Research Article

# Smart Home Automation: GSM Security System Design & Implementation

## E. Isa and N. Sklavos*

*Computer Engineering & Informatics Department, University of Patras, Greece*

___

### *Abstract*

Smart home automation has attracted the interest of the research community during the last decade, at a great manner. Home security systems consist a constantly developing research field. In this paper, a security system for smart home automation is proposed. The introduced system operation is supported by a GSM embedded mobile module, which enables the alert messages transmission to both mobile devices of end users, and central security offices. The proposed system is implemented on a microcontroller module, through an embedded platform. The proposed system operates on different levels of user's access control, based on passwords policies. Each time, the involved end users and the security offices, can be informed for operation modes change through SMS communication, via the available GSM network

*Keywords:*  Security, system design, smart home automation, GSM.

___

## 1. Introduction

In our days, the need for security makes many people look for different ways to protect their property [1]. Many systems assure limited access in both indoor and/or outdoor environments. But, even if there are many developed systems that support it, some of them have very complicated connectivity and the implementation cost reaches high values. Especially the last one, in most of the cases can make the system forbidden, for the users. These systems are related with both security and safety of private sectors such as homes, work places or other rooms that people need to protect. In smart home automation, a great number of different systems are needed to be integrated together, with as less resources as possible.

Home automation is considered as the residential extension of a building automation. It is related to home, housework or household activity. It usually includes centralized control of lighting, heating, air conditioning, appliances, gates and doors security locks, as well parts for other purposes, in order to provide improved convenience, energy efficiency and security. It essentially offers to the users access control to devices or objects in the house.

During the last decade, smart home automation has been developed at a great rate [2]. Many systems have been developed, that cover efficiently every possible security need. These needs may be different from time to time, and they can be referred with different purposes and targets of protection. So the fundamental need for security has become a field of research of great interest, the last years [3].

A security and safety system, aimed to smart home automation, has to support several different purposes. As it is shown in Figure 1, such systems detect the outbreak of fire at a very early stage by a temperature sensor, inform

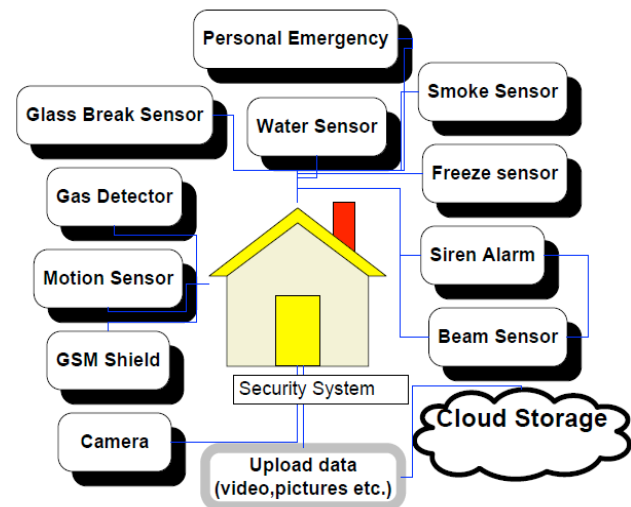about a possible flood and some limit the human access at indoor and outdoor places.



**Fig. 1.** Security & Safety System, for Smart Home Automation

The last ones and due to the fact that they have to control the access of external intruders, they usually characterized of high complexity. For this reason, these systems satisfy only some fundamental specifications. The most important of these specifications is the reliability that they have to provide. At the same time, every group of users is aimed to handle them in an efficient way. Any possible feedback information has to be simultaneously delivered to the users.

This work is aimed to propose a flexible and efficient way, for both the design and the implementation of a security system. At the same time, the proposed system is aimed to satisfy the increased needs for smart home automation. The system's implementation cost is concurrently low enough, of the used resources. The proposed system supports communication modules with the

owner, possible end users, as well as with central security offices, through the available GSM communication network.

## 2. Proposed Security System Design

### 2.1. Device platform

The proposed system design is based on a microcontroller device, embedded in an Arduino system module. However, a system like that can be based on a large variety of other available microcontrollers, if the developer makes the appropriate changes. Arduino is an open-source electronic, prototyping, computing platform used for system development. It can be used to develop both stand-alone interactive objects, or can operate efficiently with software co-design, supported by another computing system. It consists of a physical programmable circuit board and parts of software coding. The circuit board mainly includes a microcontroller device, digital and analog pins, as well as other peripheral components. The proposed system is based on an R3 Board ATmega 328, in conjunction with an R3 Ethernet Shield. The integrated development environment (IDE) runs on a computing system and it is used to write and download the code to the circuit board. IDE is based on a simplified version of C.

The implementation platforms are proven quite cheap and compatible with a great range of electronic parts. These are great reasons that make them ideal for the proposed system integration. In more details, these can be combined with many other hardware shields, and in this way the supported functionality is increased, at a great manner. In the proposed system, the circuit board is connected with a compatible GSM shield, and supports mobile transmission, in an efficient way of data communication. Besides complete shields, different types of sensors can be connected to the introduced board, in order event triggering to be enabled, with the external environment. The integration devices are programmed, based on coding downloading each time, through a USB communication interface.

The proposed system is based on a 8-bit ATmega microcontroller, which is manufactured by Atmel and belongs to the megaAVR series. Different types of memories, such as Flash memory, RAM and EEPROM, support the operation of ATmega. The device platform also includes I/O peripherals, timers, and PWM. There are many alternatives of this device platform that they differ by microcontroller model, memory blocks, etc. This series boards support the ability to combine shields, which can be plugged efficiently, into the normally supplied pin-headers interface of it.

The device programming is achieved based on a wide range of alternative libraries, which achieve the compatibility among the different types of devices and embedded shields. These libraries are basically coded with C++. Thus, they are easily constructible and readily accessible. More analytically the device programming has two reserved functions: void setup() and void loop(). The setup() function is called when a sketch starts. It is used to initialize variables, pin modes, included libraries etc. The setup() function only runs once, after each power up or reset of the board. After creating a setup() function, which initializes and sets the initial values, the loop() function does precisely what its name refers to. It loops consecutively, allowing the rest code to respond. It is used to actively control the implementation board. However, there are also other functions that are included in the libraries, which support the device programming.

### 2.2. GSM Shield

The GSM shield makes the proposed system able to send and receive short text messages, make voice calls and connect to the Internet. Shields of this kind could stand upon the microcontroller platform, but they must be compatible. Two basics connections of this shield are TX and RX pins, which allow the microcontroller to connect with the GSM shield sending serial data.

GSM operates with a SIM card. The SIM requires a subscription, with a mobile communication provider. Based on this, the user can get access to the mobile network. The UART (Universal Asynchronous Receiver Transmitter) Interface codes and decodes data between the parallel and serial formats. It takes bytes of data and transmits them in a sequence of bits. Thus, the data can be sent, in a serial mode, through TX to the microcontroller, or though an antenna to the network.

The RF PAD reduces the power of the signal, without appreciably distorting its waveform, in order to ensure that the radio signal level in the correct one. The shield uses a radio modem, which works at frequencies GSM 850MHz, GSM 900MHz, DCS 1800MHz and PCS 1900MHz. Alternative shields can provide also GPRS module and they support TCP/UDP and HTTP protocols, through a GPRS connection.

### 2.3. Ethernet Shield

The ethernet shield allows the microcontroller to connect to the Internet through an ethernet wire. It provides a network (IP) stack, capable of both TCP and UDP. The chip has an internal buffer for storing. The user must include in the code the ethernet library sketches, which support the communication with the Internet. Most of these shields have a micro-SD card slot, which can be used to store files for serving purposes over the network. For example, if the user wants to capture a photo from a camera input and upload it to a remote database, the process that is followed is described as: a) the camera takes the photo and stores it in the memory card, b) the ethernet shield initializes its connection with the internet, c) the photo is transferred from the memory card to the internal buffer, and finally d) the shield schedules the process which will send the data through the ethernet cable.

## 3. Proposed System Architecture

A modern security and safety system, of this kind, is connected with a variety of different peripherals and other devices. These are a number of alternative sensors, which are activated when an event is triggered. Also, a device can provide the optical feedback and another component allows the system to send information to the owner. Moreover, a database, where the activity of the system could be stored, is a main part of the design peripherals.

The proposed system is controlled by different levels of operation purposes, such as simple user, super user administrator etc, through password operation policies. The implementation cost of the proposed system achieves low values, in terms of area and allocated resources, which guarantees flexible and safe operation at the same time.

The basic architecture of the proposed system is illustrated in the next Figure 2. The proposed system is designed to be placed and operate efficiently as a stand alone embedded module, or in cooperation with other possible available computing platforms, in an overall automation, of a smart home [2].

The microcontroller component is connected to I/O devices. Input devices include a keypad panel, a camera and a couple of sensors. The keypad panel is used for system control, like activation and deactivation, changes of both security levels and operation modes. Sensors units detect movements, or position changes of objects, in the areas of responsibility. Camera is used for photos capture purposes, when an event happens, like a sensor activation or a change to the system's operation state: from activation to deactivation and opposite, etc. It could also be used, in case of events triggering of any kind. Later, these photos, could be sent to a dedicated database, or else to be stored, with a cloud based approach. Output units include a LCD screen, a GSM shield and a speaker. The LCD screen supports a common user interface. The embedded GSM shield contains a SIM card, and it is dedicated to send information, though short text messages to specific end users or to central security offices, in the case of alarms. Finally, the speaker is used in order to produce the appropriate alert messages.
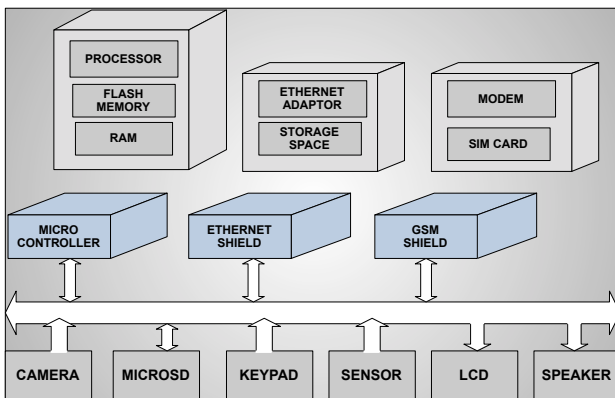


**Fig.2**. Proposed System Architecture

In Figure 3, a real depiction of the proposed system is shown.
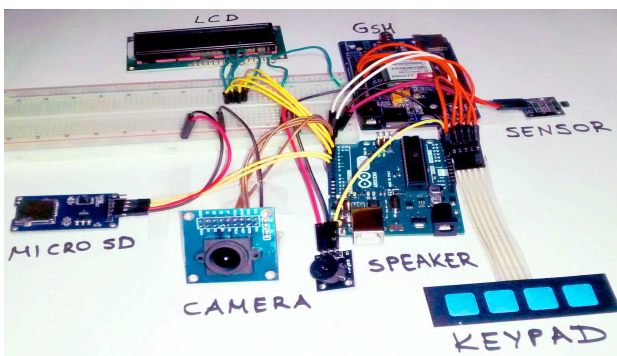


**Fig.3**. Real depiction of the proposed system

Especially the memory blocks of the implemented system, are components, which attract the designers interest. The Atmega 328 microprocessor uses memory blocks based on Harvard architecture. Most of today's microcontrollers use this model, so a possible future replacement of the microcontroller, will be compatible with these parts.

Programs are stored in Flash memory, while the data are stored in the SRAM memory. When the system is on, it recalls a part of the code from the flash memory and it stores that in the SRAM. First the setup() function is running. The execution of this initializes the pins interface that will be used, as analysed in detailed in the previous section. When this part finishes, the loop() function is called. A detailed report to the assembly and the interconnection among the system components is referred in the next paragraphs. This report explains in detail the FSM also (Figure 4), which is depicted when the system is turned on. It is considered that the data flow begins when the system has power supply, and the source code is already stored in the flash memory.
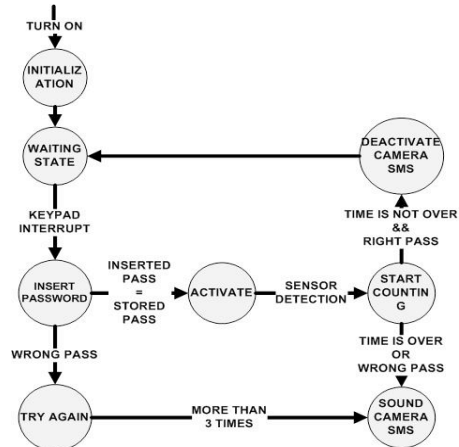


**Fig.4**. Finite State Machine (FSM)

The system is initially on a waiting state. The user, in this state, can only activate it. The activation starts only with user authentication, based on password policy. For this purpose, a keypad is used to insert the right code in the proposed system. The keypad, internally, concludes vertical and horizontal wiring. This wiring ends to the microcontroller. The code includes a dedicated part for the mapping of the pressed keys set, each time. So, the system receives a signal from two lines and the pressed key is determined. The used password is already stored, while the system in this state, verifies if the stored password is the same with the inserted one. If the process is accomplished successfully, the user will have some seconds to close the door, in order the sensor to be activated. This can be done by using a delay() function. The sensor can be a hall effect one. It is a transducer that varies its output voltage in response to a magnetic field. The output of this sensor is an analog one. Thus, the whole system can be placed on the external side of the door and a piece of a magnetic material to be on the wall, at the same height. When the door is closed the sensor will be in touch with the magnetic field and the system will receive a signal. The user has three tries to key in/type the right password. After each failed attempt, a counter in the code will be increased. If the specified failed attempts are made, the system will inform that probably a non-authorized attempt is performed. Then the system will be set on the alarm state.

In this state, the proposed system must schedule 3 different processes: a) play a characteristic sound through the speaker, b) capture a photo of the user, and finally c) send a short text message to inform the owner and the central security office. The photo can be captured using a serial TTL camera. Camera uses the TX and RX pins to communicate with the implementation platform. However,

as it was mentioned above, each microcontroller has a limited storage space. So, using a camera demands a new storage space in which photos or videos can be stored. The selection of the memory must be done based on the necessary storage of both programming codes and camera's needs. Hence, the image size of the camera determines at a crucial factor the size of the memory. For example, if the system captures only photos and the image size of a VGA camera is 640x480, the whole frame has 307.200 pixels. If the image is a grey scaled one, it is known that it needs 1 byte for each pixel to store it. So, every picture needs 0.3 KB of memory. If the protected door opens for example 10 times every day, 3 KB of memory is used per one. If the user possibly wants to store video, the frames per second and the duration of the video multiply the above amount. Depending also on the code expansion the user can estimate the appropriate memory blocks that are needed.

The third process has to do with the transmission of s short text message. The system informs the owner about the situation, in real time through a mobile communication feedback. As it has been mentioned before, the GSM is the appropriate network for this. When the proposed system operates in order to to send a text message, the GSM shield is enabled and the necessary information is transferred using the TX and RX pin. In order this process to be performed correctly, the GSM coding library is applied. This library enables the board to perform most of the operations of GSM mobile communication. The GSM shield has a modem that transfers the data from a serial port to the GSM network. The library abstracts low-level communications between the modem and SIM card. The modem performs operations via a series of AT commands. The dial up and wireless modems need these commands to interact with a computing system. It relies on the Software Serial Library for communication between the modem and the device platform. The LCD module helps the communication between the user and the system. The integrated LCD component has 8 pins for data transfer and a couple of other pins, which are responsible for the control of the performed functions. Many LCD modules support two modes of operation, 8-bit and 4-bit. Using the 4-bit mode is more complex, but reduces the number of active connections needed. The operation mode must always be set using the Function Set command. In 4-bit mode the data is sent in nibbles, first the higher and then lower nibble.

## 4. Implementation Comparisons

Up to our days, alternative have been developed which support some of the proposed system security services, as it presented in detail in the following Table I. Some of them are developed in industry sector, while some other come from the research community and academia. In most of the cases, systems from industry support a number of services. These usually offer a reliable remote control of the system via a mobile device, support services for all day long, or a friendly interface designed to be used by all home residents.

On the other hand, many research results, offer a part of these facilities at lower cost, generally. A point of comparison, between all the examined security systems is their scalability. Some of these systems do not allow the users to add any additional sensors or coding functions, or even to change the operations source code. The applied system is fixed after it is fully integrated. In contrast, in open systems, the user has the option to install, to add, to change or to modify.

**Table I.** Implementation Comparisons

| | GSM/SMS | camera | voice control | low power | phone application | phone | PC | bluetooth | low cost | wireless remote control |
|---|---|---|---|---|---|---|---|---|---|---|
| Ramlee, Leong, Singh, Ismail, Othman,, Said Sulaiman, Misran [4] | | | ✗ | | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Madan, Reddy [5] | ✗ | | | ✗ | | | | ✗ | | |
| Babu, Narasimhulu [6] | | ✗ | | | | ✗ | | ✗ | | ✗ |
| Bhagyalakshmi, Divya, Aravinda [7] | | | | ✗ | | | | | | ✗ |
| Sukumar, Abhinay [8] | | | | | | | | | | ✗ |
| Javale, Mohsin, Nandanwar, Shingate [9] | | | | | | ✗ | | | | ✗ |
| Das, Chite, Peterson, Shirazi, Bhadkamkar [10] | | ✗ | | | ✗ | ✗ | | | | ✗ |
| Proposed System | ✗ | ✗ | | | | ✗ | | | ✗ | |

## 5. Conclusions

This work introduces a security system, with GSM mobile communication support, for smart home automation. The proposed system is compared with related integrations in the field. Future directions of this research could adopt additional security and safety schemes [11], [12].

## References

1. N. Sklavos, "Cryptographic Hardware & Embedded Systems for Communications", proceedings of the 1st IEEE-AESS Conference on Space and Satellite Telecommunications, Rome, Italy, October, 2-5, 2012.
2. A.J. Bernheim Brush, Bongshin Lee, Ratul Mahajan, Sharad Agarwal, Stefan Saroiu, and Colin Dixon, "Home automation in the wild: challenges and opportunities", proceedings of the SIGCHI Conference on Human Factors in Computing Systems '11, ACM, USA, 2011.
3. N. Sklavos, P. Kitsos, O. Koufopavlou, "VLSI Design and Implementation of Homophonic Security System", proceedings of IEEE Computer Society Annual Symposium on VLSI (IEEE ISVLSI'12), Amherst, USA, August 19-21, 2012.
4. R.A.Ramlee, M.H.Leong, R.S.S.Singh, M.M.Ismail, M.A. Othman, H.A. Sulaiman, M.H. Misran, M.A. Meor Said, "Bluetooth Remote Home Automation System Using Android Application", The International Journal of Engineering And Science, Volume 2, pp. 149-153, January 2013.
5. Vini Madan, S.R.N Reddy, "GSM-Bluetooth based Remote Monitoring and Control System with Automatic Light Controller", International Journal of Computer Applications, Volume 46-No.1, May 2012.
6. B.Suresh Babu, Dr. C. Venkata Narasimhulu, "Robust Model to Access Consumer Appliances Using Android", International Journal of Research in Advent Technology, Vol.2, No.10, October 2014.

7. P.Bhagyalakshmi, G.Divya, N.L.Aravinda, "Raspberry PI And Wifi Based Home Automation ", International Journal of Engineering Research and Applications, pp. 57-60, January 2015

8. N.Sukumar, A.S.Abhinay, "Web Server Implementation for Embedded Home Automation by Using IP Protocol", Proceedings of International Conference on Emerging Trends in Engineering & Technology, pp. 147-151, September 2014.

9. Deepali Javale, Mohd. Mohsin, Shreerang Nandanwar, Mayur Shingate, "Home Automation and Security System Using Android ADK", International Journal of Electronics Communication & Computer Technology, Vol.3, Issue 2, 2013.

10. Somak R. Das, Silvia Chita, Nina Peterson, Behrooz A. Shirazi, Medha Bhadkamkar, "Home Automation and Security for Mobile Devices", Ninth Annual IEEE International Conference on Pervasive Computing and Communications, March 2011.

11. N. Sklavos, "Securing Communication Devices via Physical Unclonable Functions (PUFs)", Information Security Solutions Europe (isse'13), Brussels, 22-23 October, Belgium, 2013, pp. 253-261, Springer, ISBN: 978-3-658-03370-5.

12. G. Kalogeridou, N. Sklavos, A.W. Moore, "A Hardware Trojan Detection Framework", proc. of Designing with Uncertainty - Opportunities & Challenges Workshop, UK, 17-19 March 2014.