iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** III **Month of publication:** March 2020

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue III Mar 2020- Available at www.ijraset.com

Mitigation for Brute Force Attack against IP/CCTV Camera Login

Devang Thakar[1], Hepi Suthar[2]
[1]*M. Tech Student, Department of Computer Engineering, Marwadi University, India*
[2]*Assistant Professor, Department of Computer Engineering, Marwadi University, India*

Abstract: ***In recent years, world has been threatened by cybercrime and cyber frauds. As a result, many countries have endeavour to enhance their public security through the usage of video security apparatus such as IP camera and surveillance system. Unfortunately, IP cameras and surveillance system devices are known for their vulnerabilities and Brute Force attacks present a significant privacy and security concern. Because the attacks are easily performing and highly effective, this allow attacker to steal the user id and password of the IP camera and to gain the access of the IP camera. We have evaluated the different vulnerabilities of the IP camera which can be used by attackers to exploit and misuse the IP camera. Our finding shows the different vulnerabilities of the IP camera and not much strong mitigation system to prevent against those vulnerabilities. We suggest method to counter Brute Force attack and reiterate the need of good login system.***
Keywords: CCTV Hacking, Mitigation, CCTV Security, Brute Force Attack, CCTV vulnerabilities

I. INTRODUCTION

Cyber Security: Computing and communication have undergone significant changes in recent decades. Reckoning is preferred on the go with a huge demand of movability support in communicating [16, 17]. Gratuitous to say, the advancement in handheld apparatus and marvellous popularity of mobile application leads to necessity of timely analysis and security provisioning of communication environment [18, 19]. The video surveillance industry is part of the Information Technology (IT) industry that set up added value business that beholds toward the future [15]. As technological developments in the last four decades have made IP/CCTV cheaper, smaller and easier to operate [12]. IP cameras have become far and wide in today's world due to their price and accessibility in comparison to CCTV. IP cameras embody camera, encoder, and web server within itself that is why it can be easily managed even if the IP cameras are dispersedly established. It typically structured in an application, network layer and device layer [4]. It can be accessed wherever and whenever through the web or smart-phone in real-time. IP cameras are much easier to install than analogue cameras because they do not require a separate cable run or power boost to be able to send images over a longer distance [8]. Now a days IP cameras can be found in most shops, organizations, company and in many homes [1]. Nonetheless, IP cameras have deficiency, too, in terms of admittance authorization and user attestation for the IP camera web server, or attestation of IP cameras which are newly placed in the network [5]. Contemporary reports and studies have shown that IP cameras cover less than ideal security, and could be exploited and fully controlled by miscreants to infringe user confidentiality and even bombard large-scale DDoS attacks. Username and password is the utmost extensively used form of authentication in habitude to prevent illegitimate access. However, an unimaginable number of IP cameras are found to have no password safeguard and are having their live video feeds streamed [7].

Study shows that 70% of the examples utilized had the default merchant passwords that had not been commutated [2]. Default username password or no username password is not only the security weakness in the IP camera. There are many more vulnerabilities have been found in IP camera which can lead to the serious cause to surveillance system and to the society as well. Vulnerabilities found in different connected cameras can range from weak passwords, poorly protected credentials, insecure configuration management [9], Remote Code Execution (RCE), Denial of Service (DoS), weak authentication and authorization, insecure video feed transfer etc. Due to these vulnerabilities IP camera are most easily exploitable and more used targets for the attackers to cause harm to the society. Using these vulnerabilities an attacker may violate a system's integrity for a goal which is not directly related to the video content [20].

In this article, we will provide the mitigation for the Brute Force Attacks performed by the attackers against the IP camera. As weak authentication is most common vulnerability found in IP camera, attackers use Brute Force Attack against IP camera to gain access. To prevent the IP camera from being leveraged, we will provide the mitigation for the Brute Force Attack.

II. RELATED WORK

A wide range of camera manufacturers use very similar hardware and software in their cameras. The main difference is with the UI and specific firmware updates [6]. IP camera convey video feed on the basis of IP network, so that it is "open" and its expandability and resilience is more than the CCTV camera. In addition, IP camera enclose web server inside itself and facilitate keep an eye on through web browser, so that keeping an eye on is feasible from wherever and whenever [5]. The core of the surveillance camera system is forged by a process in which video cameras collect images, which are shipped to a monitor from which they can be watched and taped [14].

On the one hand, some of the researchers have worked for the better security of the IP camera and surveillance system such as Jung-ohPark and SanggeunKim worked on Strengthening Plan of Safety Network CCTV Monitoring [3] to transfer the video feed safely from IP camera to monitoring system. J. Kang, J. Han and J. Hyuk Park has design IP camera access control protocol [5] to prevent the IP camera from un authorized access by the attacker and making IP camera and surveillance system more secure. Whereas Chaeyoung Moon and Kwangki Ryoo [10] focused on the physical security of the IP/CCTV camera to prevent it from being stolen or damaged by the unauthorized person.

While on the other hands, researchers have reviewed and analyzed the vulnerabilities and strength and weaknesses of the IP/CCTV camera and surveillance system based on different perspectives such as physical security, authentication and authorization, network security etc. All of them have used different criteria according to their views and analyze the weaknesses or vulnerabilities of the IP/CCTV camera and surveillance system. Some of them has also found out the types of threats and types of attacks that can be performed on the IP/CCTV camera. Other researchers have reviewed that how the IP/CCTV camera and surveillance systems used to prevent the crimes or terrorism. Some of the researchers also provided basic the mitigations to prevent the IP/CCTV camera to from being hacked or leveraged.

Below table shows the summery of the threats, vulnerabilities and attacks classification of the IP camera and surveillance systems.

TABLE I
Threat, Vulnerability And Attack Classification [11]

Attack Category	Attack Surface	Attack Type	Direct affected components	Exploitation complexity
Software	Web Interface Other Interfaces	Weak access control or Weak authentication	-Firmware of DVR, NVR, IP-camera -Software of VMS, CMS, video server	Easy
Software	Web Interface Other Interfaces	Insufficient Transport layer protection	-Firmware of DVR, NVR, IP-camera -Software of VMS, CMS, video server	Easy
Software	Web Interface Other Interfaces	Denial-of-Service (DoS)	-Firmware of DVR, NVR, IP-camera -Software of VMS, CMS, video server	Easy
Optical	Visual Layer Malicious Images (Imagery Semantics)	-Command and control -Data infiltration	-Cameras -Video sensors -NVR/DVR -Video/Image processing elements	Easy to complex
Optical	Visual Layer (Imagery Semantics)	Data exfiltration	-VSS, Cameras, DVR,NVR connected to LCD displays visible to attacker	Complex

During the literature review we have observed that researchers have discussed about the vulnerabilities or strengths and weaknesses about IP/CCTV camera and surveillance system and they have also suggested some basic mitigation to keep IP/CCTV camera and surveillance systems secure. But, we have observed some serious vulnerabilities that are harmful to the IP /CCTV camera. So, we will provide the mitigation for one of the vulnerability we have noticed during literature review.

III.RESEARCH METHODOLOGY

The aim of this research is to determining the most common and most attacked vulnerability in to IP/CCTV camera or surveillance system, post determination providing the mitigation for that particular vulnerability. To fulfil the aim of the research we have gone through the literature review and vulnerability assessment phases. In these two faces we have observed one or more common vulnerabilities such as Remote Code Execution (RCE), Denial of Service (DoS), weak authentication and authorization, MITM attack vulnerability, ARP poisoning etc. After vulnerabilities assessment and literature review we have found that weak authentication and authorization is most common and most attacked vulnerability attackers used to gain access of the IP camera. So, in this research we have provided the mechanism to mitigate weak authentication and authorization vulnerability to make login process of IP/CCTV camera safer from attackers who used this vulnerability to leverage the system.

Following are the diagrams illustrate proposed registration and login process to mitigate the weak authentication and weak authorization vulnerability.

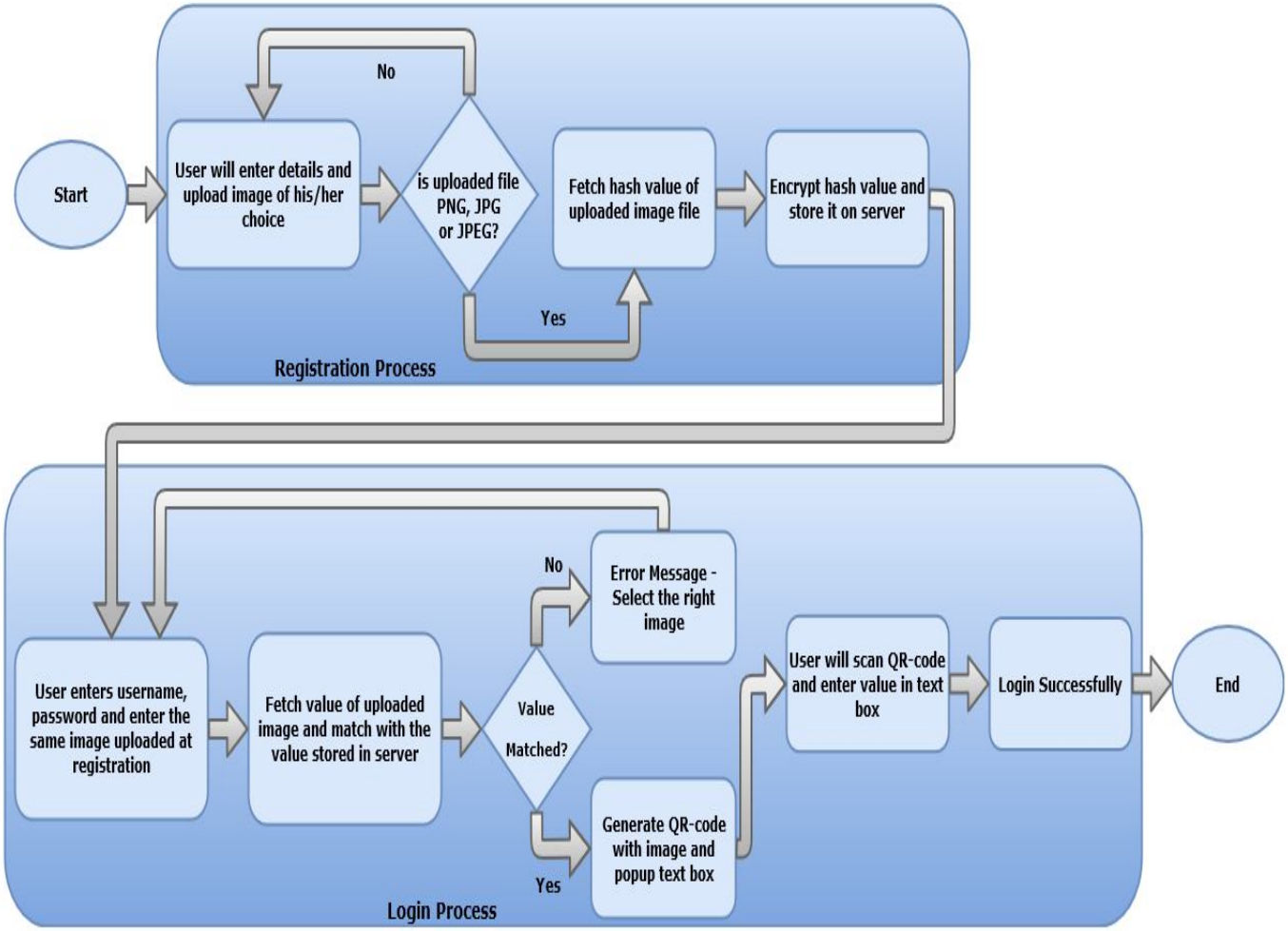


Fig. 1 Flow of proposed mechanism

Above flow diagram shows that how mitigation system for the brute force attack will work to mitigate the IP/CCTV camera against the brute force attack. First of all when user opens the portal of ip camera he/she will see the registration page where he/she has to fill-up the details such as username, password, email id. Along with the basic details one more thing he/she has to input for registration which is an image of his/her choice. The only allowed file types for the image are PNG, JPG and JPEG. As soon as user enters the details and click on registration button. System will fetch the hash value of the image file using MD5 and SHA1 hashing algorithms. After fetching the hash value system will encrypt that hash value and finally store that value into the database. Here the registration process will end.

Post registration user will redirect to the login page of the system. Here he/ she has to enter the user name, password and image that he/she has selected at the time of registration. As soon as user selects the image system will check for the has value of the image and compare it with value stored in the database. If the value of the image will not match than system will generate and error message that "please select the right image!" and user have to select the right image and right credentials. When user will enter the correct credentials and image system will match the credentials and image with database and if very thing will match than system will generate a QR-code with user's selected image file and a text box. Then user have to scan that QR-code with any QR-code scanner from his mobile device. By scanning the QR-code user will get one value, user have to enter that value into the txt box below the QR-code and click on login button. If everything goes right than user will successfully logged in and will get the access of IP/CCTV camera. Otherwise system will generate an error and user will not be able to login.

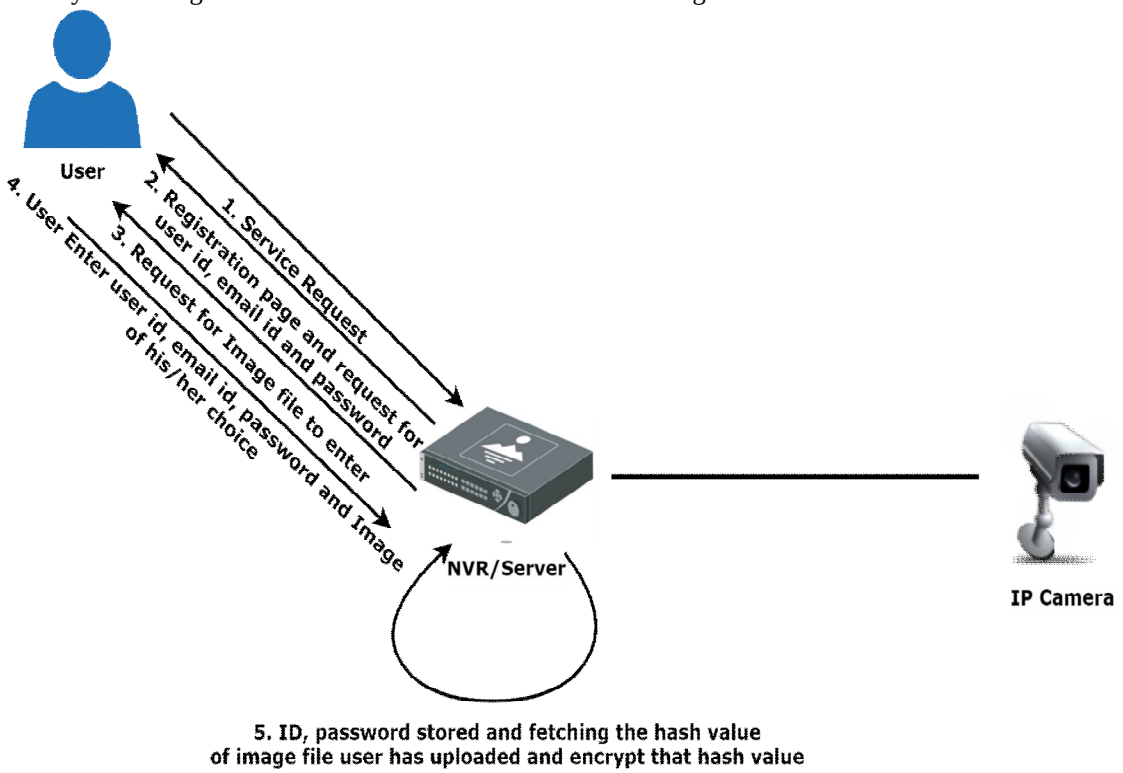


Fig. 2 Proposed User Creation Process

As shown in figure following steps are performed to register new user in NVR or Server to access the IP/CCTV camera.

1) *Step 1:* At first user will request for the registration page of the NVR/Server to register new user by entering IP address of the IP camera in web browser.
2) *Step 2:* In response to the users request NVR/Server will respond the registration page in the user's web browser and asks user to enter the registration details such as user id, email id and password of user's choice.
3) *Step 3:* At last NVR/Server will ask user to select the image file of his/her choice.
4) *Step 4:* Here user will enter the user id, email id, password and also select the image of his/her choice to make registration successful.
5) *Step 5:* In this step details entered by user such as user id, email id and password will be stored in database and the hash value of the image which user has selected in previous step will be generate using combination of MD5 and SHA1 hashing algorithms and further that hash value will be encrypted and stored in the database.

After registering as new user, user will be redirected to login page and user will try to login for accessing IP/CCTV camera. Diagram for the proposed system is as follows.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue III Mar 2020- Available at www.ijraset.com

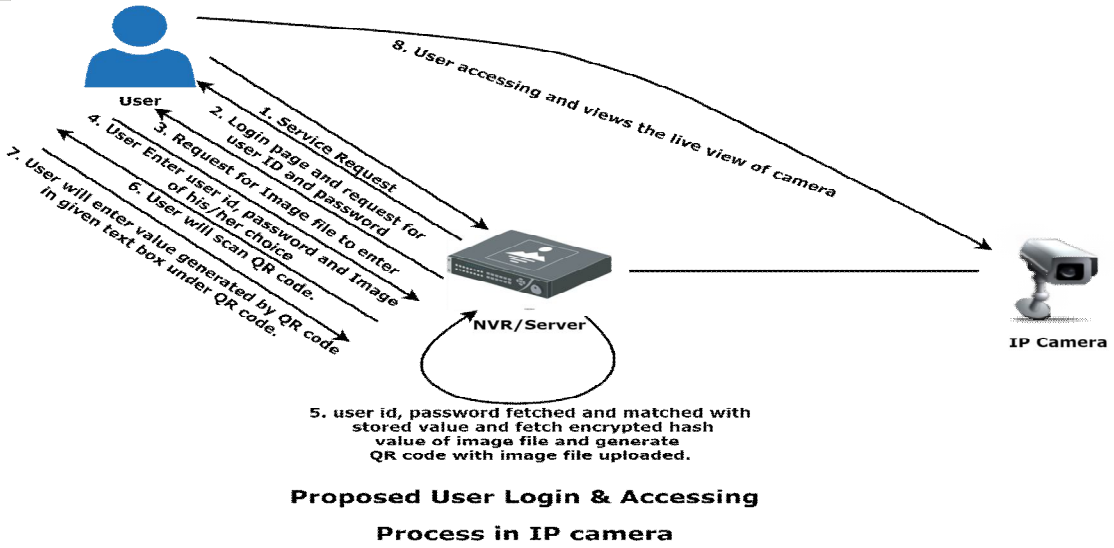


Fig. 3 Proposed User Login Process

For login process steps are shown in above figure as our proposed systems to prevent the login from Brute Force Attack.

a) *Step 1:* User will request for login page.

b) *Step 2:* NVR/Server will respond to user's request and provide the login page to the user's browser and asks user to enter the user id and password.

c) *Step 3:* After entering the user id and password login page asks user to select the image that user has selected at the time of registration.

d) *Step 4:* Here in user will enter login details such as user id, password and image that he/she has selected at the time of registration.

e) *Step 5:* In this step NVR/Sever will match the details entered by the user such as user id and password and in addition it will match the hash value of the image selected by the user and the hash value in the database. If user id, password and hash value of the image matches system will generate QR code based on the value of the user details such as user id, and hash value of the image with the image inside it

f) *Step 6:* As soon as the QR code generated by the system user will scan the QR code with the QR code scanner from his/her mobile phone and by scanning the QR code user will get some value on his/her mobile screen.

g) *Step 7:* User will enter the value that he/she got by scanning QR code into the text box given below the QR code.

h) *Step 8:* At the final step system will check for all details entered by the that is it match with the database or not and also match the value of QR code, if and only if all the details correct then and then only the user will be able to logged in into the system otherwise system will generate an error message.

For this proposed system implementation, we have used PHP and java script as a development language, wamp server for locally hosting the web page like registration and login page of the IP/CCTV camera and mysql as database.

Below are the screen shots of the developed login system which will be the mitigation for the Brute Force attack.

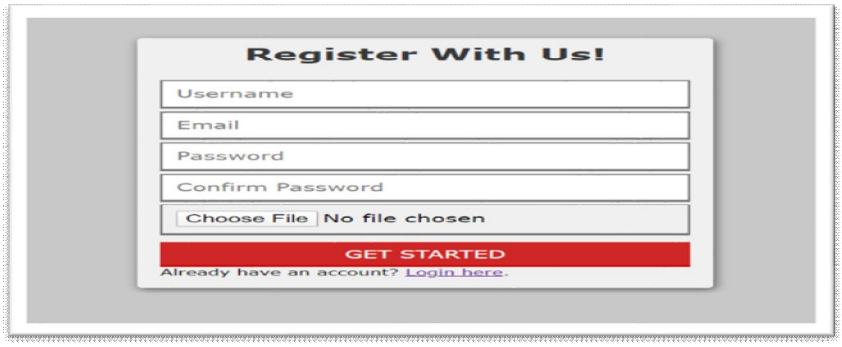


Fig. 4 Registration Page

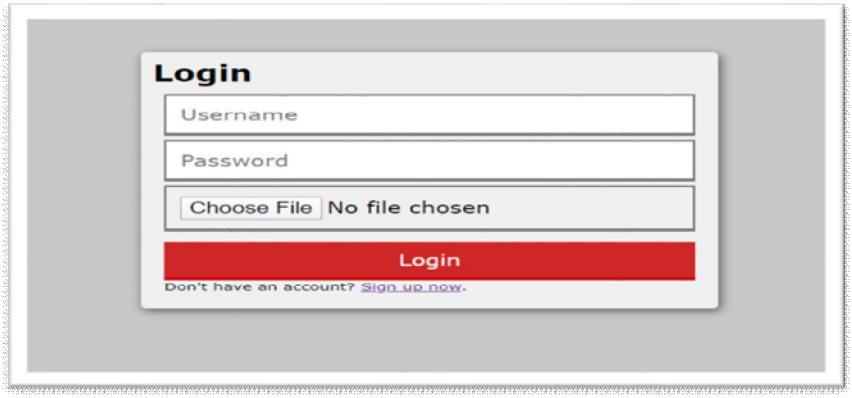


Fig. 5 Login Page

In above screenshot it is seen that in registration page user have to select the image of his/her choice along with the other details to register his/her self. As shown in the other screenshot in login page user have to select the image that he/she has selected while registration to be able to login into the system and gaining access of the IP camera. As soon as the user select the image in login portal the QR code with the user selected image will be generated on the same page and user have to scan that QR code which will generate value that user will enter and proceed to login.

IV. RESULT

As a result of the proposed login system for the IP camera, Current scenario will be changed and Login of IP camera will be secure against the Brute Force attack. Attackers will not be able to perform the Brute Force of the user id and password and they will not be able to break down the login system to gain unauthorized access of IP camera. Attackers will not get access of the IP camera by just guessing or try and catch of user id and password. By mitigating Brute Force attack against the IP camera login will helps the legitimate users to make secure their IP camera and surveillance system. In addition, it also helps those users who are not very much aware about the security of IP camera, they are just using the camera to for monitoring or securing their places like shop owners, small business holders, residential societies etc. Implementing the propose system in the IP camera NVR/Server helps to improve the system security and make the system more secure from attackers. Better security for IP camera systems leads to safe and secure society environment.

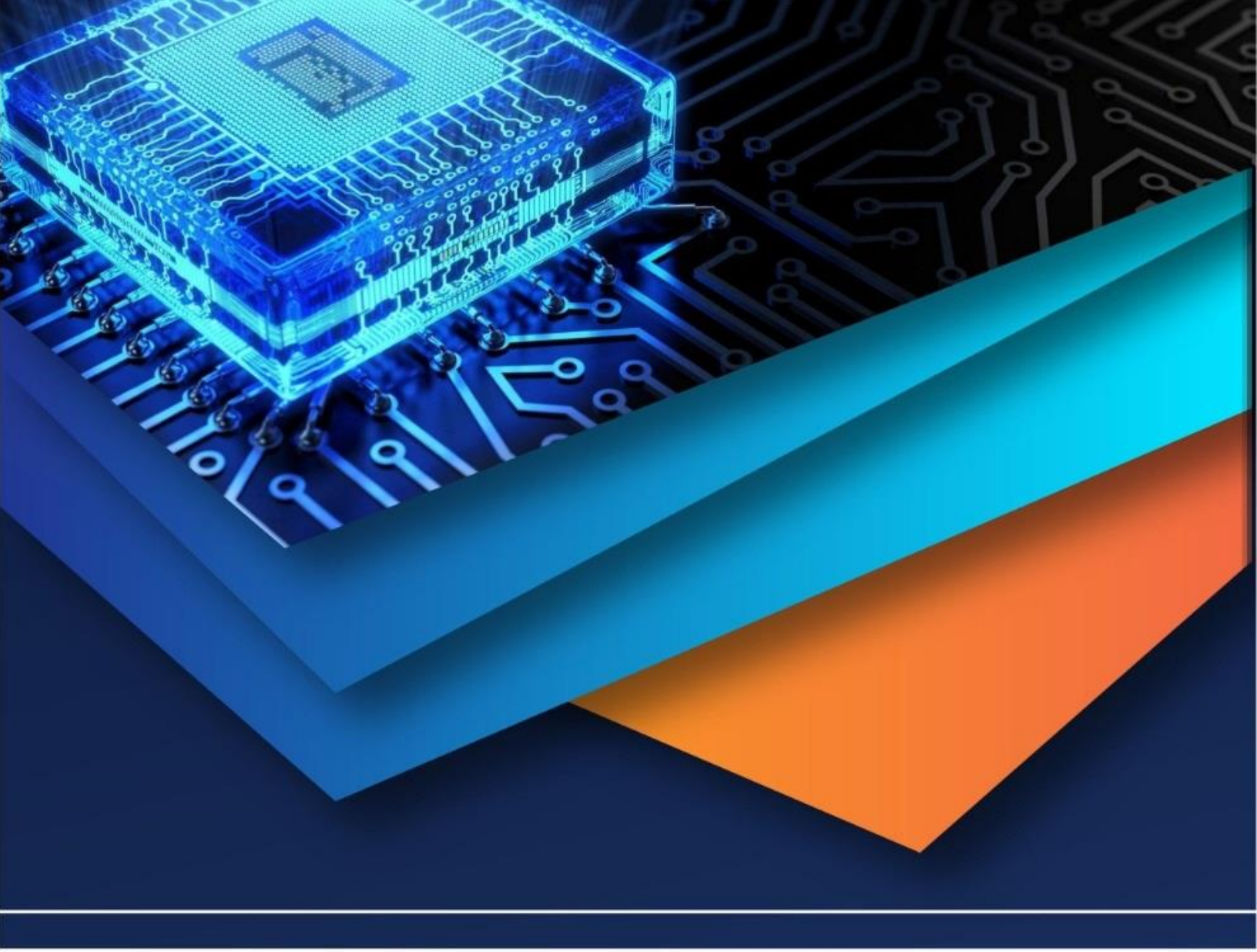
V. CONCLUSION

We have shown that some of the vulnerabilities which are very common in the IP camera till the time. We have observed those vulnerabilities found out that how those vulnerabilities are used to exploit the IP camera and misuse it by the attackers. Available mitigation or solution of those vulnerabilities and how much affective it is to reduce the risk of the particular vulnerability. Than we have observed the most common vulnerability that is weak authentication against which attackers try Brute Force attack to exploit that vulnerability. To make secure IP camera from Brute Force attack we required strong mitigation mechanism, to fulfill that requirement we have developed registration and login system for NVR/Server of the IP camera. In this article we have stated define those vulnerabilities their mitigation provided till date and mitigation we have developed for the Brute Force attack against IP camera. In conclusion, IP camera manufacturers should now think about the securing the IP camera against the different attacks. They have to aware of different vulnerabilities in their product and try to mitigate those vulnerabilities. They should worry for better security of their products to make society safe and secure. Besides, the inventions and continuous development of IP/CCTV camera, the weaknesses would be addressed and it is likely to be more effective in future days.

REFERENCES

[1] T. Doughty, N. Israr and U. Adeel “VULNERABILITY ANALYSIS OF IP CAMERAS USING ARP POISONING”, 8th International Conference on Soft Computing, Artificial Intelligence and Applications (SAI 2019), June 29-30, 2019, Copenhagen, Denmark
[2] B. Cusack, Z. Tian “Evaluating IP surveillance camera vulnerabilities”, 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia
[3] CC Compliant Citation: Jung-oh Park and Sanggeun Kim, “Study on Strengthening Plan of Safety Network CCTV Monitoring by Steganography and User Authentication,” Advances in Multimedia, vol. 2015, Article ID 960416, 9 pages, 2015. doi:10.1155/2015/960416, http://creativecommons.org/ licenses/by/3.0/
[4] C.H.M. van den Bogaard, “Security Analysis of Cloud-Based Video Cameras” Cloud Computing (CLOUD), 2012 IEEE 5th International Conference

[5] Jungho Kang, Jaekyung Han and Jong Hyuk Park, "Design of IP Camera Access Control Protocol by Utilizing Hierarchical Group Key", Symmetry 2015, 7(3), 1567-1586
[6] Tsitroulis, Achilleas & Lampoudis, Dimitris & Tsekleves, Emmanuel. (2014). Exposing WPA2 security protocol vulnerabilities. International Journal of Information and Computer Security. 6. 93-107. 10.1504/IJICS.2014.059797
[7] Haitao Xu*, Fengyuan Xuy, and Bo Chenz, "Internet Protocol Cameras with No Password Protection: An Empirical Investigation", International Conference on Passive and Active Network Measurement PAM 2018
[8] M. Rafiuddin, P.S. Dhubb, H. Minhas "RECENT STUDY OF CLOSE CIRCUIT TELEVISION (CCTV) IN HACKING", 3rd international conference on latest trends in engineering science, humanities and management, Indian Federation of United Nation Association, New Delhi (India), 8th April, 2017
[9] J. Bugeja, D. Jönsson, and A. Jacobsson, "An Investigation of Vulnerabilities in Smart Connected Cameras", Second International Workshop on Pervasive Smart Living Spaces, Internet of Things and People Research Center and Department of Computer Science and Media Technology, Malmö University, Malmö, Sweden
[10] C. Moon, K. Ryoo, "Control System for Security Enhancement of CCTV Camera Maintenance Devices", International Journal of Engineering & Technology, 7 (3.24) (2018) 104-109
[11] A. Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations", 6th International Workshop on Trustworthy Embedded Devices, Vienna, Austria — October 28 - 28, 2016
[12] Harris, Vandra Marie Elizabeth and Harris, Crispin, "Information overload: CCTV, your networks, communities and crime," IndraStra Global Index (IGI), accessed March 19, 2020
[13] Falah Chamasemani, Fereshteh & Affendey, Lilly. (2013). "Systematic Review and Classification on Video Surveillance Systems". International Journal of Information Technology and Computer Science. 5. 87-102. 10.5815/ijitcs.2013.07.11
[14] Quirine A.M. Eijkman & Daan Weggemans (2011), "Visual surveillance and the prevention of terrorism: What about the checks and balances?", International Review of Law, Computers & Technology, 25:3, 143-150, DOI: 10.1080/13600869.2011.617480
[15] June-Suh Cho, "Video Surveillance Systems and Future Requirements of the Security Market in United Kingdom and Korea", IJTEMT, EISSN: 2321-5518; Vol. III, Issue V, October 2014
[16] N. Dutta, HKD Sarma and Z. Polkowski, "Cluster based routing in cognitive radio Adhoc networks: reconnoitering SINR and ETT impact on clustering", Com. Com., (Elsevier), pp. 10-20, vol. 115, 2018.
[17] N. Dutta and HKD Sarma, "A probability based stable routing for cognitive radio Adhoc networks", Wire. Net., (Springer), vol. 23(1), pp. 65-78, 2017.
[18] N. Dutta and IS Misra,"Multilayer hierarchical model for mobility management in IPv6: a mathematical exploration", Wire. Pers. Comm.(Springer), vol.78 (2),pp.1413-1439, 2014.
[19] N. Dutta and IS Misra, "Mathematical modelling of HMIPv6 based network architecture in search of an optimal Performance", IEEE 15 th ADCOM, Guwahati, India, pp. 599-605, 2007.
[20] Kalbo, Naor & Mirsky, Yisroel & Shabtai, Asaf & Elovici, Yuval. (2019). "The Security of IP-based Video Surveillance Systems".



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY