International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

AI In Surveillance System

Suyash Deshmukh

Ashish Saji

Keraleeya Samajam's Model College, Dombivli East, Mumbai, Maharashtra, India

***Abstract*— Artificial intelligence and its social and ethical implications are complex and subject to contradictory interpretations. While AI has applications across many industries, one area where it is widely used is in AI surveillance and facial recognition technology to fight crime. In 2019, at least seventy-five countries around the world were actively using artificial intelligence technologies for surveillance purposes, including smart city/safe city platforms, facial recognition systems, and smart policing initiatives. However, the widespread use of artificial intelligence in the name of fighting crime comes at a price; A number of ethical issues have surfaced in recent times that challenge the feasibility of enforcing AI technology to fight crime. In the field of artificial intelligence, this research is carried out by, among others thematic modeling analysis of scientific research on the concept of monitoring. This study adds to the body insights into AI ethics focusing on controversial aspects of AI monitoring.**

***Keywords*— Road rage, driving, offense, aggressive**

INTRODUCTION

Artificial intelligence has had a significant impact on civilization, both in the form of machine learning algorithms and models, and in the form of robots and autonomous systems. Improved tracking and tracing is one of the most important applications of AI. According to the Global Surveillance Index (GSI), at least 75 out of 176 countries in the world are actively investing in and using artificial intelligence (AI) for surveillance purposes, mainly in smart cities, facial recognition and smart fonts. Governments, in collaboration with tech companies, have integrated AI into cameras, video management software, and mobile phones, and standardized biometric surveillance in pandemic control like the current global COVID pandemic. Chinese and American tech companies are the world's leading providers of artificial intelligence (AI) surveillance technologies, according to the GS Index. However, the incorporation of AI-powered surveillance technologies has changed the game, spurring effective action across sectors including healthcare, transportation and manufacturing. Others denounce AI-based surveillance technologies for their unexpected or intentional harmful effects, particularly on citizens' lives, and for their potential to support undemocratic politics and violations of privacy and human rights. Research expresses outrage at human rights abuses by governments using surveillance technology to manage the pandemic.

As global concerns mount over the battle between digital authoritarianism and liberal democracy, academic researchers from all walks of life are harnessing different dimensions of AI for surveillance; as there are conflicting and confusing views on the impact of AI on surveillance. While some studies only focus on the positive effects of AI on surveillance, others highlight the negative aspects of AI on surveillance.

TYPES OF AI SUPPLIERS

There are three types of services to consider when implementing AI in a security system - Video Management Systems (VMS), AI cameras, and AI systems.

1) *Video Management Systems (VMS)*:

Video management systems are the "command center" of an organization's surveillance system and, in many cases, the center of their security approach. When an organization wants to upgrade their VMS, there are several vendors to choose from, some focusing solely on the needs of the VMS and others acting as a full vendor covering all aspects of the security system. A growing number of VMS providers have AI capabilities, and some even offer real-time alerts such as vehicle tracking. Using AI in a VMS system also gives a company the benefit of leveraging these AI capabilities with videos stored in the system. This means that the organization can look back.

Things to consider before working with a VMS provider :–

- VMS can be deployed to on-premises and cloud providers. Note that some providers claim to work in the cloud but still require local hardware, can compress videos significantly, or delay downloads up to off-peak times.

- Some vendors may require the organization to use vendor cameras, which may become unusable if the organization decides to switch vendors. While the VMS provider may be able to work with existing cameras, not all cameras may be compatible.
- To ensure your VMS stays current with the latest AI developments, consider vendors that use an open integration platform. This allows you to integrate the best AI solutions into your existing VMS without upgrading your hardware.

2) *AI cameras* :

Standalone AI cameras are basically IP cameras with AI processing in the camera itself. Closed Circuit Television (CCTV), commonly used in large cities, is a good example of how these cameras work. AI cameras can be a good choice for specific locations and real-time AI detection functions (e.g. license plates or traffic tracking).Camera-level processing is usually limited, so detection options can be limited to very specific tasks or large objects such as people or vehicles. Cameras with built-in AI capabilities are more expensive than cameras without AI, so they may not be the best choice for businesses that need to host multiple security cameras. The use of AI cameras also means that all current surveillance cameras must be removed and replaced, resulting in the installation of additional equipment and disruption to the facility.

Things to Consider Before Choosing AI Cameras :-

- Many AI cameras have additional SaaS fees that users must pay to implement AI functionality in the cameras.
- Some vendors may require an organization to charge SaaS fees for camera operations even if the organization stops using AI capabilities. Failure to follow this recommendation may render the cameras unusable.

3) *AI systems* :

The AI system integrates with your existing surveillance system and network to analyze video feeds in real time. These systems are separate from the cameras and VMS but integrated with these and other security systems. Typically, AI systems require an edge device to process the large amounts of data required by the AI, but allow multiple cameras to harness the power of the AI simultaneously. AI systems do not typically store video as most organizations use their own VMS or NVR to perform this task. AI systems typically monitor camera footage in real-time and are generally unable to perform post-analysis of archived recordings.

Things to consider before choosing an AI system :-

- AI systems may not be compatible with all being cameras(e.g. analog cameras or cheap cameras that don't support ONVIF).
- Some AI systems claim to be “cloud-based”, but this usually refers to their online applications as opposed to their real system. Given the size of the video data and the need for real-time processing, most (if not all) AI systems require a device or peripheral as bandwidth requirements in the cloud are too high.

ETHICAL CONCERNS OF AI SURVEILLANCE

Thanks to new research on artificial intelligence, facial recognition technology is more popular than ever. However, it is not always accurate in its conclusions. According to a recent study in the National Institute of Standards and Technology (NIST) Journal of Research, facial recognition software exhibits some race, age, and gender biases. Patrick Grother, computer scientist at NIST, conducted this unique study. Grother and his team evaluated 189 software algorithms from 99, developers to measure whether those algorithms exhibit demographic differences, a term that measures whether an algorithm's ability to match images varies across demographics (NIST 2019). Based on four photo collections with 18.27 million photos of 8.49 million people provided by various government agencies, the team evaluated the ability of these algorithms to match demographic data. The results were amazing; Although imprecision varied from algorithm to algorithm, most showed demographic differences. Specifically, Grother points out that Asian, African American, and Native American groups are 10 to 100 times more likely to be misidentified than Caucasians. In addition, algorithms also have difficulty distinguishing females from males and the elderly from middle-aged adults (NIST 2019; Grother, Ngan & Hanaoka 2019).These results are critical as they reveal vulnerabilities in facial recognition systems that make these technologies difficult to implement securely. "An incorrect match can lead to delayed flights, lengthy interrogations, a checklist, tense police meetings, false arrests, or worse," said Jay Stanley, an analyst with the American Civil Liberties Union (Stanley in Singer and Metz, 2019). The reality of widespread demographic diversity regarding AI's inherently discriminatory facial recognition systems remains a priority ethical issue to be addressed.

Unfortunately, prejudice in facial recognition technology has already led to injustices in the United States. The earliest known example of this is the case of Robert William, an African-American man who was arrested after a facial recognition system incorrectly linked his photo to a thief (Porter 2020). In the end Williams was shot dead, his fingerprints and DNA taken and held overnight (Porter 2020). When the detective showed the image from the surveillance video, William said, "No, it's not me, do you think all black people look the same?" (Hügel 2020). While William was

released, his experience was traumatic and those around him, including his five-year-old daughter, were never allowed to see him being handcuffed and taken away (Porter 2020). Robert Williams' story is a powerful testament to the damage that flawed facial recognition technology can do to society.

EVALUATION OF POSSIBLE SOLUTIONS

AI solutions are not one-size-fits-all, and an organization should determine what is most important based on its needs and defined risk profile.

For example, if using artificial intelligence to search historical documents is more important than real time threat detection, upgraded VMS solutions may be the best choice for your organization. Actual and promised costs, disruptions, and opportunities are also obvious considerations, and it's often best for a company to test a solution before fully committing. If the supplier is confident in their product, they should offer an on-site trial period to assess their capabilities. This is particularly important given AI is a fleetly evolving assiduity without clear quality norms.

1) *Think incredulous :*

- It's easy to make everything look good in a demo environment. The real test is to see if the AI works in the organization's specific environment.
- Ask questions and make sure everything meets the needs of your business, and then ask vendors how their capabilities meet those needs.

2) *Set realistic expectations for realistic AI solutions :*

- Artificial intelligence isn't equal to mortal intelligence. For illustration, an AI can tell you if a person is there, but it can not tell you if that person is allowed to be there.
- AI platforms can be fooled, but the more real operations the AI platform has to learn, the less foolable it can be.
- Real recordings from surveillance cameras are important to further develop AI platforms for deep learning, including in test phases.
- All AI will have bugs. The important thing is to make sure that the AI you choose can correct them in time.

3) *Channel Matters :*

- Some AI vendors sell directly to organizations. There are pros and cons to this approach, but it's important to realize that AI solutions cannot exist in a vacuum. Selected vendors must have a thorough understanding of the organization's overall security posture and the many different systems in use.
- Some vendors use AI to sell major system upgrades. In addition to focusing less on the nuances of AI, these vendors are encouraged to encourage potentially unnecessary and expensive upgrades.
- Other AI vendors offer their services through resellers who have a more comprehensive suite of security solutions. These channel partners also have experience integrating various systems, including integrating AI with other existing systems as part of an organization's broader security strategy.

BENEFITS OF AI

While it is of paramount importance to address the ethical issues surrounding integrating AI into the fight against crime, it is also necessary to acknowledge some of the benefits that AI brings. According to the Oliver Wyman Risk Journal, AI is being used to detect crimes such as employee theft, online fraud, false billing, money laundering and terrorist financing. These AI applications have triumphed in the fight against financial crime. Banks in particular have reduced false positives by 50%, and have had success using AI-based tools to track down criminals. In addition, the range of uses of AI is almost unlimited when used correctly. Future applications include detection and tracking of illegal goods, terrorist activity and human trafficking.

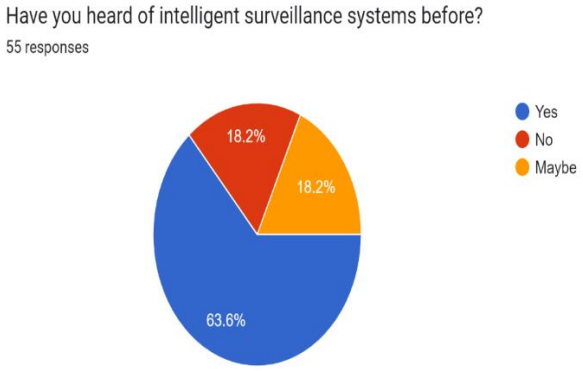
RESEARCH METHDOLOGY

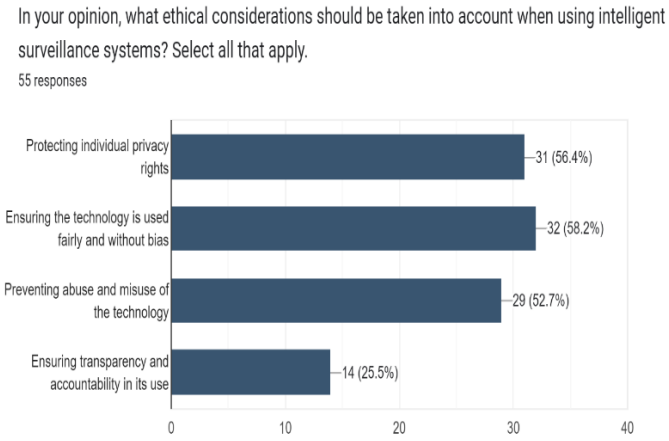
HYBRID MODEL

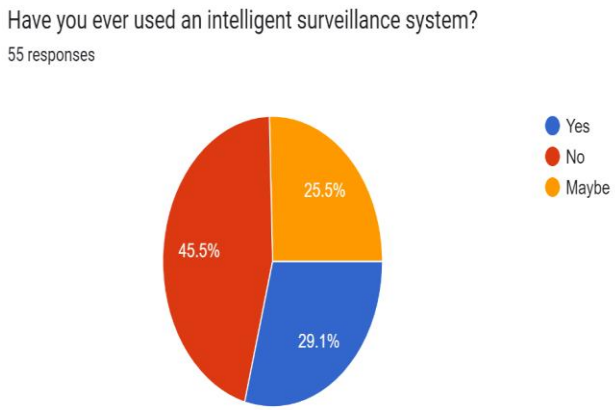
A model may include both descriptive and analytical components. A descriptive model's logical relationships can be examined, and conclusions can be drawn to reason about the system. Nonetheless, logical analysis yields quite different conclusions than a quantitative chemical investigation of system properties.

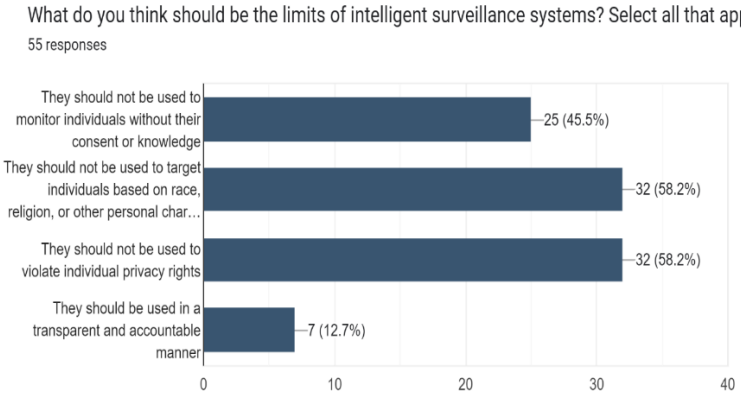
We first conducted a poll of people utilizing an online form creator and data collection service to acquire information regarding people's awareness.

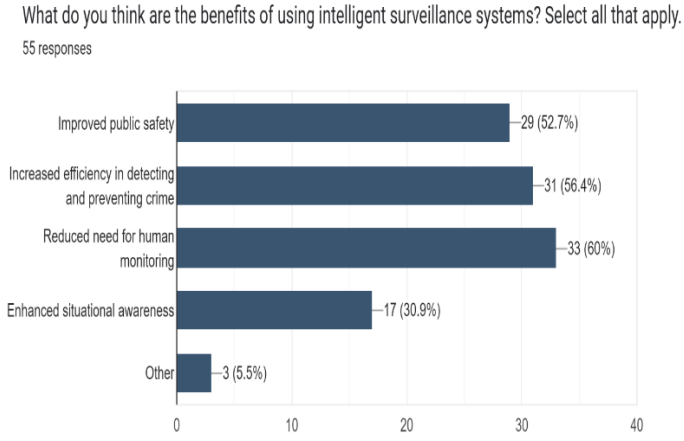
SURVEY RESULTS





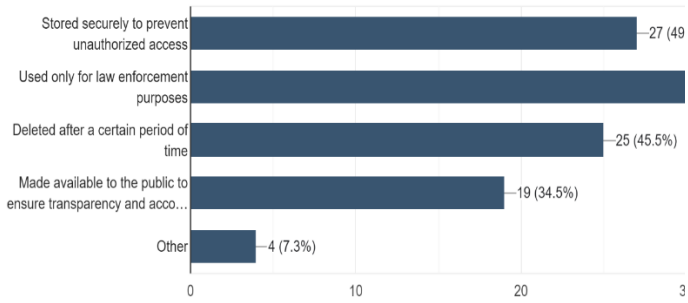






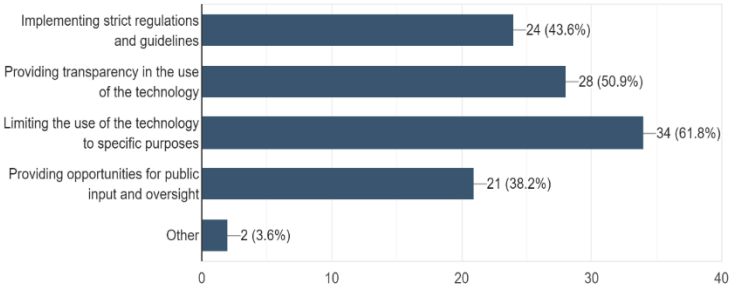
How do you think the data collected by intelligent surveillance systems should be stored ar responsibly? Select all that apply.

55 responses



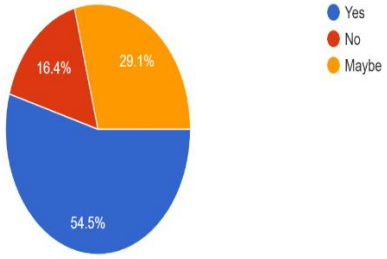
What steps do you think can be taken to address concerns about privacy and civil liberties in relation to the use of intelligent surveillance systems? Select all that apply.

55 responses



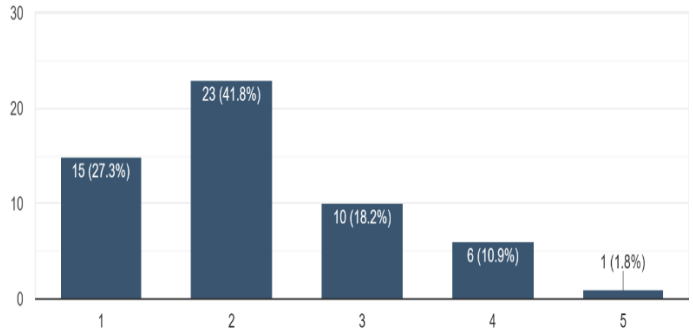
Do you think that the use of intelligent surveillance systems should be regulated by law?

55 responses



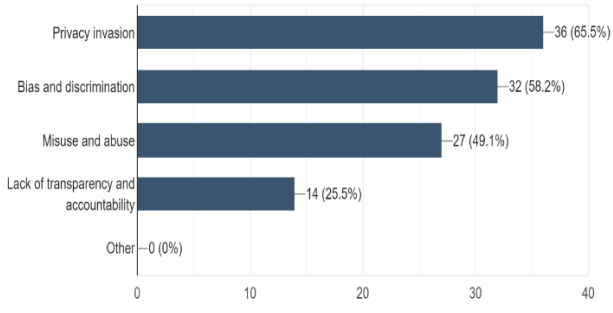
How concerned are you about the ethical implications of AI intelligent surveillance systems?

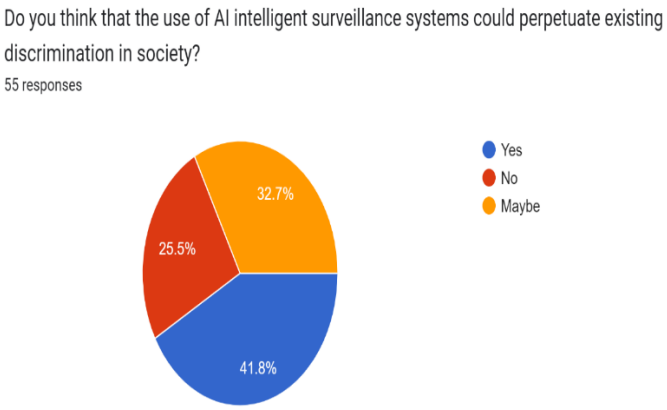
55 responses

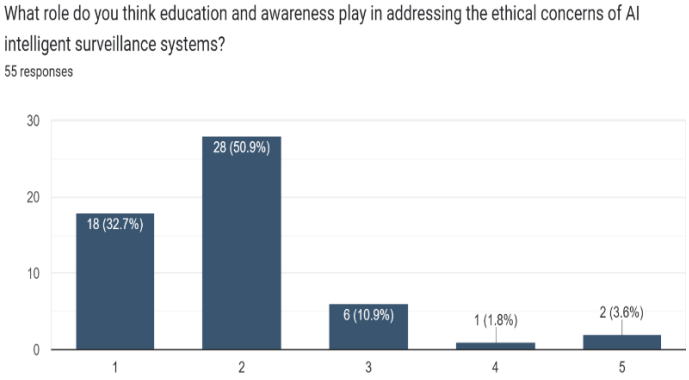


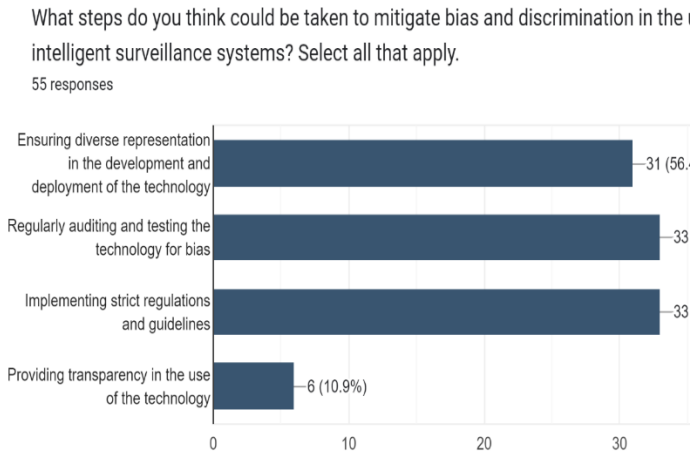
Which of the following ethical concerns do you think are most important to consider when using AI intelligent surveillance systems? Select all that apply.

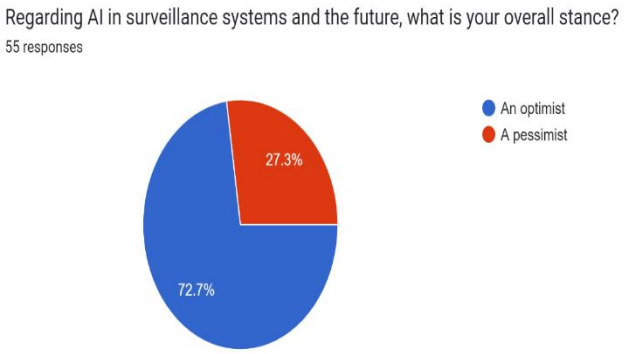
55 responses

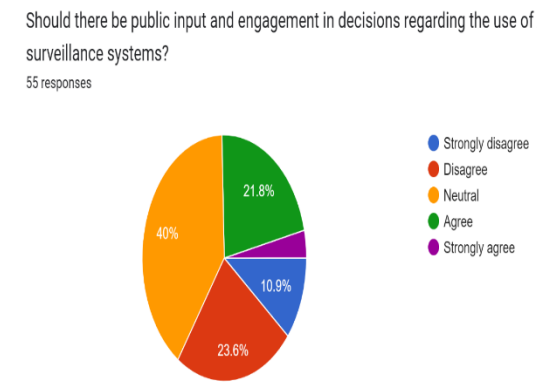












HYPOTHESIS TESTING

Hypothesis testing is a sort of statistical reasoning that includes analyzing data from a sample to derive inferences about a population parameter or probability distribution. First, a hypothesis is created regarding the parameter or distribution. This is known as the null hypothesis, abbreviated as H0. After that, an alternative hypothesis (denoted Ha) is defined, which is the polar opposite of the null hypothesis. Using sample data, the hypothesis-testing technique determines whether or not H0 may be rejected. The statistical conclusion is that the alternative hypothesis Ha is true if H0 is rejected.

For this paper,

Null hypothesis (H0): Ethical concern of AI Surveillance can not be mitigate.

Alternative hypothesis (Ha): Ethical concern of AI Surveillance can be mitigate.

TEST (STATISTICS)

There are 3 tests available to determine if null hypothesis is to be rejected or not. They are:

1. Chi-squared test

2. T-student test (T-test)
3. Fisher's Z test.

For this paper, we will be using a 2 tailed T-student test.

A t-test is an inferential statistic that determine if there is a significant difference in the means of two groups that are related in some manner.

- *Level Of Significance:* The chance of rejecting the null hypothesis when it is true is the significance level (also known as alpha or α). A significance level of 0.05, for example, means there's a 5% probability of discovering a difference when there isn't one. Lower significance level indicate that more evidence is required to reject the null hypothesis.
- *Level of confidence:* The confidence level indicates that probability that the location of a statistical parameters (such as the arithmetic mean) measured in a sample survey is also true for the entire population.

Sr. No.	Data
1	63
2	45
3	33
4	32
5	32
6	30
7	54
8	34
9	23
10	36
11	41
12	33
13	40
14	28
15	72
Mean (x)	39
Standard Deviation (s)	13.12740983168

Level of Significance = 0.05 i.e., 5%

Level of Confidence = 95%

A t-score (t-value) is the number of standard deviations away from the t-mean. distribution.

The formula to find t-score is:

$t = (x- \mu) / (s/\sqrt{n})$

where x is the sample mean,

μ is the hypothesized mean,

s is the sample standard deviation,

and n is the sample size.

The p-value, also known as the probability value, indicates how probable your data is to have happened under the null hypothesis. Once we know the value of t, we can find the corresponding p-value. If the p-value is less than some alpha level (common choices are .01, .05, and .10) then we can reject the null hypothesis and conclude that smart devices are not secure and cannot be trusted with our privacy.

Calculating t-value:

Step 1: Determine what the null and alternative hypotheses are.

Null hypothesis (H0): Ethical concern of AI Surveillance can not be mitigate.

Alternative hypothesis (Ha): Ethical concern of AI Surveillance can be mitigate.

Step 2: Find the test statistic.

In this case, the hypothesized mean value is considered 0.

$t = (x-\mu) / (s/\sqrt{n}) = (39-0) / (13.12740983168/\sqrt{15})$

$= 11.12$

t-value = 11.12

Step 3: Calculate the test statistic's p-value.

The t-Distribution table with n-1 degrees of freedom is used to calculate the p-value. In this paper, the sample size is n=15, so n-15= 14.

By plugging the observed value in the calculator, it returns p-value. In this case the p-value returned is less than 0.0001.

Since this p-value is less than our chosen alpha level of 0.05, we reject the null hypothesis. Thus, we have sufficient evidence to say that Ethical concern of AI Surveillance can be mitigate.

CONCLUSION

The ethics surrounding the use of AI technology to fight crime will remain a critical issue for academics, government agencies, and the general public. While AI has the potential to fight crime and make citizens around the world safer, it is undeniable that there are ethical concerns about using AI to fight crime. Key issues include the abuse of AI surveillance by totalitarian regimes and the use of fundamentally flawed facial recognition systems by every government. Several policies have been released in recent years in response to emerging concerns about AI technology. Ultimately, as AI becomes a gatekeeper technology, humanity can choose which direction to take, whether it is exponential advances in human well-being or significant risk potential. Increasing integration of AI around the world inevitably leads to serious ethical issues, but if leaders and researchers are willing to take action against unethical behavior and follow the right guidelines, AI could be an invincible force on the road to a better tomorrow.

REFERENCES

[1] Saheb, T. "Ethically contentious aspects of artificial intelligence surveillance: a social science perspective". *AI Ethics* (2022). https://doi.org/10.1007/s43681-022-00196-y

[2] Bohai L. "Ethical Concerns of Combating Crimes with AI Surveillance and Facial Recognition Technology". Towards Data Science (2021). https://towardsdatascience.com/ethical-concerns-of-combating-crimes-with-artificial-intelligence-surveillance-and-facial-a5eb7a09abb1

[3] Porter, J. (2020, June 24). A black man was wrongfully arrested because offacialrecognition. *TheVerge*. https://www.theverge.com/2020/6/24/21301759/facial-recognition-detroit-police-wrongful-arrest-robert-williams-artificial-intelligence

[4] IntelliSee. "WHICH AI-ENABLED SURVEILLANCE SYSTEM IS RIGHT FOR YOU?" https://intellisee.com/which-ai-enabled-surveillance-system-is-right-for-your-organization/

[5] Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. *The Alan Turing Institute*. https://doi.org/10.5281/zenodo.3240529

[6] Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test (FRVT) part 3: Demographic effects. *The Journal of Research of the National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.IR.8280

[7] Almeida, D., Shmarko, K., Lomas, E.: The ethics of facial recog nition technologies, surveillance, and accountability in an age of artifcial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI Ethics 2021, 1–11 (2021). https://doi.org/10.1007/S43681-021-00077-W