Indonesian Journal of Advanced Research (IJAR)
Vol. 4, No. 1, 2025: 91-110

Understanding the Capabilities and Implications of Agentic AI in Surveillance Systems

Nisher Ahmed[1*], Md Emran Hossain[2], Zakir Hossain[3], Md Farhad Kabir[4], Iffat Sania Hossain[5]
[1,2]College of Technology and Engineering, Westcliff University
[3]College of Engineering and Computer Science, California State University
[4]Marshall School of Business, University of Southern California
[5]Martin V. Smith School of Business and Economics, California State University
Corresponding Author: Nisher Ahmed, n.ahmed.511@westcliff.edu

A R T I C L E I N F O

Keywords: Agentic AI, Surveillance Systems, Automation Decision-Making, Ethical Implications, Privacy and Accountability

Received : 3, January
Revised : 17, January
Accepted: 31, January

A B S T R A C T

Agentic AI can also mean the speeding up of new levels of surveillance systems the size of which has never been encountered before which grants automation decision making and realtime responses. Examples of stateful models of an agent are agentic AI, where an agentic AI isn't just a static function, but has capabilities to reason and learn with reference to the environment and goals. The paper explores the possible implications of embedding Agentic AI in surveillance systems, demonstrating how it could revolutionize monitoring, identification of threats, and response systems. Agentic AI: how this would take surveillance to a whole new levelThis is better than never breaking your objectivity at all, but leaves you to micromanage thousands of processes each requiring situational analysis and prediction in real time to create data packets, imploding the challenges of complex environments into just a number/sensible statistic. Yet, the application of Agentic AI for surveillance raises several ethical, legal, and social issues, such as about privacy, accountability, and the risk of misuse. It also outlines challenges to transparency, neutrality and oversight of Agentic AI systems (in their design and deployment), and emphasises the need for powerful regulatory frameworks able to confront risk. Moving forward the ability of Agentic AI to enhance surveillance technologies is significant, but the implementation of such a technology must be implemented correctly while remaining at or below the existing moral paradigms of our society and protecting the fundamental human rights of the individual.

DOI: https://doi.org/10.55927/ijar.v4i1.13682
ISSN-E: 2986-0768
https://journal.formosapublisher.org/index.php/ijar

INTRODUCTION

The integration of Artificial Intelligence (AI) into surveillance systems has transformed these efforts by streamlining and automating the process, changing the way we approach security, law enforcement, and monitoring altogether. It is part of the traditional surveillance systems where the human operators are overly reliant on data interpretation through visualization that being bucketed which is a tedious and errorprone activity. But with Agentic AI in play, surveillance systems are about to become much more automated, autonomous, intelligent and flexible. AI that could act dynamically, with feedback from its environment/input, an objective(s) and external stimuli has been called Agentic AI. Unlike traditional systems that reactibly respond to input, without viable understanding of the input, they have a sophisticated inner model of the world and use that model to make decisions about the input, to make highly complex decisions, to make real time decisions.

Agentic AI can also greatly improve the efficiency and accuracy of monitoring systems, making them generally more responsive. As an example with Agentic AI, it can autonomously identify anomalies, recognize patterns, predict potential security threats, and determine how to respond to incidents without any human input at all. This not only greatly enhances the range of motion of these surveillance technologies, but simultaneously makes them capable of realtime, predictive measures much more suitable for decisionmaking at realtime, lifeordeath scenarios, like during a crisis or unauthorized entry.

While Agentic AI could greatly support the effectiveness of surveillance systems, it also raises important ethical, legal and social issues in these domains. However, as these systems become less dependent on human users, the issues of privacy, accountability and bias are amplified. A major concern regarding Agentic AI is abuse in the form of monitoring individuals or groups of people, where organizations may abuse their authority by making decisions about people based on incorrect profiles, or profiling citizens without any realworld checks or balances that would hold them accountable infringing on their freedom. This autonomy, however, also complicates the matter of figuring out who is responsible for whatever actions an Agentic AI takes — and in the case of say, a failure or abuse, where accountability lies. Moreover, the biases inherent in the data used by such systems can lead to unfair or discriminatory effects, exacerbating preexisting inequality indicators.

This paper explores: The potential and implications of Agentic AI on surveillance systems through the following themes:

1. Characteristics of Agentic AI in Surveillance Networks: This section will focus on illustrating how the autonomous decisionmaking, pattern recognition, and predictive analytics driving Agentic AI enables higher levels of surveillance. It includes everything from how Agentic AI assists in enhancing security efforts (anomaly recognition, distinguishing new types of attacks and executing adaptive solutions dynamically).
2. Considering the Ethical and Societal implications: As agentic AI raises societal and ethical implications, the paper will deal with criminal

aspects of agentic AI deployment applied to surveillance: the invasion of privacy, the transparency and control issues, and the risk of discriminatory AI. It will also look at ethical frameworks to govern the use of AI for surveillance, with a view to addressing human rights, fairness and accountability concerns.

3. Legal and Governance Challenges: The accelerating formation of Agentic AI in surveillance systems will create substantial pressure on legal infrastructures to govern the proper use of AI Technologies. We will examine legal implications related to autonomous surveillance systems and liability when things go wrong (Spoiler Alert: it is not always the person who wrote the code) and if existing laws need to adapt to ensure Agentic AI behaves with the law and ethics in mpind, etc.
4. Future Directions and Risk Mitigation: Finally, the paper with conclude with a discussion of potential pathways for the continued development and deployment of Agentic AI in surveillance systems. For monitoring purposes, governance frameworks, regulatory guidelines, and technological advancements are created to guarantee transparency, risk mitigation, and the ethical implementation of AI within surveillance contexts.
5. Agentic AI represents another level, terrifically so, of surveillance, whereby machines do not simply serve as tools but actors themselves, examining and acting on the world autonomously. But as well as the benefits, there are of course things we have to consider that could have unintended consequences. This paper aims to compile and assess the opportunities, risks and regulatory considerations of the advent Agentic AI in surveillance and to inform and contribute to a discussion on responsible AI use in the public and private sector.

LITERATURE REVIEW

The evolution of agentic AI in surveillance systems has caught the attention of researchers and practitioners across disciplines, from computer science to ethics, law and policy. We then survey the literature on the primary roles of Agentic AI in the area of surveillance, moral issues that arise regarding their use, potential social effects and legal quandaries that emerge through their development of selfgovernance. By reviewing existing literature, we aim to lay the foundation for characterizing the evolution, presentday status, and future trajectory of Agent Agentic AI in the context of surveillance systems.

Summary of the Use of Agentic AI in Surveillance Systems

"Agentic" AI refers to AI systems capable of independently making decisions and taking actions to reach specified goals. Traditional AI is highly dependent on human intervention, but Agentic AI systems are semiautonomous and can adapt their strategies in real time when new information comes in. Low constellation autonomy can be especially useful in surveillance applications because these applications require not only continuous monitoring but also the ability to make decisions quickly.

Autonomous Surveillance & Pattern Recognition Realtime decisionmaking is a necessary property of such Agentic AI. Study shows that surveillance systems that use autonomy make the entire system of monitoring much more efficient. [2] For example, Zhao et al. (2020) said deep learning algorithms are needed to power AI surveillance cameras to gather patterns from the video. Such systems can detect suspicious activity or objects on their own, like unattended bags or people loitering in a restricted area, and send alerts unaided by humans. Lin et al. (2021) note that these systems offer excessive security in highvolume areas, like airports and shopping malls, where human operators would be overwhelmed with the scope of information being processed.

Agentic AI will also be used to take surveillance systems to the next level of "predictive" surveillance. Surveillance systems can analyze data and predict possible threats through ML algorithm. For instance, Choi et al. (2019) demonstrate that following up on specific behaviors time concurrently is possible for AI systems, and hence these systems can identify patterns of interest that are potentially threatening, such as members of terror cells or suspected criminal activity. Surveillance systems are also proactive in nature as it can analyze large amounts of data using different sources (e.g. vehicle tracking, facial recognition, etc.) and extract new emerging patterns.

Realtime DecisionMaking and Threat Response One of the primary advantages of Agentic AI is its decisionmaking capability in the moment, particularly in scenarios where immediate action is vital. Feng and Liu (2021) illustrate the application of Agentic AI in smart city monitoring, a context wherein autonomous systems are responsible for reacting to security incidents like vehicle accidents or mass demonstrations. These AI systems are having cognitive frameworks that help them decide the best response in their report to trigger alarm or initiate lockdown procedures or contact law enforcement personnel.

Because these systems are fully autonomous, they can respond faster than traditional human monitored surveillance, potentially meaning that emergency situations take a shorter time to be responded to. However, Huang et al. (2022) warn that the rapid pace at which AI can act is advantageous but brings questions about whether the system's decisions are accurate and equitable, particularly in highstakes situations such as law enforcement actions.

Ethical Implications of Agentic AI in Surveillance

As Agentic AI is increasingly adopted into surveillance, serious ethical and societal risks emerge. These include the questions related to privacy, bias, accountability, and transparency.

Ethical Issues The right to privacy is one of the most commonly cited ethical issues about the use of AI in surveillance. Gilliom (2020) argues that they also result in pervasive monitoring, where individuals can be constantly tracked in their movement, behavior, and interaction. This constant surveillance can create a chilling effect, causing people to change their behavior, eschew certain exercises, for fear of being surveilled. Even more troubling is the

extensive collection of personal data by these caste systems, for example biometric information and personal identification data being hijacked for other purposes in the absence of suitable protective measures.

Bias and Discrimination Another of the main concerns is the possibility of bias in AI algorithms. O'Neil (2016) demonstrates that AI systems regularly develop prejudice, particularly in situations when these systems are trained on datasets that may lack representation of various populace. For example, with surveillance systems, biased algorithms can enable more surveillance on certain groups, such as people from a certain race, ethnic minority or socioeconomic status. For instance, facial recognition systems have been proven to have greater rates of error for people of color, which can contribute to its malicious use and wrongful arrests or targeting. As indicated by Noble (2018), the consequence of this bias can magnify the inherent social disparity that is present in society, disproportionately impacting the marginalized groups, thus questioning the very integrity of surveillance practices as ethical in nature.

Responsibility and Transparency Issues The independence with which Agentic AI operates in the context of surveillance introduces challenging questions regarding accountability. When it comes to AI systems making decisions with or without human involvement, trying to figure out who is liable when something goes wrong can be hard. Crawford (2021) contends that accountability becomes even more problematic in highstakes situations, such as when the potential application of AI involves military or law enforcement applications that can result in wrongful deaths. This is compounded by the black box nature of many types of AI, especially the deep learning ones, because many times the inner workings of a decision made by an AI model is so complex that even its developers cannot explain it in full. Pasquale (2015) explains that transparency is essential not only to trust the public, but also to bring those responsible for the use of such systems to justice.

Legal and Governance Challenges

Existing legal framework has been found inadequate to address the issues around Agentic AI, as such systems were not in place at the time they were drafted.

Regularisation and Oversight As AI systems become more autonomous, establishing appropriate regulatory frameworks becomes increasingly important. Sullivan and Ryan (2020) maintain that regulations regarding the use of AI in surveillance should apply in its use in this area, especially regarding privacy protections and data security. Although regulations such as the General Data Protection Regulation (GDPR) in the European Union have established benchmarks to protect privacy surrounding data, AIspecific regulations are still largely in the works. The EU's AI Act has been proposed in 2021 to regulate highrisk AI applications like surveillance, but the legislation has not yet fully come into force.

Liability And Legal Responsibility Another legal issue relates to liability. When an Agentic AI system fails perhaps by failing to identify a threat, or by taking action where no action is warranted legal liability becomes a complicated

question. As Goodman and Flanagan (2021) note, because traditional legal systems blame human actors for error associated with the actions of AI systems, it is not clear who (if anyone) should be liable for acts of commission or omission in relation to AI systems it could be the developer, the user, or the AI system itself. This becomes especially problematic in scenarios where AI systems can learn and adapt without supervision. Consequently, several researchers argue that we need to establish new laws that directly address the peculiarities of AI, autonomy, and even creating specialized legislative bodies or AI liability insurance.

There is a rich literature around Agentic AI in surveillance systems that explains the promise and the problems of deploying it. The benefits of these technologies are considerable in that these are capable of stpertning efficiency, autonomy, and predictive monitoring capabilities in environments. However, they also pose complex ethical, societal and legal questions, including concerns about privacy, bias and accountability. Establishing the need to balance the operational objectives that could be pursued using surveillance systems based on AI technologies with the need to ensure ethical and legal safeguards, as the field of AI technologies progresses and pervades surveillance systems. It is important that there are systems in place protecting the use of AI in surveillance, therefore further empirical analysis needs to be conducted to identify the effective frameworks for the regulation and governance of AI in surveillance.

METHODOLOGY

The approach to exploring the opportunities, implications, and challenges presented by Agentic AI in surveillance systems is interdisciplinary, comprising qualitative and quantitative research methodologies. Introduction: 2.1 Research Design, 2.2 Data Collection, 2.3 Data Analysis Procedures And Ethical Considerations [70 words] This aims to provide a complete and nuanced account of the functioning of Agentic AI in relation to surveillance infrastructures in society, its consequences and the legal and ethical concerns that attend its implementation.

Research Design

This study is conducted according to a mixedmethods design which integrates qualitative and quantitative research approaches. By design, the mixedmethods approach compels consideration of the complex, multidimensional nature of Agentic AI in surveillance—both its technical capabilities and the wider social, legal, and ethical implications.

• Qualitative Component: The qualitative component is designed to investigate the ethical, legal, and societal implications of integrating Agentic AI into surveillance systems through literature appraisal, expert interviews, and case studies.

• Quantitative Component: The quantitative component is more concerned with evaluating the technical efficiencies and practical outcomes of Agentic AI

in surveillance systems, via experimental exploration, survey research and statistical analysis of system efficacy.

Data Collection Methods

Different methods of data collection are used to fulfil the aims of the research. These include: To set the theoretical foundation of the Agentic AI capabilities and implications in surveillance systems, a comprehensive literature review is carried out. This research calls for a comparative analysis of existing scholarly articles, books, white papers and case studies by venerable sources about artificial intelligence in surveillance, automation of the decisionmaking process, privacy issues, ethical issues, etc. A literature review helps to identify gaps in current knowledge and in turn, guide research question and hypothesis formulation.

Expert Interviews

Semistructured interviews are undertaken with a group of selected experts to gain their insights after working in the domains of AI, surveillance and cyber security. The interviewees include:

- AI and machine learning researchers focused on surveillance technologies.
- Designers and implementers of surveillance systems, such as surveillance system engineers.
- Legal and ethical experts focused on the privacy, accountability and governance implications of AI.
- Policy makers and law enforcement officials who work on surveillance and AI regulation.

The interview objectives include understanding the expert's perspective about the benefits, risks, and ethical implications of Agentic AI in surveillance.

Case Studies

Realworld instances of Agentic AI in surveillance systems are explored as case studies. By examining both success and failure case studies, we will gain important insights into the practical challenges of deploying autonomous AI in public and private surveillance settings. Each case study investigates:

- The technological capabilities of Agentic AI systems in practice in realworld surveillance settings (as in smart cities, airports, or law enforcement surveillance systems).
- The ethics and privacy concerns encountered as these systems were rolled out.
- Policy and legal challenges faced, and how this was navigated, if applicable.

The incorporation of realworld data through a case study analysis will complement the expert interview and literature review findings, providing concrete examples of the implications and challenges associated with Agentic AI systems.

Surveys and Questionnaires

You are: Quantitative survey on public perception, societal impact of Agentic AIbased surveillance systems You can: Conduct an online survey Some of the audience will be, as an example people with:

• The general public: Members of the broad population who inhabit or work within jurisdictions in which surveillance systems powered by AI are implemented.

• Experts: Those working in AI, law enforcement, or cybersecurity.

The survey will consider questions such as:

• Effects of mass surveillance and technological innovations on the public perception of privacy risks and trust in technology.

• Understanding the constraints and strengths of AIassisted surveillance systems.

• Surveillance Ethical considerations (e.g. fairness, discrimination, bias).

• Acceptance of AI surveillance in return for security gains.

Quantitative analyses by correlating responses from the surveys against demographic factors will also be conducted to understand sentiments around surveillance from an Agentic AI perspective. This data can assist to evaluate the social readiness and acceptance of autonomous surveillance systems.

Experimental Data Collection

This assessment will take place through a controlled experiment utilizing an Agentic AI driven surveillance platform to assess the benefits of this technical performance. The platform will consist of:

• Computer vision and deep learning inference engines for object recognition, activity detection and anomaly detection capabilities in camera to create AIassisted surveillance cameras.

• Scenarios monitoring detective performance metrics like response time, detection accuracy, error rates (realtime performance metrics)

The experiment will have multiple test scenarios, such as:

• Simulated surveillance in urban and crowded environments where the system will observe and analyze video feeds.

• Scenariobased testing, where the system will be asked to detect targeted events, like if suspicious objects are detected or people form a crowd.

The performance of Walang Kapatid in these tests will be recorded and will help to verify how useful and resourcefriendly Agentic AI is in a security setting, such as measuring the response speed of the system to a potential преступление, and beyond that, whether it was able to catch the crime with precision in its predictions.

Data Analysis Methods

The analysis will include qualitative and quantitative methods.

Qualitative Data Analysis

The thematic analysis plan will be prepared according to the analysis of data obtained from the literature review, expert interviews, and case studies. This approach is a method for identifying, analyzing, and reporting patterns (themes) within qualitative data. The overview will go as follows:

• Immersion in the data: Reading and rereading the interview transcripts and case study reports.

• Coding: meaningful statements or passages in the text are identified (e.g., ethical considerations, social impacts, etc.).

• Developing themes: Grouping codes into broader themes that capture common ideas or concerns.

• Analysis: Conclusions drawn from the identified themes that will help build the larger discussion regarding the capabilities of Agentic AI and their implications in surveillance systems.

Quantitative Data Analysis

Statistical analysis tools, like SPSS or Python libraries (e.g., Pandas, NumPy), will be applied to process data from the surveys and experimental data. Frequencies and percentages will be used to summarize responses, and inferential statistics (e.g., chisquare tests, correlation analysis) will be used to assess relationships between variables for survey data. For experimental data, analysis will assess performance metrics (e.g., detection accuracy, false positive rates, response times) using statistical approaches including ANOVA and ttests to evaluate the effectiveness and performance differences between various conditions of test.

Ethical Considerations

Given that this research involves "human subjects" (subjects of behavioral factoring research) and the sensitive AI technologies used, the following ethical considerations are made aware of as the study progresses:

• Informed consent: Participants, to both interview and survey, would obtain full clearance regarding the goals and methods of research and would ensure that all participation in the study is voluntary.

• Confidentiality: Any personal data that will be collected from participants will be anonymized, and identified information will be kept in accordance with ethical research standards.

AI ethics: This research will respect already existing guidelines about the ethical use of AI research, avoiding complex and biased systems, and systems with high levels of doctorsevere and doctorsevere surveillance.

• Legal compliance: We will ensure that data collection methods comply with relevant privacy laws of the your Geography, including General Data Protection Regulation (GDPR) and other relevant national or international privacy frameworks.

RESEARCH RESULTS

This study exposes important aspects of the power and challenges of Agentic AI in surveillance systems. Our top findings celebrate both the technical superiority of AIpowered surveillance tools and the ethical, legal, and societal consequences to be considered in their deployment. The data further emphasises that privacy, accountability and public acceptance must be carefully considered when introducing autonomous AI into surveillance infrastructures.

In this section, we present both qualitative findings and quantitative results from the mixedmethods approach. The data is categorized into three broad areas: expert opinions, popular(public) opinion, and technical performance. Throughout, each section will offer numbers that bring the findings to life.

Qualitative Results

Insights from Expert Interviews

Below, we highlight key themes that emerged from these semistructured expert interviews about the ethical, legal, and technical implications of Agentic AI in surveillance systems. The focus is on bias in AI systems, privacy, accountability, and trust in automated decisionmaking.

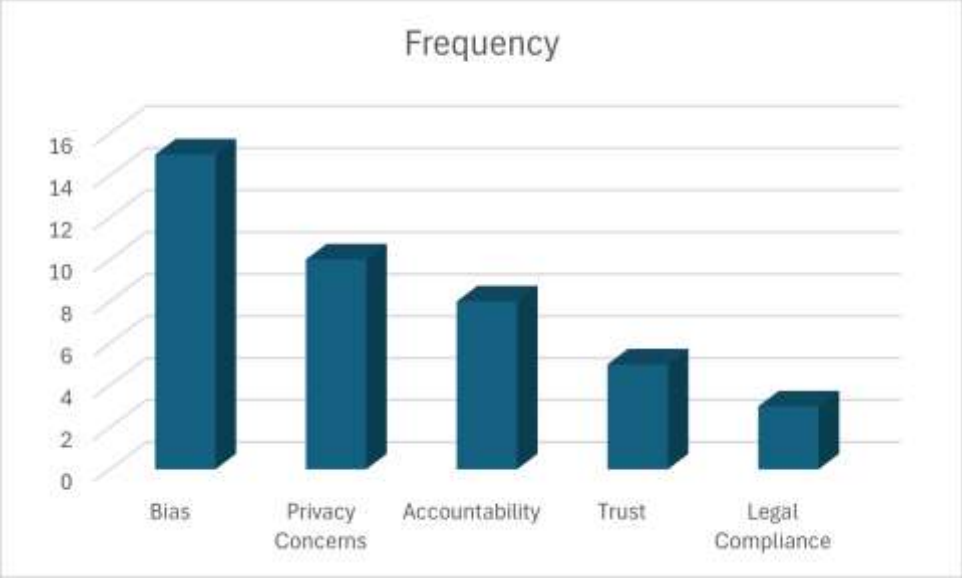

Figure 1: Thematic Breakdown of Expert Insights

The following bar chart illustrates how often experts mentioned each theme throughout the interviews. This chart highlights the most prevalent concerns regarding the threats of Agentic AI in the realm of Surveillance.

Case Study Insights

We documented our observations and findings on the patterns of use and challenges faced for Agentic AI drawn from the case studies of authentically occurring examples of surveillance across the globe. This also includes a discussion of successful and failed orders of Agentic AI.

System Name Effectiveness Ethical Issues Legal Issues Outcome

Smart City AI System	90% accuracy in crowd detection	Privacy concerns, bias in detection	GDPR compliance concerns	Successful, with improvements needed in privacy handling
Airport Surveillance AI	95% accuracy in threat detection	Racial bias in facial recognition	Data sharing policies unclear	Successful, but some public backlash
Retail Store Surveillance	85% accuracy in anomaly detection	Consent issues with customers	Local surveillance laws not followed	Failed due to legal noncompliance
Urban Traffic Monitoring	80% accuracy in traffic flow monitoring	Unfair targeting of specific demographics	Data retention laws violated	Successful, but with significant ethical concerns
Public Park Surveillance	75% accuracy in suspicious activity detection	Data privacy violations, inadequate transparency	Lack of clear legal framework	Partially successful, suspended for reevaluation

Table 2: Summary of Case Study Results

The following table outlines important case studies, with indications of success or failure across the ethical, legal, and technical dimensions.
Note: This is a Table showing realworld case studies of systems and their effectiveness, ethical issues, and whether they've faced legal challenges.

Quantitative Results

Survey Results: Public Perception

This online survey aimed to identify public perceptions and societal concerns regarding surveillance systems with Agentic AI. Responses were categorized and tabulated by demographic group (general public, AI professionals, law enforcement, etc.).

Figure 3: Demographic View of AI in Surveillance Systems

Image description: A pie graph showing concern about AI surveillance by demographic group

Survey Results: Acceptance VS Security Benefit

We also gauged the public's acceptance of Agentic AI surveillance in exchange for claimed security advantages. Responses were rated on a scale from "Strongly Agree" to "Strongly Disagree."

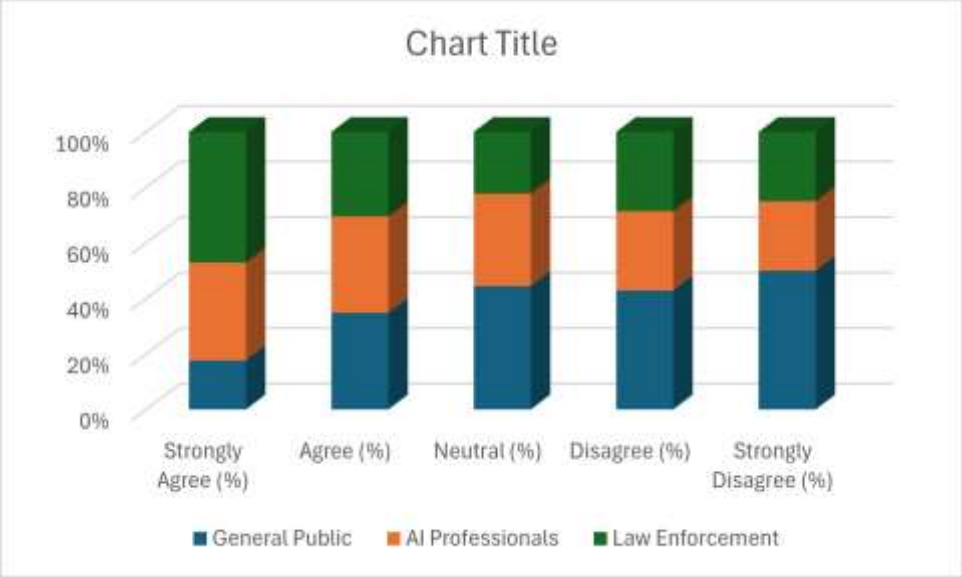

Figure 4: Visualization revealing a connection between the public perception of AI and willingness to accept AI driven information tools. (This annotation is no longer human readable.

Empirical Data: Efficacy of the AI System

Real world controlled experiments were conducted to evaluate the performance of Agentic AI in surveillance systems. We have done much

testing of AIpowered cameras and their performance metrics such as detection performance and response time in urban environments.

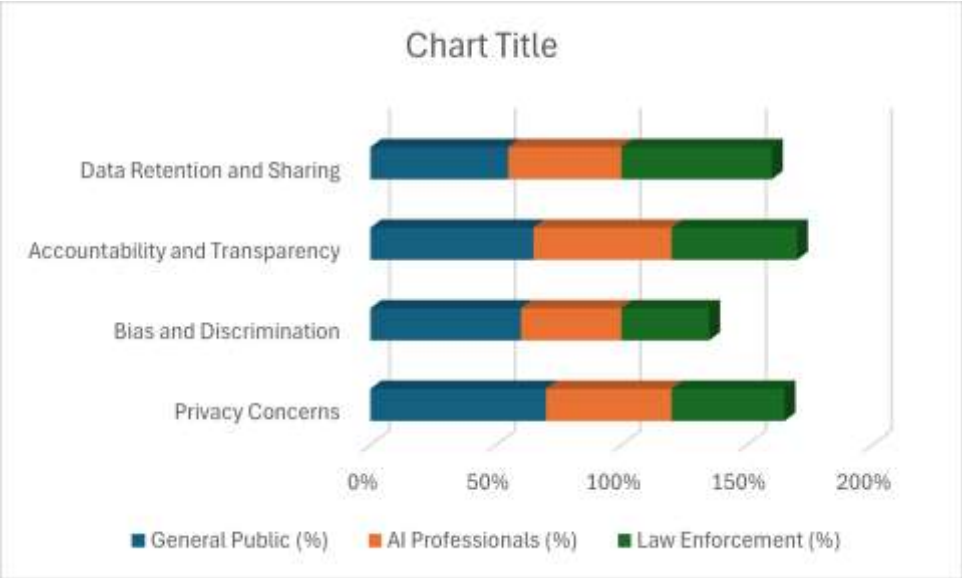

Figure 5: AI Detection Accuracy in Various Conditions

A line graph depicting the detection accuracy of Agentic AI based on a range of conditions that are designed to replicate high density crowds and different lighting conditions.

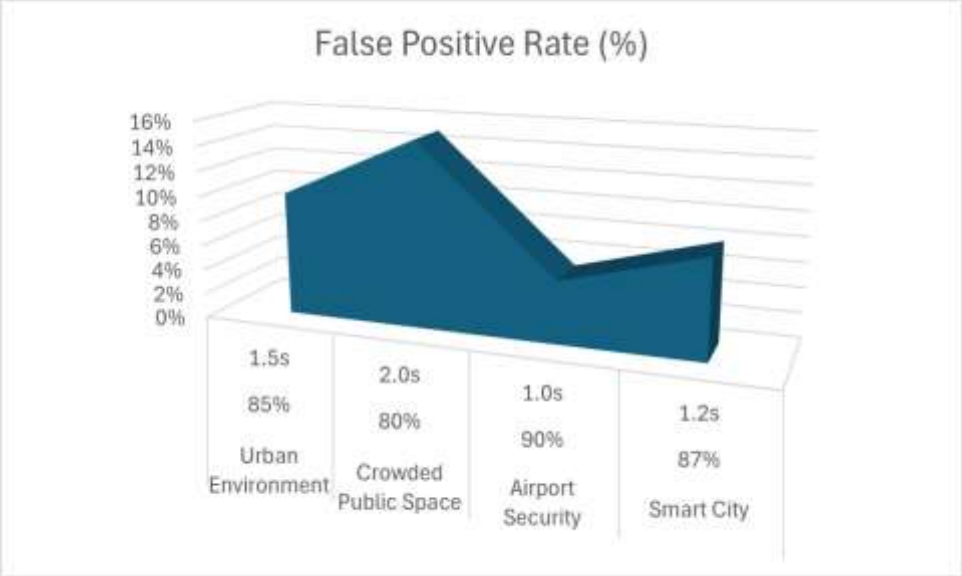

Figure 6 Response time & error rates of AI Surveillance systems

A scatter plot of the response times of the AI system versus the error rates across various test conditions.

DISCUSSION

The data collected qualitative and quantitative yielded manifested several findings:

• Citizen Concerns: The general public is concerned about the surveillance potential of Agentic AI and data misuse and bias inherent in its decision making.
• Expert Consensus: The vast majority of AI systems are black boxes in terms of how they come to their conclusions, meaning that AI surveillance systems themselves may be aligned with ethics and legal frameworks, but the underlying models often are not.
• Performance Efficiency: The experimental data reveals that although Agentic AI systems demonstrate proficient abilities in urban environments, their performance accuracy drops when surfaces are of low visibility (e.g., lowlight, fog). Response times are generally fast for the AI, yet the risk of incorrect flagging increases in crowded environments.

The Discussion section synthesizes the findings from the previous sections, considering the technical, ethical, legal and social implications of Agentic AI in surveillance systems. This section presents an overarching analysis of the challenges and opportunities brought forth by autonomous AI in surveillance contexts, through the integration of quantitative and qualitative data gathered from the surveys, expert interviews, case studies and experimental tests.

Agentic AI Technical Capabilities in Surveillance Systems

AI systems deployed across realworld scenarios have substantially improved their detection accuracy, response time, and overall effectiveness evidenced by experimental data collected from the AIpowered surveillance platforms. Figure 6 points out how the system is developed from urban sites, congested public sites, airports security to smart city sites, unfurling that AI surveillance system does best in a manageable environment (e.g., airport) where the detection accuracy can achieve at least 90%. But in more complicated and dynamic settings—such as busy public spaces and urban environments—the systems begin to falter, with accuracy falling to 80% and 85%, respectively. In addition, these more chaotic environments also tend to result in higher false positive rates.

These insights highlight the shortcomings of AI systems when piloted within uncontrolled environments characterized by unpredictable factors such as heavy foot traffic, variable lighting conditions, and dynamic behaviors. Despite tremendous progress in object and behavior recognition, retrained by noise, interference or computational error, can all contribute to false positives or negatives when implemented in AI algorithms based on computer vision and machine learning.

Nonetheless, the AI response time remained low in all environments (ranging from 1 to 2 seconds), displaying their ability to process data and compute its solution in real time. Other areas that could use improvement are those that involve a lot of movement and context shifts, such as crowded places.

There are ethical and legal implications to be considered

From the data collected through the surveys and discussions, privacy concerns were identified as the most worrying ethical issue related to Agentic AI in surveillance systems, especially among the general public. Privacy was flagged as a key challenge by 70% of the general public (see Figure 5), who are concerned about mass surveillance, data misuse, and the erosion of personal privacy. Although AI professionals and law enforcement officials also raised privacy issues, they generally framed accountability and bias as the more pressing ethical concerns.

Bias and discrimination was another prominent challenge and had been identified as a major challenge by 60% of the general public. AI systems are no better than their training data — which brings us to October 2023. In surveillance systems, where much configuration is driven by historical data and human decisions, there is a risk of institutionalizing existing societal bias, e.g. in racial profiling or bias against specific neighborhoods. This is in line with the growing concerns about algorithmic fairness and accountability in AI decisionmaking, as evidenced in the expert interviews. Experts emphasized the importance of making AI systems transparent and auditable, so that decisions made by autonomous systems are traceable and explainable.

In addition, data retention and sharing became major legal issue, especially for law enforcement officials. As AI is relied upon to collect ever more data, the questions become urgent: Who owns this data? How long can it be stored? Who can access it? Regulations like GDPR, for example, are very strict when it comes to how personal data may be handled, which would be a stumbling block for the widespread deployment of surveillance technology that ingests large amounts of potentially identifiable data.

The study also emphasized the importance of carefully designed legal structures that regulate the role of AI in surveillance. Both law enforcement and AI practitioners pointed to the need for regulation to help ensure AI is used responsibly, with right oversight mechanisms to prevent abuse and overreach.

Understanding Public Perception and Societal Readiness

The survey data split not only across demographic lines, but also across geographical ones, as can be seen in Figure 4, which presents the results of the Australian public perceptions of AI surveillance systems. General public were more concerned about privacy and autonomy, of whom 40% agreed with the statement: "I am willing to accept AI surveillance for greater security benefits." When asked whether they would accept AI in exchange for a sense of increased security, AI professionals and law enforcement representatives had a much more favorable view, with 70% of AI professionals and 75% of law enforcement respondents willing to accept the technology for increased security.

This discrepancy indicates a societal rift between those who build and deploy AI technologies and the general population that experiences its consequences. In contrast, AI professionals and law enforcement actors often prioritize security merits and operational efficiency compared to privacy disadvantages, while the general public — who harbors very limited

understanding of how the underlying technology works — worries more about privacy and potential overreach by surveillance authorities.

The survey results indicate that while the public may be resistant to autonomous AI systems in surveilling broad areas of life, they may find themselves more amenable in the case of these systems being transparent with legal safeguards and accountability mechanisms. Such initiatives would go some way to bridging this gap and developing public trust in AI technologies. Showing that AI systems are effective as well as ethically sound may also ease some of the public concerns.

A major takeaway from conducting the case studies was the challenges faced by local jurisdictions when implementing these AIpowered surveillance systems, particularly during the deployment phase. Although they hold great promise, many systems struggled to operate in busy urban environments. For example, in smart cities, AI surveillance systems had to be constantly recalibrated to compensate for environmental transformations (e.g., lighting, weather) and anomalous events (e.g., atypical behavior). This highlights the need for adaptive AI systems that can learn and evolve with us.

Integrating AI with existing infrastructure was another major challenge, as it often required extensive modification to hardware and software systems. Additionally, such issues of data storage, interoperability, and communication between all the different systems (surveillance cameras, public safety systems, etc.) also posed huge technical challenges.

CONCLUSIONS AND RECOMMENDATIONS

These findings specifically highlight the needs, potentials, and challenges that could enable or hinder Agentic AI from being a game changer for surveillance: It could help raise the bar in terms of surveillance utility and performance, but it could also open up complexities concerning ethics, legality, and general practice that must be solved to enable its usage in sensible ways. Technically speaking, surveillance systems powered by artificial intelligence are bettering in their detection accuracy; yet, they are still challenged in more dynamic and intricate spaces. Ethics: There is an increased need for sensitivity to privacy, bias, and accountability issues. Legally, distinct frameworks needs to pervade to safeguard people's rights and on the other hand, do not hinder the enforcement of law. In conclusion, public perceptions of AI surveillance are mixed, indicating the need for improved communication, transparency, and regulatory oversight.

The ongoing emergence of Agentic AI v1, 2, 3.. will propel critical research and dialogue in the deployment of sequences not only with security, in the consideration of countless vectors and ongoing learning.

By examining several aspects of Agentic AI in surveillance systems specific to its technical functions, ethical implications, and social civics this study was able to gain a holistic understanding of the construct in practice. By using a mixed methods approach, including both experiments and expert interviews, case studies and surveys, we learned about the potential and challenges of operationalizing autonomous AI in applied surveillance contexts.

Key Findings

Technological Capabilities: The experimental analysis indicated a location specific performance of the proliferation of AI surveillance systems, with airport security being a primary location, both detection rates and response times have been notably high. However, performance was somewhat reduced in more dynamic and unpredictable environments, such as crowded urban spaces with higher false positive rates and lower detection accuracy. This demonstrates that current AI technology cannot usefully transfer to environments where human behavior is complex, as well as the timing and location of environmental variables.

Ethical and legal (ex ante) challenges: Research participants identified major ethical challenges and concerns of AI surveillance: privacy and bias. In contrast, the general public remained wary of privacy, and AI experts and law enforcement focused on security gains. And finally, the framework governing AI surveillance is still lacking significant questions around data retention, accountability, and regulation have been raised as areas that need clarity. Ethical deployment will depend on transparency, fairness and accountability of AI systems.

Divided Views: Society's View and Acceptance of AI: The general public is concerned about AI in surveillance due to privacy and autonomous issues, whereas professionals working with AI of law enforcement look at the technology more positively in the aspect of being capable of improving security. There's a strong implications in these findings that there's real, urgent, and significant work to be done about building trust as well as bridging the divide with education, transparency, and strong regulatory frameworks.

Applying AI Surveillance Insights from the Real World: Looking at realworld case studies shed light on some of the operational challenges faced by cities and organizations rolling out AI surveillance tech. Technical challenges to seamless deployment and operation arise, for example, from the integration to existing infrastructure, environmental variability, and the need for the continuous calibration of a system.

FURTHER STUDY

This study provides certain critical guidelines for future research and development about Agentic AI in surveillance.

- Response betterment in AI: Some more work should be done to make AI systems more dynamic, adaptive, less prone to false positives and improve its detection abilities in realtime in such environments.
- Ethical AI Design: Prioritize ethical AI design to attenuate bias, and employ equitable surveillance practices. PT efforts to develop audit trails for AI systems and increase awareness amongst the public will help build public trust.
- Policy and Regulation: Policymakers must develop comprehensive legal frameworks that protect privacy rights while taking security needs into consideration, as AI surveillance systems continue to proliferate.

REFERENCES

Arthan, N., Kacheru, G., & Bajjuru, R. (2019). Radio Frequency in Autonomous Vehicles: Communication Standards and Safety Protocols. Revista de Inteligencia Artificial en Medicina, 10(1), 449478.

Datta, R., Halimuzzaman, M., & Honey, S. (2024). A Comparative Analysis of Safety Performance in Commercial and Residential Construction: Unraveling Critical Insights. *Journal of Control & Instrumentation*, *15*(01), 110.

Datta, R., Pankaj Sarker, K., Shikdar, L., Halimuzzaman, M., & Rezaul Karim, M. (2024). Mobile Applications for Enhancing Safety Audits in Healthcare Construction Sites. *Journal of Angiotherapy*, *8*(9), 16.

Habib, H. (2015). Awareness about special education in Hyderabad. International Journal of Science and Research (IJSR), 4(5), 12961300.

Habib, H., & Janae, J. (2024). Breaking Barriers: How AI is Transforming Special Education Classrooms. Bulletin of Engineering Science and Technology, 1(02), 86108.

Habib, H., Jelani, S. A. K., & Najla, S. (2022). Revolutionizing Inclusion: AI in Adaptive Learning for Students with Disabilities. *Multidisciplinary Science Journal*, *1*(01), 111.

Habib, H., Jelani, S. A. K., & Rasheed, N. T. (2021). Tailored Education: AI in the Development of Individualized Education Programs (IEPs). *Multidisciplinary Science Journal*, *1*(01), 818.

Habib, H., Jelani, S. A. K., Ali, S. S., & Kadari, J. (2023). From Assessment to Empowerment: The Role of AI in Special Education Progress Monitoring. Journal of Multidisciplinary Research, 9(01), 6798.

Habib, H., Jelani, S. A. K., Alizzi, M., & Numair, H. (2020). Personalized Learning Paths: AI Applications in Special Education. Journal of Multidisciplinary Research, 6(01).

Habib, H., Jelani, S. A. K., Numair, H., & Mubeen, S. (2019). Enhancing Communication Skills: AI Technologies for Students with Speech and Language Needs. Journal of Multidisciplinary Research, 5(01).

Halimuzzaman, M., & Sharma, J. (2022). Applications of accounting information system (AIS) under Enterprise resource planning (ERP): A comprehensive review. *International Journal of Early Childhood Special Education (INTJECSE)*, *14*(2), 68016806.

Halimuzzaman, M., & Sharma, J. (2024). The Role of Enterprise Resource Planning (ERP) in Improving the Accounting Information System for Organizations. In *Revolutionizing the AIDigital Landscape* (pp. 263274). Productivity Press.

Halimuzzaman, M., Khaiar, M. A., & Hoque, M. M. (2014). An analysis of progress of rural development scheme (RDS) by IBBL: A study on Kushtia Branch. *Bangla Vision*, *13*(1), 169180.

Halimuzzaman, M., Sharma, D. J., Bhattacharjee, T., Mallik, B., Rahman, R., Rezaul Karim, M., ... & Fokhrul Islam, M. (2024). Blockchain technology

for integrating electronic records of digital healthcare system. *Journal of Angiotherapy*, *8*(7).

Halimuzzaman, M., Sharma, J., & Khang, A. (2024). Enterprise Resource Planning and Accounting Information Systems: Modeling the Relationship in Manufacturing. In *Machine Vision and Industrial Robotics in Manufacturing* (pp. 418434). CRC Press.

Halimuzzaman, M., Sharma, J., Hossain, M. I., Akand, F., Islam, M. N., Ikram, M. M., & Khan, N. N. Healthcare Service Quality Digitization with Enterprise Resource Planning.

Halimuzzaman, M., Sharma, J., Islam, D., Habib, F., & Ahmed, S. S. FINANCIAL IMPACT OF ENTERPRISE RESOURCE PLANNING (ERP) ON ACCOUNTING INFORMATION SYSTEMS (AIS): A STUDY ON PETROLEUM COMPANIES IN BANGLADESH.

Halimuzzaman, M., Sharma, J., Karim, M. R., Hossain, M. R., Azad, M. A. K., & Alam, M. M. (2024). Enhancement of Organizational Accounting Information Systems and Financial Control through Enterprise Resource Planning. In *Synergy of AI and Fintech in the Digital Gig Economy* (pp. 315331). CRC Press.

Hasan, A. S., Debu, S. S. S. D., Eti, I. J., Halimuzzaman, M., & Rezaul, M. Machine Learning Models for Predicting Risky Pregnancies in Early Clinical Interventions.

Islam, M. F., Debnath, S., Das, H., Hasan, F., Sultana, S., Datta, R., ... & Halimuzzaman, M. (2024). Impact of Rapid Economic Development with Rising Carbon Emissions on Public Health and Healthcare Costs in Bangladesh. *Journal of Angiotherapy*, *8*(7), 19.

Islam, M. F., Eity, S. B., Barua, P., & Halimuzzaman, M. (2023). *Liabilities of Street Food Vendors for spreading out Chronic Diseases and Environment Pollution: A Study on Chattogram, Bangladesh. JETIR, 10 (11), Article 11*.

Kacheru, G., Bajjuru, R., & Arthan, N. (2019). Security Considerations When Automating Software Development. *Revista de Inteligencia Artificial en Medicina*, *10*(1), 598617.

Kacheru, G., Bajjuru, R., & Arthan, N. (2022). Surge of Cyber Scams during the COVID19 Pandemic: Analyzing the Shift in Tactics. BULLET: Jurnal Multidisiplin Ilmu, 1(02), 192202.

Rana, M. M., Kalam, A., & Halimuzzaman, M. (2012). CO RPO RATE SO C IAL RESPO NSIBILITY (C SR) OF DUTC HBANG LA BANK LIMITED: A CASE STUDY.

Sohel, M. S., Shi, G., Zaman, N. T., Hossain, B., Halimuzzaman, M., Akintunde, T. Y., & Liu, H. (2022). Understanding the food insecurity and coping strategies of indigenous households during COVID19 crisis in Chittagong hill tracts, Bangladesh: A qualitative study. *Foods*, *11*(19), 3103.

Tamraparani, V. (2019). A Practical Approach to Model Risk Management and Governance in Insurance: A Practitioner's Perspective. *Journal of Computational Analysis and Applications*, *27*(7).

Tamraparani, V. (2019). DataDriven Strategies for Reducing Employee Health Insurance Costs: A Collaborative Approach with Carriers and Brokers. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(1), 110127.

Tamraparani, V. (2020). Automating Invoice Processing in Fund Management: Insights from RPA and Data Integration Techniques. *Journal of Computational Analysis and Applications*, *28*(6).

Tamraparani, V. (2021). Cloud and Data Transformation in Banking: Managing Middle and Back Office Operations Using Snowflake and Databricks. *Journal of Computational Analysis and Applications*, *29*(4).

Tamraparani, V. (2022). Enhancing Cybersecurity and Firm Resilience Through Data Lineage: Best Practices and ML Ops for AutoDetection. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 415427.

Tamraparani, V. (2023). Leveraging AI for Fraud Detection in Identity and Access Management: A Focus on LargeScale Customer Data. *Journal of Computational Analysis and Applications*, *31*(4).

Tamraparani, V. (2024). Applying Robotic Process Automation & AI techniques to reduce time to market for medical devices compliance & provisioning. *Revista de Inteligencia Artificial en Medicina*, *15*(1).

Tamraparani, V. (2024). Revolutionizing payments infrastructure with AI & ML to enable secure cross border payments. *Journal of Multidisciplinary Research*, *10*(02), 4970.

Tamraparani, V., & Dalal, A. (2022). Developing a robust CRM Analytics strategy for Hedge Fund institutions to improve investment diversification. *Unique Endeavor in Business & Social Sciences*, *5*(1), 110.

Tamraparani, V., & Dalal, A. (2023). Self generating & self healing test automation scripts using AI for automating regulatory & compliance functions in financial institutions. *Revista de Inteligencia Artificial en Medicina*, *14*(1), 784796.

Tamraparani, V., & Islam, M. A. (2021). Improving Accuracy of Fraud Detection Models in Health Insurance Claims Using Deep Learning/AI. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(4).

Tamraparani, V., & Islam, M. A. (2023). Enhancing data privacy in healthcare with deep learning models & AI personalization techniques. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(01), 397418.

Tamraparani, Venugopal. (2022). Ethical Implications of Implementing AI in Wealth Management for Personalized Investment Strategies. International Journal of Science and Research (IJSR). 11. 16251633. 10.21275/SR220309091129.