SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V11I8P104

Volume 11 Issue 8, 26-36, August 2024

Original Article

Privacy, Bias, and Transparency: Analysing User Perceptions and Trustworthiness in AI Integrated Domestic Technologies Adoption

Sanat Punj

British School Jakarta, Jakarta, Indonesia.

Corresponding Author :sanatpunj94@gmail.com

Received: 21 June 2024 Revised: 30 July 2024 Accepted: 18 August 2024 Published: 31 August 2024

Abstract *- Artificial Intelligence (AI) models have become more sophisticated than ever, as their performance optimizes at a groundbreaking rate with the rapid advancement of technology. Increasing AI adoption amplifies the need for trustworthy systems and may threaten social confidence, reflecting negative user perceptions. This could heighten threats posed by privacy concerns, transparency of AI systems, and data biases. The present study aims to statistically evaluate user trust and attitudes towards AI-integrated domestic (ubiquitous) technologies by analyzing privacy concerns, transparency of AI systems, and the data bias they are prone to. Broadly, this research is intended to understand the vulnerabilities developed by the use of common, domestic AI systems on users based on several parameters. A quantitative primary study was conducted by surveying 40 financially stable individuals of diverse age groups (10-80), nationalities (Indonesia, India, and USA), educational qualifications, and genders. This research analysis elucidates the critical factors within specific AI-domestic models that drive user trustworthiness, offering valuable insights for businesses. The research could be utilized to guide R&D direction for businesses, enhance the robustness of AI systems, improve AI user experience for society, and increase user retention rates for such technologies.*

Keywords *- Artificial Intelligence, Machine Learning, Bias, Transparency, Data privacy.*

1. Introduction

Artificial intelligence, referred to as AI is an interdisciplinary branch of Computer Science revolving around the field of developing intelligent machines through science and technological progress, particularly software that is a stimulation of human cognition [1]. AI has become a structural part of our society due to its integration in a wide array of sectors, ranging from the education sector for individualized learning, the banking industry for data analytics, the healthcare sector for diagnosing diseases by radiographic analysis [2], and even the retail sector for customer support using NLP - based Virtual Assistants.

AI is being leveraged to streamline operational efficiency as organizations are channeling their algorithmic power to optimize supply chain management [3]. Firms are adopting AI to automate routine and mundane tasks to minimize errors and overhead time and increase cost savings by cutting labor. Furthermore, AI has started to be recognized by organizations due to its ability to carry out predictive analysis and dynamic resource allocation effectively, which can help firms improve decision-making and productivity [4]. As time progresses, an increasing number of organizations are incorporating AI into their workflows [5] due to its ability to automate operations [6] and optimize data analytics [7]. A significant proportion of organizations, over 80%, perceive AI as a strategic opportunity, and almost 85% recognize it as a tool to gain a competitive advantage [8].

AI merges vast datasets with sophisticated iterative algorithms that enable machines to analyze data, extract insights, and generate intelligent judgments [9]. These algorithms are based on advanced mathematical modeling techniques utilized to learn and understand patterns embedded in the datasets [10]. Through time, machine learning algorithms have developed and drastically changed. The first ever machine learning algorithm was the perceptron, which was developed in 1957 by Frank Rosenblatt [11].

The perceptron was a basic single-layer feedforward neural network algorithm for the supervised learning of binary classifiers. However, a limitation was that the value outputted by the perceptron would only be a binary number(0 or 1) due to the boolean activation method [12]. This prevented the perceptron from handling complex tasks requiring probabilistic outputs.

In the last 15-20 years, AI has experienced rapid growth due to the advancement of technology and corporate interest, which have enabled software engineers to construct highly advanced and complex AI algorithms [12]. A new spectrum of concepts and technologies have been adopted by machine learning models, which incorporate sophisticated supervised, unsupervised, and reinforcement learning with unique algorithms for robotics and the Internet of Things [11].

In the modern world, even more powerful and capable AI technologies, such as generative AI, have recently been introduced, and they can not only be trained to recognize patterns but are capable of producing artificial content that mimics the training data [13]. These algorithms incorporate both creativity and personalization, making them particularly useful for general users and enterprises [14].

However, while the growth of AI has the potential to spark positive changes in society further, the widespread use of AI has led to a growing recognition in society of the need for these systems to uphold trustworthiness [15]. Many occurrences underscore AI's shortfall in achieving complete reliability and functionality and maintaining ethical standards [16].

The accuracy of AI algorithms is directly related to the quality and quantity of data they are being trained with since machine learning models require data for the algorithms to learn and recognize patterns. These patterns are required to be able to find trends and relationships with unseen data to make accurate predictions or produce precise output(s). While algorithms could be fed with a larger volume of (additional) data and could undergo feature engineering or even algorithmic tuning to choose optimal hyperparameters, inherent uncertainties will always exist in the inputs provided. All AI models are subject to inaccuracies and ethical lapses due to obscure data input during live deployment, heterogeneity, superfluous data, and algorithmic limitations due to unidentified patterns and relationships [17]. However, all models are subject to inaccuracies to different degrees of extent.

A single loophole in an AI system or a single malfunction could potentially threaten human life. For instance, in 2023, 130 fully automated car accidents were reported by 25 companies [18]. Additionally, the alleged utilization and collection of data by AI could jeopardize the privacy and security of millions of users owing to the extensive databases involved (Drapkin & Drapkin, [19] [16].

Recently, the rising value of the Global Artificial Intelligence market (Compound Annual Growth Rate (CAGR) of 38.1% between 2022 and 2030) has led to experts questioning the potential dangers of AI, in particular, whether it can be trusted, as its market is valued over $136 billion [20]. The size of the AI market is an indication of technological advancement and the stake it holds in recent years.

Last year, Forbes conducted an advisory survey that showcased the perception of users towards AI tools in general [21]. The survey illustrated that over three-quarters of the respondents were concerned over the misinformation from artificial intelligence and the impact artificial intelligence may have on future jobs and workspaces. Additionally, on aggregate, more than 60% of the respondents felt vulnerable regarding the use of artificial intelligence by businesses due to the invasion of privacy [8], underscoring growing concern about trustworthiness and vulnerabilities during the adoption of AI-integrated domestic technologies.

To conduct a literature review, a selective examination of various scholarly papers and studies focusing on relevant parameters within the field was undertaken utilizing terms including "Artificial Intelligence," "Domestic Technologies," "Bias," "Privacy Concerns," and "Transparency." The literature review was undertaken to gain a comprehensive understanding of current trends in AI-integrated domestic technologies for the purpose of analysis.

The most popular study carried out previously on privacy concerns of AI includes a study carried out by Jillian Carmody, Samir Shringarpure, and Gerhard Van de Venter in the year 2021 entitled "AI and Privacy Concerns: A Smart Meter Case Study". This paper aimed to exhibit the privacy concerns posed by AI-integrated technology, using the case study of domestic systems. The authors used smart meters to obtain energy metrics in domestic establishments and presented how household energy providers could use the collected data to procure private user information. These details consist of data regarding households' electrical appliances, including their model, number, and time and frequency of usage.

The writers showed how personal data and information, including lifestyle and household income, could be revealed by the employment of AI technology due to their advancements. The main findings of the paper are the threats domestic AI technology could pose to the privacy of users and their security when AI is trained on vast granular data sets. This research implies how the lack of legislation regarding the boundaries of AI usage could profoundly alter user trustworthiness, questioning privacy regulation policies [22].

Existing studies have primarily focused on the privacy risks users might face while utilizing AI-domestic systems using secondary analysis (minimal involvement in users), leaving a significant gap in understanding user perceptions towards the vulnerabilities created by AI-domestic technologies directly, using a primary first-hand approach and comparatively between different parameters. Building upon previous studies, this research directly analyzes user perceptions and trustworthiness in AI-integrated domestic technologies to determine whether AI can be trusted for daily activities. A primary survey methodology was conducted with

participants to assess their perceptions of data collection by AI directly, data biases, accuracy errors, and trustworthiness based on the transparency of AI-integrated systems and vulnerabilities in AI data servers. The study aims to discover whether the findings of threatening security issues of AI, as found by previous papers, are experienced by users and whether it impacts their trustworthiness towards AI systems. This research will delve into privacy concerns, the transparency of AI systems, and the data bias it is prone to in order to identify vulnerabilities users experience with the presence/usage of AI-integrated domestic technologies.

This research aims to elucidate the critical factors within routine AI models that drive user trustworthiness and vulnerabilities. The findings could be instrumental in guiding R&D directions for businesses, enhancing the robustness of AI systems, and improving AI-user interactions, thereby increasing user retention rates for such technologies. By addressing these factors, businesses can prevent users from feeling vulnerable, thereby increasing satisfaction with their products while safeguarding societal well-being. Furthermore, this study is crucial for businesses working in AI, as neglecting these risks could jeopardize security and impact lives due to the complexity and advanced state of AI technologies.

2. Methodology

2.1. Research Aim

The primary objective of this study is to examine and analyze user perceptions and trustworthiness in AI-integrated domestic technologies with a primary focus on Virtual Assistants (Chatbots, i.e. Siri, Alexa, ChatGPT), Autonomous Cars (Self-Driving Cars) and Biometric Facial Recognition Technology (AI-Powered Cameras, Facial Recognition Systems) for the study using a quantitative approach. This research aims to evaluate the extent to which AI can be relied upon for daily activities. It will explore the privacy concerns, transparency of AI systems, and the data bias it is prone to, ultimately discovering the vulnerabilities users experience in AI-integrated domestic technologies.

Objectives:

- Review the uses and applications of common AI-integrated systems owned by individuals domestically - Virtual Assistants (Chatbots, i.e. Siri, Alexa, ChatGPT), Autonomous Cars (Self-Driving Cars), and Biometric Facial Recognition Technology (AI-powered cameras, Facial Recognition Systems)
- Research and analyze existing papers on AI systems and their privacy concerns, transparency, and data biases
- Design a survey to understand the perceptions and trustworthiness of users/surveyees towards AI-integrated domestic technology based on the parameters of the study - privacy concerns, transparency of AI systems, and data biases.
- Analyse and understand the perceptions of users towards AI systems to identify vulnerabilities and insecurities faced by users while using or experiencing specific AI-integrated domestic technologies.
- Evaluating user impressions on AI systems to derive the extent to which each different parameter impacts user trustworthiness

2.2. Sample

The study comprises a sample size of 40 respondents, employing a combination of convenience and snowball sampling. Respondents range in age from 10 to 80 years. The majority have postgraduate (65%) or high school (32.5%) education. Of the respondents, 62.5% are unemployed, with a similar distribution of male (60%) and female (37.5%) participants. A significant majority (92.5%) reported regular personal use of AI.

2.3. Informed Consent

To ensure the integrity of each individual in the study, the importance of and methodologies used to protect personal data were thoroughly researched. Compliance with the Data Protection Act of 2018 was maintained to prevent the exposure and misuse of personal data.

Table 1. Tabular representation illustrating the gender, age, education, and occupation demographics [N=40]

Gender	Frequency
Male	24
Female	15
Other	1
Age	
10 - 15	7
16 - 20	6
21 - 25	0
26 - 30	1
31 - 35	0
36 - 40	4
41 - 45	10
46 - 50	8
51 - 55	2
56 - 60	0
61-80	2
Other	0
Highest Education Qualification	
High School	13
Post Graduate	26
Undergraduate	1
Occupation	
Self Employed	2
Service	23
Other	15

Consent was obtained from all respondents before they participated in the survey. The survey assured respondents that there were no right or wrong answers and that the information provided would be kept confidential, with no disclosure of their identities to third parties. Respondents were informed that they could choose to remain anonymous and were given the option to decline data collection before participating. Additionally, respondents were assured that they could contact the surveyor if they experienced discomfort and terminate their participation at any time.

2.4. Tool Used

The survey consists of 48 questions divided into 6 sections, designed to accurately identify user perceptions and trustworthiness in AI-integrated domestic technologies. Most of the survey features quantitative responses via Likert scales for precision and standardization, facilitating data visualization and statistical analysis.

Section 1: Collects personal information to enable demographic-based analysis, reflecting the real-world population. It includes 7 questions about user backgrounds and AI experience.

Sections 2-5: Focus on the three primary research parameters—privacy concerns, data biases, and transparency of AI systems in AI-integrated domestic technologies.

- Section 2: Addresses privacy concerns associated with AI technologies (e.g., self-driving cars, virtual assistants, biometric facial recognition). Comprising 12 questions in 5 sub-sections, it explores user thoughts on data storage and usage, forming the first research parameter.
- Section 3: Examines security measures and vulnerabilities in AI data servers through 2 questions, contributing to the privacy concerns parameter.
- Section 4: Investigates AI systems' data biases, focusing on task accuracy and user trust. With 15 questions in 4 sub-sections, it explores training data biases and user experiences, forming the second research parameter.
- Section 5: Explores the explainability and transparency of AI decisions with 7 questions, examining the impact of AI decision opacity on user trust. This section constitutes the third research parameter.

Section 6: Comprises 5 questions on the future of AI systems, assessing user perspectives on AI development and societal impact. This section supports future research expansions.

2.5. Rationale for Approach

The rationale for employing a survey methodology lies in its ability to gather quantitative data for robust analysis, as opposed to subjective data. This method is particularly suitable for measuring user perceptions, as it allows for direct assessment while minimizing biases that could arise from personal interactions with the respondents. Additionally, leveraging familial connections with individuals from diverse age groups and backgrounds ensures the inclusion of varied perspectives, further enhancing the suitability and comprehensiveness of this approach.

3. Results and Discussion

3.1. Prevalence of AI

The current section of the paper focuses on analyzing user perceptions and trustworthiness regarding privacy concerns, biases, and transparency of AI-integrated domestic technologies, specifically autonomous cars, virtual assistants, and biometric technology.

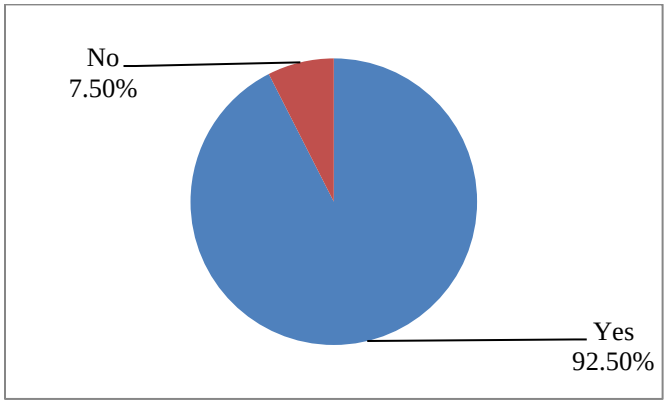

Fig. 1 Pie chart representing that a substantial proportion of participants utilize AI-based systems [N=40]

Figure 1 indicates the percentage of respondents who regularly use AI-based systems. The chart reveals that a substantial majority, 92.5% (37 out of 40), of the respondents are frequent users of AI, highlighting the widespread adoption and prevalence of AI technologies among the surveyed population.

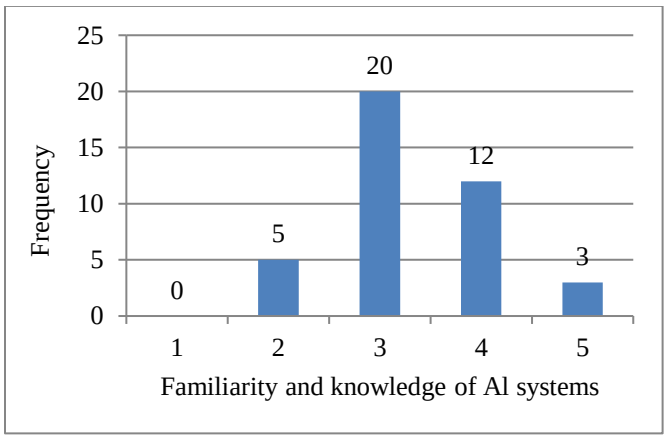

Figure 2. Graphical Representation of how familiar and knowledgeable respondents are with AI systems [N=40]

Figure 2 illustrates the respondents' understanding and familiarity with AI. Notably, 35 out of the 40 respondents (87.5%) rated their knowledge of AI as three or higher on a five-point scale, indicating a substantial comprehension of AI functionalities. This suggests that a significant majority have engaged with AI systems sufficiently to form informed opinions on the associated risks and benefits. Importantly, none of the respondents selected the lowest rating of 1, underscoring the widespread recognition of AI's significance and the critical need for trustworthy AI systems.

3.2. Privacy Concerns that AI Systems Might Develop in Users

Figure 3 demonstrates respondents' perceptions regarding AI data storage. The chart reveals that 92.5% (37 out of 40) of respondents believe that AI systems store their data. This high percentage indicates a widespread awareness and concern about data storage practices among users. It emphasizes the importance of responsible data management in AI-integrated technologies as a potential vulnerability risk that could be created if this data is handled poorly.

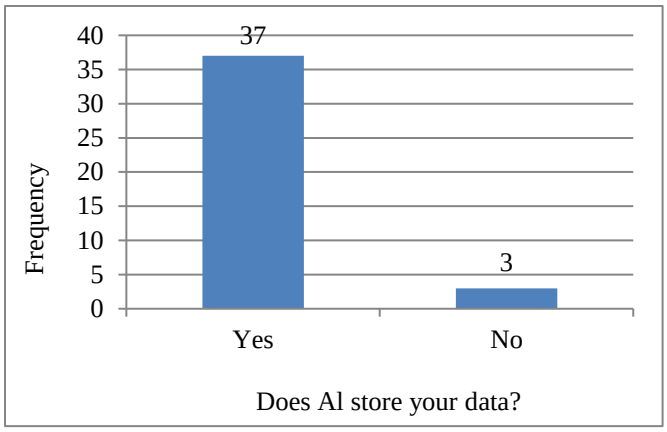

Fig. 3 Bar chart illustrating that most respondents feel that AI stores their data [N=40]

Table 2. Tabular representation elucidates that respondents perceive autonomous vehicles to gather and retain data extensively [N=40]

Data Classification	Frequency	Percentage (%)
Autonomous Cars Location	40	100
Surroundings	33	82.5
Owner Information	37	92.5
Passenger Information	21	52.5
Vocal conversational data	28	70
Emergency Data	24	60
Contacts Data	28	70

This table portrays how a majority of AI systems collect and store user data, as each of the classified data has a corresponding percentage of more than 50. The extensive data collection portrays the security risks of autonomous vehicles and the vulnerability risks developed by such autonomous cars. 100% [40], a unanimous number of participants have agreed that autonomous vehicles can access your location data. This represents how the usage of such personal data could present privacy concerns to users as they are constantly being tracked.

33 out of 40 people, 82.5% of the people believe that autonomous cars store surrounding information. The notable fraction presents that autonomous cars could be a potential risk to society as all the cars and people located near an autonomous car would be susceptible to privacy risks due to the liability of being tracked.

Furthermore, Table 2 represents how extensively the vehicle's owner's data is recorded and stored. It can be seen that 92.5% [37] of respondents feel that autonomous cars store owner information. Hence, autonomous vehicle databases can uniquely identify each of its owners, creating a potential vulnerability as the statistic presents how the personal data of an owner could potentially be trackable. In addition, 60% [24] of the surveyees believe that autonomous cars are also collecting emergency data. Therefore, it is evident that a majority of participants feel that autonomous cars store emergency data, a crucial piece of information that includes blood type, allergy information, existing medical conditions, and more components of medical data for conducting diagnostic treatments. Consequently, this creates a vulnerability risk as the exposure or leakage of such data could result in exploitation. Thus, the figures risk security breaches posed by autonomous car vehicle data collection.

Table 2 also presents how significant data from passengers is collected. It can be seen that 52.5% [21] of the respondents believe that autonomous vehicles possess passenger information. While only a small percentage of people (2.5%) [1] believe that autonomous vehicles collect passenger information, which is statistically insignificant. 70% [28] of the surveyees believe autonomous cars store vocal conversational data and contact data. Hence, it can be seen that a majority of participants feel that autonomous cars store vocal conversational data and contact data, implying a sense of insecurity that passengers might witness in autonomous cars. This is because passengers would feel exposed and fragile as their conversations are possibly being tracked, and they feel vulnerable to security threats as the passenger's contact data is being stored.

Table 3. Tabular representation illustrating that surveyees perceive virtual assistants to gather and retain data extensively [N=40]

Virtual Assistants Data Storage	Frequency	Percentage (%)
Contact Information	31	77.5
Location Data	31	77.5
Conversation History	34	85
Biometric Data	25	62.5

Table 4. Tabular representation depicting that smart home integrated virtual assistants probabilistically receive and store the data from sensors and IoT devices such as smart lights and cameras [N=40]

Smart-home-integrated virtual assistants can collect and store received data from sensors and IoT devices.	Frequency
1	2
2	1
3	10
4	16
5	11

Table 3 portrays the extent to which virtual assistants store user data. It is shown that 77.5% [31] of respondents believe that virtual assistants store location data, and 62.5% [31] of respondents believe that virtual assistants also store biometric data. Therefore, it is evident that a majority of the respondents feel that AI stores their location and biometric data, portraying the susceptibility of virtual assistant tool users as they would be recognizable to anyone who gains possession of their data, and their location would be tracked. If data is not held securely, users would also be susceptible to identity thefts and fraud due to the possession of data that corresponds with their identity. Hence, it can be seen that virtual assistants track personally identifiable information, and virtual assistant suppliers and data handlers play a fundamental role in handling critical data, all of which portray a sense of vulnerability built by virtual assistant users.

Furthermore, 77.5% [31] of the surveyees feel that virtual assistants track their contact information, and 85% [34] of the respondents feel that virtual assistants are also tracking users' conversational history. This depicts that a majority of the participants felt that their conversational history and contact information were being tracked, creating a sense of vulnerability to their social identity as insecure data management would allow people to track their daily activity.

Table 4 provides insights into respondents' perceptions regarding the data collection practices of smart home-integrated virtual assistants from sensors and IoT devices within a connected home environment. The findings highlight significant concerns about data security and privacy among users of smart home technologies.

A substantial majority, 67.5% (27 out of 40) of respondents, believe that smart home-integrated virtual assistants collect and store data received from IoT devices such as smart lights and cameras. This perception underscores concerns about the potential collection of personally identifiable information (PII) and sensitive data from various sensors linked via cloud connectivity. Such data may include biometric information, facial recognition data, auditory recordings, and environmental data like motion, light, temperature, and humidity levels. These findings emphasize the critical need for robust security measures to safeguard against unauthorized access and misuse of sensitive data collected by smart home systems.

Conversely, a minority of respondents, only 7.5% (3 out of 40), indicated a belief that smart home virtual assistants do not collect and store data received from sensors and IoT devices, rating this possibility as 2 or below on a scale of 1 to 5. While this view is less prevalent among participants, it highlights varying perceptions regarding the extent of data collection and privacy risks associated with smart home technologies.

Table 5. Tabular representation outlining the extensive storage of personal data by biometric facial recognition technology [N=40]

Do you believe that biometric AI systems such as face recognition technology store user data and recordings?	Frequency
1	0
2	0
3	7
4	17
5	16

In conclusion, the perceptions outlined in Table 4 underscore the importance of implementing stringent data protection practices and transparent data handling policies within smart home environments. Addressing these concerns

is crucial to enhancing user trust and confidence in the secure deployment of smart home-integrated virtual assistants, ensuring privacy while leveraging the benefits of IoT-driven home automation technologies.

Table 5 portrays whether respondents feel that biometric AI systems such as face recognition technology store user data and recordings. 40% [16] of the respondents feel that biometric AI systems constantly survey and record the surroundings if a device is booted up and store this footage. This is a sizable percentage portraying the confidential disclosure risk and personal secrecy threat posed by biometric technology, as such visual data would compromise intimacy and privacy.

Furthermore, 42.5% [17] of the surveyees believe that biometric AI systems only record digital device footage during the usage of AI-facial recognition services. The substantial fraction underscores the importance of vulnerabilities developed while using such services, even for security purposes, as mishandling of data would leak personally identifiable information, which can be exploited for further offences such as identity theft and fraudulent activity.

The data emphasizes the need for robust measures of data protection and transparent data handling practices. Addressing these concerns is crucial to mitigating privacy risks and fostering user trust in the secure deployment and use of facial recognition technologies.

3.3. Transparency of AI systems

Table 6. Overview of how respondents perceive the transparency and explainability of AI systems across various scenarios, including self-driving cars, virtual assistants, biometric facial recognition scans, and generalized AI frameworks [N=40]

Likert scale Rating	Self-driving cars' driving patterns hamper	Decisions and responses of virtual assistants are not	Lack of explainability of AI decisions decreases user trust	Biometric facial recognition scans are not explainable	User comfort decreases due to the inability to understan	AI has become overwhelming with the vast advanceme	Total
1	1	3	1	7	3	4	19
2	12	20	5	18	14	11	80
3	15	13	10	10	12	15	75
4	8	3	22	2	9	9	53
5	4	1	2	3	2	1	13

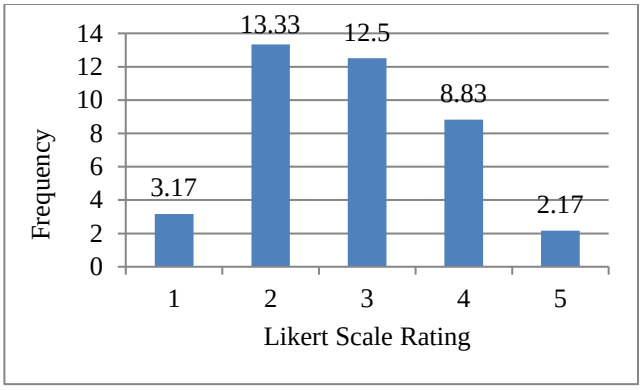

Fig. 4 Bar chart representing the extent to which the opacity of AI model's decisions is concerning and impacts user experience and interaction

Figure 4 represents the impact of the explainability and transparency of AI systems on user trust and, consequently, user experience. The magnitude ratings shown in Figure 4 are an aggregate of all the questions (7) related to AI transparency and explainability in the study.

In 72.5% of the scenarios (with ratings ranging from 1 to 3), the explainability and transparency of AI had a minor to average impact on user trust. This means that in roughly three out of four scenarios, AI transparency generally has a minimal effect on AI trust. Therefore, it can be inferred that user experience and interactions are not significantly influenced by the level of transparency exhibited by AI-integrated domestic technologies.

Additionally, Table 6 shows that 70% of respondents feel that self-driving cars' driving patterns do not hamper passenger or driver comfort, and 90% believe that the decisions made by virtual assistants are understandable. These significant fractions indicate that both self-driving cars and virtual assistants are predominantly explainable and do not negatively impact user trust. However, the median and mode rating regarding whether self-driving cars' driving patterns hamper comfort lies at 3. This suggests that while self-driving cars occasionally exhibit unclear driving patterns, these do not substantially impact driver comfort.

In 7.9% of the scenarios (3.17 out of 40), respondents felt that the transparency of the AI model did not matter. This relatively small percentage is statistically marginal, indicating that the explainability and transparency of AI systems primarily influence user experience and confidence. Among these 7.9% of scenarios, 17.5% of respondents felt that biometric facial recognition scans are completely transparent and do not affect user engagement with the technology, as shown in Table 6. Additionally, only 12.5% of respondents felt that biometric facial recognition technology is not

transparent, which is a minor percentage. This indicates that biometric facial recognition technology is generally perceived as transparent and does not significantly affect user trust in AI. Furthermore, 60% of users felt that a lack of explainability in AI decisions decreases user trust, highlighting a preference for transparent AI systems.

As depicted in Figure 4, 22.1% of the time (8.83 out of 40 scenarios), respondents found the explainability and transparency of AI systems to have a moderate impact on user trust. This underscores the importance of transparency for a substantial portion of AI users, as it influences their experience and interactions with AI systems. While domestic AI systems like autonomous cars, virtual assistants, and biometric facial recognition technology generally exhibit minimal impact on user trust due to transparency, the preference for transparent AI decisions is clear.

In conclusion, although autonomous vehicles, virtual assistants, and biometric AI systems do not necessarily need to be transparent to maintain user trust, users prefer AI systems to explain their decisions. This allows users to understand whether the AI's thought process aligns with their intentions for utilizing such services, a preference expressed by 75% of users.

3.4. AI Systems Data Biases

Figure 5 highlights the significance of biases in AI as a measure of the dependability of AI-integrated domestic systems. It compares the perceived prevalence of biases in these systems with the frequency with which survey participants encounter them. According to the data, 45% of participants believe that biases are prevalent in AI systems, yet only 12.5% report encountering them regularly. This suggests that biases primarily emerge in less utilized and explored aspects or features of autonomous cars, virtual assistants, and biometric technology. Conversely, 55% of participants do not perceive biases in AI systems, and 87.5% do not encounter them regularly. This indicates that while biases are observable, they are not deeply ingrained in AI systems during daily usage. Consequently, biases do not significantly undermine user confidence in AI-integrated domestic technologies.

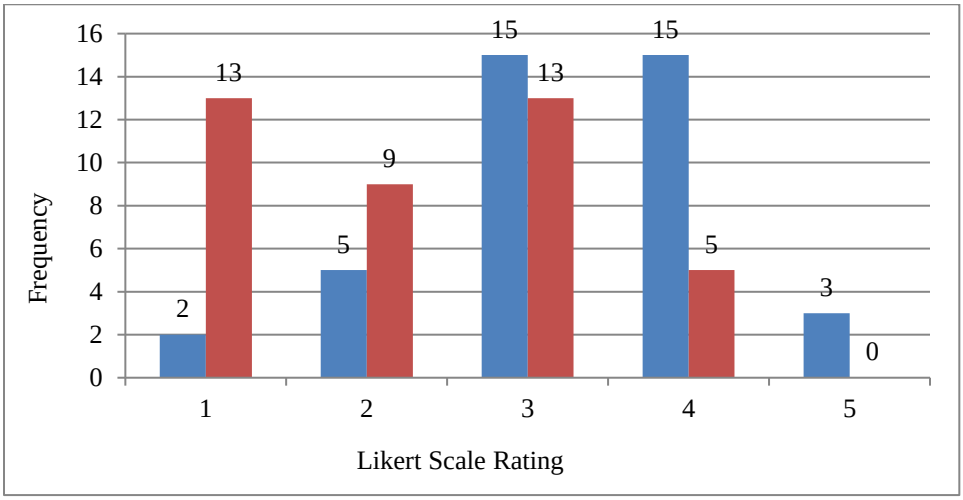

Fig. 5 Bar graph comparing and illustrating the presence of biases in AI and how frequently people encounter them [N=40]

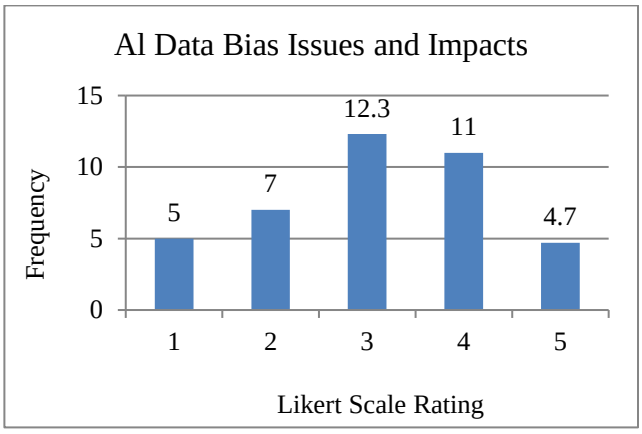

Fig. 6 Bar chart representing the extent to which the AI system data biases are relevant and concerning to user experience and interaction with AI while utilizing such technology [N=40]

Figure 6 illustrates whether users perceive biases to introduce limitations and challenges in AI systems and impair user trust. The magnitude ratings shown in Figure 6 are an aggregate of all 13 Likert scale questions included in the section of the survey addressing AI system data biases. From the figure, it can be inferred that there is a 39.25% probability that AI exhibits data biases that influence user trust. This average is calculated based on various AI-integrated technologies and scenarios.

Conversely, in 30% of the scenarios, users perceive AI biases to have a negligible impact on user trust. Therefore, it can be derived that a larger number of users (39.25% compared to 30%) felt that the presence of AI data biases impacts trustworthiness and consequently limits the scope of utilizing AI systems.

However, out of the 39.25% of users whose trust was significantly impacted by AI data biases, a smaller percentage experienced these biases predominantly (29.9%, rating of 5) compared to those who did not (71.1%, rating of 4). Furthermore, the difference between the percentages of users whose trust was significantly impacted by biases and those whose trust was not impacted (9.25% [39.25% - 30%]) indicates limited variation, portraying that AI data biases have only a mild impact on user confidence. Additionally, in 30.75% of the scenarios, users felt that AI systems sporadically exhibited biases that influenced their trustworthiness.

Hence, the data affirm that biases exhibited by AI-integrated technologies can undermine user trust in certain AI systems. However, the statistics also indicate that AI biases exist infrequently, suggesting that while biases are present, their impact on user trust is generally mild.

3.5. Comparative analysis of AI Biases, transparency, and privacy

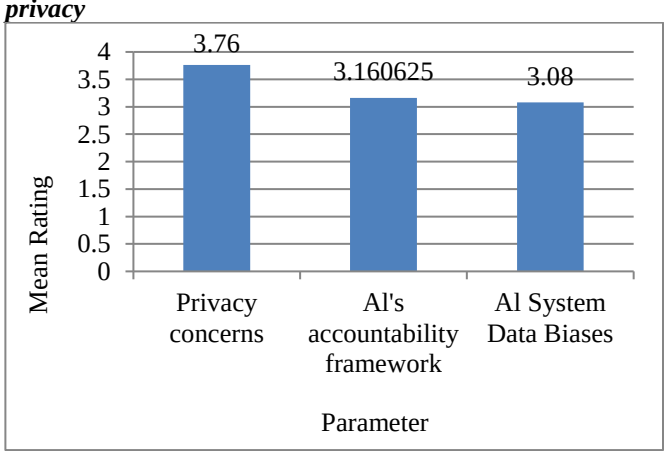

Fig. 7 Bar chart representing the extent to which AI-integrated domestic technology poses privacy concerns, transparency risks, and displays biases [N=40]

Figure 7 illustrates that users perceive AI privacy concerns as the most significant risk factor, with a mean rating of 3.76. This rating is 0.76 points above the neutral average of 3, indicating that users' trust in AI systems is notably compromised by potential vulnerabilities related to the storage and collection of personal data by AI.

The difference in concern levels between the AI accountability framework and AI system data biases is minimal, with a statistically insignificant magnitude difference of 0.08. Specifically, the mean rating for user concerns regarding the AI accountability framework or transparency is 3.16, while the mean rating for AI system data biases is 3.08. Both ratings are only slightly above the neutral average of 3, suggesting that although users are aware of issues related to AI transparency and biases, these factors do not significantly impact their overall trust in AI systems.

These findings highlight that while privacy concerns are a major issue affecting user trust in AI, concerns about accountability and data biases are relatively less impactful. However, they still contribute to users' cautious approach towards AI-integrated technologies.

4. Conclusion

This study analyzes user perceptions and trustworthiness towards AI-integrated domestic technologies with a primary focus on autonomous cars, biometric facial recognition technology, and virtual assistants. It aimed to understand the extent and impact of the privacy concerns, transparency of AI systems, and the data bias it's prone on user trust, discovering the vulnerabilities users experience with such AI-integrated and routine technologies.

The study found that users perceive all AI systems to collect and gather data extensively. Individuals believe that all autonomous cars, biometric facial recognition technology, and virtual assistants store vast volumes of personal data, which reduces user trustworthiness towards AI systems. It was identified that users feel a sense of vulnerability as insecure data management and security breaches would allow their daily activity to be tracked due to the storage of personally identifiable information by AI systems. The results are correlated with the Forbes AI Consumer Sentiment Survey, carried out in 2023, in the context of business employees [21].

Results demonstrated that people feel autonomous cars are a potential risk to society. They perceive them to increase users' and third-party liability as they track passengers, surroundings, and crucial emergency data. Furthermore, users believe that insecure storage of data collected by (smart home integrated) virtual assistants and biometric AI-recognition systems would reveal their social identity and make their routine traceable due to the storage of traceable data and activity logs. They experience a sense of vulnerability as the leakage of such data leakage could exploited for further offences such as identity theft and fraudulent activity. A study titled *Privacy Risks in Vehicle Grids and Autonomous Cars* by Joshua Joy and Mario Gerla supports the concerns related to autonomous cars and smart IOT devices. It expresses the risks posed by V2I and V2V communications intelligence, which are commonly used in Smart IoT devices and autonomous cars [23].

It was observed that a majority of users don't feel that autonomous vehicles, virtual assistants, and biometric AI systems have to be transparent but prefer that AI systems should explain their decisions to understand whether their thought process matches with the user's intentions of utilizing such services. Additionally, the study also found that AI biases could undermine user trust in certain AI systems. However, biases are experienced infrequently while utilizing AI systems, and hence, the parameter of data biases has a relatively small impact on user trustworthiness.

Moreover, the research paper discovered that AI privacy concerns pose the largest and most significant risks to users, including privacy risks, transparency concerns, and data biases. This is also illustrated and supported by previous research, such as the hypothesis and theory article "AI Technologies, Privacy, and Security", published in 2022 by David Elliott and Eldon Soifner, which concludes that the presence of large amounts of information about people within the AI systems does create an increased risk. It states that privacy is the most recurrent concern individuals have about AI systems, as discovered by this research.

This research is separated from other papers as it analyses user perceptions and trustworthiness of AI and the vulnerabilities they face using a first-hand survey methodology; previous research papers focused on a secondary analysis of privacy risks. The research elucidates the critical factors within routine AI models that drive user trustworthiness and develop vulnerabilities in them. The findings of the research could be utilized to guide R&D direction for businesses, enhance the robustness of AI systems, improve AI user experience for society, and increase user retention rates for such technologies.

By bridging these factors, businesses can prevent users from feeling vulnerable, increase user satisfaction with products, and safeguard societal well-being. Moreover, the study is crucial for businesses working in the field of AI, as neglecting such risks could jeopardize security and impact lives due to the complexity and advanced state of AI technologies.

This paper is imperative for voicing user concerns by analyzing their perceptions and trustworthiness toward AI. It aims to improve user satisfaction and decrease the sense of vulnerabilities they are facing due to AI systems.

References

[1] What Is Artificial Intelligence (AI)?, IBM, 2024. [Online]. Available: https://www.ibm.com/topics/artificial-intelligence

[2] Dheeraj Kumar, Navreet Boora, and Mahendra Kumar Verma, "Role of Artificial Intelligence in Radiography Techniques and Procedure," *International Journal of Medical Science and Current Research*, vol. 5, no. 1, pp. 134-140, 2022. [Google Scholar] [Publisher Link]

[3] Chatbot Guides Students to Learn and Reflect, Digital Education, 2022. [Online]. Available: https://digitaleducation.stanford.edu/chatbot-guides-students-learn-and-reflect

[4] AI in Streamlining Workplace Operations and Maximizing Efficiency, ESS Global Training Solution. [Online]. Available: https://esoftskills.com/ai-in-streamlining-workplace-operations-and-maximizing-efficiency/

[5] Sajid Ali et al., "Explainable Artificial Intelligence (XAI): What We Know and What Is Left to Attain Trustworthy Artificial Intelligence," *Information Fusion*, vol. 99, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] How AI Is Rewriting the Rules of Data Analysis, IIBA, 2023. [Online]. Available: https://www.iiba.org/business-analysis-blogs/how-ai-is-rewriting-the-rules-of-data-analysis/

[7] Ida Merete Enholm et al., "Artificial Intelligence and Business Value: A Literature Review," *Information Systems Frontiers*, vol. 24, pp. 1709-1734, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Katherine Haan, and Rob Watts, Over 75% of Consumers Are Concerned About Misinformation from Artificial Intelligence, Forbes Advisor, 2023. [Online]. Available: https://www.forbes.com/advisor/business/artificial-intelligence-consumer-sentiment/

[9] Artificial Intelligence (AI): What It Is and Why It Matters, SAS. [Online]. Available: https://www.sas.com/en_id/insights/analytics/what-is-artificial-intelligence.html

[10] Michael Chen, What Is AI Model Training & Why Is It Important?, Oracle Indonesia, 2023. [Online]. Available: https://www.oracle.com/id/artificial-intelligence/ai-model-training/

[11] Keith D. Foote, A Brief History of Machine Learning, Dataversity, 2021. [Online]. Available: https://www.dataversity.net/a-brief-history-of-machine-learning/#:~:text=Machine%20learning%20is%2C%20in%20part,excitement%20and%20communication%20between%20neurons

[12] David Elliott, and Eldon Soifer, "AI Technologies, Privacy, and Security," *Frontiers in Artificial Intelligence*, vol. 5, pp. 1-8, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Stefan Feuerriegel et al., "Generative AI," *Business & Information Systems Engineering*, vol. 66, pp. 111-126, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Erik Brynjolfsson, Danielle Li, and Lindsey R. Raymond, "Generative AI at Work," *National Bureau of Economic Research*, pp. 1-67, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Daniella Allen, and E. Glen Weyl, "The Real Dangers of Generative AI," *Journal of Democracy*, vol. 35, no. 1, pp. 147-162, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Summer Lin, Google to Pay $93 Million after State Investigation Finds Company Used Location Data Without Consent, Los Angeles Times, 2023. [Online]. Available: https://www.latimes.com/california/story/2023-09-14/google-to-pay-93-million-after-state-investigation-finds-company-used-location-data-without-consent

[17] How to Train Artificial Intelligence Models for Better Accuracy, Syncrux, 2024. [Online]. Available: https://syncrux.com/how-to-train-artificial-intelligence-models-for-better-accuracy/
[18] 2023 Autonomous/Self-Driving Car Accident Statistics, Dordulian Law Group, 2023. [Online]. Available: https://www.dlawgroup.com/self-driving-car-accident-statistics-2023/
[19] Aaron Drapkin, AI Gone Wrong: An Updated List of AI Errors, Mistakes and Failures, Tech.Co, 2024. [Online]. Available: https://tech.co/news/list-ai-failures-mistakes-errors
[20] Josh Howarth, 57 New Artificial Intelligence Statistics (Aug 2024), Exploding Topics, 2024. [Online]. Available: https://explodingtopics.com/blog/ai-statistics
[21] Forbes AI Consumer Sentiment Survey, Forbes advisory, 2023. [Online]. Available: https://www.forbes.com/advisor/resources/forbes-ai-consumer-sentiment-survey
[22] Jillian Carmody, Samir Shringarpure, and Gerhard Van De Venter, "AI and Privacy Concerns: A Smart Meter Case Study," *Journal of Information, Communication & Ethics in Society*, vol. 19, no. 4, pp. 492-505, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[23] Joshua Joy, and Mario Gerla, "Privacy Risks in Vehicle Grids and Autonomous Cars," *Proceedings of the 2nd ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services*, pp. 19-23, 2017. [CrossRef] [Google Scholar] [Publisher Link]