e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

TO CHECK THE PUBLIC OPINION ABOUT THE RELIABILITY OF CCTV CAMERAS

Prashik Shinde[*1]

[*1]B.Sc. Information Technology, B.K. Birla College, Kalyan, Maharashtra, India.

DOI : https://www.doi.org/10.56726/IRJMETS29656

ABSTRACT

CCTV is becoming an essential part of our society as it occurs everywhere. Most of the part of our society is come under cyberspace. And a massive amount of cyberspace has been covered by CCTV. To secure our cyberspace, our IT facilities should be secured and CCTV is one of the most important of all of them. There are several ways to secure a CCTV camera. Due to CCTV cameras are turning from a cyber security device to a cyber threat due to poor security measures, resulting in our cyberspace being vulnerable. This research paper suggests public opinion on the reliability of CCTV. The government also relies on CCTV so much and people are worried about their privacy so this study is also about the awareness camp for security measures in CCTV are required or not. Several articles have done practical exercises on CCTV reliability and CCTV security methods. This research will help to find out the public's views on the reliability, security, and privacy support of CCTV, which will help in deciding whether there is a need to increase awareness of CCTV and whether or not any security measures need to be added.

Keywords: Cyber space, Vulnerable, Reliability, Privacy support.

I. INTRODUCTION

While the earliest known CCTV camera was developed almost a century ago back in 1927, currently, it's assumed as granted there are about 770 million CCTV cameras all over the globe, and their number is casually predicted to surpass 1 billion in 2021.[1] As this count is increasing exponentially, almost the largest part of the planet is coming under the Cyber Space through CCTV. As CCTV surveillance continues to expand its reach in both public and personal spaces and evolve with new technology, the policy will get pleasure from high-quality evaluations of outcomes and implementation.[2] So if that much area is coming under Cyber Space because of CCTV then this one amongst the largest Cyber equipment must be made secured. With recent advances in both AI and IoT capabilities, it's possible than ever to implement surveillance systems that may automatically identify those who might represent a possible security threat to the general public in real time.[3] But at the identical time, closed-circuit television has effects on the privacy of the general public. “Unobservable observer”[4]is the term that was getting used for CCTV earlier. The widespread use of photographic camera surveillance systems has also raised concerns about privacy violations. Because video surveillance systems are invasive, it's difficult to search out an appropriate balance between the privacy of the monitored public and also the functionality of the systems. Tools for the cover of visual privacy available today lack either all or a number of the important properties like the security of protected visual data, reversibility (ability to undo privacy protection), simplicity, and independence from the video encoding used.[5]

As this number of CCTVs increases, will people's confidence in CCTV be maintained? If people's trust is maintained, are CCTVs as safe because of the people that depend upon them? These and a few other questions associated with CCTV and their answers are going to be a part of this research.

First, what's CCTV, and also the history of CCTV? CCTV could be a short variety of circuit Television. it's also referred to as Video Surveillance, which is the use of video cameras to transmit proof to a selected location on a limited set of monitors. Different from a broadcast signal like CCTV, the signal isn't broadcast openly, although it should use point-to-point (P2P), point-to-multipoint (P2MP), or network wired or wireless connections. While all video cameras meet this definition, the term is most ordinarily used for those used for surveillance in areas that need additional security or continuous monitoring.

CCTV was first utilized in 1942 in Germany when the system was installed to observe the launch of V-2 rockets. Unlike broadcast television, which might be viewed by anyone with an aerial, CCTV footage can not be viewed by people outside the range. In earlier times, CCTVs required continuous monitoring thanks to the unavailability

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

of equipment, but within the 1970s VCR technology developed then, and the recorder began in CCTV. within the 1990s, digital multiplexing began to be used, allowing multiple cameras to record simultaneously, likewise to time-lapse and motion-only recording. This saved time and money, which then led to a rise in the use of CCTV. Proponents of CCTV cameras argue that the cameras are effective in deterring and solving crime, and appropriate regulation and legal restrictions on the surveillance of public spaces can provide sufficient protection to reasonably weigh a person's right to privacy against the advantages of surveillance. However, anti-surveillance activists argued that there's a right to privacy in public spaces. Furthermore, while it's true that there are also scenarios where an individual's right to public privacy is both reasonably and justifiably compromised, some scholars have argued that such situations are so rare that they are doing not sufficiently justify the frequent threats to public privacy rights to which occurs. in regions with widespread CCTV surveillance.

As mentioned before CCTV is widely used the research is going to be about whether people trust them or not and if people find CCTV reliable the way to confirm the device is trustworthy if people don't find CCTV reliable, a way to make them feel safe with CCTV awareness.

II. METHODOLOGY

In order to gather public opinion on CCTV, a questionnaire was created which includes multiple responses from different locations. In that questionnaire.

Questionnaire

- Do you have CCTV cameras around you?
- Do you agree that CCTVs are reliable?
- How many marks do you think you will give to CCTV based on a security basis?
- Do you think CCTVs are hackable?
- Do you trust CCTV cameras?

These are the questions and these questions can inform public opinion about CCTV and its reliability. After getting enough outputs of this form, it decides on the following things.

Methodology of analysis and conclusions

Analysis of the data obtained will show what percentage of people consider CCTV to be reliable. And even if it is considered reliable, other information or opinions about CCTV security are collected. The data will be available in a suitable graphical format, it will be a bar chart and a pie chart, which will help us to review and analyze these opinions properly and more interactively. Data analysis will be performed using methods of quantitative and statistical analysis.

You also need to do your research and talk to experts in the field to learn about other security fields that can be applied to CCTV. With reference to old research papers and old data to reduce extra work and save time. Some methods have already been developed to add or enhance CCTV security, which may also be included in this document. One of the methods is presented in a research paper that will also be referenced and referenced. If the inputs are from the questionnaire, give positive feedback about the reliability of the CCTV and then find a way to make the device more trustworthy or give some additional security fields to make the CCTV more secure. If the input turns negative, then awareness of CCTV needs to be raised and explained to them what security companies are already in CCTV and what other big security companies CCTV operators can add to make the facility more reliable.

III. MODELING AND ANALYSIS

The questionnaire was shared on social media and 53 responses were collected. In this questionnaire, the first question is about how many people have CCTV cameras around them.

As the pie chart above shows, 81.1% of people have CCTV around them and therefore 81.1% of people are under CCTV surveillance.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

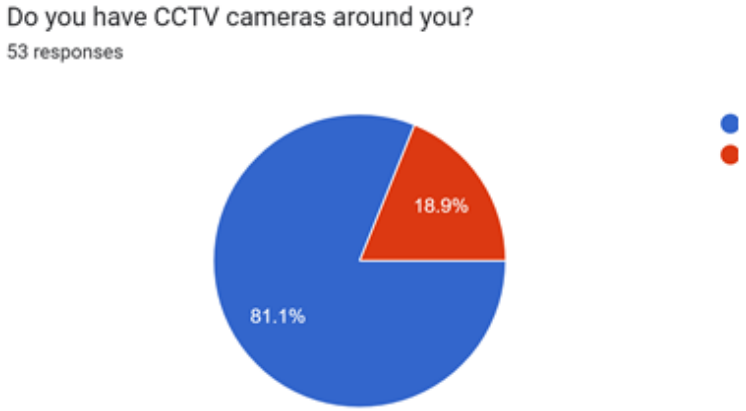

Figure 1

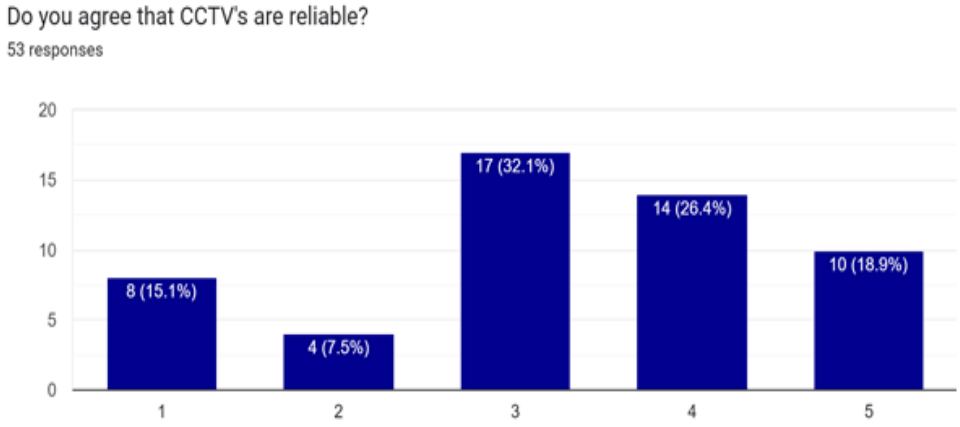

Figure 2

Figure 2 shows data on how reliable people think CCTV is. This question uses a Likert scale where a value of 1 is assigned to Strongly Disagree and a value of 5 to Strongly Agree. 15.1% of people strongly disagree that CCTV is reliable, while 7.5% disagree with the reliability of CCTV. 32.1% of people neither agree nor disagree with the reliability of CCTV. 26.4% agree with the reliability of CCTV and 18.9% of people strongly agree that CCTV is reliable.

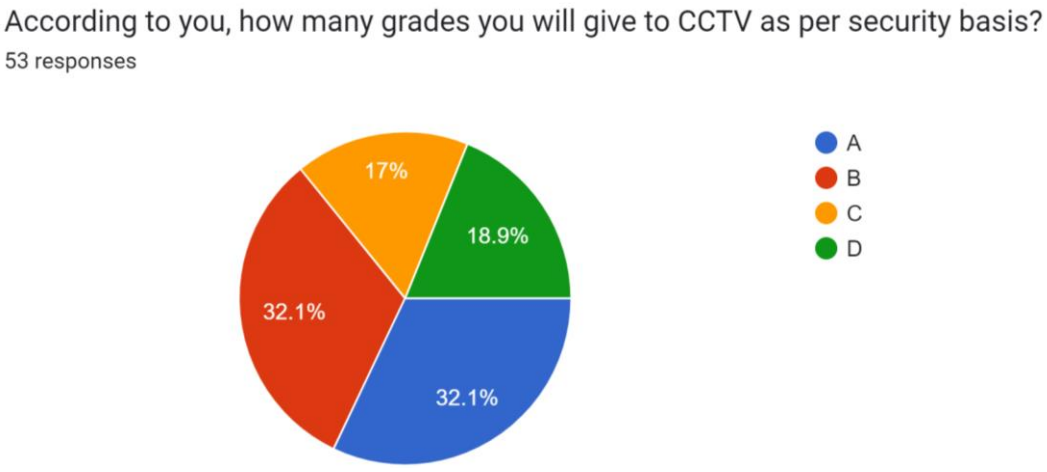

Figure 3

Figure 3 shows the third question. The third question is the CCTV security rating, where grades A to D are available as an option, where A is considered the most secure and D is the least secure. 32.1% of people rated CCTV security as A. Another 32.1% of people rated CCTV security as B. 17% of people rated CCTV security as C and 18.9% of people rated CCTV security as D.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

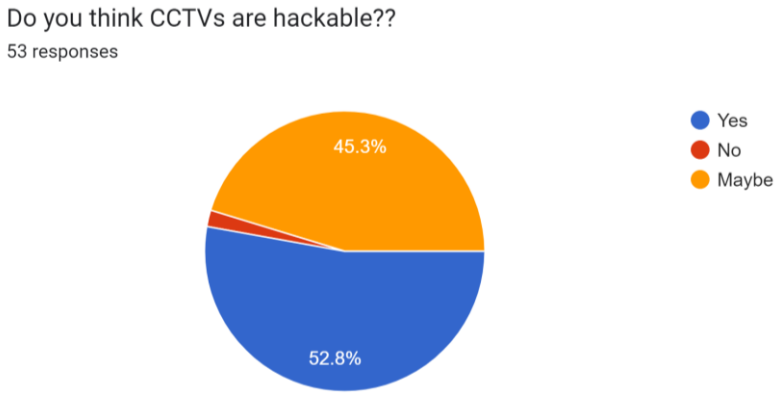

Figure 4

52.8% of people think, that CCTV is hackable according to Figure 4. 45.3% are not sure about the hackability of CCTV and only 1.9% people think that CCTV is not hackable and consider CCTV as a secure device.

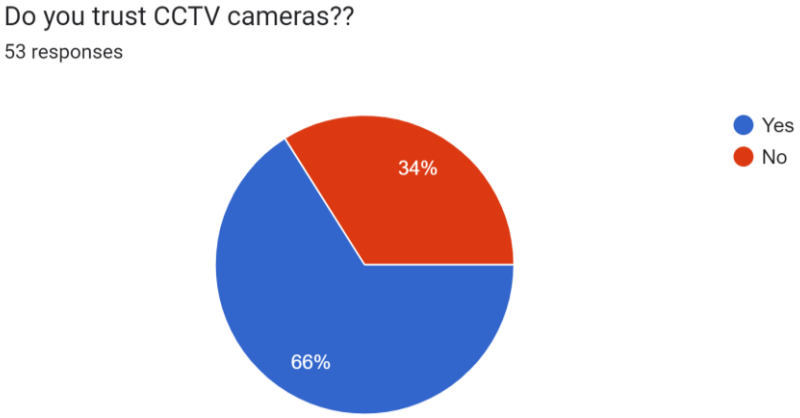

Figure 5

The final question is about people's trust in CCTV cameras and 66% of people trust CCTV while 34% do not have some confidence in CCTV.

IV. RESULT AND DISCUSSION

According to the analysis, 53 people gave their answers, out of which 81.1% of individuals are in cyberspace thanks to CCTV surveillance, which could be a sizable amount. Now, if 81.1% of individuals are under CCTV surveillance, then the reliability of CCTV should be a minimum of above 70%, but only 18.9% of individuals consider CCTV to be the foremost reliable, while 26.4% of individuals consider it only reliable and 32, 1% of individuals, which is that the largest column in Figure 2, find it neither reliable nor unreliable. 15.1% of individuals consider CCTV to be very unreliable and seven.5% of individuals only consider it unreliable. Now out of this integer, the Likert scale is slightly tilted towards people that find CCTV reliable. Now to work 3, 32.1% of individuals consider CCTV security to be Grade A and another 32.1% to be Grade B. But 18.9% of individuals consider it to be Grade D or least secure and 17% of individuals believe that CCTV has a security grade C. It appears that folks who consider CCTV as a secure device is over average, which explains that CCTV is secure for over the common and therefore the average number of individuals. However, Figure 4 tells us that 52.8% of individuals think that CCTV is hackable and 45.3% of individuals are unable to allow an accurate opinion about CCTV hacking. Figure 5 shows that 66% of individuals trust CCTV and only 34% of individuals don't trust CCTV. As these data show, people consider CCTV to own more security measures, and yet it's hackable, which implies that somewhere the protection features added to CCTV cameras aren't as reliable as they ought to be. And over average people consider CCTV as a trusted device, explaining that CCTV has security measures that are least trusted and have vulnerabilities, but CCTV is trusted and reliable.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

As the above discussion concludes, people trust CCTV cameras but the protection majors applied on CCTV don't seem to be the maximum amount trusted because it should be, so for that purpose awareness should be spread. Cameras are particularly troublesome which the general public should know after they are being watched by CCTV. ensuring that CCTV surveillance is disbursed overtly is merely a partial solution to the matter. it's also essential to confirm that the general public knows more about who is watching them and for what purposes. the problem, however, lies with deciding what proportion of information the general public needs and the way best to produce it while also ensuring that CCTV systems are ready to operate effectively and securely.[4] There should be something like "Watchdog agency". Ideally, this agency would be empowered to conduct random inspections of CCTV control rooms and required to publish regular, detailed reports on such things as operator targeting practices and therefore the use of data collected by CCTV. Furthermore, this "watchdog" agency would even be to blame for keeping the final public informed about how CCTV surveillance is being conducted, and guaranteeing that individuals aren't being subjected to unwarranted or unnecessary surveillance.[4] People should even be aware of how surveillance cameras are secured and what measures have gotten added to form them secure. Some basic security measures should be added to CCTV such as: -

1. Choose a router with Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access 2 (WPA2) security, which encrypts your data instead use the secured network for CCTV.

2. Enable your camera's built-in firewall, which monitors and controls information coming to and from the camera. Instructions for doing so are going to be included together with your cameras.

3. Protect your cameras with a robust password. If your cameras include default passwords, change them immediately.

4. Change the password for the CCTV camera frequently.

5. Protect your Wi-Fi router with a powerful password (different from those for your cameras).

6. Activate two-factor authentication if it's offered.

7. Keep your camera's firmware up to now.

And after adding security measures, the info about this could even be published publically so it'll make them secure about their privacy. These are some staple items but another technique might be wont to enhance the safety of CCTV. Pavel Korshunov has developed and method for privacy protection in video surveillance using warping[5] which might enhance the security of CCTV.

V. CONCLUSION

By all counts and with proven results, we can conclude that CCTV are trusted devices which are with least security measures and with less awareness about security build in it. The security measures provided in IV. Result and Discussion will be applied to make it more secured and enhance it's trustworthiness. People should also make aware about their data captured by CCTV is being safe and not getting misused.

ACKNOWLEDGEMENT

I would like to express my gratitude to my advisory Prof. Swapna Nikale who has given me opportunity to publish the research paper as a part of curricular activity. I would also like to thank my friends, my parents and all other supporters who has supported and encouraged me and helped me during this research work.

VI. REFERENCES

[1] H. Turtiainen, A. Costin, T. Lahtinen, L. Sintonen, and T. Hamalainen, "Towards large-scale, automated, accurate detection of CCTV camera objects using computer vision. Applications and implications for privacy, safety, and cybersecurity. (Preprint)." arXiv, Aug. 20, 2021. Accessed: Jul. 31, 2022. [Online]. Available: http://arxiv.org/abs/2006.03870

[2] E. L. Piza, B. C. Welsh, D. P. Farrington, and A. L. Thomas, "CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis," Criminol. Public Policy, vol. 18, no. 1, pp. 135–159, Feb. 2019, doi: 10.1111/1745-9133.12419.

[3] A. A. Ahmed and M. Echi, "Hawk-Eye: An AI-Powered Threat Detector for Intelligent Surveillance Cameras," IEEE Access, vol. 9, pp. 63283–63293, 2021, doi: 10.1109/ACCESS.2021.3074319.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

[4] B. J. Goold, "Privacy rights and public spaces: CCTV and the problem of the 'unobservable observer,'" Crim. Justice Ethics, vol. 21, no. 1, pp. 21–27, Jan. 2002, doi: 10.1080/0731129X.2002.9992113.

[5] P. Korshunov and T. Ebrahimi, "Using warping for privacy protection in video surveillance," in 2013 18th International Conference on Digital Signal Processing (DSP), Fira, Santorini, Greece, Jul. 2013, pp. 1–6. doi: 10.1109/ICDSP.2013.6622791.