International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Special Edition: Volume: 04 PKDAL – 2025 DOI: 10.55041/ISJEM.PKDAL046
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Establishing a Cyber-Secure Knowledge Management Ecosystem for preservation through Artificial Intelligence intervention

Dr.Manju N. Dubey
Librarian
R.S Mundle Dharampeth Arts and Commerce College, Nagpur, Maharashtra-440010
Email: admin@rsmdacc.edu.in

Abstract:

Emerging Artificial Intelligence (AI) technology has revolutionized and pervaded various sectors, organizational systems and activities including Knowledge Management (KM).Libraries since time immemorial are engaged in knowledge management. In the knowledge domain, AI holds great promise in transferring tacit knowledge in useful explicit form. AI offers powerful tools for automating tasks, analyzing vast datasets, and extracting valuable insights. However, integrating AI into knowledge management systems introduces new cyber security challenges. This research article explores the interplay between AI and knowledge management, analyzing the influence of AI on knowledge management strategies and the cyber security risks associated with such integration. This paper explores case studies that illustrate the impact of AI on knowledge management practices and discusses real-world examples of cyber security incidents related to AI-powered knowledge management systems.

Keywords: Artificial Intelligence, Knowledge Management, Cyber Security, Knowledge Management System, Knowledge Sharing

1. Introduction

Knowledge management (KM) refers to the creation, capture, storage, retrieval, utilization, and sharing of knowledge within an organization. Effective KM practices are crucial for organizational success in today's knowledge-driven economy and libraries are in the forefront in doing it . In the digital age, KM is critical for organization to sustain and survive due to major influencers like 'Information Overload', breaking Information silos, demand for improved and innovative decision making, competition survival instinct, and expertise preservation for future reference. Artificial intelligence (AI) has brought disruptive transformation in various fields including the domains of knowledge management. AI presents a range of tools and techniques that can significantly enhance existing KM practices. In general, we can say KM is a sum total of two emerging field namely Computer science and Cyber security.

Emerging artificial intelligence (AI) capabilities is continuing to pervade nearly all organizational contours and activities, including knowledge management (KM).AI technologies ushered KM into a renewed landscape with enhanced capabilities in exploring the sources of expertise inside and across organizational setup and for expanding social interactions that serve as conduits of knowledge. But codifying tacit knowledge which revolves as a human-centered practice is always a challenging aspect. It get augmented through social interactions and informal correlates such as apprenticeships enabling practice-centered knowledge encounters. Hence tacit knowledge has always been a fascinating regime wherein even technological interventions failed to transform tacit knowledge experiences into extrovert usable form.AI holds a great promise and prospects in refurbishing the entire spectrum of KM practice and strategies.

2. Artificial Intelligence and Knowledge Management

AI has emerged as a game changer in all domains of human interface. AI is a broad spectrum of interplay of technologies that enable machines to exhibit human-like intelligence, including machine learning, deep learning, and natural language processing (NLP). On one hand Machine learning (ML) algorithms can learn from data without explicit programming, allowing them to identify patterns and make predictions. Deep

learning, a subfield of machine learning, utilizes artificial neural networks to process complex data sets and extract insights. NLP empowers machines to understand and manipulate human language, enabling them to analyze text documents and facilitate communication.

These AI functionalities hold immense potential for enhancing knowledge management practices. AI can automate tedious tasks like document classification, knowledge tagging, and content retrieval. Machine learning algorithms can analyze user behavior and search patterns to personalize knowledge delivery and recommend relevant information to users. NLP can facilitate the creation of intelligent chatbots that answer user queries and provide real-time knowledge support.

Artificial intelligence (AI) is rapidly transforming the field of knowledge management. By applying machine learning, natural language processing, and other AI techniques, organizations can significantly improve the way they capture, store, retrieve, and share knowledge.

Libraries being the major institution engaged in knowledge management. it is essential for libraries to explore the ways and means as well as major interventions due to Artificial intelligence in the knowledge management ecosystem.

Some of the key ways AI is being used in knowledge management are:

- **Automated content tagging and classification:** The content within documents, emails, and other data sources are automatically tagged and classified from vast amounts of unstructured data through automated AI tools. This makes it easier to find the information required in future.
- **Intelligent search and retrieval:** AI-driven search engines can understand the context of your query and return more relevant results. They can also learn from your past searches to personalize your experience.
- **Content synchronization and summarization:** Numerous documents are skinned into meaningful summary through automatized AI tools thus saving you time and gain key insights without tedious one to one analysis and sifting of data. It results in codification of knowledge by streamlining low level high volume knowledge [1] processes
- **Predictive analytics:** AI can be used to identify patterns and trends in your knowledge base. This information can be used to anticipate future needs and proactively surface relevant content to users.AI tools helps to accomplish task centered intelligence and manage content, process content as emergent references.

Chatbots and virtual Personal Intelligent assistants: These AI tools are like next to door companion to answer employee questions, troubleshoot problems, and provide step-by-step guidance. This can free up human knowledge workers to focus on more complex tasks. They helps to filter, sort and navigate information. They work to increase cognitive bandwidth and refrain from laxity due to information overload. AI technological evolution has improvised innovative applications for knowledge management ecosystem and the benefits of using AI in knowledge management includes:

- Improved efficiency
- Increased productivity
- Better decision-making
- Enhanced innovation
- Cost efficiency

3. Influence of AI on Knowledge Management Strategies

AI can significantly influence various aspects of knowledge management, including:

- **Knowledge Capture:** In any KM system data is the oil and AI-powered tools automates and fastens the process of data capture from various sources, such as emails, documents, and user interactions. Machine learning algorithms further analyze unstructured data and extract valuable

insight knowledge. For instance, sentiment analysis can be used to gauge employee sentiment from internal communications, providing insights into organizational culture and knowledge gaps.

- **Knowledge Retrieval:** AI can revolutionize knowledge search by leveraging natural language processing. AI-powered search engines can understand user intent and surface relevant information regardless of keywords used. Similarly AI can customized search results based on user profiles and past interactions with the knowledge base.
- **Knowledge Sharing:** AI-powered chatbots facilitates knowledge sharing by providing real-time assistance and answering user queries. AI can also recommend relevant knowledge assets to users based on their roles and current tasks. Additionally, AI can personalize learning experiences by tailoring content delivery to individual learning styles and preferences. This results in connecting people and generating know-how.

- **Knowledge Mapping:** AI facilitates easy access to collected data by synchronizing data across multiple platforms and using various collaboration tools. Intelligent content management, proactive decision] making, future challenges and opportunities anticipation are few key areas where AI reigns supreme.

- **Knowledge Democratization:** AI-driven solutions break the information silos by extracting, organizing and disseminating knowledge across the system fostering transparency and inclusivity.

Table 1 Impact of AI on traditional Knowledge Management practices

Aspect of KM	**Traditional Approach**	**AI-powered Approach**
Knowledge Capture	Manual data entry	Automated data capture from various sources, Conversion of Knowledge Assets in documented form
Knowledge Retrieval	Keyword-based search	Natural language processing-powered search, Taxonomy Tagging, Metadata Management, Knowledge Navigation, automated data harvesting from multiple levels
Knowledge Sharing	Static knowledge repositories	Personalized knowledge delivery through chatbots and recommendations, Just in time Contextual Prompts
Knowledge Mapping	Human inferences	Text abstraction, voice to text transcript,

4. Convergence of KM and AI

AI is transforming knowledge management (KM) in organizations in several groundbreaking ways. In KM ecosystem tacit and explicit knowledge both forms the core of system. Explicit knowledge is available in documented forms and available for use. Tacit knowledge got accumulated through amalgamation of various problem solving methods, innovative measures employed, inherent human expertise .KM strategies are augmented to a new level by hand holding by AI technologies.

Artificial intelligence technologies can enhance knowledge management by enabling advanced analytics and streamlining the retrieval of relevant information. Machine learning algorithms can detect patterns and insights within large datasets, thereby enhancing the value and usefulness of knowledge. Chatbots and virtual assistants enable real-time knowledge sharing, providing quick support and solutions to both customers and

employees. As AI evolves, it has the potential to transform the way businesses gather and use knowledge, leading to more informed decision-making.

The complementing role of AI in KM results in the following value additions in overall KM framework:

1. Powers Intuitive Management of Knowledge-AI empowers intuitive knowledge management by tailoring content, understanding user intent, and organizing information smartly.

2. Enhances Search Functionalities-AI employs natural language processing (NLP) to understand and comply with the user's intent behind queries.

3. Automates Processes-AI automates tasks like data organization, content creation, and search, freeing up human experts for deeper analysis.

4. Streamlines Content Creation-AI assists knowledge authors by creating new content or flipping existing standard of procedures (SOPs) into near accurate decision trees. It analyses existing data, identifies patterns, and generates new content

5. Offers Multilingual Support- Multilanguage support through AI mediation enriches KM ecosystem

6. Fortifies Data Security-KM systems often house sensitive information like trade secrets, intellectual property, customer data, and internal processes. Protecting this information is paramount for businesses.AI improves security with advanced techniques like anomaly detection, automated threat detection, and adaptive access control.

7. Provides Real-time Analytics-AI offers real-time insights into user interactions, common queries, and system performance.

8. Personalized User Experiences-AI personalized user experiences in knowledge management analyzing user behavior, preferences, and past interactions to proactively customized content, recommendations, and search results.

9. Facilitates Real-time Collaboration and Knowledge Sharing- AI integrates data from multiple sources, enabling instant updates, alerts and new insights and changes facilitating access to the latest knowledge, fostering a more collaborative and informed environment.

5. AI can boost Cyber Security in KM system

The domain of knowledge management can provide numerous benefits by harnessing the power of AI. AI applications in KM domain comes with automation piloting of so many fronts where earlier humans where indispensable.AI can supersede as a valuable tool for enhancing security in KM systems. Here are some ways AI can be leveraged for cyber security:

Anomaly Detection: AI algorithms can be used to analyze user behavior and system activity to detect anomalies that might indicate a potential cyber-attack. By identifying unusual patterns, AI can help organizations take proactive measures to prevent security breaches.

Threat Analysis: AI can be used to analyze and extrapolate large datasets to identify emerging and susceptible cyber threats and vulnerabilities. This helps organizations focus on security efforts and accordingly share resources effectively.

User Behavior Monitoring: AI can be used to monitor user behavior within KM systems and identify suspicious activity. This can help detect unauthorized access attempts or insider threats.

5.1 Few examples showing synergies between AI and KM organizations for cyber secure system:

- **Accenture and Palo Alto Networks**: Accenture, in partnership with Palo Alto Networks, has implemented AI-driven cyber security solutions within their Security Operations Center (SOC). Using Cortex XSIAM, they ingest comprehensive security data to enhance threat detection and incident management. This partnership emphasizes real-time intelligence and rapid response to threats, leveraging AI to maintain secure technology modernization and robust digital defenses(Palo Alto Networks).
- **Google Threat Intelligence**: Google integrates Mandiant expertise, VirusTotal threat intelligence, and the Gemini AI model to develop a threat intelligence platform. This platform uses conversational AI to analyze and summarize potentially malicious code, aiding in real-time threat detection and response.
- **Cloudera and Ollama:** The Cloudera platform, combined with Ollama's open-source LLM localization service, builds a customized knowledge management system using Retrieval-Augmented Generation (RAG). This system is designed to provide contextualized, secure, and efficient information retrieval for enterprises.

6. Cyber Security Issues in AI-powered KM Systems

In the knowledge management system, AI applications can emerge as a major game changer. On one hand AI empowers the whole KM ecosystem with its enormous capabilities but at the same time AI application itself are susceptible to major challenges like data security breaches, unauthorized access, manipulation in AI models datasets, reversing and automating cyber-attacks, launch phishing campaigns, or spread disinformation.

Table 2 Cyber Security Challenges in AI-Based Knowledge Management Systems

Challenge	Description	Impact
Data Breaches	Unauthorized access to sensitive data, leading to leaks, deletions, or falsification.	System outage, compromised customer trust, and potential loss of business.
AI-Generated Threats	AI can be used to create sophisticated phishing emails, malware, or deep fake videos.	Increased risk of successful cyber-attacks and potential financial losses.

Bias in AI Systems	AI systems can produce biased results if trained on biased data.	Discriminatory outcomes, false identifications, and potential legal issues.
Lack of Human Oversight	AI systems can make decisions without human intervention, leading to unintended consequences.	Potential for AI-driven attacks and lack of accountability.
Vendor Security	Inadequate security measures by vendors can compromise the entire system.	Data breaches, system downtime, and loss of customer trust.
AI Environment Isolation	Failure to isolate AI environments can lead to compromise of models and training data.	Potential for AI-driven attacks and data breaches.
Regulatory Compliance	Failure to comply with regulations and laws can result in legal issues and fines.	Potential legal and financial consequences.
User Adoption	Employees may resist AI-based systems due to lack of training or understanding.	Reduced system effectiveness and potential security risks.
Data Quality	Low-quality data can lead to poor AI performance and inaccurate results.	Inaccurate decision-making and potential business losses.

Model Deviation	AI models can deviate from intended behavior, leading to unintended consequences.	Potential for AI-driven attacks and data breaches.
Federated Learning	Federated learning can introduce new security risks, such as data leakage.	Potential for data breaches and compromised system security.

7. Real time cases reflecting the interplay of AI and KM from cyber security perspectives: Cyber security issues discussed above can be practical reflected through real time cases in KM systems of various organizations**.**

Table 3 Real Time cases of Cyber Security issues in AI based KM system

Incident	What Happened	Impact	Relevance to AI
Microsoft Exchange Server Hack (2021)	Hackers exploited vulnerabilities in Microsoft Exchange Server, gaining access to email accounts and installing malware for long-term access to victim environments.	Sensitive information was stolen from thousands of organizations worldwide, including personal data, business emails, and proprietary information.	If an AI-based knowledge management system was integrated with these servers, the attackers could potentially access AI-generated insights, decision-making algorithms, and confidential data processed by AI, leading to a larger-scale breach.
SolarWinds Cyber Attack (2020)	Attackers inserted malicious code into Solar Winds' Orion software, used by thousands of organizations, including several U.S. government agencies.	The malware created a backdoor into the systems, allowing attackers to spy on and steal data over an extended period.	AI-based systems relying on compromised infrastructure could have their models manipulated or used to infer sensitive data trends, affecting everything from operational strategies to national security.
Tesla Autopilot Data Breach (2020)	A hacker accessed Tesla's internal network and extracted data from the company's AI-driven autopilot system.	Exposed sensitive data related to the autopilot system's functioning and potentially proprietary information about Tesla's AI algorithms.	Breaches like this can lead to the theft of intellectual property, manipulation of AI models, and loss of trust in AI-driven products.
Facebook Data Leak (2019)	A vulnerability in Facebook's platform allowed the scraping of data from over 530	User data was exposed to the public, leading to privacy violations and	AI-based knowledge management systems processing this data could inadvertently train on leaked or maliciously altered

Incident	What Happened	Impact	Relevance to AI
	million users, including phone numbers and personal information.	potential phishing attacks.	data, skewing insights and decision-making.
AI Chatbots Compromised (Various incidents)	AI chatbots used by companies for customer service have been hacked or manipulated.	Hackers could extract sensitive information from conversations or inject malicious responses, leading to financial loss and reputational damage.	Compromising the AI models that power these chatbots can lead to the spread of misinformation, data theft, and a breach of customer trust.

8. Strategies for Ensuring Robust Cyber Security: To ensure robust cyber security in AI-powered KM systems, organizations can implement the following strategies:

- **Develop and implement a comprehensive security framework** that outlines security policies, procedures, and controls for AI systems.
- **Security Audit Monitoring** to identify and address vulnerabilities in AI-powered KM systems.
- **Employees Sensitization** on cyber security best practices and cyber security risks associated with AI.
- **Access controls** to restrict access to sensitive data and AI models.
- **Counter unauthorized access** by encrypting transit and in transit data to check misuse
- **Use secure coding practices** to develop AI models and KM systems.
- **Checkout with latest cyber security threats and related updates** and vulnerabilities.

9. Conclusion

AI offers tremendous potential for enhancing knowledge management practices within organizations. KM Organizations can leverage the power of AI to optimize outcomes from knowledge management practices while mitigating cyber security risks.The dual role of artificial intelligence (AI) in enhancing Cyber Security defenses while enabling sophisticated AI-driven attacks necessitates prototyping a comprehensive framework for secure AI adoption and strategies to mitigate emerging cyber threats effectively. AI-specific security protocols, fostering interdisciplinary collaboration, and ensuring continuous framework updates to match the evolving cyber threat landscape strengthens Cyber Security resilience in critical digital infrastructures. Libraries are key players in knowledge management and hence by proactively addressing these concerns and implementing appropriate security controls, organizations can harness the power of AI for knowledge management while minimizing cyber security risks.

References

[1] S. Sundaresan and Z. Zhang, "AI enabled Knowledge Sharing and Learni8ng: redesigning roles and processes," *International Journal of organizational analysis,* vol. 30, no. 4, pp. 983-999, 2022.

[2] M. Manesh, M. Pellegrini, G. Marzi and M. Dabic, "Knowldege Management in the fourth industrial revolution: Mapping the literature and scoping future avenues," *IEEE Transactions on Engineering Management,* vol. 68, no. 1, pp. 289-300, 2020.

[3] M. Jarrahi, D. Askay, A. Eshraghi and P. Smith, "Artificial Intelligence and Knowledge Management: A Partnership between human and AI," *Business Horizons,* vol. 66, no. 1, pp. 87-99, 2023.

[4] A. Bensick, "The Sixth generation -the headway of artificial intelligence," *Journal of International Studies,* vol. 14, no. 2, pp. 84-101, 2021.

[5] S. K. M. a. C. i. t. E. o. A. Intelligence, "Secure Knowledge Management and Cybersecurity in the Era of Artificial Intelligence," *Information Systems Frontiers,* vol. 25, no. 2, pp. 425-429, 2023.

[6] A. M. Ahmed, M. Shahbaz, R. Zareen, S. M. UlHassan, M. A. S. Uddin, M. V. U. Kaif and M. A. Uddin, "Cyber Security and Artificial Intelligence," in *14th International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2023*, 2023.

[7] T. Stevens, "Knowledge in the grey zone: AI and cybersecurity," *Digital War,* vol. 1, no. 1-3, pp. 164-170, 2020.

[8] N. Fteimi and K. Hopf, "KNOWLEDGE MANAGEMENT IN THE ERA OF ARTIFICIAL INTELLIGENCE-DEVELOPING AN INTEGRATIVE FRAMEWORK," *Research in Progress,* 2023.

[9] H. C. Hoeschl[1] and V. Barcellos[2], "ARTIFICIAL INTELLIGENCE AND KNOWLEDGE MANAGEMENT," 2022.

[10] R. Gururajan and V. Gururajan, "An Examination into the Role of Knowledge Management and Computer Security in Organisations," 2023.

[11] M. H. Jarrahi, D. Askay, A. Eshraghi and Preston Smith, "Artificial intelligence and knowledge management: A partnership between human and AI," *Business Horizons,* vol. 66, no. 1, pp. 87-99, 2023.

[12] M. Nick, S. Groß and B. Snoek, "How Knowledge Management Can Support the IT Security of eGovernment Services".

[13] H. Reisinger and P. D. Cin, "How AI-Powered Security Capabilities Implement Real-Time Cybersecurity," January 2024. [Online]. Available: https://www.paloaltonetworks.com/blog/2024/01/ai-powered-security-capabilities/. [Accessed 3 July 2024].

[14] A. Fitzgerald, "How Can Generative AI Be Used in Cybersecurity? 10 Real-World Examples," 16 May 2024. [Online]. Available: https://secureframe.com/blog/generative-ai-cybersecurity. [Accessed 3 July 2024].

[15] C. Snell and V. Rajagopalan, " Building and Evaluating GenAI Knowledge Management Systems using Ollama, Trulens and Cloudera," 23 May 2024. [Online]. Available: https://blog.cloudera.com/building-and-evaluating-genai-knowledge-management-systems-using-ollama-trulens-and-cloudera/. [Accessed 4 July 2024].

[16] M. Bastian, "Challenges," 25 October 2023. [Online]. Available: https://www.linkedin.com/pulse/challenges-implementing-ai-knowledge-management-martin-bastian-gduof/)/. [Accessed 4 July 2024].

[17] Microsoft, "Cyber Security," 2 March 2021. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/. [Accessed 4 July 2024].

[18] Z. Whittaker, "Hackers stole passwords for accessing 140,000 payment terminals," 1 August 2022. [Online]. Available: https://techcrunch.com/2022/08/01/wiseasy-android-payment-passwords/. [Accessed 3 July 202].

[19] A. Holmes, "533 million Facebook users' phone numbers and personal data have been leaked online," 4 April 2021. [Online]. Available: https://www.businessinsider.in/tech/news/533-million-facebook-users-phone-numbers-and-personal-data-have-been-leaked-online/articleshow/81889315.cms. [Accessed 3 July 2024].

[20] F. Lambert, "Tesla sues two former employees over 'Tesla Files' data leak," 21 August 2023. [Online]. Available: https://electrek.co/2023/08/21/tesla-sues-two-former-employees-tesla-files-data-leak/. [Accessed 3 July 2024].

[21] S. Oladimeji and S. M. Kerner, "SolarWinds hack explained: Everything you need to know," 3 November 2023. [Online]. Available: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know. [Accessed 3 July 2024].

[22] S. Meenakshisundaram, "Navigating Security Challenges In The Age Of AI Chatbots," June 2024. [Online]. Available: https://www.forbes.com/sites/forbesbusinesscouncil/2024/06/17/navigating-security-challenges-in-the-age-of-ai-chatbots/. [Accessed 3 July 2023].