Vol. 14, Sp. Issue: 1, December: 2025
ISSN: (P) 2347-5412 ISSN: (O) 2320-091X

Artificial Intelligence , Machine Learning and Data Protection Mechanisms

Dr. Sadhna Dixit

Assistant.Professor Govt. B.P.L.P.G.College Aarang (C.G.)

Abstract— AI (Artificial Intelligence) is the field of creating system . It is the broad concept of creating machines that can mimic humen intelligence. (AI) Artificial intelligence- Technologies are transforming industries worldwide, yet their integration raises significant challenges related to data protection. It considers challenges and opportunities for individuals and society. ML (Machine Learning) is the technology that has made many modern (AI) applications. It is a specific subset of (AI) that focuses on enabling system to learn from data.(ML) Machine- Learning is an artificial intelligence methodology . It is a vast and fascinating field. (AI) & (ML) are used for data protection through advanced threat detection, real-time monitoring & automated incident response. (AI) Artificial intelligence is an excellent tool for data protection. Data protection mechanisms are processes and technologies designed to safeguard sensitive information from unauthorized access, theft, or damage. These mechanisms are crucial in today's digital age, where data breaches and cyberattacks are increasingly common. Artificial intelligence (AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. It has rapidly increased in various fields such as health care, medical science, finance, & travel. This is because it can manage a lot of data effectively and make wise dicisions. (AI) continues to become more advanced. (AI) technologies have positive impacts towards all people. (AI) advancements & data protection imperatives , emphasizing the need for collaborative efforts across disciplines to foster a secure & ethical digital ecosystem.. Digital asset management (DAM) has been a foundational technology for (AI).

Keywords— Artificial intelligence, Machine Learning, Data protection, Digital ecosystem, Mimic action, Digital age, Digital assets.

Introduction:

Artificial Intelligence refers to the simulation of human cognitive processes by machines particular those capable of learning, reasoning, and adapting. (AI) , a blooming technology that seeks to provide a more efficient and easily accessible dataset for individual and organizational use . Artificial Intelligence is short for making machines as smart as humans by teaching them to think and learn like people. It has rapidly increased in various fields such as health care, finance, travel and transport, and entertainment (1) Wachter et al; 2017 This is because it can manage a lot of data effectively and make wise dicisions (2) Khassawneh et al; 2023. (AI) is the field of creating system. It is the broad concept of creating machines that can mimic human intelligence. (AI) is a branch of Science. (AI) Artificial Intelligence is changing data privacy and security. AI system have the capability to study data and then examine the behaviors that are considerd normal in comparison with what is looked at as weird , this means security risk (3) Bertino et al; 2021. Artificial Intelligence (AI) is then called the process of creating computer system that can do activities that require human intelligence. (4) Elliott et al; 2022.(AI) continues to become more advanced . AI technologies have positive impacts towards all people (5) Villegas et al; 2023. In the modern world protecting personal information has become

Vol. 14, Sp. Issue: 1, December: 2025
ISSN: (P) 2347-5412 ISSN: (O) 2320-091X

crucial since highly complicated algorithms used in (AI) & (ML) readily recognize peoples intimate details even when given uncomplicated dataset. The inter section of (AI) & (ML) and data protection presents a complex challange: even though these technologies are valuable. (Future of Privacy Forum 2020). (AI) advancements and data protection imperatives, emphasizing the need for collaborative efforts across disciplines to foster a secure & ethical digital ecosystem.

Overview

ARTIFICIAL INTELLIGENCE:

AI (Artificial Intelligence) is the field of creating system. It is the broad concept of creating machines that can mimic humen intelligence. (AI) Artificial intelligence is then called the process of creating computer system that can do activities that require human intelligence. The term can also be applied to any machine that exhibits traits associated with a human mind such as learning and problem solving. In the fast-paced digital era , (AI) Artificial intelligence has greatly transformed various sectors(06) (Vinuesa et al; 2020) , & its role in cyber security is becoming increasingly important. The current trend in digital threats portrays a grim reality. The advancement of (AI) integration into digital asset & data protection is a revolution. (AI) keeps data protection and privacy environments. Proper (AI) application can enhance security, but regulation must balance innovation & misuse. In the future, (AI) may be able to predict potential threats. (AI) is not just for large corporations. (AI) in (DAM) is also prevalent in scientific and cultural heritage communities.

MACHINE LEARNING

Machine learning is a powerful technology that's transforming industries and revolutionizing the way we live and work. It's a subset of (AI) that enables system to learn from data and improve their performance over time. Its ability to learn from data and make prediction or decisions. Machine learning has numerous applications, such as: Image recognition, Natural language processing, Predictive analytics, Recommendation systems. Key benefits of machine learning include-Automation, Insight generation, Prediction, & Personalization. .(ML) Machine Learning is an artificial intelligence methodology . It is a vast and fascinating field. (AI) & (ML) approaches have been created to manage big and complicated financial data with the goal of preventing data breaches in Fintech & other financial organization (7) Novick et al (2019). (ML) can detect suspicious activity in many ways . (ML) can accept & examine data to detect threats , trends, & ways of cybercrime attacks. (ML) systems process data to learn valuable patterns that solve and improve the performance of a specific task at hand. These systems have demonstrated high performance & accuracy, which have led them to become drivers of innovation in several disciplines & sectors such as computer vision(8) (Chai et al., 2021), autonomous transportation, health care (9)(Ghassemi et al., 2020), Biomedicines (10)(Mamoshina et al ., 2016), and law (11) (Surden, et al.,2014).Now a days , ML system are at the core of common technologies such as automatic hand writing, natural language recognition (12) (Md Ali et al .,(2021) ,speech processing (13) (Vila et al ., 2018), & biometric data analysis.

Advantage of Machine Learning

1. Fast, Accurate, Efficient.
2. Automation of most applications.
3. Wide range of real life applications.
4. Enhanced cyber security & spam detection.
5. Handling multi dimensional data.
6. Challanges Considerations.
7. Identify & rectify the errors.
8. Data Acquisition

DATA PROTECTION

Data protection mechanisms are processes and technologies designed to safeguard sensitive information from unauthorized access, theft, or damage. These mechanisms are

Vol. 14, Sp. Issue: 1, December: 2025
ISSN: (P) 2347-5412 ISSN: (O) 2320-091X

crucial in todays digital age , where data breaches and cyberattacks are increasingly common. Data protection refers to the protection of personal information from unauthorized access or use (14). Effective data protection helps build trust , prevent data breaches , and safeguard individuals rights. Key aspects of data protection include- Encryption, Access control, Data minimization, Transparency, and Compliance. Data is the life blood of any organization.

(AI) & (ML) Applications in Dataprotection

1. 1.Detecting threats
2. 2.Behavioral Analysis
3. 3.Real-timeMonitoring
4. 4.Encryption
5. 5.Adaptive Security Measures

Challanges Considerations

1. 1.Growing ethical concerns
2. 2.Autimation abuse
3. 3.Data security & associated privacy risk
4. 4.High set-up costs
5. 5.Lack of a notable framework
6. 6.Data volume and sensitivity

Significance of Data Protection

1. 1.Protects against harm
2. 2.Builds trust
3. 3.Avoids financial and reputational damage
4. 4.Safe guards
5. 5.Prevents fraud and cybercrimes
6. 6.Integrity and confidentiality

DIGITAL ECOSYSTEM

The digital ecosystem and (AI) are closely intertwined. (AI) is a key driver of innovation and growth in the digital ecosystem. The digital ecosystem provides the infrastructure and platforms for AI to thrive, including: Data analytics, Cloud computing, and Internet of things, & Analyze vast amount of data, Automate processes, Enhance customer experiences, & Drive innovation. The digital ecosystem and (AI) are transforming industries and revolutionizing the way we live and work. Using (AI) and loT to predict equipment failures. Leveraging (AI) and data to improve urban planning and services. The digital ecosystem and (AI) also raise important questions about Ethics and bias , data privacy, workforce development .

Digital Assets

A digital asset is anything that exists only in digital form and comes with a distinct uses right or distinct permission for use. Digital assets have data security , privacy, and personal control features that greatly improve the exchange of items of value over the internet. Digital asset management (DAM) has been a foundational technology for (AI).

Methodology

A Qualitative research approach is used. The study contributes to the theoritical knowledge of (AI) & (ML) applications in data privacy protection. The research method of this study is theoretical based. The research involves a systematic review, and studies. The literature search was conducted with (4) -database (Scopus, Web of science, Digital library, Google search). After the search 50 papers were analyzed.[2017-2023].

Result and Discussion

Finding reveal that (AI) system significantly advanced in today. (AI) advancement & data protection imperatives , emphasizing the need for collaborative efforts across disciplines to foster a secure and ethical digital ecosystem. The wide adoption of (ML) to solve a large set of real-life problems came with the need to collect & process large volume of data, some of which are considered personal and sensitive, raising serious concern about data protection. (ML) methods represent a landmark development to meet the dual challenge of innovation & security. Technology has become

an important part of our lifestyle with various advancement in different sectors including health care, medical science, finance, business, and transport & travel. This work serves as a guide for (AI) & (ML) researchers in this field.

Conclusion

(AI) Artificial intelligence plays an important role in enhancing data security by identifying threats & responding to them effectively. (AI) driven tools such as (ML) detection deep learning models for identification automated threat intelligence systems and advanced encryption techniques empower individuals & organizations to safeguard sensitive data. The research involves a systematic review, case studies to assess the effectiveness of AI in mitigating cyber threats. Technology has become an important part of our lifestyle with various advancement in different sectors including health care, medical science, travel & transport, and business sector with respect to detection , diagnosis and treatment. (AI) is a main driver of the 4th industrial revolution, driving innovation , reshapping products , services & creating new economics. (AI) advancement and data protection imperatives, emphasizing the need for collaborative efforts across disciplines to foster a secure & ethical digital ecosystem. (AI) & (ML) are evolving technologies that could help limit the growing data breaches .Despite the regulatory & privacy questions surrounding these technologies, their future use in business looks bright.

Final thought ---ARTIFICIAL INTELLIGENCE is a concept of creating intelligent machines that stimulates human behaviour where as MACHINE LEARNING is a subset of (AI) that allows machine to learn from data without being programmed.

References

- *Y. A. AL. Khassawneh, "A review of AI in security and privacy Research advancesapplication, opportunity, & challenges .Indonesian Journal of Science & Technology , Vol. 8, no. 1, pp.79-96 (2023)*
- *E Bertino, M. Kantareioglu, S, Mittal, M. Gupta "AI for Security 11th ACM Conference on Data application , security & privacy pp-333-334, (2021) .*
- *D. Elliott & E. Soifer (AI) Technology frontiers in AI , Vol.5, (2022) .DOI: 10.3389/ Frai .(2022) 826737*
- *W. Villegas-Ch and J. Garcia-Qrtiz Vol-12, no.18, pp .3786(2023). Comprehensive framework for Ensuring Security & privacy in (AI).*
- *Vinuesa et al ., (2020)*
- *Novick, B., Mayston, D., Marcus, S., Barry, R., Fox, G., Betts.(2019) (AI) & (ML) IN asset management Black rock .October(2019).*
- *Chai et al., (2021) Junyl Chai , Hao Zeng , Anmingli , Eric W.T. Ngai .Deep learning in computer vision: Acritical review of emerging techniques & applications scenarios .Mach. Learn. Appl, 6 (2021) , Article 100134 [SCOPUS] .*
- *Ghassemi et al ; (2020) Marzyeh Ghassemi , Tristan Naumann , Peter Schulam , Andrew L. Beam , Ireney . Chen , Rajesh Ranganath . A review of challenges and opportunities in Machine Learning for health . AMIA Summits Transl. Sci. Proc ; (2020) , pp. 191*
- *Mamoshina et al., (2016) ;Polina Mamoshina , Armando Vieira , Evgeny Putin , Alex Zhavoronkov Applications of Deep learning in biomedicine Mol.Pharm ; 13 (5) (2016) , pp.1445-1454 [SCOPUS] .*
- *Surden et al; (2014) ,Harry Surden Machine learning and Law Wash. L. Rev; 89 (2014) , pp.87 [SCOPUS] .*
- *Md Ali et al., (2021)Nawab Yousuf Md Ali, Lizur Md Rahman , Jyotismita Chaki , Nilanjan Dey , K.C.Santosh et al ; Machine translation using deep learning for universal networking language based on their structure . International journal Mach. Learn . Cybern ; 12 (8) (2021) , pp.2365-2376*
- *Vila et al., (2018)Laura cross vila , carlos Escolano , Jose A.R. Fonollosa , Marta R. Costa-Jussa End-to-end speech translation with the transformer Iber Speech (2018) , pp.60-63 [SCOPUS].*
- *M. K. Hasan, T. M. Ghazal, R. A. Saeed, B. Pandey, H. Gohel, , A.A.Eshmawi, S. Abdel-Khalek, & H.M.Alkhassawneh, "A, review on security threats, Vulnerabilities & counter measures of 5 G enabled Internet- of- Medical -Things," IET communications , Vol.16, no.5, (2022) DOI : 10. 1049 / cmu2 . 1230|*
- *ACM (2018) Data privacy and (ML) Challenges & opportunities .ACM Digital Library.*
- *Future of privacy forum (2020) Data privacy in the age of (ML).*
- *IBM (2021) What is AI.*
- *Sharma , P. (2020) (AI) in cybersecurity . The future of protecting Digitasl assets CRC Press.*