# PREVENTING HACKING IN CCTV DEVICES AND THEIR SERVERS USING NETWORKS SECURITY

Sandra Robin
*Department of computer science and engineering*
*Panimalar institute of technology , affiliated to Anna University, Chennai*
chennai, India

Swathipriya.S
*Department of computer science and engineering*
*Panimalar institute of technology , affiliated to Anna University, Chennai*
chennai, India

Dr.Kalaichelvi
*Department of computer science and engineering*
*Panimalar institute of technology , affiliated to Anna University, Chennai*
chennai, India

Dr.Subedha V
*Department of computer science and engineering*
*Panimalar institute of technology , affiliated to Anna University, Chennai*
chennai, India

**Abstract— Nowadays, new emerging technologies influence the world. Our lives depend on these emerging technological devices which make our life way much accessible. On the other hand, there is a constant rise in cyber attack and hacking which is a threat to our privacy.**

**CCTV(closed-circuit television) systems have become nearly very common and mandatory for safety purposes in many organizations, businesses, and stakeholders. The main purpose is to provide security and crime. In this paper, a systematic analysis of existing and contemporary threats in closed-circuit TV systems are conducted based on openly available data. The observations can then be used to better perceive and analyze the security and the confidential hazards associated with the advancement, deployment and the use of these systems. This paper studies existing and unique peril, alongside their existing or probable antidote, and summarizes this data into a complete table which will be utilized in a constructive way as a security checklist when determining cyber-security level of existing or new CCTV designs and formations. This paper also provides a group of suggestions and remissions which will help improve the safety and privacy levels provided by the hardware and therefore the operations of loop television systems.**

**Keywords: Security, Hacking, CCTV Hacking, Prevent Hacking.**

## I. INTRODUCTION

Closed-circuit television is a prominent part of the world we are in. CCTV and IPcam cameras have become exceedingly common all around the world. Nowadays their use is exceedingly vast. They are used in public institutions and at homes. Using a direct transmission system a CCTV system links a camera to a video monitor. Open architecture and transmission methods are the new approaches within the closed-circuit television network industry. These systems have numerous components with a variety of functions, features, and specifications. In this type of technology the security of the information transmitted is important.

A lot of crimes are solved using CCTV for example, almost 6 crimes are solved in London daily with the help of CCTV.
This paper intends to provide information on the capabilities and limitations of CCTV security that will aid an agency in procuring a new CCTV system or upgrading an existing one.
.

## II. RELATED WORKS

Many new techniques are made to prevent hacking. Infringement activities and crimes that are intended to harm others are being prohibited these days. To overcome this serious issue, many new technologies and new inventions have arrived. In such a way a technology called Physical Unclonable Function (PUF) is physical hardware used to provide uniqueness of the ID using the Internet of Things (IoT). By using these technologies the threat and culpability being denied, the crimes happening these days can be refused completely. Therefore, even the studies on the strengthening of the CCTV network security have been going on and the

many works are implemented successfully to safeguard the people..

## III. IPADDRESS

The IP address is a unique number which is assigned to every single device connected to the internet. An IP address is a special, unique serial number used for identification. A device connected to any network will have an IP address for communication and identification. From PC to smartphones to even a coke machine has an IP address.

### *A.* Phishing

Hackers hack IP addresses of devices through a process called phishing. Phishing will mislead people into sharing information and details like passwords. The most common game plan in phishing is sending an email to the victims and they trick the email recipient into believing that message is useful for them or something they need. The message imitates as a trustful organization when the victim opens the mail that message demands him or her to go that particular website if the user types the password and username, the information will go to the hacker then the hacker tricks and sells the personal information on the black market. In this modern world social networking sites became the prime phishing target.

### *B.* Types of Phishing

1. CEO Fraud/Business Email Compromise: Steals user data, like login credentials and credit card numbers and passwords. It happens when an attacker, pretending to be a trusted entity, spoofs a victim into opening an email, instant message, or text message.

2. Clone phishing: Phishing Attackers will view the appropriate delivered email messages and make an exact copy of it and then change an attachment or link into something mischievous.

3. Evil Twin: An evil twin is a wireless access point that camouflages as an appropriate Wi-Fi access point so that an attacker will be able to gather information without the end-user's knowledge.

4. Smishing and Vishing: Smishing and vishing are types of phishing attacks that try to lure victims via SMS message and voice calls.

5. Spear phishing: Spear phishing email messages won't look as other general phishing attempts. Attackers will collect information about their targets and fill email messages with more convincing context. Some of the attackers also hijack business email communications and create customized messages.

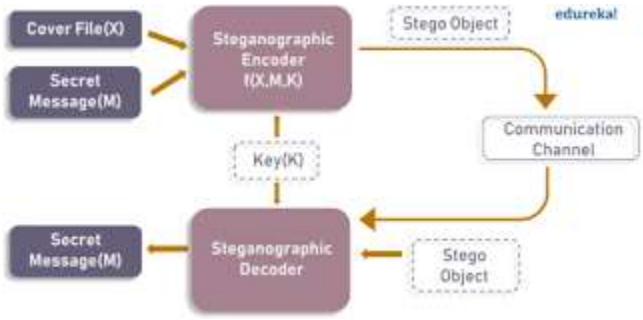
6. Whaling: Whaling particularly targets high profile executives in an organization. The whaling attempt will often present as a legal communication or other high-level executive business

## IV. Existing Technology

There are some existing technologies used to secure data.

**Steganography**

The word steganography means covered or secret. Steganography is the art of hiding information in such a way that its presence cannot be exposed and a communication is happening. A confidential information is concealed in such a manner that the very existence of the information is unknown. Paired with existing communication methods, steganography can be used to finalize concealed transfers.




*1)* **Steganography Pros**

The advantages of using steganography are one-way hashing and hiding information.

*2)* **Steganography Cons**

The disadvantages of using steganography are pornography, terrorism.

## V. Bar Graph

The following bar graph shows the amount of cyber related crimes in year-wise.

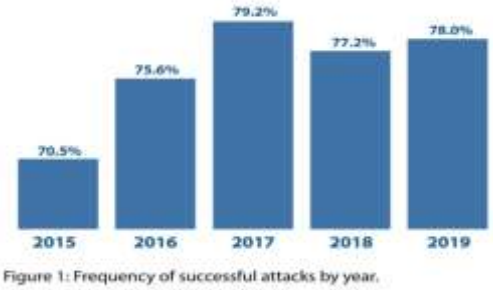



Figure 1: Frequency of successful attacks by year.

*Fig. 1. Yearwise frequency of successful cyber attacks*

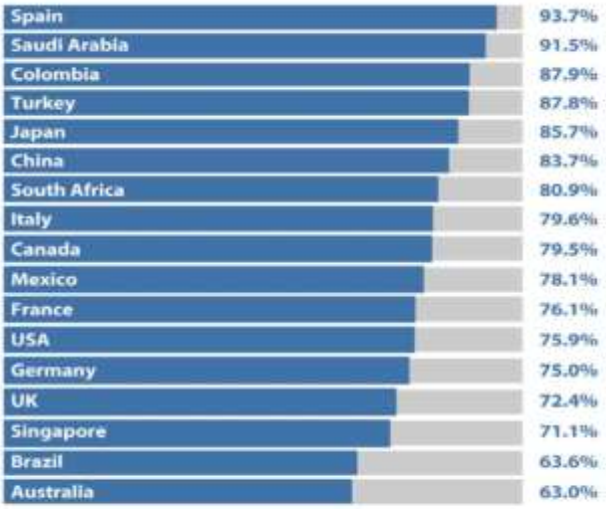



Figure 2: Percentage compromised by at least one successful attack in the past 12 months.

*Fig. 2. Percentage compromised by at least one successful attack*

Worldwide, the frequency of cyber attacks has only grown over the years. In fact, during a period of five years since 2015, the attacks have grown by nearly 7.5 percent. From 2015 to 2017, the cyber attacks worldwide grew at an alarming 9 percent.

According to another data (see figure 2), Spain, Saudi Arabia and Colombia were among the most vulnerable countries in the cyber domain.

In India, the scene has been no different. A Data Security Council of India (DSCI) report said that India was ranked second in the list of countries that bore the brunt of cyber attacks between 2016 to 2018.


*Fig. 3. Data chart showing number of attacks during a 3-year period. India is one of the vulnerable countries.*

The intent of the paper is to stress the need to check and contain the rate of cyber attacks in our country.

## VI. **Proposed Work**

In this software, we develop a web server which is used to view the video through CCTV. If the server detects an IP address which is not present in its database, it immediately sends an email and sms to the user of the CCTV. The sms is sent through an API (application program interface).

The email and the sms asks the user to confirm if the unknown IP address belongs to him. The user is asked to reply immediately. If the user responds and assures that it was him, then the video will be shown. Otherwise, the software immediately blocks the unknown IP address to prevent the hacker from hacking private information of the user.


*Fig.4 Flowchart for CCTV SECURITY*

## VII. Preliminary Results

The preliminary results will be the sending of sms and mail to the user when the system detects an unknown IP address which doesn't belong to the user. By this we can confirm that the system is working.

## VIII. Social benefits

*Prevent hacking.
*User information is secure.

## IX. Conclusion

Hacking is one of the major crimes happening in the digital world. Hacking, especially CCTV hacking is frequent nowadays. It is something which is equal to stealing someone's privacy. Stealing someone's privacy and watching their activities and collecting information about them and misusing them. These crimes are common nowadays. To prevent hacking, the Government should enforce strict laws to control it and should take severe actions against those hackers. To prevent hacking and protect naive users, the zealful idea to prevent hacking is introduced. This algorithm gives the notification whenever CCTV is getting hacked by someone. The owner gets the notification and he'll immediately be alerted and the user will be saved from hackers.

## ACKNOWLEDGMENT

***I've taken the opportunity on this initiative. However, it wouldn't have been possible without the good help and assistance of many individuals and organizations. I would like to express to both of them my heartfelt thanks. I am sincerely grateful to Dr. T.KALAICHELVI mam for their advice and continuous monitoring, as well as for the provision of the requisite knowledge on the project and also for their cooperation support. I would like to express my unique gratitude and appreciation to the audience for granting me some focus and time. My gratitude and admiration always go to my colleague for the production of the project and the individuals who gladly helped me out with their skills.***

## REFERENCES

[1] Jung-oh Park and Sanggeun Kim 'Study on Strengthening Plan of Safety Network CCTV Monitoring by Steganography and User Authentication.'

[2] Mohammed Farook Bin Rafiuddin , Prethpal Singh Dhubb , Hamza Minhas 'RECENT STUDY OF CLOSE CIRCUIT TELEVISION (CCTV) IN HACKING'

[3] Andrei Costin 'Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations'

[4] .Haripriya Rout, Brojo Kishore Mishra 'Pros and Cons of Cryptography, Steganography and Perturbation techniques'

[5] Andrei Costin 'Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations'

[6] Shih- Hsuan Chiu, Chuan- Pin Lu, Che- Yen Wen 'A Motion Detection- Based Framework for Improving Image Quality of CCTV Security System'