Cloud Based intrusion Detection System

Pooja Nandasana, Ritesh Kumar, Pooja Shinde, Akanshu Dhyani, R.S.Parte

JSCOE,Hadapsar, Pune-28 , Dept. of Computer Engg., University Of Pune

Abstract- Today security and safety is just a click of the appropriate technology away, and with such advancements happening, the security of one's home must also not be left behind. Modern advances in electronics and communi-cations technologies have led to the miniaturization and improvement of the performance of computers, sensors and networking. These changes have given rise to the development of several home automation technologies and systems. Surveillance can be defined as monitoring of the behavior, other changing information, activities, observing or analyzing particular area for the purpose of influencing, directing, managing or protecting. A home security system should provide security and safety features for a home by alarming the residents from natural, accidental and/or human dangers such as: fire, flooding, theft, animals invading, etc.

To design a software application for intrusion detection system to identify malicious activities using cloud tech-nology.

Index Terms- intrusion detection,Image Processing,Cloud Computing

I. Introduction

Intrusion Detection System (IDS) is meant to be a software application which monitors the network or system activities and finds if any malicious operations occur. Tremendous growth and usage of internet raises concerns about how to protect and communicate the digital information .Intrusion detection system is a software application which monitors target system for any malicious activity. It inspects the network to find any activity which can be considered to compromise the confidentiality, integrity and security of the system in a safe manner. We mainly introduce the Design of Mobile Video Surveillance Based on Android, the system structure, the streaming media transmission.

1.1 Cloud Computing

Cloud computing refers to the logical computational resources (data, software) accessible via a computer network (through WAN or Internet etc.), rather than from a local computer. Data are stored on Server Farms generally located in the country of the service provider. The on-line service is offered from a cloud provider. Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Cloud computing differs from the classic client-server model by providing applications from a server that are executed and managed by a client's web browser, with no installed client version of an application required. Centralization gives cloud service providers complete control over the versions of the browser-based applications provided to clients, which removes the need for version upgrades or license management on individual client computing devices. The phrase "software as a service" (SaaS) is sometimes used to describe application programs offered through cloud computing. A common shorthand for a provided cloud computing service (or even an aggregation of all existing cloud services) is "The Cloud"[1].

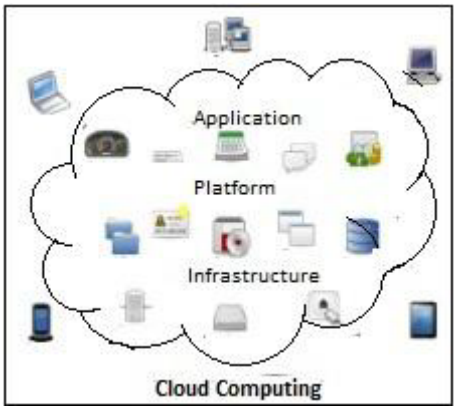


Fig 1 Cloud Computing Logical Diagram

private company, such as their employer. Cloud computing works on a client-server basis, using web browser protocols. The cloud provides server-based applications and all data services to the user, with output displayed on the client device. If the user wishes to create a document using a word processor, for example, the cloud provides a suitable application running on the server which displays work done by the user on the client web browser display. Memory allocated to the client system's web browser is used to make the application data appear on the client system display, but all computations and changes are recorded by the server, and final results including files created or altered are permanently stored on the cloud servers. Performance of the cloud application is dependent upon the network access, speed and reliability as well as the processing speed of the client device.

II. Related Works

In Digital video recorder(DVR) captures videos continuously but it requires some human resource to monitor it which is applicable only in organizations and business areas whereas this will not be suitable for a home environment. If any motion is detected by the camera, it will be sent to the controller. Controller analyses the signal and processes it by using thresholding algorithm [4]. By using LAN connection in the room, it can be transferred to the cloud server and stored in it. To inform the status of the room, the user will be receiving the SMS

alert in his/her mobile. So, user can view the video of the intruder by entering the URL of the server using internet connection anywhere from the world. If an alert is to be given, the alert button on the page can be clicked so that the alarm rings. Alert is also sent to the nearby police station to protect the house.

2.Literature Survey

No	Name	Year	Advantages	Disadvantages
1	Design of Mobile Video Surveillance Based on Android	2012	It Support iPhone , Android Phone And Windows Phone	High Cost
2	A Domestic Robot for Security Systems by Video Surveillance Using Zigbee Technology	2013	low cost high throughput low latency.	short range low Complexity High Power Consumption

III. IDENTIFIED PROBLEM

- Interface between hardware
- Saving live video on the cloud
- Extracting frame from the video
- To convert extracted frames into binary images
- Matching that binary image with my constant image
- Sending that image to device through mail service
- Live streaming from cloud

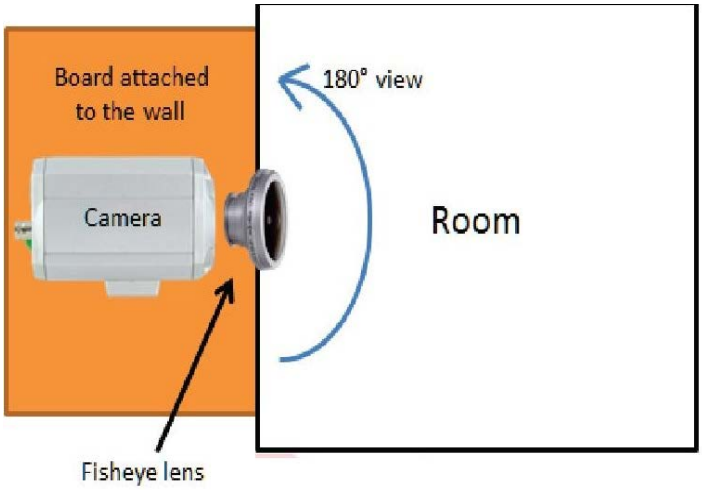


Fig. Camera Connect in Wall

IV. MERITS AND DEMERITS

Merits:

- Provides better security
- Allows fast recognition of the moment abandonment to determine whether a threat exists.

Demerits:

- Interface between hardware

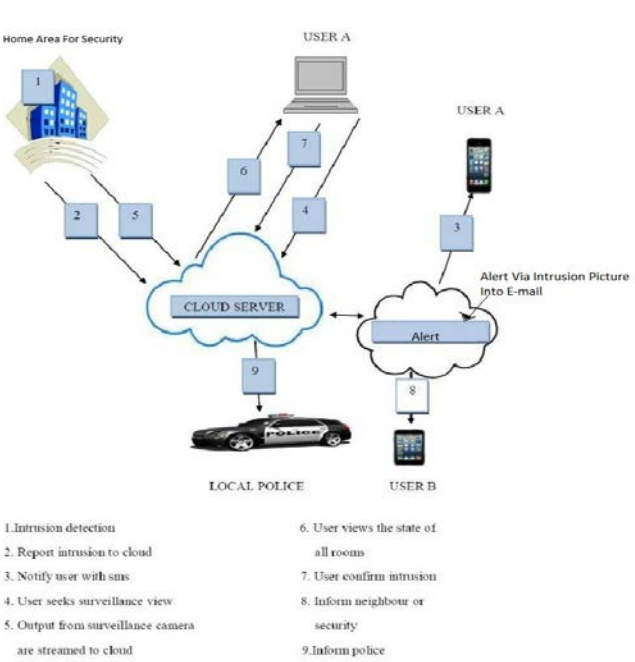
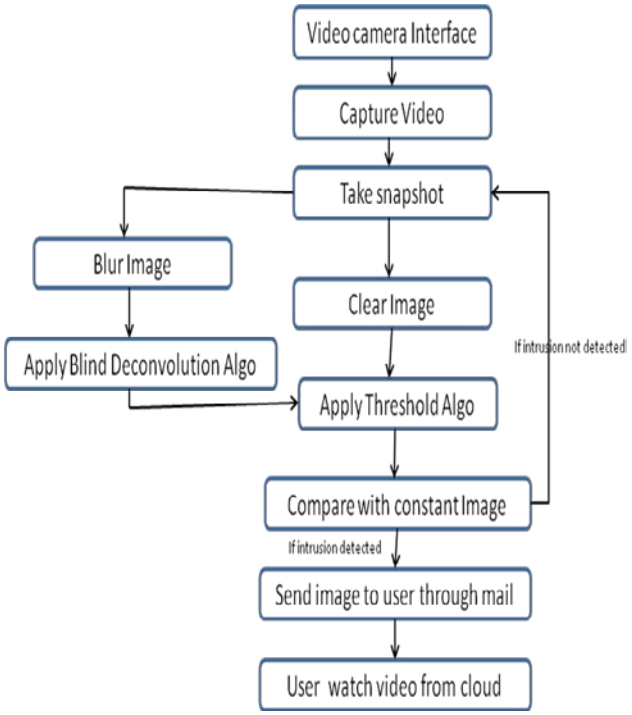


fig. Basic Infrastructure Of Intrusion System

5. Flow Chart :-



V. System Features

- Intrusion Prevention Systems (IPS) are simply described as network threat detection systems acting as a security guard for your IT environment.
- Intrusion prevention systems are designed to proactively block incoming threats whereas an IDS or Intrusion Detection System is more reactive in nature.
- Many of the features of IPS and IDS systems are today integrated into firewalls and network protection devices

VI. Acknowledgment

We are grateful to a number of individuals whose professional and personal encouragement and assistance have made the entire duration of the project a pleasant endeavour We would like to express our gratitude and appreciation to our guide Prof. R. S. Parte madam for giving us proper guidance and directing us to achieve the goal.

VII. Conclusion

- Proposed an innovative periodic concept based framework that enables multifunctional unattended objects in a human surveillance system for consumer use.
- System can also be applied for detecting special events such as recording a burglary, robbery or monitoring school zone safety problems, for school children, thereby contributing to the safety of people in the home and schools.
- The occlusion problem is also thoroughly tackled and successfully dealt with various aspects.

VIII. Feature Scope

- To provide security
- To detect any malicious activity before loss to confidential data
- To detect criminals before any crime
- To detect criminals before any crime

References

[1] E. Brown, "NIST issues cloud computing guidelines for managing security and privacy," National Institute of Standards and Technology Special Publication 800-144, January 2012. View at Google Scholar

[2] P. M. a. T. Grance, Effectively and Securely Using the Cloud Computing Paradigm (V0. 25), US National Institute of Standards and Technology, 2009.

Authors

First Author – Pooja Nandasana, JSCOE,Hadapsar, Pune-28 , Dept. of Computer Engg., University Of Pune, 7709869639, poojanandasana76@gmail.con
Second Author – Ritesh Kumar, JSCOE,Hadapsar, Pune-28 , Dept. of Computer Engg., University Of Pune, bpsdude@gmail.com
Third Author – Pooja Shinde, JSCOE,Hadapsar, Pune-28 , Dept. of Computer Engg., University Of Pune, shindepooja79@gmail.com
Fourth Author – Akanshu Dhyani, JSCOE,Hadapsar, Pune-28 , Dept. of Computer Engg., University Of Pune, akanshu.dhyani@gmail.com
Fifth Author – R.S.Parte, JSCOE,Hadapsar, Pune-28 , Dept. of Computer Engg., University Of Pune