Cloud Controlled Security Surveillance For Intrusion Detection In IT Infrastructure

U.Muthumathi Vathana[1] , K.Revathi[2]

[1]M.E.Student, [2]Assistant professor
Department of Computer Science and Engineering, Dhanalakshmi College of Engineering,Chennai.

***Abstract* — A system delivers comfort, energy efficiency and security, by providing control and monitoring of illumination, heating, ventilation, air conditioning, appliances, security surveillance, multimedia and other systems. Security surveillance systems are an integral part of numerous systems. Own cloud services are used in IT infrastructure around the world to control and monitor cloud connected IT infrastructure remotely.Cloud is based on the standard cloud computing model, in which services available to the general public over the internet as long as they use the web interface. The camera is used to detect motion. In case of an intrusion event the camera will automatically start to record the video and save to the cloud controlled website, another cloud service alerts the user with a SMS conversation. The user can then monitor the intrusion from anywhere, on any Internet enable device by accessing the cloud's web interface. If the intrusion is genuine, the user is provided with options to stealthily alert neighbours, play alarm sounds or even report to the police. Using these techniques, burglary can be evaded effectively and own cloud services which can be used in IT industry around the world to control and monitor cloud connected automation system remotely.**

***Keywords* - burglary; intrusion detection; motion detection.;alarm;cloud controlled security.**

I. INTRODUCTION

Cloud computing (or simply cloud) refers to the online services provided over the Internet together with the hardware and software resources of the servers that offer those services. A SMS modem connected to the cloud server is used to notify the users, in case of intrusion events. A schematic diagram of how a user is notified and how he/she controls and monitors the security surveillance system via the cloud services is illustrated in diagram. The figure portrays a direct connection of all boards (nodes) to the cloud over Internet which may or may not be through thread-hoc wireless network gateway, depending on configuration. 32 bit embedded CPU control program: it is mainly responsible for system initialization, interrupt control, hardware control, the audio and video data package send trough the network and reliable communication with the microcontroller**.** Cloud computing (or simply cloud) refers to the online services provided over the Internet together with the hardware and software resources of the servers that offer those services. A SMS modem connected to the cloud server is used to notify the users, in case of intrusion events. A schematic diagram of how a user is notified and how he/she controls and monitors the security surveillance system via the cloud services is illustrated in diagram. The figure portrays a direct connection of all boards (nodes) to the cloud over Internet which may or may not be through thread-hoc wireless network gateway, depending on configuration. 32 bit embedded CPU control program: it is mainly responsible for system initialization, interrupt control, hardware control, the audio and video data package send trough the network and reliable communication with the microcontroller**.**

Embedded Linux typically refers to a complete system, or in the context of an embedded Linux vendor, to a distribution targeted at embedded devices. Although the term "embedded" is often also used in kernel discussions (especially between developers who have "embedded concerns"—words often used in the community), there is no special form of the Linux kernel targeted at embedded applications. Instead, the same Linux kernel source code is intended to be built for the widest range of devices, workstations, and servers imaginable, although obviously it is possible to configure a variety of optional features according to the intended use of the kernel. For example, it is unlikely that your embedded device will feature 128 processors and terabytes of memory, and so it is possible to configure out support for certain features typically found only on larger Linux system.

Cloud computing security referred to simply as "cloud security" is an evolving sub-domain of computer security, network security and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing**.** Organizations use the Cloud in a variety of different service models (SaaS, PaaS, IaaS) and deployment models (Private, Public, Hybrid). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: Security issues faced by cloud providers (organizations providing software, platform, or infrastructure-as-a-service via the cloud) and security issues faced by their customers. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

The rest of the paper is organized as follows. Section II presents a description about the previous research which is relevant to the protein structural classes and the possible solutions. Section III involves the detailed description about the proposed model and explains overall architecture and its components.

II. PROPOSED METHODOLOGY

Service-Oriented Architecture (SOA) is seen as a promising technique to bridge the gap between sensor nodes and enterprise applications such as factory monitoring, control, and tracking systems where sensor data is used. Research efforts have focused on middleware software systems located in gateway devices that implement standard service technology, such as Devices Profile for Web Services (DPWS), for interacting with the sensor network. This paper takes a different approach deploying interoperable Simple Object Access Protocol (SOAP) based web services directly on the nodes and not using gateways. This strategy provides for easy integration with legacy IT systems and supports heterogeneity at the lowest level.

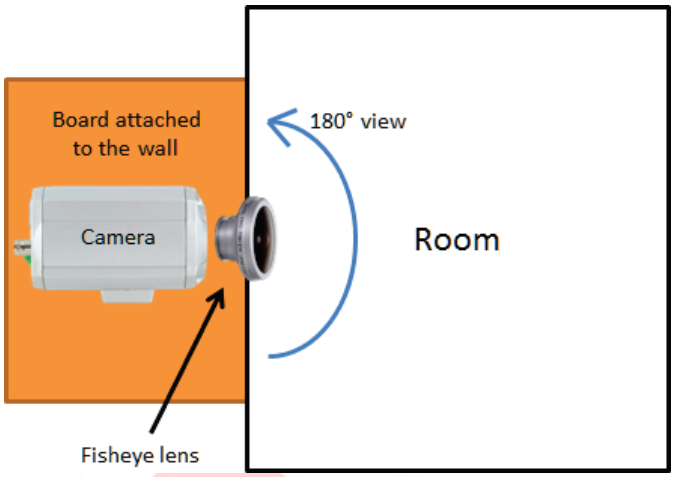

Fig.1. An illustration of how an infrared camera attached to each room would get a full 180° view of a room.

Security surveillance partakes in significant number of industries, home, bank, deploying microDVR cameras to monitor and report intrusion events and thereby reducing damages caused by burglary. In this paper, the design, implementation on and operation of a cloud connected adhoc wireless environment of IT industry with en suite intrusion detection and burglary prevention stratagems. In case of an intrusion event, another cloud service alerts the user with a SMS conversation using SMS modem. The user can then monitor the intrusion from anywhere, on any Internet enable device by accessing the cloud's web interface. If the intrusion is genuine, the user is provided with options to stealthily alert neighbours, play alarm sounds or even report to the police. Using these techniques, burglary can be evaded effectively.

A. Intrusion detection

An intrusion detection system is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization. IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports.

Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

Presently, the security services offered in cloud are:

- Real-time Monitoring of all rooms.
- Toggling the security surveillance on or off.
- Automatic storing and updating location of each room. In case of genuine intrusion, as confirmed by the user: Stealthily alert neighbours by playing low sound alarms in that particular place.

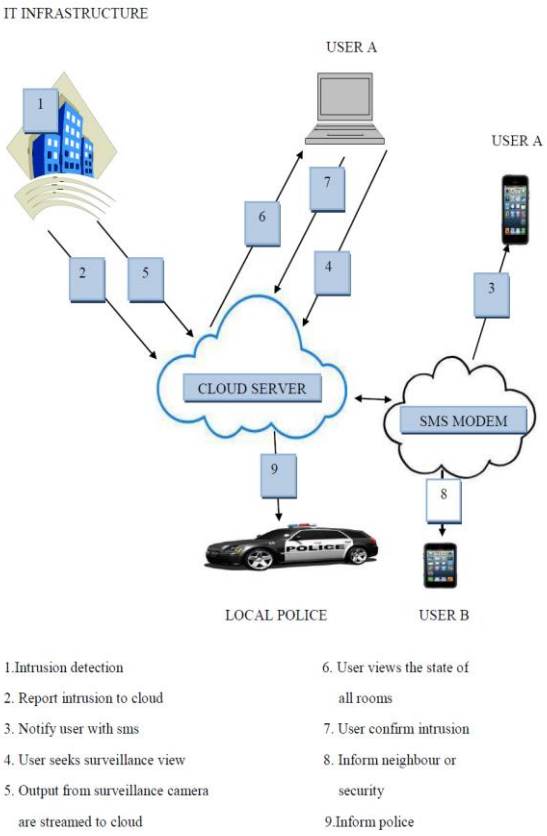

Fig.2. Intrusion detection

B. Remote controlling and monitoring

The cloud services can be accessed from anywhere in the world on any Internet enable device over an enforced Hypertext Transfer Protocol Secure (HTTPS) connection, encrypted by Secure Sockets Layer (SSL) version 3.0. The web interface of the cloud requires password based user authentication. A user is entitled to add any number of board (nodes) to his account, which can also be removed if necessary after authentication, the user is directed to the security surveillance page where controlling options and monitoring view from individual boards (nodes) are displayed. In case of genuine intrusion, as confirmed by the user then inform local police.

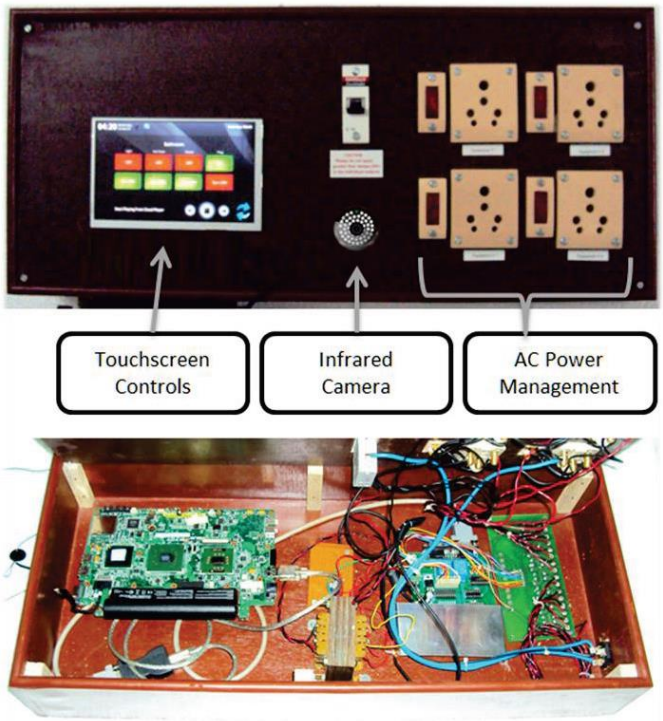

Fig. 3. External (top) and internal (bottom) snapshots of an operational cloud connected board (node).

In IT infrastructure motions can be detected using the micro DVR and starts to record automatically if any motion detected and the recorded file will be saved to the cloud server. There is no special cloud server is required for the user. The user can have the login account in cloud server. Once the motion detected the SMS notification will send to the user. The user then can login to the account and view the video file. If he found that as a real intrusion he can click the compliant option and the alarm sound will be played to the neighbor.

III. THE CLOUD SERVICES

Cloud computing (or simply cloud) refers to the online services provided over the Internet together with the hardware and software resources of the servers that offer those services . To construct our cloud, we deployed an Intel Xeon and Windows Server 2008 R2 based system. A SMS modem connected to the cloud server is used to notify the users, in case of intrusion events. A schematic diagram of how a user is notified and how he/she controls and monitors the security surveillance system via the cloud services is shown in Figure 2.The figure portrays a direct connection of all boards (nodes) to the cloud over Internet which may or may not be through the ad-hoc wireless network gateway, depending on configuration. Presently, the security services offered in our cloud are:

- Real-time Monitoring of all rooms.
- Toggling the security surveillance on or off.
- Automatic storing and updating geolocation of each board.
- SMS notifications and user's confirmation in case of intrusion detection.
- In case of genuine intrusion, as confirmed by the user.
- Stealthily alert neighbors, who are also using our home automation system, using SMS, email or by playing low sound alarms in their home.
- Inform local police.
- Play loud alarm sound.

IV. ADVANTAGES OF CLOUD CONTROLLED HOME SECURITY SYSTEMS

A. No dedicated web server required

Our cloud connected home automation network doesn't require a dedicated web server, to be remotely controlled and monitored over the Internet, whereas ordinary Internet enabled home automation network require a 24/7 running web server [10]. Furthermore, every mere Internet enabled home automation system would require a static public IP address for the web server.

B. No dedicated or specialized gateway required

Our home automation network doesn't require a dedicated or specialized gateway to connect to an external network because the communication base of the network is Internet Protocol, which can be directly connected to the Internet. Our choice of using 802.11n standard enables us to form this IP network.

C. Resource Sharing

Resources in the cloud are being shared among all users. For example, a single SMS modem is serving to notify all users in case of intrusion event. This type of resource sharing reduces cost and saves energy.

D. Location Awareness

The location of each node helps the cloud services to stealthily alert the accurate neighbors (who are using our home automation system) or local police, in an event of genuine intrusion.

E. Remote Control & Monitoring

The security surveillance system can be controlled and monitored in real-time, from anywhere, via the Internet.

F. Social Interaction

Since all users are using a central cloud service, we easily locate and contact the neighbors who are also using our cloud based home automation system.

V. Quality Of Service

As with any real-time process, the process of security surveillance should comply with good operability and integrity So, I did a few benchmark tests of the network gateway and found the result to be encouraging. On an average, less than 10% of the gateway bandwidth is in use, while carrying out security surveillance in 5 rooms simultaneously. This leaves out enough bandwidth to set up Resource Reservation Protocol - Traffic Engineering (RSVP-TE) across the IP network , which is anticipated to give real-time controlling and monitoring authority to the users.

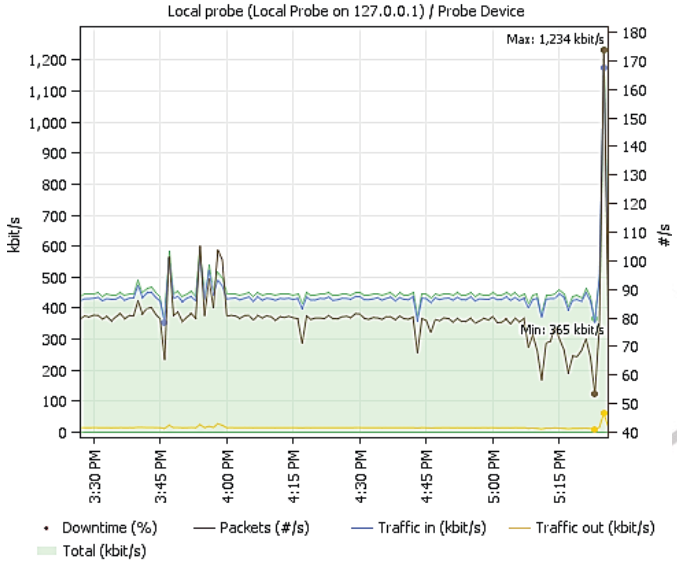

Fig. 4. A graph showing gateway bandwidth usage for duration of 2 hours. The maximum down-link network bandwidth is 7.2 Megabit/s and the maximum up-link network bandwidth is 1.8 Megabit/s.

VI. Conclusion and Future Work

The intrusion is detected and automatically recorded using micro DVR .This implies if any intrusion, motion or changes in an industry happens the camera automatically starts to recorded. The use of cloud services in IT industry derives many benefits extending from cost reduction to value added services. No special gateway or server is required. So it can be applicable to all the fields due to its simplicity. Resources in the cloud are being shared among all users. For example, a single SMS modem is serving to notify all users in case of intrusion event. This type of resource sharing reduces cost and saves energy.

Future enhancement involves remote controlling and monitoring the system. The web interface of the cloud requires password based user authentication for remote login to the system. After authentication, the user is directed to the security surveillance page where controlling options and monitoring view from individual boards (nodes) are displayed. The user is directed to the security surveillance page where controlling options and monitoring view from individual boards (nodes) are displayed. In case of genuine intrusion, as confirmed by the user then inform local police.

References

[1] V. Gungor and G. Hancke, “Industrial wireless sensor networks: Challenges, design principles, and technical approaches,” IEEE Trans. Ind. Electron., vol. 56, no. 10,

[2] I. K. Samaras, J. V. Gialelis, and G. D. Hassapis, “Integrating wireless sensor networksinto enterprise information systems by using web services,” SENSORCOMM,.

[3] A.Wolff, S. Michaelis, J. Schmutzler, and C.Wietfeld, “Network-centric middleware for service oriented architectures across heterogeneous embedded systems,” in Proc. IEEE 11th Int. EDOC Conf. Workshop, EDOC’07, 15–16, 2007.

[4] R. Bosman, J. Lukkien, and R. Verhoeven, "Gateway architectures for service oriented application-level gateways," IEEE Trans. Consumer Electron., no. 2,2011.
[5] J. Johansson, M. Völker, J. Eliasson, Å.Östmark, P. Lindgren, and J. Delsing, "Mulle: A minimal sensor networking device—Implementation and manufacturing challenges," Proc. IMAPS Nordic, 2004.
[6] J. L. Ryan, "Home automation", Electronics & Communication Engineering Journal, Volume: 1, Issue: 4, August 1989.
[7] Guangming Song, Yaoxin Zhou, Weijuan Zhang and Aiguo Song, "A multi-interface gateway architecture for home automation networks", IEEE Transactions on Comsumer Electronics, Volume: 54, Issue: 3,August 2008.
[8] Metkar Shilpa P. and Talbar Sanjay N., "Dynamic Motion Detection technique for fast and efficient video coding", IEEE Region 10 Conference (TENCON) 2008, November 2008.
[9] Ali Ziya Alkar and Umit Buhur, "An Internet based wireless home automation system for multifunctional devices", IEEE Transactions on Comsumer Electronics, Volume: 51, Issue: 4, November 2005.
[10] E. Topalis, L. Mandalos, S. Koubias and G. Papadopoulos, "QoS support for real-time home automation networks management via highspeed Internet connection", 10th IEEE International Conference on Networks (ICON) 2002, August 2002.
[11] R. T. Fielding and R. N. Taylor, "Principled design of the modern web architecture," ACM Trans. Internet Techno 2002.
[12] A. Boyd, D. Noller, P. Peters, D. Salkeld, T. Thomasma, C. Gifford, S. Pike, and A. Smith, "SOA in Manufacturing—Guidebook," IBM Corporation, MESA International and Capgemini, Tech. Rep., 2008. [Online].
[13] N. B. Priyantha, A. Kansal, M. Goraczko, and F. Zhao, "Tiny web services: Design and implementation of interoperable and evolvable sensor networks," in Proc. 6th ACM Conf. Embedded Network Sensor Syst., SenSys'08, New York, NY, USA, 2008.
[14] A. Dunkels, "Full TCP/IPfor 8-bit architectures," in Proc. 1st Int. Conf. Mobile Syst., Appl. Services, MobiSys'03, New York, 2003.
[15] C. Lerche, N. Laum, G. Moritz, E. Zeeb, F. Golatowski, and D. Timmermann, "Implementing powerful web services for highly resource-constrained devices," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOM Workshops), Mar. 2011.