

Cloud Based Intrusion Detection and Burglary Prevention Stratagems

Ashwini Abhyankar, Prof. V .D. Shinde

Department of Electronics & Telecommunication, R.M.D Sinhgad School of Engineering, Pune, India

Abstract—Security surveillance plays in significant role security systems, Deploying digital cameras and sensors to monitor and report intrusion events and thereby reducing damages caused by burglary. In recent years, virtualize on-demand access to a shared pool of computing resources such as networks, servers, storage, applications and services. This has enabled the lots of organizations to adopt cloud based computing to provide scalable, efficient and cost effective security systems. Detecting human beings in a video scene of a surveillance system is attracting more attention due to its wide range of applications in abnormal event detection. In this paper we propose a cloud based cloud based intrusion human detection system and burglary prevention scheme which can be adapted in Home automation, Offices, Banks etc.

Index Terms-Security Systems, Intrusion detection, Cloud computing, Digital camera.

I. INTRODUCTION

Fast development in the technology has increased the risk of intrusion. Intrusion detection systems (IDS) are an essential component of defensive measures protecting computer systems and network against harm abuse. It becomes crucial part in the Cloud computing environment. The main aim of IDS is to detect computer attacks and provide the proper response. An IDS is defined as the technique that is used to detect and respond to intrusion activities from malicious host or network.

Using security cameras allows a person to monitor his property. The majority of organization and administrations are making use of such security cameras with the intention to save their business as well as property from intrusion and illegal entry. Nowadays, the security cameras have become much more advanced, reasonable, smaller and straight forward. Organizations are often faced with major cost and installation nightmares while providing in person security protection. For a growing number of security sensitive enterprises, an automated system is more reliable, affordable surveillance, securing even the most difficult environments [1]. Automation helps in reduction of manual intervention in the systems and reduces the errors caused due to human intervention or human error. It also provides round the undisrupted service with minimum error. In security surveillance system detecting human beings in a video scene of a surveillance system is attracting more attention due to its wide range of applications

in abnormal event detection. An intelligent system detects and captures motion information of moving targets for accurate object classification. The classified object is being tracked for high-level analysis. Detecting humans and do not consider recognition of their complex activities. Human detection is a difficult task from a machine vision perspective as it is influenced by a wide range of possible appearance due to changing articulated pose, clothing, lighting and background, but prior knowledge on these limitations can improve the detection performance. The detection process generally occurs in two steps: object detection and object classification. Object detection could be performed by background subtraction, optical flow and spatio-temporal filtering. Background subtraction is a popular method for object detection where it attempts to detect moving objects from the difference between the current frame and a background frame in a pixel-by-pixel or block-by-block fashion. There are few available approaches to perform background subtraction. Apart from their vulnerability to image noise, color and non-uniform lighting, most of the flow computation methods have large computational requirements and are sensitive to motion discontinuities. Security services provided in the cloud have the potential to provide cost savings and faster deployment compared with equivalent capacity, premises-based equipment, but providers are yet to deliver on customer expectations. Currently many traditional security systems are provided as services in the cloud. These systems have been made available to end user to provide the security products for users in a service-based manner. Such model is referred to as Security-as-a-Service model.

II. SECURITY SERVICE IN CLOUD

Cloud computing has revolutionized the IT world with its services provisioning infrastructure, less maintenance cost, data & services availability assurance, rapid accessibility and scalability. Cloud computing has three basic abstraction layers i.e. system layer (which is a virtual machine abstraction of a server), the platform layer (a virtualized operating system of a server) and application layer (that includes web applications). Currently the biggest hurdle in cloud adoption by most of the corporate organizations is its security. Due to its distributed nature, cloud environment has high intrusion prospects and suspect of security infringements. While there are many definitions of cloud computing, Mell and Grance highlight five essential characteristics [5]:

On-demand Service: A user can be provided by oneself with computing abilities such as server time and network storage whenever it is needed without any provider and human interaction.

Wide Network Accessibility: Cloud computing has to be held abilities, which are standardized on the network and can be accessed by different kinds of devices (mobile phones, tablets, laptops, workstations etc.).

Resource Pool: The provider’s computing resources such as a storage area, processing power, network bandwidth and memory must be in a physical or virtualized pool, can be allocated dynamically or according to demand of the end-users and can be served multitenant at the same time. Users do not need to have any authority on the resources and do not know where the resources are.

Rapid Elasticity: Opportunities and abilities have to be provided, unserved and scaled interior or exterior in an elastic way. These services are introduced to end-users generally unlimited and provided as much as the requests.

Regular Service: Among to services, which are provided in cloud computing systems; resource usage can be monitored, controlled, reported; resource usage amounts can be determined and providers can serve these to users transparently.

We propose developed our own cloud services which can be used in homes around the world to control and monitor cloud connected security surveillance systems remotely. Connecting the surveillance systems to the cloud not only reduces the setup and maintenance cost by eliminating the need of dedicated detection system in each household creating a Unified Threat Management (UTM) system.

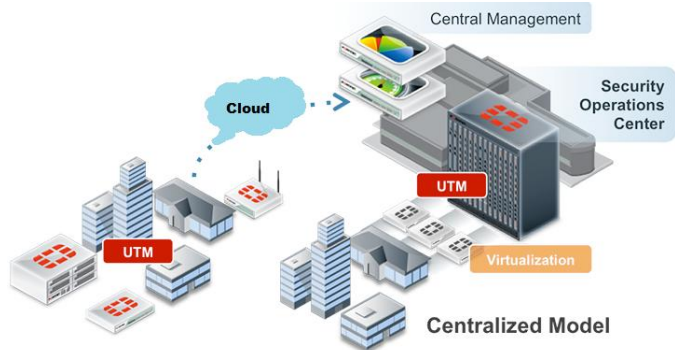


Fig 1. Conceptual diagram of cloud based security surveillance system.

III. HUMAN DETECTION FOR SURVEILLANCE

A. Overview

A standard surveillance system attempts to recognize the regions of interest in a video scene, i.e. the moving entities in the scene. The classification of the moving entity forms a critical part of the system, as the subsequent modules analyze the moving entity based on whether it is a vehicle, a human or a group of humans. Detecting human beings accurately in a visual surveillance system is crucial for diverse application

areas including abnormal event detection, human gait characterization, congestion analysis, person identification, gender classification and fall detection for elderly people. The first step of the detection process is to detect an object which is in motion. Object detection can be performed using background subtraction, optical flow and spatio-temporal filtering techniques. Once detected, a moving object could be classified as a human being using shape-based, texture-based or motion-based features.

B. Algorithm for intelligent image detection

The efficient algorithm is used for image segmentation. The gray scale image has a very low threshold value it is also known as template matching algorithm. It is used in finding small parts of image to match the template image [3]. Large number of sample points can be reduced by reducing the resolution of the search and template image. It uses a mask for specific feature of search image and it is performed by gray image or edge image [3]. Typically, an object pixel is given a value of “1” while a background pixel is given a value of “0”. Finally a binary image is created by coloring each pixel white or black, depending on a pixel’s labels .The gray and binary image are represented in figure 2.The Blob detection is also the technique implemented in this algorithm.

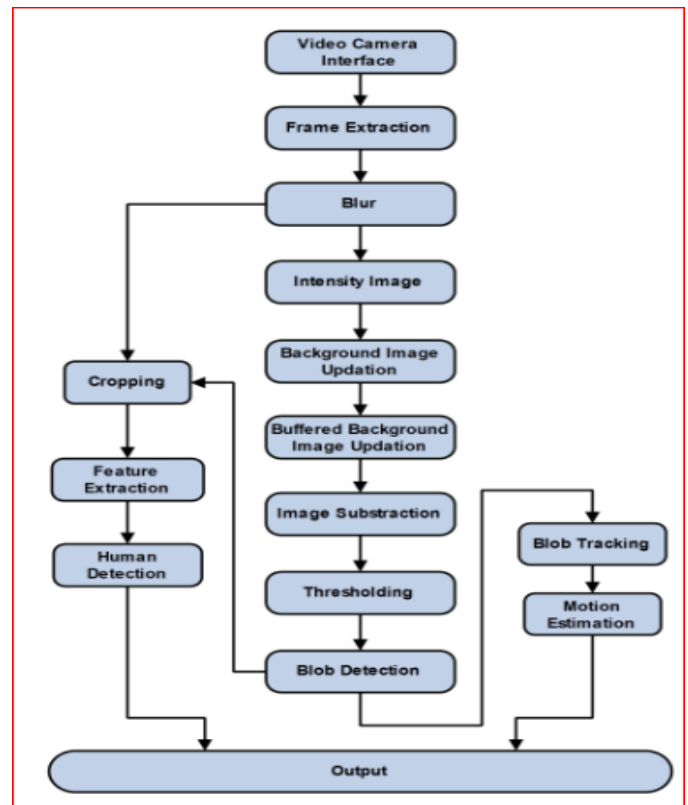


Fig 2. Flow diagram for Image Detection

The system has been designed to detect the motion of the human object in the target area [4]. The background situation detection is also implemented in this algorithm. Under this, the changes in the background such as brightness/contrast change are detected using this [4]. These are the points or facilities covered by this algorithm which differs from normal threshold algorithm. This kind of facilities provided by this algorithm makes the surveillance system human intelligent which would be able to detect all types of the changes and not only random objects in the area. The motive to make the detection system more intelligent is achieved by this algorithm [4].

The motive of precision will also be satisfied with such kind of algorithms. This makes the system efficient and usable in the really critically secured algorithm without manual intervention [4].

IV. IMPLEMENTATION DETAILS

In order to have a cloud based intrusion detection system we need to implement a client server communication. A camera will be interfaced to the client and the surveillance system will be controller from the server side.

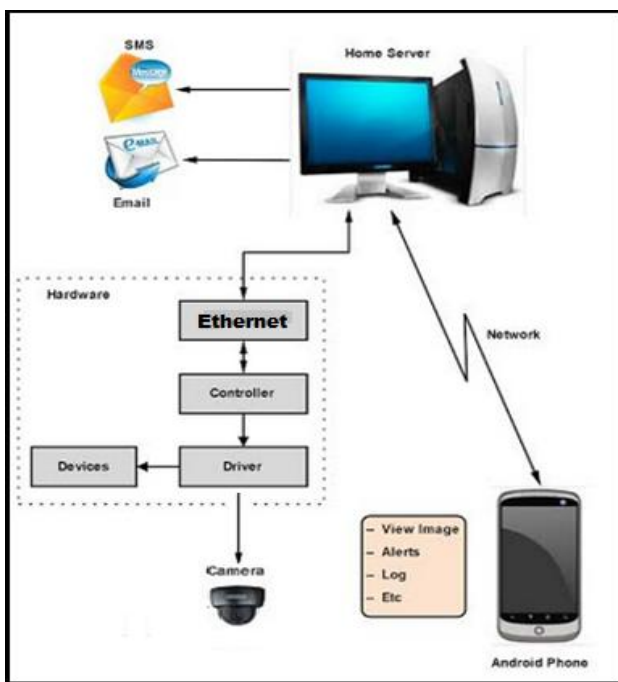


Fig 3. Implementation setup for client server setup

The system consist of two parts

1. The Cloud enabled server
2. Client with camera interface

A. The cloud enabled server

A server will be desktop PC with a standard operation system. The human detection algorithm shall run on the server. The input images will be provided for detection form the clients. The job of the server is to receive data form the client, analyse and send the results back to the client. The client

should be able to handle multiple clients in parallel. The server will be connected in the cloud with multiple clients.

J2SE (Java 2 Standard Edition) Java would be the required as language for development of the project. JDK is the development kit used to compile java programs. The NetBeans are just like visual studio provides development environment for VB and .Net, NetBeans provides an integrated development environment (IDE) for Java.

B. The client with camera interface

The client will be an embedded device with camera interfaced to the system. The role of the client is to capture the images and send it over the cloud to the server. The system should be portable and small in size. The basic requirement of the client will be

1. High resolution Camera interface
2. Ethernet enabled communication
3. High performance processor
4. Small in size and portable
5. Should operate on Linux operation system

The proposed solution for client is the Raspberry Pi. The Raspberry Pi is a credit-card sized computer. The Raspberry Pi is based on the Broadcom BCM2835 system on a chip (SoC) which includes an ARM1176JZF-S 700 MHz processor, 256 megabytes of RAM. It has a 100mbps Ethernet port for cloud interface. While operating at 700 MHz by default, the first generation Raspberry Pi provided a real world performance. The Raspberry Pi primarily uses Linux-kernel-based operating systems. This supports different programming language like C, C++, Python, Socket programming.

V. CONCLUSION

The use of cloud services in security surveillance has many benefits extending from cost reduction to value added services. By using cloud services in home automation and security, we can reduce the cost of surveillance systems, can easily detect any intrusion in house, easily informs to the neighborhood and alerts police. Human Intrusion detection makes the surveillance system more accurate. This paper presents a concept of human detection and cloud based surveillance system which can be adapted in home automation, offices, banks for intrusion detection and burglary prevention.

REFERENCES

[1] Sindhulakshmi.K, Soundarya.J, Sowmya.U "Cloud Controlled Intrusion Detection and Burglary Prevention Stratagems in Home Automation Systems" *Published in International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 2, March 2014*

- [2] Anindya Maiti and S. Sivanesan, School of Computing Science & Engineering, VIT University, Vellore, India “Cloud Controlled Intrusion Detection and Burglary Prevention Stratagems in Home Automation Systems”*Published in Future Internet Communications, April 2012. in International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 2, March 2014*

- [3] Guangming Song, Yaoxin Zhou, Weijuan Zhang and Aiguo Song, “A multi-interface gateway architecture for home automation networks”, *IEEE Transactions on Consumer Electronics, Volume: 54, Issue: 3, August 2008 pp. 1110 – 1113*

- [4] Manoranjan Paul, Shah M E Haque and Subrata Chakraborty”Human detection in surveillance videos and its applications - a review”,*Published in Paul et al. EURASIP Journal on Advances in Signal Processing, 2013*

- [5] Irfan Gul, M. Hussain ”Distributed Cloud Intrusion Detection Model”,*Published in International Journal of Advanced Science and Technology Vol. 34, September, 2011*