ISSN: 2321-7782 (Online)
Volume 3, Issue 1, January 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

AI in Surveillance: Ensuring Judicious Blending of Security and Personal Liberty

Dr. Harindra Singh
Associate Professor,
Department of Physics,
CRA College, Sonipat, Haryana 131001

Abstract: In a swiftly changing technological scenario, artificial intelligence (AI) is playing a pivotal role in the arena of surveillance, enabling security in homes and establishments with modern, state-of-art and sophisticated systems supported by advanced software. Government offices, hotels, educational institutions, industry, shopping malls, residential buildings besides police, security and traffic management agencies are heavily relying on AI for ensuring security and continuous monitoring. All this is raising a major concern about personal liberty and individual freedom which is being encroached upon. The current study is thus targeted towards exploring ethical issues that has surfaced by continuous AI surveillance, emphasizing upon the ever increasing conflict between security and personal liberty. Adverse effect of new and advanced AI techniques on individual freedom and human civil rights are also under scanner in this study. Relevance of enacting proper regulatory bylaws and rules addressing ethical matters to ensure that AI surveillance operate within a well-defined framework without compromising personal freedom, are also being high lightened here.

Keywords: Ethics, surveillance, personal liberty, security, artificial intelligence.

I. INTRODUCTION

In recent years the overwhelming entry of artificial intelligence (AI) in all sorts of surveillance devices has altogether revamped the monitoring systems of government departments, security forces, private establishments and organizations etc. By incorporating face recognition and matching, involving high resolution pan, tilt and zoom (PTZ) cameras, doing precise behaviour interpretation, monitoring and analyzing smallest activities both inside and outside buildings, AI has highly improved the efficacy of surveillance techniques to ensure security and subdue crime. This digital advancement has however, sparked over a row over personal security and civil freedom rights all over the world [1]. With the help of advanced digital electronics and the development of high capacity data storage devices, the AI systems are getting more nail and teeth. The newly developed capabilities of mass storage of data is opening debatable questions such as up to what extent data should be collected, with whom this data needs to be shared and how this is going to be utilized for security without jeopardizing privacy. The current challenge therefore lies in establishing a delicate balance between using AI for ensuring security and protecting human civil rights in general and right to privacy in particular. The widespread use of AI in monitoring activity is thus pointing towards its wrong and unlawful use by authorities [2].

The current study is zeroing on to investigate the ethical issues involved in AI monitoring and finding ways for a judicious blending of security and privacy. The primary focus here thus is to explore ways for utilizing AI techniques for surveillance ensuring the genuine compliance of ethics. Finally, workable suggestions will be given to minimize the indiscriminate use of AI and ensuring security without scarifying privacy. Various objectives to critically investigate the ethical aspects of AI in surveillance machinery, with a special emphasis on ensuring judicious balance between enhancing security and protecting privacy are summarized in Fig. 1.

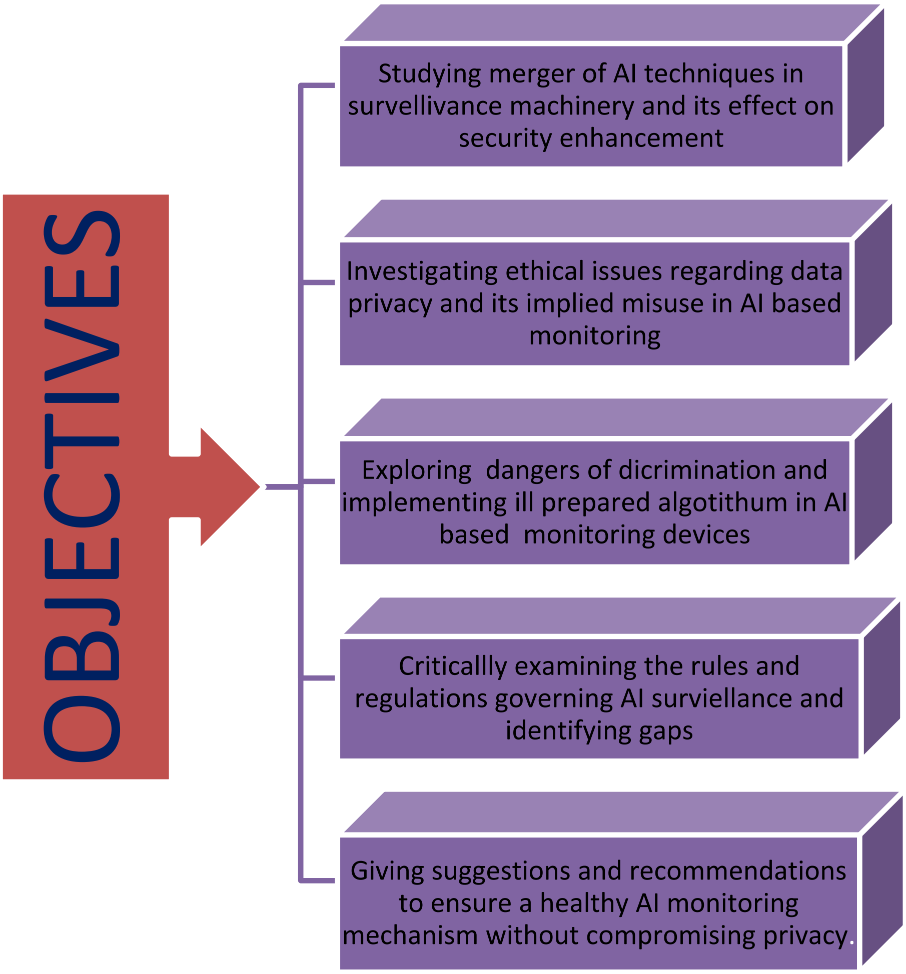
OBJECTIVES
Studying merger of AI techniques in survellivance machinery and its effect on security enhancement
Investigating ethical issues regarding data privacy and its implied misuse in AI based monitoring
Exploring dangers of dicrimination and implementing ill prepared algotithum in AI based monitoring devices
Criticallly examining the rules and regulations governing AI surviellance and identifying gaps
Giving suggestions and recommendations to ensure a healthy AI monitoring mechanism without compromising privacy.

Fig. 1 Basic objectives for investigating ethical aspects of AI in surveillance

By fulfilling the objectives shown above the study aims to contribute to ongoing burning issue regarding how AI techniques can be developed with enhanced accountability and transparency towards ethical use of AI in electronic monitoring services.

II. Literature Review

The emerging trend of regarding the AI based monitoring has triggered widespread investigations regarding its influence on ethical considerations especially related to privacy and personal freedom. Various parameters involved in literature survey are represented in Fig.2.

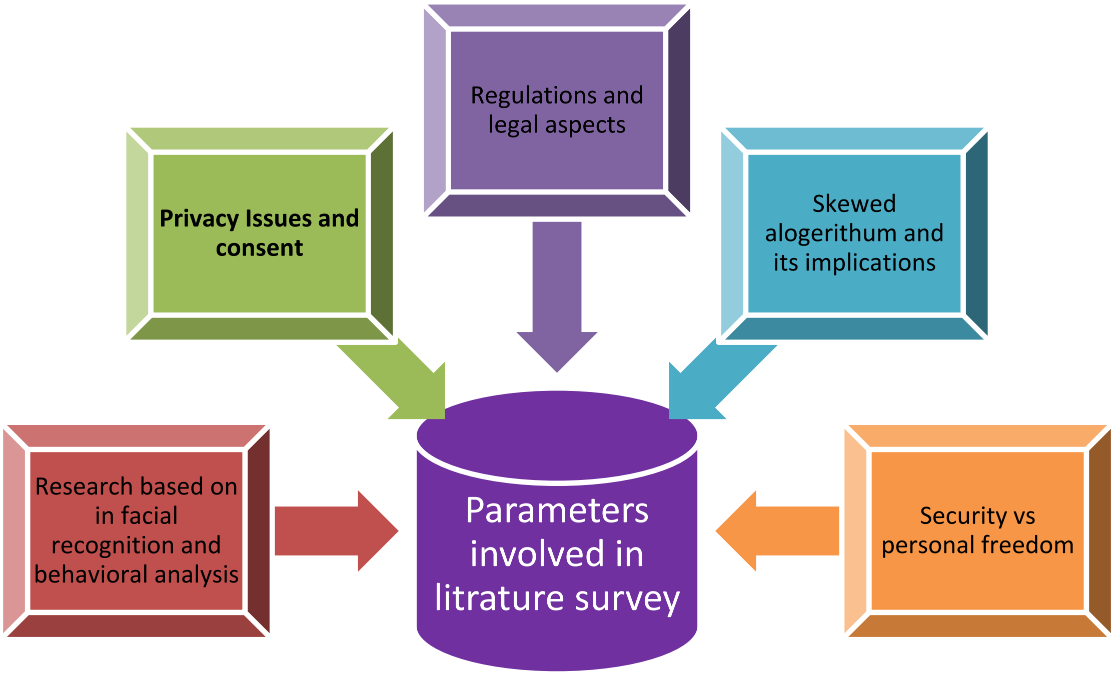
Regulations and legal aspects
Privacy Issues and consent
Skewed alogerithum and its implications
Research based on in facial recognition and behavioral analysis
Parameters involved in litrature survey
Security vs personal freedom

Fig. 2 Pictorial representation of various parameters involved in literature survey

Research has demonstrated how AI enhances surveillance systems, particularly in facial recognition, behavioral analysis, and predictive policing. Researchers have reported [3] capability of AI to handle mega data collections and analyze it in real time which helped in controlling crime and improved public safety. AI-based techniques are capable of identifying suspicious behavioral patterns, paving roadmap for dynamic security actions. However, it is contended that such capabilities come at the expense of privacy, as AI systems often operate in public and private spaces without individuals' consent. A major concern in the literature, however, is jeopardizing privacy because of the extensive expansion of AI monitoring. Various studies carried out by [4] throw light on how AI permits huge data harnessing without personal consent compromising individual freedom. This obviously draws attention towards ethical issues regarding privacy violating basic human civil rights. [5] have drawn the attention towards skewed algorithmic being employed in AI surveillance machinery and mentioned that several AI- based face identification systems display ethnic, cultural and gender biases, promoting discrimination which is unjustified and intolerable from ethical point of view. In the present investigation it is stressed that how biased algorithms can perpetuate societal inequalities.

Regulatory and legal aspects are of paramount importance in the current scenario of indiscriminate proliferation of AI monitoring. However, literature pertaining to this matter, which is limited but growing has pointed out that existing regulatory mechanism is lagging far behind the recent AI-technological developments, creating wide gulf in governance. It has been stressed [6] that only stringent regulations all over the globe will be capable of resolving the ethical issues regarding AI monitoring. The issue of a harmonious conglomeration of security and personal freedom has been raised by many researchers [7,8] emphasize that AI based monitoring should not overlook human civil rights. The literature review built an extensive knowledge of the ethical aspects regarding AI based monitoring, including terms and conditions of privacy, personal consent, skewed algorithm and governance. Whereas, AI has in numerous advantages for promoting security, its indiscriminate use in surveillance creates ethical issues that require urgent attention. This study is targeted towards examining existing framework and proposing new ethical guidelines for AI surveillance.

III. Ethical Challenges Involved in AI-Based Monitoring

The invasive nature of AI based monitoring technologies has evolved innumerous ethical challenges [9] which can be broadly classified into the following two categories.

3.1 Deprivation of personal freedom during data harnessing

A serious concern of AI surveillance is erosion of personal freedom during data collection as the systems are capable of storing huge amount of data of people without seeking their consent. Whether through facial identification, location tracking, behavior monitoring, or during surfing net, people are being continuously monitored, leading to anonymity deprivation and an atmosphere of fear and harassment. The ethical question which needs to be addressed is whether the advantages of improved digital security should be allowed at the cost of compromising privacy.

3. 2 Absence of permission and involvement of opacity

AI monitoring mechanisms usually perform recording without the permission of the stake holders. The absence of transparency by these devices in data acquisition, storage and utilization is of paramount concern. Usually people are unaware of their regular monitoring, and the opacity encroaches upon autonomy and personal consent.

IV. Blending Security and Privacy: Ethical Aspects

Improving security and safeguarding personal freedom is a debatable issue ever since the inception of AI based surveillance. In this section an investigation of the ethical aspects for ensuring a judicious blend between these conflicting issues will be carried out.

4.1 Security vs Privacy

AI based monitoring devices are usually supported for improving people's safety and security. State authorities plead that continuous surveillance of public places by government and private agencies is capable of predicting crime and hence guide to take preventive measures to combat it, besides helping in identifying criminals and law evading citizens during post crime investigation. [10]. This security, however comes at a hefty price and security outweighs privacy as illustrated in Fig. 3.

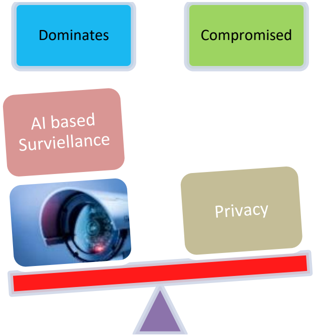

Fig. 3 Security vs Privacy imbalance

4.2 Quantum of Surveillance

AI driven surveillance should be in proportion to the magnitude of threat they are targeted to resolve. Overdose of surveillance i.e. excessive or indiscriminate surveillance involving whole populations, is unnecessary and condemnable. Ethical guideline for AI based monitoring must be adhered and data acquisition and surveillance must be limited to need based matters where there is a clear requirement of security. The concept of proportionality is of paramount importance in ensuring a judicious blend of security and privacy.

4.3 Anonymization and Encryption

Anonymizing acquired data is vital for safeguarding privacy and personal freedom. AI based monitoring devices must use methods like minimizing individual information involving pseudonyms. In organizations, anonymized data is still capable of detecting security related issues without scarifying worker's privacy. Excess vigil i.e. massive data collection and undesired surveillance of people will certainly lead to erosion of privacy and hence devices should also be equipped with data encryption techniques to ensure personal freedom. The incognito mode in search engines is an appreciable effort towards this matter. Thus monitoring services must be used smartly, striking a delicate balance between security and privacy.

4.4 Clarity and Lucidity

A prominent ethical aspect of AI surveillance in judiciously blending security and privacy is clarity, devoid of any hidden agenda. People must be knowing about how AI monitoring devices are being used, what information is under scanner and how that is going to be utilized. Clarity built mutual faith and permits the people to challenge agencies in case of any misuse of data. There should also be provision for the public to allow or disallow AI Monitoring when they sense that their privacy is being encroached upon [11].

4.5. Need of Ethical Guidelines

AI surveillance usually creates rift between individual rights and public interest for obvious reasons. On one side it supports public interest by enhancing security and curtailing crime and on the other, mass surveillance can encroach upon personal freedom, autonomy and right of expression. There must be well written ethical guidelines clearly mentioning when and how much surveillance is justified and when it going beyond limits. These guidelines should be framed keeping in view aspects such as lucidity, justification of AI and proportionality. State and private agencies entrusted with the task of carrying out AI monitoring must implement these properly. At the implementation stage it must be ensured that actions taken for surveillance do not unnecessarily pinpoint a particular category of people for discrimination. There must also be some provision for hearing and redressal of grievances.

V. Results and Regulations Governing AI Monitoring and Identifying Gaps

Keeping pace with the vast expansion of AI-based monitoring in all spheres of life, there is an urgent requirement for lucid rules and regulations for governance. Current regulatory system seems to lag behind fast changing technological developments taking place in this field creating a gulf resulting in immolation of privacy and indiscriminate monitoring. Thus a proper study is essential to examine existing regulatory frameworks, finding gaps and exploring way out so that AI monitoring is emphatically carried out.

5.1 Existing Legal Protection

Keeping in view the large scale violations in AI surveillance all nations across the globe have formulated data handling laws for safeguarding civil rights of citizens in the digital age e.g.in 2000, India passed Information technology (IT) act which looks after the affairs associated with AI Surveillance. In 2009, IT (procedure for safeguards for interception, monitoring and decryption of information) rules were framed to strengthen the legal framework for electronic surveillance. [12]. Whereas, these rules provide few privacy safeguards, they fail to regulate AI monitoring practices, leaving space for misuse. In Europe also there are laws pertaining to this issue, but stringent rules need to be framed. Other countries in Asia and Africa are also strongly working to face the AI monitoring related challenges.

5.2 Visible Gaps in AI monitoring Legislation

In spite of enacting of several data protection laws by nations across the globe, a gulf still exits which needs to be identified:

5.2.1 Inadequate AI-oriented regulations: The present data regulatory framework fails to limit capabilities of AI devices to incessantly acquire and analyze mammoth datasets in real time. Without framing AI-specific rules, monitoring devices can keep on encroaching upon privacy of public.

5.2.2 Unregulated inter-country data movement: Satellite communication and internet has enabled AI monitoring devices to share data globally [13]. To promote sales and expand business private companies presently are doing so at an alarming rate. The absence of common international framework makes it much easier for big business houses to carry on it jeopardizing privacy of public. Formation of a global regulatory body to supervise and check this unregulated data transmission, that threaten civil liberties, is the need of the hour.

5.2.3 Pathetic Enforcement system: Even in countries with robust data acquisition and handling laws, enforcement can be weak. Lackluster attitude of enforcement agencies and insufficient resources to properly monitor and punish agencies that violate privacy norm let such agencies flourish and violations keeps on going unhampered.

5.3. Responsibility of Government and the Private Organizations

Government and private organizations have a crucial role to play in formulating the rules and framework for AI based monitoring. It is Governments duty to frame stringent acts and regulations which are capable protecting individual rights by framing legislation that holds agencies responsible in matters of data acquisition and it's sharing during surveillance [14]. Simultaneously, private organizations fabricating AI machinery must ensure that ethical aspects have been embedded to safeguard privacy and transparency in AI systems.

VI. Proposals and Recommendations

For ensuring a judicious blending of security and privacy AI based monitoring requires a multi-pronged effort that includes robust regulatory mechanism, technical advancements, and ethical aspects. The recommendations and proposals shown in Fig.4, if implemented properly will surly ensure that AI monitoring devices can perform in a manner that that will keep a harmonious balance between security and civil liberty.

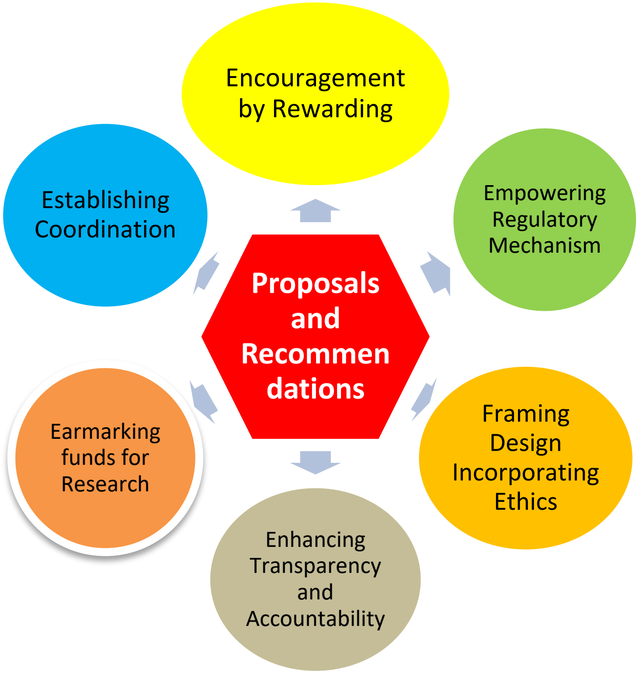
Encouragement by Rewarding
Establishing Coordination
Empowering Regulatory Mechanism
Proposals and Recommendations
Earmarking funds for Research
Framing Design Incorporating Ethics
Enhancing Transparency and Accountability

Fig.4 Proposals and Recommendations for balancing Security and personal liberty

6.1. Empowering Regulatory Mechanism

6.1.1. Frame AI-oriented rules and regulations: Existing data handling laws should be modified with directions mainly formulated for AI monitoring techniques. The new framework must be capable of handling issues like real-time data acquisition and proper behavioral monitoring. Guidelines in a lucid manner be prepared for data acquisition, safe and fool proof storage, and setting limits to ensure unnecessary data is not required [15].

6.1.2. Seeking international cooperation: International cooperation is very essential for regulating AI monitoring across the globe. Defining proper mechanism for AI monitoring at world level will ensure privacy within the framework of ethical practices internationally. UNO should also come forward towards framing rules and enforcing these, fostering harmony among countries to control cross-border data transmission issues.

6.1.3. Strengthening Enforcement agencies: Controlling agencies must be empowered with proper equipment and authority to implement data handling rules and checking violations of civil rights. Empowering enforcement set-up, to perform regular checks and penalize violators, will definitely compel organizations to work properly and comply ethical standards during AI monitoring.

6.2. Framing Design Incorporating Ethics

6.2.1. Embedding Privacy in Design: AI monitoring equipment should embed privacy in initial design itself, ensuring that privacy aspects are incorporated from the very beginning of mechanism [16]. It should necessarily involve data curtailment technology, so that only the required data for security purpose is acquired and utilized.

6.2.2. Observing Impact: Agencies using AI monitoring must invariably observe privacy impact regularly to assess possible threats and eliminate anything found eroding privacy. These observances should always take into consideration the impact on individuals' privacy and judge whether monitoring measures are proportional to security issues.

6.2.3 Eliminating Bias from Surveillance Software: Transparency in AI monitor should always be given utmost importance by eliminating potential biases from software. By carrying out regular checks for finding and eliminating biases will definitely mitigate discrimination and ensure that all ethnic and demographic groups under scanner are being treated at par.

6.3. Enhancing Transparency and Accountability

6.3.1 Enhance Transparency: All government agencies and private companies should be transparent in AI monitoring by revealing the forms of data acquired, its purpose and use. Transparency practices may include sending notifications to the stakeholders and opening communication channels for resolving grievances.

6.3.2 Fixing Responsibility: A well framed mechanism should be developed to fix proper responsibility in case of any misuse of AI monitoring devices. Duties of algorithm developers and operators of AI surveillance machinery in organizations must be properly conveyed so that in case of any lapse, violator can be identified and action can be taken. Besides it a system for appeal must be there to enable people to seek relief in case of erosion of their privacy.

6.4 Earmarking funds for Research

Financial support should be arranged for research which explores ways for the implications of AI monitoring on civil rights. Innovative techniques like advanced encryption and privacy-enhancing methods can limit the risk of any misuse of system. Funding projects for developing safety techniques which can safeguard privacy will surely give in impetus to the research in this field and help in zeroing on innovative ways for preventing encroachment upon it.

6.5 Establishing Coordination

By establishing a proper coordination among policy framers, researchers, software developers, and public a mechanism can be framed out with general consensus to address ethical concerns. It will contribute towards framing guidelines which will resolve myriad of problems and address required ethical aspects

6.6 Encouragement by Rewarding

Giving awards and honors to recognize the efforts of organizations that ensure ethical aspects during AI monitoring will definitely encourage other agencies to work towards protecting privacy of the public. This will help in developing AI surveillance environment which will provide security without compromising personal freedom.

VII. Conclusion

AI based monitoring techniques are instrumental in ensuring security and public safety. These techniques, however, pose innumerous ethical challenges that must be looked into deeply to ensure that privacy and personal freedom are not scarified at any cost. As AI techniques are being continuously embedded in surveillance practices, more care and thoughtfulness is definitely needed to address these challenges through stringent regulation, robust ethical design, and transparent operations. The acts and laws governing AI surveillance are still in primary stage. Although existing data handling laws give some relief, there is still a wide gulf that must be addressed to ensure a public friendly surveillance system. Thus both government and private sector should work in harmony to formulate AI operational rules. By adopting the proposed solutions and recommendations, organizations can head towards a balanced mechanism that can ensure to develop an AI monitoring system that treats security as well as personal freedom at equal footing. Thus if AI techniques are framed and used in a manner that protects privacy while enhancing security, maintaining trust and upholding personal freedom in this electronic era will become an easy task. As AI monitoring techniques continuously keep on improving, research in developing new safety techniques for safeguarding public privacy must also go side by side to keep pace with the changing scenario. Thus a concerted effort with a multi-faceted approach for maintaining a delicate balance between security needs and privacy rights will create win-win situation for both AI based surveillance operators and the public at large.

References

1. Korba, L. and Kenny, S. “Towards meeting the privacy challenge: adapting drm”, Digital Rights Management, LNCS 2696/2003, Springer, Berlin, pp. 118-36, 2003.
2. Information technology Security Techniques Evaluation criteria for IT security, 2005.
3. Acquisti, A., “Privacy and security of personal information: technological solutions and economic incentives”, in Camp, J. and Lewis, R. (Eds), The Economics of Information Security, Kluwer, Boston, MA, pp. 165-78,2004.
4. Jentzsch, N. Theory of Information and Privacy, Springer, Berlin, pp. 7-59, 2007.
5. Bostrom, N., Yudkowsky, E. The ethics of artificial intelligence. In The Cambridge handbook of artificial intelligence (pp. 316-334). Cambridge Press ,2014.
6. D. Choffnes, J. Duch, D. Malmgren, R. Guierma, F. E. Bustamante, and ´L. Amaral. Swarmscreen: Privacy through plausible deniability in p2p systems. Technical report, Northwestern University, 2009.
7. Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. http://dud.inf.tu-dresden.de/literatur/Anon Terminology vol.34.pdf, 2010.
8. Bingdong Li, Esra Erdin, Mehmet H. Gunes, George Bebis, and Todd Shipley. An overview of anonymity technology usage. Computer Communications, 36(12):1269–1283, 2013.
9. Anderson, M., & Anderson, S. L. . Machine ethics. Cambridge University Press,2011
10. Katsikas, S., Lopez, J. and Pernul, G. “Trust, privacy and security in e-business: requirements and solutions”, Proceedings of the 10th Panhellenic Conference on Informatics (PCI’2005), LNCS, Springer, Berlin, pp. 548-58, 2005.
11. Lee, H.-H. and Stamp, M. “An agent-based privacy-enhancing model”, Information Management & Computer Security, Vol. 16 No. 3, pp. 305-19,2008.
12. https://www.indiacode.nic.in
13. Aggarwal, G., Bawa, M., Ganesan, P., Garcia-Molina, H., Kenthapadi, K., Motwani, R., Srivastava, U., Thomas, D. and Xu, Y. “Two can keep a secret: a distributed architecture for secure database services”, Proceedings of the 2005 CIDR (Conference on Innovative Data Systems Research) Asilomar, CA, USA, January 4-7, pp. 186-99,2005.
14. Lederer, S., Hong, J., Dey, A. and Landay, J. “Personal privacy through understanding and action: five pitfalls for designers”, Designing Secure Systems That People Can Use, pp. 421-45, 2005.
15. Samuelson, P. “Privacy as intellectual property?”, Stanford Law Review, Vol. 52, p. 1125,2005.
16. Anderson, M., & Anderson, S. L. Machine ethics: Creating an ethical intelligent agent. AI Magazine, 28(4), 15–26, 2007.