International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT206496

Anomaly Detection in Banking Using A Video Surveillance System

Saravanan S
Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India

Article Info
Volume 6, Issue 4
Page Number: 1-10
Publication Issue :
July-August-2020

Article History
Accepted : 20 Aug 2020
Published : 27 Aug 2020

ABSTRACT

An anomaly detection scheme is proposed for encrypted video bitstream with secure video encryption. Human beings are recognized by their unique facial characteristics. In the present work time based movement and face recognition approach will be implement to detect person in unwanted time.In video sharing , ROI (Region of Interest) extraction can be implement to detect the region to hide. An efficient encryption technique is used to encrypt the extracted region.

Keywords : Antivirus and antimalware software, Behavioral analytics, Email security, Firewalls, Network segmentation, Security information and event management, Web security, Wireless security.

I. INTRODUCTION

NETWORK SECURITY

Network security contains policies and practices adopted to hinder and screen unauthorized entry, misuse, modification, or denial of a pc community and community-accessible assets. Network security involves the authorization of access to information in a network, which is managed with the aid of the community administrator. Customers decide upon or are assigned an identification and password or other authenticating information that allows for them access to expertise and packages within their authority. Community safety covers a type of pc networks, each public and personal, which can be used in day-to-day jobs; conducting transactions and communications amongst organizations, government organizations and participants. Networks can be personal, equivalent to inside a enterprise, and others which might be open to public access. Network security is concerned in corporations, organizations and other forms of associations. It does as its title explains: It secures the community, as good as defending and overseeing operations being achieved. Probably the most fashioned and easy means of defending a community resource is by means of assigning it a precise title and a corresponding password.

Network security starts with authenticating, usually with a username and a password. Due to the fact that this requires just one element authenticating the person title i.e., the password this is generally termed one-element authentication. With two-factor authentication, anything the consumer 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile) and with three-component

authentication, whatever the user 'is' can be used (e.g., a fingerprint or retinal scan).

As soon as authenticated, a firewall enforces entry policies similar to what services are allowed to be accessed by way of the network customers. Though effective to prevent unauthorized access, this component may just fail to investigate probably harmful content material reminiscent of computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps observe and inhibit the motion of such malware. An anomaly-founded intrusion detection process may additionally display the network like wire shark traffic and is also logged for audit purposes and for later high-level analysis. Newer methods combining unsupervised laptop finding out with full community traffic analysis can discover lively community attackers from malicious insiders or detailed external attackers which have compromised a person desktop or account. Verbal exchange between two hosts making use of a community may be encrypted to maintain privateness.

Honeypot, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, because the honeypot will not be most often accessed for respectable functions. Techniques utilized by the attackers that attempt to compromise these decoy resources are studied for the duration of and after an assault to preserve a watch on new exploitation strategies. Such analysis may be used to additional tighten protection of the genuine community being protected via the honeypot. A honeypot may also direct an attacker's concentration far from authentic servers. A honeypot encourages attackers to spend their time and vigor on the decoy server while distracting their concentration from the info on the actual server. Much like a honeypot, a honeynet is a community established with intentional vulnerabilities. Its intent can also be to ask assaults so that the attacker's approaches will also be studied and that know-how can be utilized to broaden community protection. A honeynet mostly includes a number of honeypot.

TYPES OF ATTACKS

Networks are field to attacks from malicious sources. Attacks will also be from two classes: "Passive" when a network intruder intercepts data travelling via the network, and "active" where an outsider initiates commands to disrupt the network's usual operation or to behavior reconnaissance and lateral action to seek out and achieve access to belongings available through the network.

The security threat to the network can be the attacker who attempts to grasp information to exploit the network vulnerability. This kind of attack is also known as passive attack. On the other hand, the attacker is attempting to disrupt the network communication and also affect the user productivity of a network. It is also known as an active attack. Here listed below are some of the most common types of the security threats.

DoS

The DOS-denial of service attack overwhelms the network host with the stream of bogus data which keep it to process the designed data. The DoS attacks will be launched against the computers and against the network devices. The DoS attack is the security threat which implies that the larger attacks are in progress. Then the DoS attack is a part of the attack that the hijacks communication from the user who already authenticated to the resource. When the users computers are blocked by a DoS attack, then the attacker access the resource and receive the needed information and returns the control to a user who does not know what occurred in it.

DDoS

The distributed denial of service is the attack occurs when the multiple system is used to flood the resources or bandwidth of a group of servers or one server. The main purpose of this attack is to saturate a resource so that it is not available longer for the legitimate use. It is used as the decoy to hide more malicious attack which attempts to steal sensitive information or other data.

Man in the middle

The man in the middle attack occurs when the person keep a logical connection or equipment between two communicating parties. These two communicating parties assume they are directly communicating with each other, but the information is being sent to a man in the middle who forwards it to the proposed recipient. This attack is very harmful to the organizations. Most of the organizations will adopt measures such as strong authentication as well as latest protocols, including IPSec/L2TP with the tunnel endpoint authentications.

Social engineering

A social engineering attacks are not relying on technology or protocols to succeed, but instead it relies on the human nature. Users generally trust each other and where the this type of attacks start. It may comprise of false sites that ask for the information from the unsuspecting web surfers. And this type of attack is known as phishing. A social engineering attacks might be prevented by just training the users not to provide their credentials who asks for the information on the web page.

Virus

The computer virus is the program which can infect the computer and copy itself without user knowledge. These viruses started infecting the computers in 1980 itself and also continued to evolve till date. Some of the viruses are able to change after it infects the computers to try to hide from the antivirus software. As the viruses changed over the years and years, companies like McAfee and Symantec have specialized in the software, which can eradicate and detect viruses from the computer system. There are nearly more than 76,000 known viruses and users can eradicate it by updating the antivirus software up to date on all the clients and servers.

Worms

The worm is the something different from the viruses, it is just a program and just not an infestation. These worms will use a computer network to send worm copies to the other computers without the user's knowledge. They are proposed to cause network problem such as resource utilization and bandwidth issues. The most famous worms such as sobig and mydoom worms have affected more thousands of servers and computers in the past. You can prevent the spread by maintaining the servers and clients up to date with latest security patches.

Buffer overflow

The buffer overflow is the attack created anomaly by the rogue program when writing data to the buffer intentionally overwrite the buffer memories and the adjacent memory. It may result in memory errors and erratic behavior and a crash or breach of the system security. Make use of the products like ProPolice and Stackguard to prevent the buffer overflow attack from succeeding.

Packet sniffing

The attacker can use the protocol analyzer to launch the attack by the packet sniffing. This is the process in which an attacker gathers the data sample with a software or hardware device which allows data inspection at a packet level. The attacker may see the IP addresses, unencrypted passwords, sensitive data and MAC addresses. After a vulnerability is discovered, the attacker will begin an active attack. The perfect method to prevent this attack is to forbid

anything except the trusted network administrators from placing the packet analyzer on a network. Most of the packet analyzers can identify the presence of the packet analyzer, unless an attacker uses software to make the attack invisible.

II. TYPES OF NETWORK SECURITY

Access control

Now not every consumer will have to have access network. To maintain out expertise attackers, you have got to appreciate each and every user and each gadget. Then that you would be able to put into effect protection policies. That you could block noncompliant endpoint devices or give them only limited entry. This process is network entry manipulate (NAC).

Antivirus and antimalware software

"Malware," quick for "malicious program," involves viruses, worms, Trojans, ransomware and spyware. Commonly malware will infect a community but lie dormant for days and even weeks. The satisfactory antimalware packages now not only scan for malware upon entry, but additionally continuously track files later on to seek out anomalies, put off malware, and fix harm.

Application security

Any software you use to run corporation desires to be covered, whether or not IT staff builds it or whether or not you purchase it. Lamentably, any software may just include holes, or vulnerabilities, these attackers can use to infiltrate community. Utility protection encompasses the hardware, application, and procedures you employ to shut those holes.

Behavioral analytics

To discover irregular network conduct, you must understand what average behavior appears like. Behavioral analytics instruments mechanically determine events that deviate from the norm. Security group can then higher identify symptoms of compromise that pose a talents crisis and rapidly remediate threats.

Email security

Electronic mail gateways are the number one danger vector for a security breach. Attackers use private understanding and social engineering methods to build subtle phishing campaigns to deceive recipients and ship them to websites serving up malware. An e mail safety application blocks incoming assaults and controls outbound messages to avoid the lack of touchy data.

Firewalls

Firewalls put up a barrier between relied on interior community and untrusted external networks, such as the internet. They use a collection of defined ideas to allow or block visitors. A firewall can be hardware, software, or both. Cisco presents unified hazard management (UTM) devices and risk-focused subsequent-iteration firewalls.

Intrusion prevention systems

An intrusion prevention procedure (IPS) scans network site visitors to actively block assaults. Cisco next-generation IPS (NGIPS) appliances do this by correlating large amounts of global risk intelligence to not only block malicious activity but additionally monitor the progression of suspect records and malware across the community to avert the spread of outbreaks and reinjection.

Mobile device security

Cybercriminals are increasingly focusing on mobile instruments and apps. Within the following three years, 90 percent of IT organizations may just help company purposes on private cellular instruments. Of path, you need to manipulate which gadgets can access ythis community. You are going to

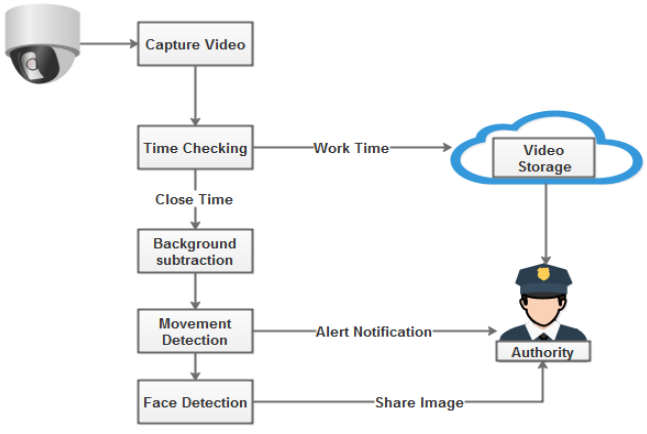
additionally must configure their connections to hold community visitors exclusive.

Network segmentation

Application-outlined segmentation puts network visitors into different classifications and makes enforcing security policies less difficult. Ideally, the classifications are headquartered on endpoint identification, now not mere IP addresses. Which you could assign access rights situated on role, place, and

III. Related Work

Software architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes. A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability. Software architecture must describe its group of components, their connections, interactions among them and deployment configuration of all components.



System Architecture

IV. EXISTING METHODOLOGY

The etraction of abnormal information from format-compliant encrypted bitstreams used for detection abnormal activity. In this scheme, we use three types of estimated values obtained from the bitstream structure and codeword structure, i.e., the data size of the macroblock (in bits), the macroblock (MB) partition mode, and the magnitude of motion vector difference (MVD).

Proposed methodology

Proposed system focuses on implementing a Smart Camera which monitors the activity in the banks, it can detect any sort of suspicious behavior, and the thieves would be tracked on the basis of motion and the time based face detection. If any such suspicious face is detected in unwanted time, the Smart Camera will automatically send an alert message to the security department.

The message mentions what type of alert is generated; it also contains the image sharing when the face was detected with a web link where the live image is stored, so that the security can come with appropriate preparation.

The typical Gaussian mixture model takes a strategy as follows: For each pixel in new image, if the pixel is well described by any of the K Gaussian distributions, we update the background model by the learning rate, otherwise we replace the least probable distribution with a new distribution with the current value as its mean value, an initially high variance and low priority weight. The Gaussian mixture model is an on-line learning method; it can adjust the background model according to the environment around, such as lighting changes. A Gaussian Mixture Model is a parametric probability density function which is a weighted sum of Gaussian component

densities. A Gaussian Mixture Model is used for modeling of the background is because it is one of the greatest model for background modeling. It models all different type of pixels. Anomaly detection which estimates the large cluster pixels value difference from the captured video. When anomaly analyzer estimates the large cluster pixel image then a mask is headed on that pixels and consequently the moving object is detected.

V. METHODOLOGY

Video encoding frameworks usually adopt prediction and compensation for compression. Most of the background and the normal contents are predicted accurately, resulting in MBs with a small size (a few bits). Compared to normal motion, anomalous motion requires more bits in the video bitstream because it is "unexpected" and usually implies rapid motion. The anomaly regions are brighter than the normal regions, which means that an anomaly uses a larger number of bits within the bitstream.

1. Video Capturing Framework
2. Set Time based Storage
3. Movement Detection
4. Face Identification
5. Send Alert Intimation

Video Capturing Framework

In this module propose a Surveillance Camera based theft detection along with tracking of thieves. Here use image processing to detect theft and motion of thieves in Surveillance Camera footage, without the use of sensors. This system concentrates on object detection. The security personnel can be notified about the suspicious individual committing burglary using Real-time analysis of the movement of any human from Surveillance Camera footage and thus gives a chance to avert the same.

Set Time based Storage

Before capturing the activities by camera, Admin should set the time for predicting abnormal activities based on unwanted time period. This module takes input from the Human Detection by surveillance camera. When the human enters into the system it checks the timer to measure the time. When the predefined time limit for human detection is reached, the system sends the alert mail to the admin.

Movement Detection

Motion Behavior of the human is analyzed in front of the system. If the system found any movement in the picture, the system without human intervention takes the snap of the detected image and executes the alarm according to the user settings. The first step is by acquiring video images from CCTV. Those images will be used for motion detection process. If a motion is detected, the information of time stamp and images with detected motion will be stored. The captured time value should check with database to predict normal or abnormal activity. The motion value will be compared to time threshold.

Face Identification

Input is in the form of real time video capturing. Video images are splited into still images. Face detection is done in the process. Facial features matching with database using grassman learning algorithm. The temporal information in video sequences enables the analysis of facial dynamic changes and its application as a biometric identifier for person recognition. There are different ways to form the feature vector for training the classifier. Some of them even use whole image as a feature vector and perform classification which needs high computation. So here feature vector is made from important values of the image from each filter Energy, mean and standard deviation forming a 40 value feature vector for every image. We have utilize the human nature that human will have at least small amount of movements such as eyes blinking and/or

mouth and face boundary movements. We can get this information easily because dealing with video sequence by which the whole sequence of the object's movements can be obtained. Taking that point in to account we can reduce the error that occurs due to false detection of a human face and minimize the time of simulation.

Send Alert Intimation

In a surveillance environment, the automatic detection of abnormal activities can be used to alert the related authority of potential criminal or dangerous behaviors, such as automatic . In proposed system unknown event alert send to the predefined contact numbers regarding particular officers. Here also implement image sharing for easy identification of criminals.

ABNORMAL MOTION INFORMATION ESTIMATION

FROM ENCRYPTED VIDEO BITSTREAMS

We consider the extraction of abnormal information from encrypted bitstreams using the format-compliant video encryption.In our scheme, we use three types of estimated values obtained from the bitstream structure and codeword structure,i.e., the data size of the macroblock (in bits), the macroblock (MB) partition mode, and the magnitude of motion vector difference (MVD).

Anomaly Detection at the Frame Level

Feature Extraction: In frame-level detection, we firstextract the MB data size, the partition level, and the MVDmagnitude at the frame level.Suppose that sij is the MB data size of MBj in the i-thframe, and si = fsi0; si1; : : :g denotes the set of sij . We useJi to denote the set of all MB addresses in the i-th frame. Ineach frame, we obtain the frame data size by computing theenergy of si as

E(si) = ksik1 =Xj2Ji sij , _s;i;

where j is the MB address, and E(_) and k _ k1 are the energyoperator and `1 norm operator, respectively. weshow an example of f_s;ign i=1 in a sequence, from which we can see that the value of _s;i is volatile due to the I-frames.To eliminate the negative effect of the I-frames, we perform median filtering on the frame data size sequence f_s;igni =1. Letus denote the frame rate of the video as _, which represents thenumber of frames displayed per second. We use _5 frames asthe size of the median filter window. After performing median filtering, we obtain the new frame data sizes from the filtered sequence. For convenience, we use _s;i to denote the newframe data size. We present the values of _s;i after we can see that noise has less influence and the curve is much smoother.For the MB partition information, we use different partitionlevels to identify different partition modes. Suppose that lij is
the partition level of MBj in the i-th frame, and li is definedas fli0; li1; : : :g in the i-th frame. Similarly, we can obtain thepartition level of each frame as

E(li) = klik1 =Xj2Jilij , _l ;i:

Detection Rate

The proposed frame-level method directly addresses video bitstream data without full decoding and decryption in the detection phase. Thus, the proposed frame-level method can achieve high efficiency compared to other video processing techniques, e.g., motion detection in the encrypted domain In terms of the detection algorithm itself, the detection rate of our frame-level method is approximately 200 frames per second for 640 _ 480 videos. For the same videos, the detection rates of [23], [24] are approximately 70 frames per second and 50 frames per second, respectively.Therefore, our scheme is more than 2 times faster than the other schemes

VI. CONCLUSION

Proposed system focuses on implementing a Smart Camera based anomaly detection which monitors the

activity in the banks, it can detect any sort of suspicious behavior, and the thieves would be tracked on the basis of motion and the face detection approach based on unwanted time period. If any such suspicious action is detected at unwanted time, the Smart Camera will automatically send an alert message to the security department. The message mentions what type of alert is generated; it also contains the face image of the thief and time detected with a web link where the live image is stored, so that the security can come with appropriate preparation.

VII. REFERENCES

[1]. Guo, Jianting, Peijia Zheng, and Jiwu Huang.(2017). "An efficient motion detection and tracking scheme for encrypted surveillance videos"- ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 13, no. 4 (2017): 61.

[2]. Sabokrou, Mohammad, Masoud Pourreza, Mohsen Fayyaz, Rahim Entezari, Mahmood Fathy, Jürgen Gall, and Ehsan Adeli (2018). "AVID: adversarial visual irregularity detection"- In Asian Conference on Computer Vision, pp. 488-505. Springer, Cham, 2018.

[3]. Sabokrou, Mohammad, Mohsen Fayyaz, Mahmood Fathy, Zahra Moayed, and Reinhard Klette (2018). "Deep-anomaly: Fully convolutional neural network for fast anomaly detection in crowded scenes"- Computer Vision and Image Understanding 172 (2018): 88-97.

[4]. Li, Huang, Yihao Zhang, Ming Yang, Yangyang Men, and Hongyang Chao (2014). "A rapid abnormal event detection method for surveillance video based on a novel feature in compressed domain of HEVC"- In 2014 IEEE International Conference on Multimedia and Expo (ICME), pp. 1-6. IEEE, 2014.

[5]. Biswas, Sovan, and R. Venkatesh Babu (2014). "Sparse representation based anomaly detection using homv in h. 264 compressed videos"- In 2014 International Conference on Signal Processing and Communications (SPCOM), pp. 1-6. IEEE, 2014.

[6]. Biswas, Sovan, and R. Venkatesh Babu (2015). "Anomaly detection in compressed H. 264/AVC video"- Multimedia Tools and Applications 74, no. 24 (2015): 11099-11115.

[7]. Cheng, Kai-Wen, Yie-Tarng Chen, and Wen-Hsien Fang (2015). "Gaussian process regression-based video anomaly detection and localization with hierarchical feature representation"- IEEE Transactions on Image Processing 24, no. 12 (2015): 5288-5301.

[8]. Sabokrou, Mohammad, Mohammad Khalooei, Mahmood Fathy, and Ehsan Adeli (2018). "Adversarially learned one-class classifier for novelty detection"- In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 3379-3388. 2018.

[9]. Sabokrou, Mohammad, Mohsen Fayyaz, Mahmood Fathy, and Reinhard Klette (2017). "Deep-cascade: Cascading 3d deep neural networks for fast anomaly detection and localization in crowded scenes"- IEEE Transactions on Image Processing 26, no. 4 (2017): 1992-2004.

[10]. Stutz, Thomas, and Andreas Uhl (2011). "A survey of h. 264 avc/svc encryption"- IEEE Transactions on circuits and systems for video technology 22, no. 3 (2011): 325-339.

Cite this article as : Saravanan S, "Anomaly Detection in Banking Using A Video Surveillance System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 4, pp. 538-545, July-August 2020. Available at doi : https://doi.org/10.32628/CSEIT206496
Journal URL : http://ijsrcseit.com/CSEIT206496