10: User Login in Page

Figure 11 shows how vibration signals are detected from the building. On detecting vibrations signals from a building, these signals are routed to the fuzzy-based system that resides in the cloud. This signals serves as crisp input into the system. The system fuzzified the input signals and determine their membership function. However, this page illustrate vibration signals whose membership function is not above 56 m/s, Hence the intensity of the signals is either medium or low, therefore no message is sent

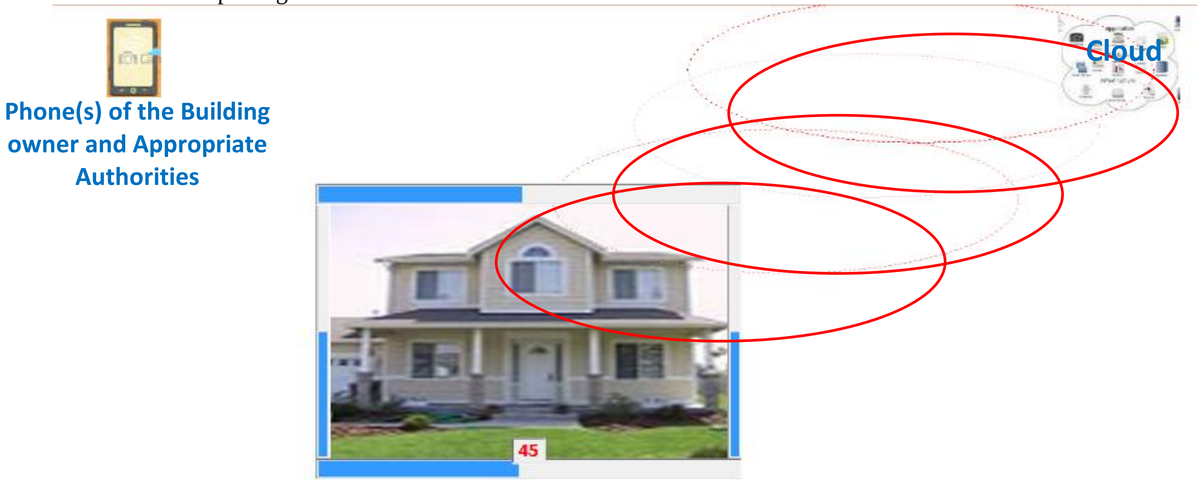


Fig 11: Main Page with Low Intensity Signal

This page shows vibration signals whose membership function is above 56 m/s, Hence the intensity of the signals is high, a message is sent to a registered user notifying him of an intrusion detected in the building. This is indicated as shown by the message on the cell phone in figure 12.

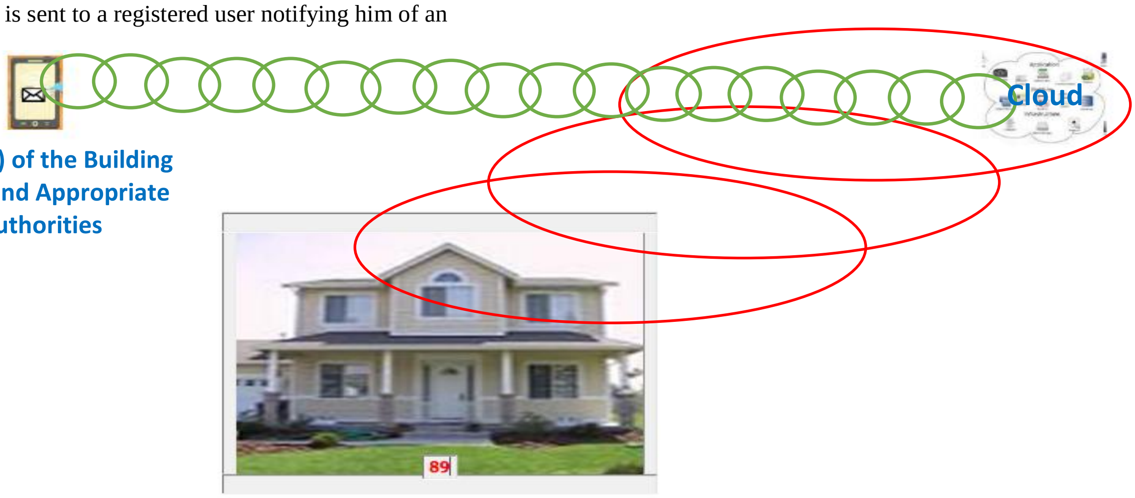
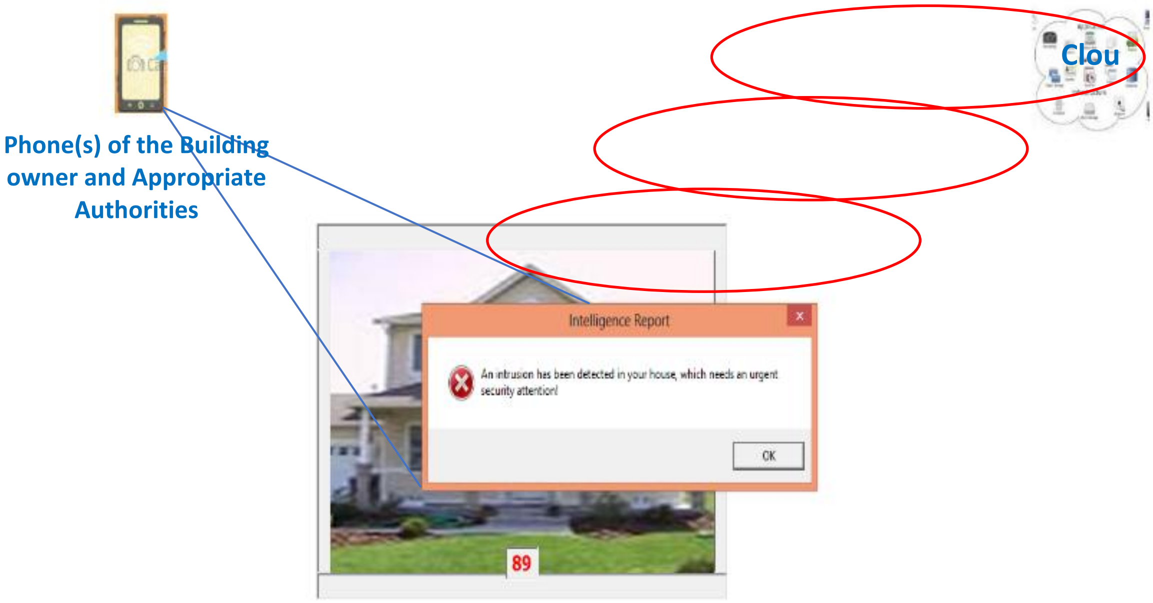


Fig 12: Main Page with High Intensity Signal

This page shows the content of the SMS that has been sent reporting the intrusion detected. The message body is "An intrusion has been detected in your home which required an urgent security attention" as shown in figure 14



An intrusion has been detected in your house, which needs an urgent security attention!

Fig 14: Main Page Displaying Message Sent to User

4. RESULT AND DISCUSSION

The Result of Automated Theft and Intrusion Detection System are analyzed as follows; forces exerted on the building that generated high vibration intensity as recoded by the sensor i.e. vibration intensity above 56 m/s, triggered an intrusion detection messages to be sent to the configured phone numbers of the building owner(s) and appropriate authorities. It was also observed that no message was sent for vibration signals whose intensity is less than 56 m/s. The result shown in Table 5 and 6 shows the various vibration signals powers(w) and frequencies(Hz) that were used testing the vibration intensity. The vibration intensities that were above 55m/s triggers intrusion detection messages while vibration intensities signals less than 56 m/s did not

Table 5. Power and Frequency Table

Attempts	Address	Power (W)	Frequencies (Hz)
1	BLOCK A	35	15
2	BLOCK A	30	30
3	BLOCK A	40	30
4	BLOCK A	8	2
5	BLOCK A	50	42

6	BLOCK A	30	18
7	BLOCK A	16	20
8	BLOCK A	35	20
9	BLOCK A	64	20
10	BLOCK A	13	12
11	BLOCK A	15	10

Table 6. Crips Inputs and Crips Outputs

Attempts	Address	Sensor Readings (Crips Input) m/s	Fuzzified Variables (Crips Output)	Membership Function
1	BLOCK A	50	0.2500	MODERATE
2	BLOCK A	60	0.5101	HIGH
3	BLOCK A	70	0.6362	HIGH
4	BLOCK A	10	0.2500	VERY LOW
5	BLOCK A	92	0.6406	VERY HIGH
6	BLOCK A	48	0.2500	MODERATE
7	BLOCK A	32	0.2500	MODERATE
8	BLOCK A	55	0.4290	MODERATE
9	BLOCK A	84	0.6248	VERY HIGH
10	BLOCK A	25	0.2500	VERY LOW
11	BLOCK A	15	0.200	VERY LOW

5. CONCLUSION

In this study, an automated building burglary and theft detection system was designed using fuzzy logic. A system that will expedite the detection of theft and building intrusion burglary crime, which was subjected to examine several vibration intensities generated by various vibration signal as a result of forces exerted on the building at various times. The proposed system was able to detect intrusion based on the vibration signal's intensity and alerted the building owner and appropriate authorities. It's clear from the result presented that fuzzy-based building intrusion and theft detection systems is cheap, efficient and effective approaches for detecting intrusion in buildings. This approach creates room for extending detection of intrusion to residential owners and appropriate authorities promptly, which is a significant advancement over the existing systems. Therefore, industries and other government bodies can implement the developed system in their establishments to mitigate crimes at their respective institutions and the society at large.

6. REFERENCES

[1] Ahn, S. W., Jung, H. S., Lee, Y. W., and Yoo, C. 2009. Network condition adaptive real-time streaming of an intelligent ubiquitous middleware for u-City. In Proceedings of the 4th International Conference on Ubiquitous Information Technologies & Applications.

[2] Anon (2001) Contractors Equipment Losses: Knowledge of Hazards Can Reduce Risk. "Insurance Journal". Retrieved 19 February 2009 from http://www.insurancejournal.com/magazines/southcentral/2001/02/19/features/22326.htm

[3] Chaudhary, T., Tiwari, H., and Kumar, U., 2019. "Fuzzy Logic Based Intrusion Detection Systems in Mobile Ad Hoc" International Journal of Information Technology, at Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA)

[4] Coole, M., Woodward, A. and Valli, C., 2012. Understanding the Vulnerabilities in Wi-Fi and the Impact on its Use in CCTV Systems.

[5] Costin, A., 2016, October. Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In Proceedings of the 6th international workshop on trustworthy embedded devices

[6] Curtin, L., Tilley N., Owen M. and. Pease K, 2001. Developing Crime Reduction Plans: Some Examples from the Reducing Burglary Initiative. Crime Reduction Research Series, Paper7. London: Home Office. First Publisher, 1-84082-632-0.

[7] Eseosa, O. and Promise, E., 2014. GSM based intelligent home security system for intrusion detection. International Journal of Engineering and Technology

[8] Fitzgerald, J. and Poynton S., 2011. The Changing Nature of Objects Stolen in Household Burglaries. NSW Bureau of Crime Statistics and Research. Issue paper no. 62.

[9] Jordal, R.L., 1989. Integrated smoke and intrusion alarm system. U.S. Patent 4,862,14

[10] Khanna, V. and Cheema, R.K., 2013. Fire detection mechanism using fuzzy logic. International Journal of Computer Applications

[11] Nancy, G., Samantha, S., Allison, M., and Joshua A., 2011. Surveillance Systems for Crime Control and Prevention: A Practical Guide for Law Enforcement and Their Municipal Partners. The Urban Institute, 978-1-935676-35-5

[12] Obermaier, J. and Hutle, M., 2016, May. Analyzing the security and privacy of cloud-based video surveillance systems. In Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security

[13] Omorogiuwa, E. and Elechi, P., 2015. Economic Effects of Technical and Non-Technical Losses in Nigeria Power Transmission System. IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), Vol. 10 No.2, pp. 89-100, 2015.

[14] One Square Metre (2019) “Small & Large Building” – https://www.onesquaremetres.com/small-large-building/

[15] Zurich, 1999. Suggestions for Use of Video Surveillance Cameras “Clear thinking on fuzzy logic “L.A. Bernardinis (Machine Design, April 1993) Fuzzy set by Ivars Perterson (Science News , Vol. 144, July 24, 1993, pp. 55).