Perspectives in Science (2016) 8, 459—461

ScienceDirect

journal homepage: www.elsevier.com/pisc

Email based remote access and surveillance system for smart home infrastructure☆

Pooshkar Rajiv[a,*,1], Rohit Raj[b,1], Mahesh Chandra[a]

[a] *Birla Institute of Technology Mesra, Ranchi, Jharkhand, India*
[b] *National Institute of Technology Patna, Bihar, India*

Received 28 January 2016; accepted 9 April 2016
Available online 2 May 2016

KEYWORDS
Internet of Things;
Smart home automation;
Embedded systems;
Perceptual hashing

Summary With the rapid rise of Internet of Things in public domain, people expect fast, reliable and on-demand home security via the Internet. However, existing remote home surveillance systems place a very rigid constraint on authentication and require customized hardware and software. In this paper we have proposed an ingenious and reliable internet based, home access system for smart homes that can be easily deployed on generic hardware. The proposed architecture uses popular email service providers to notify and update the user about the home access. It sends an email to the owner with the attached picture of the person who is at the door. It also incorporates a protected mechanism to give access of the door to a remote user by responding to that email. It essentially means that we can view and give access to the person at our door via sending and receiving an email. Furthermore, an image processing based mechanism has also been incorporated to provide access without email, to few selected personnel who are trusted by the owner. It works by capturing and comparing the visitor's image with the stored images in the database. Perceptual hashing or fingerprint matching algorithm is used for comparison purposes. Similarity percentage based on hamming distance was evaluated, and the similarity threshold for providing access was set. The simulations were performed in rigorous environment. The efficiency of the hashing algorithm was found to be 97% at the similarity threshold of 95%. The results validate that the average latency is only 155 ms with low standard deviation. The CPU utilization remained quite low with a minimum value of 10 MHz and a maximum value of 30 MHz when the payload size of the sent mail was increased to 1500 kB. Thus, the proposed system can be used for developing a larger low power infrastructure.

Introduction

Latest advancements in the field Internet of Things (IoT), has made it one of the most emerging fields of computing. Low cost of technologies and sensors have demanded an unprecedented growth for home and industrial

☆ This article belongs to the special issue on Engineering and Material Sciences.

* Corresponding author. Tel.: +91 9821480878.
E-mail address: pooshkar.01@gmail.com (P. Rajiv).

[1] These authors contributed equally to this work.

http://dx.doi.org/10.1016/j.pisc.2016.04.104

automation. The growth of IoT and its related technologies, has improved home and lifestyle. Ever increasing assimilation of these technologies is constantly fuelling more innovations from technical giants. However, these technologies, though pervasive; are often unsecure and use dedicated servers for communicating between the client and end-devices. Moreover, the problem of securely giving access to houses and industries is still unaddressed and largely depends on physical presence of user in the house. Few real time systems which do provide similar secure solutions, use a devoted gateway and plethora of sensor networks to give access to houses and workplaces and require immediate presence of access giving authority on the other end. They do not allow the owner to remotely control the access of his house. Additionally, the remote surveillance systems such as IP camera do not provide required information and filtering of potential adversary. The field of home access and control primarily relies on middleware services for granting permissions. Work done by Gayathri et al. (2014) uses middleware for separate trust and authentication manger to check the credentials and give permissions.

This paper proposes a novel and unique mechanism for access control and surveillance of the homes and industries using existing protocols. This mechanism allows completely secure access to the homes by opening the doors controlled by the embedded system. This is achieved by allowing the owner to selectively grant permissions, by enabling the remote owner to give commands by simple Email protocol to open the doors. Hence, a person sitting anywhere in the world could potentially give access to his home by sending a simple E-Mail from any client. It also supports a provision of predefined database which would give immediate access to trusted third party. Furthermore, the proposed mechanism allows pooling of requests for a fixed interval and incorporates a potential alert system.

This system proposed provides an efficient, elegant and robust solution to the problem of remote home access, security and surveillance. Apart from being effective, it is also low cost due to use of generic email service providers for communicating with the owner.

Related work

A number of home surveillance models have been previously proposed. These home surveillance models have been able to optimize the surveillance operation by making use of wireless sensor networks (Wibowo et al., 2014; Sulc, 2011), ultrasonic sensors (Bai et al., 2011), usage of a photovoltaic array, MMS Modem (Gayathri et al., 2014). There has been an effort to improve the quality of surveillance by introducing tel-monitoring (Pawlak et al., 2015), adaptive http streaming (Nguyen et al., 2013) and by the development of intelligent fish eye camera. However, none of the proposed systems are able to allow the user to remotely control the operation of the surveillance system when an event occurs for which the system has not been designed i.e. the user does not have the power to override the system remotely.

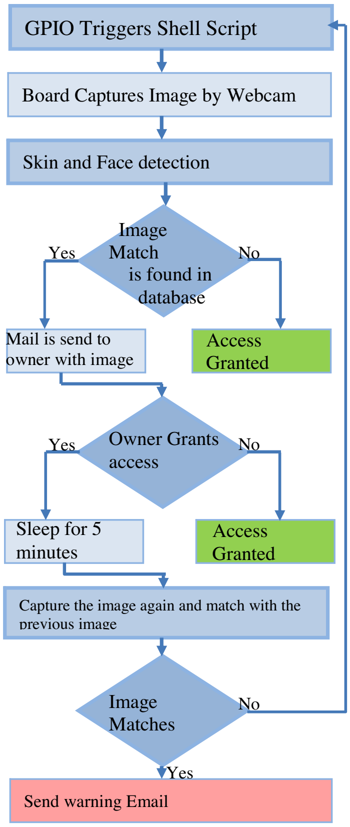
GPIO Triggers Shell Script
Board Captures Image by Webcam
Skin and Face detection
Image Match is found in database
Yes
No
Mail is send to owner with image
Access Granted
Owner Grants access
Yes
No
Sleep for 5 minutes
Access Granted
Capture the image again and match with the previous image
Image Matches
No
Yes
Send warning Email

Figure 1 Process flow.

Proposed architecture

The proposed model allows the user to remotely grant access to selected people even if the system was not designed to give access to them. The block diagram of proposed work is given in Fig. 1. Significant elements of the proposed model are face detection, image comparison, mail delivery and reply processing

Image capture and face detection

Once the GPIO event has been triggered, a shell script is executed by the C program using the system command. This shell script consists of an openCV program for capturing an image, followed by python programs for image comparison and email delivery. The captured image is converted into modified YUV colour space, then Skin detection algorithm using threshold values for YUV components is applied to separate the skin components from the captured frame. HAAR cascade classifier as proposed by Paul Viola is used for face detection. The detected face is then separated and stored for comparison with the database of allowed personnel.

The image of the face as detected by the HAAR cascade classifier is matched sequentially with the whole database of facial images of allowed personnel stored in the database in BBB. Perceptual hash functions based on average hashing are used for matching the captured facial image with the images stored in the database. The final verdict is made according to the selected threshold. Personnel authentication was made on the basis of the hamming

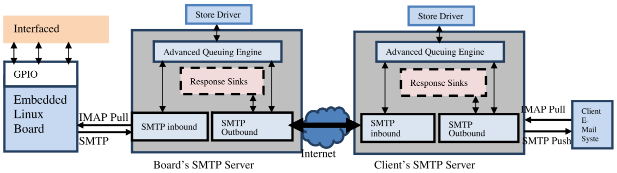

Figure 2 Proposed system architecture.

distance between the perceptual hash values of the two images.

Email from embedded system to user and reply processing

The embedded system attaches the image of the service requester along with the email containing few predefined text strings which informs the authorizer about the request he has received. The Email could be send by any of the module available in various languages. One such module which was used in our setup was smtplib in python. The email server used may belong to any provider. Most email providers today allow interfacing of non-legacy mail clients over different ports e.g. gmail provides SMTPS support over port 465. The mail will be send through account created on any email provider.

To retrieve the email from the server, a communication protocol for retrieval such as IMAP is used. The script present on the embedded Linux platform uses one such protocol to fetch the latest unread email and verify its integrity before validating it. The parameters includes: (a) The origin of the email that is, the email should only be from a list of approved sources and not from any email id. It is required to prevent any other user from bypassing the mechanism. (b) The status of email i.e. the email should be fresh and unread and should have reached within a limited timeframe. This is done so that a single instance of email is able to validate the requester only once. (c) The email should also contain some passphrase which will allow the embedded system to authenticate the person, as an accidental mail or a deliberate hacking of the authorized email address will not be enough to fail the entire mechanism. This whole process has been illustrated in Fig. 2.

Simulation results

To simulate the results in real life scenarios, a BeagleBone Black was interfaced with the FPGA board and an Email ID was setup on Gmail server. The implementation for sending the Email was done in Python and the code was saved on the board. To connect with the Gmail server from the board itself, port number 465 was used. The images were captured and multiple Emails were sent to the user. The graph for latency between picture and capturing and mail sending was recorded. A graph was plotted for 40 such reading.

Fig. 3(a) shows the latency for sending the Email. We can see that the total time taken for sending every Email varies between 180 ms and 230 ms which is fairly consistent and shows that this mechanism is feasible in real life scenarios with low delay. On the other hand, Fig. 3(b) shows the graph of CPU utilization on embedded board vs. the payload of message. The payload varied between 50 kB and 1550 kB.

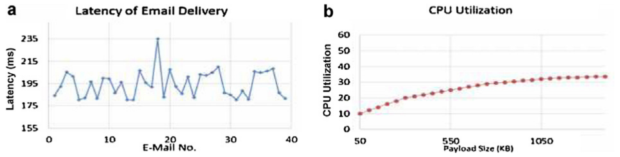

Figure 3 (a) Graph of email delivery time and latency. (b) Graph of payload size and effect of CPU on the message.

We can see that the CPU usage peaks at 30% around 700 kB and stays constant. It shows that our architecture is energy efficient and can effectively control the board without high power consumption.

Conclusions and future applications

The proposed system integrates the functionality of Image processing, embedded control and Internet of Things (IoT) into a single robust model. All the computations and calculations have been handled by the edge device, making the system more secure and private. As the work uses exiting Email clients, the security provided is quite high. In future, video feature based home authentication can be developed instead of image processing based. Moreover, it can also incorporate integration of Biometrics for the board. We hope that our work provides a basis for a more secure remote home access and control.

Acknowledgements

The authors would acknowledge Pooshkar Rajiv and Rohit Raj have contributed equally to this work and they are co-first authors.

References

Bai, Y.-W., Xie, Z.-L., Li, Z.-H., 2011. Design and implementation of an embedded home surveillance system with zero alert power using a photovoltaic array. In: 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), 14—17 June, pp. 373—378.

Gayathri, P., Krishna Paramathma, M., Paramathma, M.K., 2014. Design and implementation of embedded home surveillance system by using MMS modem. In: Electronics and Communication Systems (ICECS), 13—14 February, pp. 1—5.

Nguyen, D.V., Le, H.T., Pham, A.T., Thang, T.C., Lee, J.Y., Kugjin, Y., 2013. Adaptive home surveillance system using HTTP streaming. In: 2013 International Joint Conference on Awareness Science and Technology and Ubi-Media Computing (iCAST-UMEDIA), 2—4 November, pp. 579—584.

Pawlak, A., Horoba, K., Jezewski, J., Wrobel, J., Matonia, A., 2015. Telemonitoring of pregnant women at home — biosignals acquisition and measurement. In: 2015 22nd International Conference on Mixed Design of Integrated Circuits & Systems (MIXDES), 25—27 June, pp. 83—87.

Sulc, V., 2011. Home Automation with IQRF Wireless Communication Platform: A Case Study, no. c., pp. 212—217.

Wibowo, S.B., Putra, G.D., Hantono, B.S., 2014. Development of embedded gateway for Wireless Sensor Network and Internet Protocol interoperability. In: 2014 6th International Conference on Information Technology and Electrical Engineering (ICITEE), 7—8 October, pp. 1—4.