Smart Surveillance Monitoring System

Akshat Jain[#]
akshatjain95@gmail.com

Shraddha Basantwani[#]
basantwanishraddha@gmail.com

Owais Kazi[#]
owaiskazi19@gmail.com

Yogita Bang[#]
yogitabang24@gmail.com

[#]Computer Engineering Department
Pune Institute of Computer Technology
Pune, India

***Abstract*- In today's world, where everyone wants to keep their valuables safe and secure, video surveillance for observing a particular area has become the need of the hour. To address this problem, we have come up with a solution of smart surveillance system for certain places like bank vaults, homes where the human presence is not available. At such places, it is not worth to continuously monitor the area with the cameras. This wastes the power consumption as well as the storage required for the footages. Our system will detect human presence using PIR sensor. Raspberry Pi operates and controls motion detecting sensors and video cameras for remote sensing and surveillance, streams live video and records it for future playback. On detection of any movement the cameras will trigger the surveillance. The proposed system captures information and transmits it via Internet to smartphones and laptops. Live streaming is done throughout the WAN i.e. also available within different LANs. Extensive human monitoring of the incoming video channels is impractical, expensive and ineffective. Using a universal sample-based background subtraction algorithm called ViBe (Visual Background Extractor), we detect motion in red alert zone i.e. a place in the room where the valuables are placed, for any suspicious activity and we send an alarm to the user. The video recorded and stored can be used to identify the intruder and help in catching him. To preserve privacy and securely transmit the video footage over the network, we are using blowfish encryption and decryption algorithm to provide extra security from hackers.**

Keywords: Surveillance, IoT, Streaming, Security, Background Subtraction Algorithm, Encryption, Decryption, Blowfish Algorithm.

I. INTRODUCTION

In today's fast paced world, it has become difficult to monitor our workplaces and homes for security. Thus, there is an increased need for camera surveillance systems. By using these systems, it is possible to continuously monitor the workplaces and homes for security purposes and store it for future references. But the main drawback of these system are- manual monitoring, huge storage requirements and extensive power consumption.

To overcome these problems, we have come up with an automated smart surveillance system. For this system, we are using Raspberry Pi with Passive Infrared (PIR) Sensor for motion detection and a remote camera for video recording.

The camera is connected to Raspberry Pi via the USB port and the PIR Sensor is connected through General Purpose Input Output (GPIO) pins of the Raspberry Pi. Motion is detected using PIR sensor which turns on the camera for surveillance. The duration for recording can be set according to the user convenience. While the video is being recorded, using image processing we are diagnosing a particular area termed as red-alert zone for any suspicious activity. The whole recording is sent to the server in an encrypted form. If any suspicious activity happens in the red-alert zone, then a special signal is sent to the user.

II. MOTIVATION

Current camera surveillance systems can be used for monitoring but they require a huge amount of data storage due to continuous video recording. However, our system only monitors the area when motion is detected and there is a possibility of certain activity. Our system also sends a notification, in case of suspicious activity as it is not possible to continuously keep a watch on such activities.

III. COMPONENTS

1. Raspberry Pi 2:

It is a credit card sized single board computer. It supports Debian based Linux distribution which helps in Open-Source development. It consists of 900MHz quad-core ARM Cortex-A7 CPU with 1GB RAM. It has 40 GPIO pins, HDMI portand Ethernet port for networking. It also comes with a camera and display interface, audio video jack, MicroSD card slot and 3D graphics core. Thus, it supports full-fledged low-level computing for general purpose as well as embedded systems [2]. Refer Figure 1.

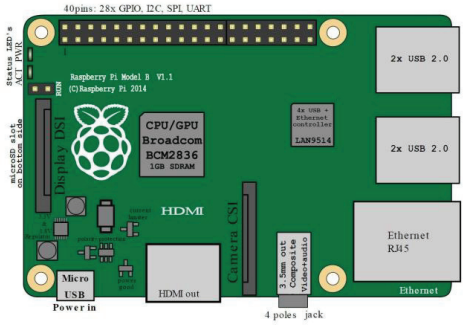

Figure 1. Raspberry Pi

2. PIR Sensor:

It is used for motion detection. It uses an electronic circuit that measures infrared light radiating from the objects in its field of view. It can sense motion within an adjustable sensing range of 7m and 110˚ sensing angle. Its adjustable delay time ranges from 5 to 300 seconds[3][4]. Refer Figure 2.

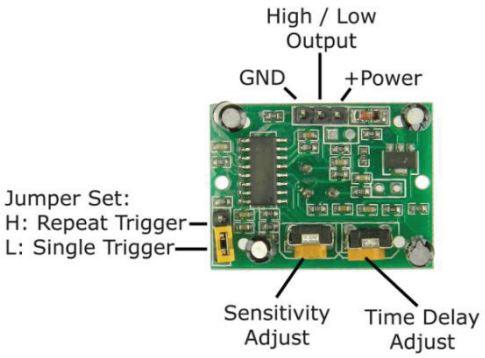

Figure 2. PIR Sensor

IV. SYSTEM ARCHITECTURE

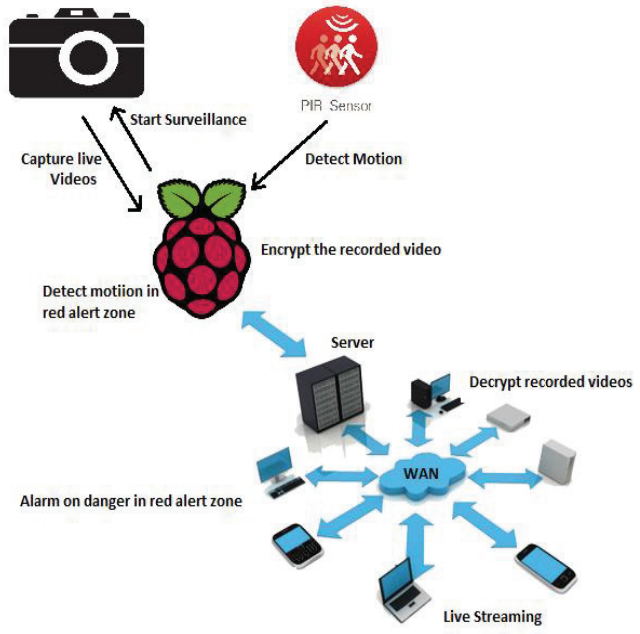

Figure 3. Architecture of Surveillance System

Figure 3 depicts the system architecture, where the camera and PIR sensor are connected to Raspberry Pi, which in turn is connected to the server. This server helps in viewing the live streaming of the video over a WAN of inter-connected devices.

V. IMPLEMENTATION

The working of surveillance system is divided into four units.

1. Streamer
2. Image Processing
3. Secured data transmission
4. Routing

1. Streamer

The system works independently without much human intervention. Raspberry Pi acts as a standalone machine which controls the PIR sensor and the camera. The PIR Sensor was connected to the GPIO pins of the Raspberry Pi and the camera through the USB port. The Raspberry Pi is connected to the server using the Ethernet port.

The PIR Sensor on movement, merely detects the change in the amount of radiated heat that reaches two parallel elements inside the sensor. This triggers, the output of sensor to be HIGH using GPIO pins which in turn, starts the camera for surveillance[1].

2. Image Processing

To gain attention of users in case of suspicious activities we monitor the surveillance using image processing. User need to specify 'Red alert zone' i.e. the area that needs special security. Whenever motion is detected in this zone user is notified to pay attention to surveillance or check the place itself. To achieve this, we use foreground detection. Foreground detection divides the observed image into two complementary setsof pixels that cover the entire image:

a. The foreground that contains the objects of interest.
b. The background, itscomplementary set.

Background Subtraction:

We detail below a background subtraction technique, called "ViBe" (for "Visual Background Extractor"). It works in 3 stages described further.

A. Pixel model and classification process:

In this stage each pixel is evaluated. If a pixel is found to be the same in 3 or more time than it is termed as background.

B. Updating the background model over time:

We believe that it is moreappropriate to ensure a monotonic decay of the probability of a sample value to remain inside the set of samples. A pixelmodel should contain samples from the recent past of the pixelbut older samples should not necessarily be discarded.

C. Spatial consistency through background samples propagation:

We consider that neighbouring background pixels share a similar temporal distribution and that a new background sample of a pixel should also update the models of neighbouring pixels. According to this policy, background models hidden by the foreground will be updated with background samples from neighbouring pixel locations from time to time.

3. Secured data transmission

To preserve privacy and securely transmit the video footage to the server, the recorded video is encrypted using the Blowfish Algorithm. Blowfish Algorithm is a symmetric key cryptographic algorithm. Refer Figure 4.

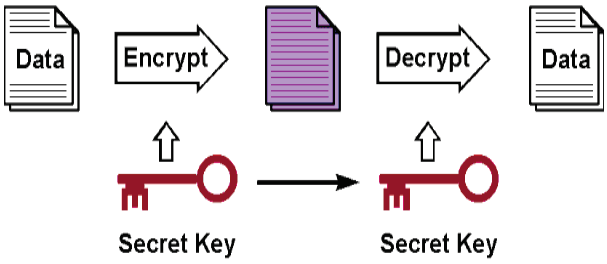

Figure 4. Private Key Encryption

It is a block cipher technique which uses a variable key length (32-448 bit) which makes it difficult for the attacker to determine the key. Also the number of rounds in the encryption process are only 16 which makes the algorithm faster. This algorithm uses only 'ADD' and 'EXOR' operations which adds to the speed of the algorithm. On comparing various private key cryptographic algorithms[5], we came to a conclusion that Blowfish algorithm is the fastest and the most secure algorithm. Ashwak Alabaichi et al in "Security Analysis of Blowfish Algorithm"[6]described Blowfish Algorithm. It uses a Fiestel Network also called as F-function. Fiestel network is a general method of transforming any function into a permutation.

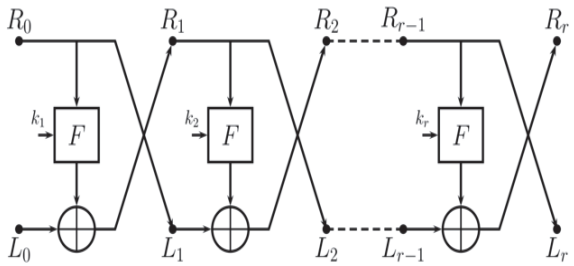

Figure 5. Fiestel Network

Blowfish Encryption Algorithm

Blowfish algorithm is mainly divided into two parts viz., Key expansion/sub key generation and Data encryption.

A. Key expansion/sub key generation:

Blowfish uses a large number of sub keys. These keys must be pre-computed and stored before any data encryption or decryption. It has two components:

1) The P-array consisting of eighteen 32-bit sub keys: P_1,P_2,....,P_{18}.
2) Four 32-bit S-boxes with 256 entries each:
   $S_{1,0}$, $S_{1,1}$, ... , $S_{1,255}$
   $S_{2,0}$, $S_{2,1}$, ... , $S_{2,255}$
   $S_{3,0}$, $S_{3,1}$, ... , $S_{3,255}$
   $S_{4,0}$, $S_{4,1}$, ... , $S_{4,255}$

The P-array and the S-boxes are initialized with a fixed string. These components are then XORed with 32 bits of the key. If A is a short key then A,AA,AAA,etc. are equivalent keys. Use the Fiestel network to generate the modified sub keys. Refer Figure 5.

In total 521 iterations are required to generate all required sub keys. Thus these sub keys must be stored by the applications rather than evaluating it multiple times.

B. Data Encryption:

The input is a 64-bit data element X.
Divide X into two 32-bit halves: XL and XR.
Repeat 16 times:
    XL = XL XOR P[i]
    XR = F(XL) XOR XR
    Swap XL and XR
Swap XL and XR to undo the last swap
XR = XR XOR P[17]
XL = XL XOR P[18]
The final encrypted data is (XL,XR)

F(XL) = ((S0 + S1 mod 2^32) XOR S2) + S4 mod 2^32

Blowfish Decryption Algorithm

Decryption in blowfish algorithm is similar to encryption algorithm, step by step in the same order only with the sub keys applied in reverse order.

4. Routing

Although smart surveillance monitor system is already developed but none of them included routing to transfer the video data from source router to client[8]. Here other routers will also be present, so routing will be used to avoid leaking of data and thus providing security. In this system, the network in which the Raspberry Pi is connected is LAN to WAN connection with DHCP turned off. This is done so that the Raspberry Pi does not connect to other router in the network. By using "tracepath" system call we are finding the shortest path from source router to client router. This will avoid attacks from intruders if any. Refer Figure 6.

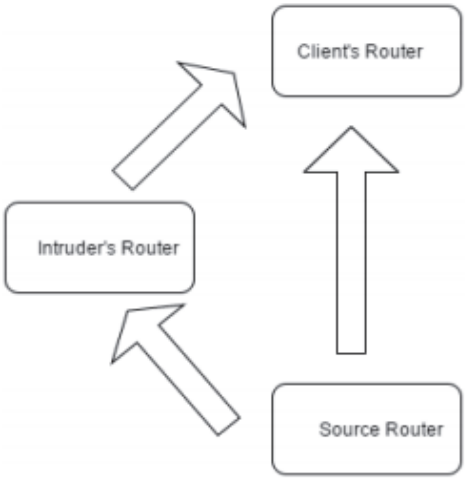

Figure 6. Connection within different LANs

We implemented routing using three routers to generate a WAN to LAN connection which was used to send the data from source router to client router avoiding the access from intruder with the help of shortest path algorithm.

VI. RESULTS

Figure 7. Output of Script to start video streaming

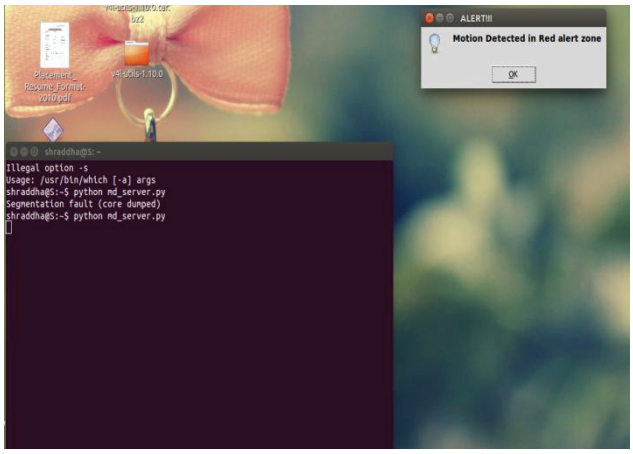

Figure 8. Alarm with pop-up when motion is detected in Red alert zone

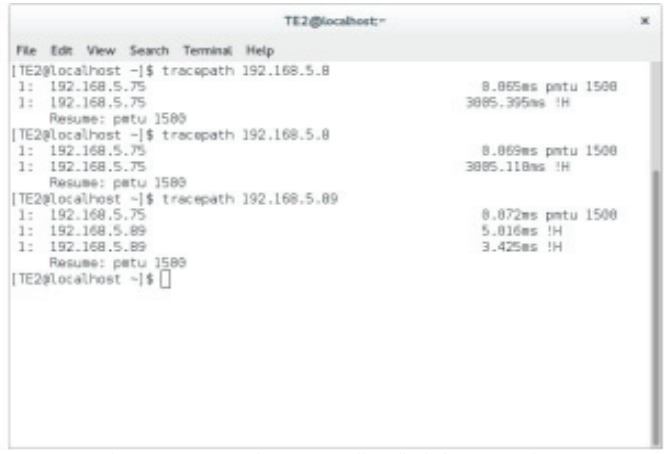

Figure 9. Tracepath system call to find shortest path

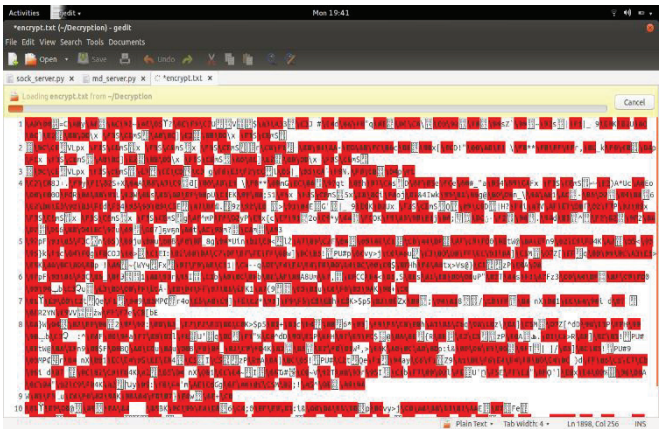

Figure 10. Video Encrypted through Blowfish Algorithm

VII. CONCLUSION

In this paper, we developed a Smart Monitoring System which smartly monitors the workplaces and homes with least human interference. Here, the Streamer on motion detection starts the video streaming and stores it for future playback. On commencement of streaming, the red alert zone is checked for suspicious activity using Image Processing. The stored video is encrypted using Blowfish Algorithm, to be transmitted securely over the network. The system senses for an intruder router and sends the encrypted data to the client without any leakage using Shortest Path Algorithm.

By using this system, manual monitoring and power consumption is reduced as well as cyber security is enhanced.

VIII. FUTURE WORK

The whole system can be made standalone by connecting PIR sensor to the camera and by providing wireless network access to Raspberry Pi.

Also, Face detection can be used in the red alert zone for known and unknown faces.

We can also improve security by using a combination of Blowfish and RC6 algorithm which is fast and more difficult to attack as described by Nusrat Jahan Oishi et al in Hybrid Algorithm of Blowfish and RC6[7].

REFERENCES

[1] Gu, Yi, et al. "Design and Implementation of UPnP-Based Surveillance Camera System for Home Security." Information Science and Applications (ICISA), 2013 International Conference on. IEEE, 2013

[2] https://www.raspberrypi.org/products/raspberry-pi-2-model-b/

[3] http://www.robotoid.com/appnotes/sensors-passive-infared.html

[4] https://www.mpja.com/download/31227sc.pdf

[5] Rajdeep Bhanot and Rahul Hans "A Review and Comparative Analysis of Various Encryption Algorithms" International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306

[6] Ashwak Alabaichi et al "Security Analysis of Blowfish algorithm" ISBN: 978-1-4673-5256-7/13/$31.00 ©2013 IEEE

[7] Nusrat Jahan Oishi et al "Short Paper: Enhancing Wi-Fi Security Using a Hybrid Algorithm of Blowfish and RC6" 978-1-5090-0203-0/16/$31.00 ©2016 IEEE

[8] Sumitha J "Routing Algorithms in Networks" Research Journal of Recent Sciences ISSN 2277-2502 Vol. 3(ISC-2013), 1-3 (2014)