International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhanced Security Encryption and Data Driven Model for Digital transition using Artificial Intelligence

Dang Thanh Le[1*], Nguyen Van Thanh[2]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: In an era of digital data security, ensuring robust security measures is paramount to safeguarding sensitive data. This paper proposes an innovative approach combining enhanced security encryption and a data-driven model empowered by artificial intelligence (AI) to fortify digital transitions. The methodology begins with a meticulous assessment of objectives, data inventory, and classification to discern the scope and sensitivity of information involved. An encryption strategy tailored to the data's sensitivity level is then devised, encompassing encryption at rest, in transit, and end-to-end encryption where applicable. Integrating AI into the security framework enables real-time threat detection through sophisticated algorithms analyzing network traffic, user behavior, and system logs. Moreover, AI-driven behavioral analytics augment monitoring capabilities, enabling the identification of anomalies indicative of potential security breaches. By amalgamating encryption with AI-driven insights, this approach presents a comprehensive solution to fortify digital transitions, ensuring data integrity, confidentiality, and compliance with regulatory standards.

Keywords: *Digital transformation, security measures, sensitive data, enhanced security encryption, data-driven model,*

1. Introduction

The inception of the internet in the mid-1990s has accelerated the digitization process in western societies[1]. The availability and accessibility of data through multiple digital communication channels (email, websites, forums) contributed directly to the transformation of modern business models as well as the ways governments deliver services. Digitization also includes the adoption of digital processes to enhance organizations' engagement with their customers, patients, employees, and constituents. More recently, the development and application of new technologies such as cloud computing, artificial intelligence (AI), and Internet of Things (IoT) have directly contributed to the expansion of the digitization of businesses and allowed for innovative digital transformation across industry verticals. For the purposes of this chapter, our analysis focuses on the rise of AI in digital transformation and the challenges related to its use. It is now undeniable that AI is one of the main core technologies that is enabling digital transformation[2]. More specifically, AI combined with digital transformation currently generates the most results or value in these three areas: (1) 360-degree view of customers; (2) dynamic analytics; and (3) AI-driven automation for customer service. To better understand the development of AI and its impact on digital transformation, this chapter will examine the following topics: (1) from computerization to artificial intelligence; (2) AI performance and digital solutions; (3) ethical challenges; (4) security challenges; and (5) protecting AI solutions.

Digital transformation, fueled by advancements in artificial intelligence (AI), has become a cornerstone for organizational evolution across various sectors. This paper explores the profound impact of AI-driven digital transformation on state management, focusing on governmental agencies and public institutions.

The integration of AI technologies such as machine learning, natural language processing, and robotic process automation has revolutionized traditional bureaucratic processes, enhancing efficiency, transparency, and decision-making capabilities within government bodies[3].

2. Key areas of Impact Include:

Improved Service Delivery: AI-powered systems streamline citizen services, reducing bureaucratic hurdles and enhancing overall service quality.

Data-Driven Governance: AI algorithms analyze vast datasets to extract actionable insights, facilitating evidence-based policymaking and resource allocation.

Enhanced Security: AI-driven cyber security measures bolster state infrastructure against cyber threats, ensuring data privacy and integrity.

Cost Optimization: Automation of repetitive tasks through AI leads to cost savings and resource optimization, enabling governments to allocate funds strategically.

[1]*National Academy of Public Administration, Hanoi city, Vietnam*
[2]*Central Theoretical Council of the Communist Party of Vietnam, Hanoi city, Vietnam*

Citizen Engagement: AI-driven platforms foster greater citizen engagement through personalized interactions, feedback mechanisms, and efficient communication channels.

However, the adoption of AI in state management also raises concerns regarding data privacy, algorithmic bias, and job displacement. Addressing these challenges requires robust governance frameworks, ethical guidelines, and continuous monitoring mechanisms.

This paper synthesizes insights from existing literature, case studies, and expert opinions to provide a comprehensive overview of how AI-driven digital transformation is reshaping state management practices. It underscores the need for responsible AI deployment, stakeholder collaboration, and adaptive policy frameworks to harness the full potential of AI while mitigating associated risks.

3. AI Performance and Digital Solutions

Artificial intelligence (AI) performance has experienced remarkable advancements in recent years, catalyzing a profound impact on digital solutions across various sectors. This section delves into the evolving landscape of AI performance and its implications for the development and deployment of digital solutions[4].

Machine Learning Algorithms: The performance of AI is largely driven by advancements in machine learning algorithms. Algorithms such as deep learning have demonstrated unprecedented capabilities in tasks such as image recognition, natural language processing, and predictive analytics. This enhanced performance has enabled the development of more sophisticated and accurate digital solutions[5].

Automation and Efficiency: AI-driven automation has revolutionized processes within organizations, leading to increased efficiency and productivity. Tasks that were once labor-intensive and time-consuming can now be automated with high accuracy, allowing human resources to focus on more complex and strategic endeavor[6]s.

Personalization and Customer Experience: AI-powered digital solutions have enabled a new era of personalization in customer experience. By analyzing vast amounts of data, AI algorithms can tailor recommendations, content, and interactions to individual preferences, enhancing customer satisfaction and loyalty[7].

Decision Support Systems: AI's improved performance has bolstered the development of decision support systems that assist professionals in making data-driven decisions. These systems leverage AI algorithms to analyze data, extract insights, and provide recommendations, empowering organizations to make informed and strategic choices[8].

Real-Time Insights: The speed and accuracy of AI algorithms have enabled real-time data analysis and insights generation. This capability is particularly valuable in dynamic environments where timely decisions are critical, such as financial markets, supply chain management, and emergency response systems.

Ethical Considerations: Despite the impressive performance gains, AI deployment raises ethical considerations related to bias, fairness, transparency, and accountability. Ensuring that AI systems operate ethically and responsibly is paramount to building trust and mitigating potential harms.

In summary, AI's performance improvements have significantly influenced the development and deployment of digital solutions, driving automation, personalization, decision support, real-time insights, and ethical considerations. As organizations continue to leverage AI capabilities, striking a balance between innovation and ethical responsibility will be key to maximizing the benefits of AI-driven digital transformation.

Within the framework of the 4.0 revolution, digital transformation offers a solution that does more than just boost efficiency and save expenses; it also creates new opportunities for growth, enriching the organization's value chain beyond its core principles. To put it simply, digital transformation is the process by which people and businesses undergo radical changes to their lifestyles, ways of working, and production techniques via the use of digital technology [9]. When an organization undergoes digital transformation, its operational model is updated to make better use of digital technologies and data. Actually, the next stage in the evolution of IT applications is digital transformation: Typically, when IT is used, it doesn't alter current models or processes. However, digital transformation occurs when IT is used at a high level and causes modifications to these things. The two concepts of digital transformation and information technology application are clearly distinct. In contrast to digital transformation, which entails the digitization of an entire organisation, the former involves the digitization of preexisting processes, models, and methods of service delivery, while the latter refers to the digitization of new services provided by an organization's operations. For instance, in state agencies, there are three ways that work is handled:

(1) the traditional method, where civil servants handle tasks on paper and communicate directly; (2) the application of information technology, where civil servants draft documents, print them, submit them for signature, and communicate directly;

(3) the digital transformation, where civil servants draft, edit, and submit signatures online in the Office system; and online exchange in an environment using digital technology. In this instance, the conventional method of processing work by state agencies has been superseded by an online alternative brought about by digital transformation.

The reality is that different types of organisations' management styles dictate different ways to approach the subject of digital transformation. When it comes to corporate governance, digital transformation means incorporating digital technologies into every part of a company. This allows the business to take advantage of these technologies to change its operations and business model, speed up its operations, and provide new values to its customers [10]. The term "digital transformation" refers to the process of transitioning from an analogue to a digital business model. This entails implementing changes to leadership, operations, processes, and corporate culture as well as new technologies like the internet of things (IoT), cloud computing, and big data (DP, 2023). Digital transformation, in this view, necessitates a shift in company culture and operational practices, as well as an openness to trying new things and learning from mistakes.

When it came to state management, some nations' government apparatuses jumped into a new digital transformation race after realising the relevance of the technology for improving operational efficiency and guaranteeing national security. As a result, digital transformation is a strategy that involves using digital data and technology to alter the state's service delivery to its citizens, as well as its business operations, management models, and activity methodologies (DCI, 2022). Researchers and managers use this method to highlight the idea of "digital transformation" by differentiating it from "digitalization": In contrast to digital transformation, which entails using data acquired through digitalization and applying technology to analyse, change, and produce newer values, digitalization refers to the process of modernising and transforming traditional systems to digital ones (e.g., moving from paper documents to electronic documents on computers, or switching from analogue to digital broadcasting in television). As a result, digitalization is best understood as an aspect of digital transformation.

Therefore, there are several ways to define digital transformation, but the following are some of the most common: the widespread use of digital technology throughout an organisation; the use of digital technologies to radically alter the structure and operation of an organisation; Make data digital, then use it to your advantage by transforming and exploiting it to generate new benefits for your business. While developing the idea of digital transformation linked to the structure and operations of state agencies, the author draws on the aforementioned methods based on research into the features of state management activities, namely: New values will be created in the organisation and functioning of state agencies via the use of digital technology and digital data.

Developing an enhanced security encryption and data-driven model for digital transition using artificial intelligence (AI) involves several key steps and considerations. Here's a high-level overview of the process:

Identify Objectives and Requirements: Determine the specific goals of the digital transition and the requirements for security, privacy, and compliance. Consider factors such as data sensitivity, regulatory requirements (e.g., GDPR, HIPAA), and industry standards.

Data Inventory and Classification: Conduct a thorough inventory of the data that will be involved in the digital transition. Classify the data based on sensitivity and importance to ensure appropriate security measures are applied.

Encryption Strategy: Develop an encryption strategy based on the sensitivity of the data and the desired level of protection. This may include encryption at rest, encryption in transit, and end-to-end encryption for communication channels.

AI-Powered Threat Detection: Implement AI-powered threat detection mechanisms to identify and respond to security threats in real-time. This may involve using machine learning algorithms to analyze patterns in network traffic, user behavior, and system logs to detect anomalous activities indicative of security breaches.

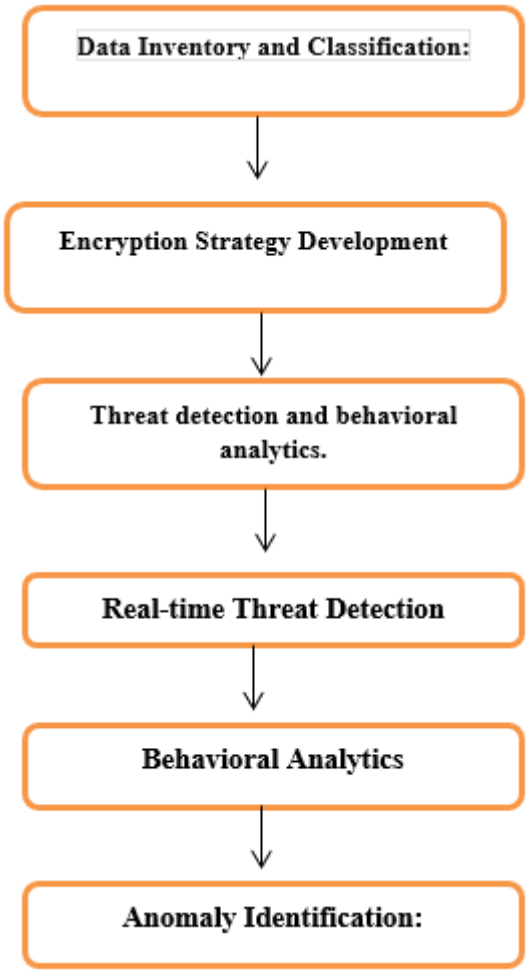

Fig 1. Flowchart of Enhanced Security Encryption and data driven Model for Digital transition

Internet of things: Is a key component of the 4.0 revolution, bridging the gap between the physical and virtual worlds to enable seamless digital transformation. In the same way that the internet allows for the interchange and sharing of data between various devices (computers, cellphones, etc.), the internet of things enables the simultaneous connection of any and all physical objects.

Big data: Resulting from the proliferation of network-enabled smart gadgets and sensors that link physical objects and human actions. On a daily basis, this data is produced to the tune of what would have previously been saved on one billion DVDs. Processing and analysing such data now takes a fraction of the time it did with older technologies, allowing for the extraction of knowledge, information, and insights in a fraction of the time. choose the right choices.

Cloud computing: Cloud computing is a technology that allows providers to store computing power on virtual servers on the internet, rather than in people's homes or workplaces, and then make that capability accessible as a service when required. Just with grid energy, which eliminates the need for people, households, and businesses to buy generators, cloud computing allows users to connect to the power company's grid services, pay only for the power they really use, and forget about the management and maintenance of the system.

b) Digital data

Digital data is data formed through digitizing documents using information technology applications - the process of modernizing and converting conventional systems to digital systems, such as converting from documents paper format to electronic documents on the computer. State agencies apply information technology to digitize documents such as policy documents, direction documents, instructions... issued and still in effect related to each management field, thereby forming up the agency's digital data.

When digital transformation, with the use of digital platforms such as document access systems, agencies, organizations, and citizens can exploit data (free or pay for access services) to carry out legal transactions and requests with state agencies. Example of commune-level digital transformation platform: Instead of developing 10,599 software for 10,599 communes, wards and towns across the country today (GSO, 2023), using a common platform for 10.599 communes and wards, the town will shorten implementation time and optimize costs;

Agencies, organizations, and citizens will access this digital platform to conduct transactions and request administrative records with commune-level government agencies.

4. Conclusion

The integration of enhanced security encryption and a data-driven model empowered by artificial intelligence (AI) represents a promising approach to fortify digital transitions. Through meticulous assessment of objectives, data inventory, and classification, organizations can discern the scope and sensitivity of information involved, laying the groundwork for robust security measures. The synergy between enhanced security encryption and a data-driven model empowered by AI offers a holistic approach to safeguarding sensitive data in the era of digital transformation. Embracing this approach can enable organizations to navigate the complexities of digital transitions with confidence, mitigating risks and enhancing overall cybersecurity posture.

References

[1] Developing an enhanced security encryption and data-driven model for digital transition using artificial intelligence (AI) involves several key steps and considerations. Here's a high-level overview of the process:

[2] Identify Objectives and Requirements: Determine the specific goals of the digital transition and the requirements for security, privacy, and compliance. Consider factors such as data sensitivity, regulatory requirements (e.g., GDPR, HIPAA), and industry standards.

[3] Data Inventory and Classification: Conduct a thorough inventory of the data that will be involved in the digital transition. Classify the data based on sensitivity and importance to ensure appropriate security measures are applied.

[4] Encryption Strategy: Develop an encryption strategy based on the sensitivity of the data and the desired level of protection. This may include encryption at rest, encryption in transit, and end-to-end encryption for communication channels.

[5] AI-Powered Threat Detection: Implement AI-powered threat detection mechanisms to identify and respond to security threats in real-time. This may involve using machine learning algorithms to analyze patterns in network traffic, user behavior, and system logs to detect anomalous activities indicative of security breaches.

[6] K. Ingole and D. Padole, "Design Approaches for Internet of Things Based System Model for Agricultural Applications," 2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP), Nagpur, India, 2023, pp. 1-5, doi: 10.1109/ICETET-SIP58143.2023.10151606.

[7] Stahl, B.C. (2021), Ethical Issues of AI. In: Artificial Intelligence for a Better Future, SpringerBriefs in Research and Innovation Governance, Springer, pp. 35-53.

[8] Trung, N.S. (2022). “Digital transformation and conditions for implementing digital transformation in state management activities”. State Management Review,

[9] Zemmar, A., Lozano, A.M., and Nelson, B.J. (2020). The rise of robots in surgical environments during COVID-19, Nature Machine Intelligence, vol. 2, pp. 566–572

[10] Lee, K., & Trimi, S. (2020). The impact of artificial intelligence on public governance: Opportunities and challenges. Public Administration Review, 80(6), 992-1002. DOI: 10.1111/puar.13255

[11] Lee, K., & Trimi, S. (2020). The impact of artificial intelligence on public governance: Opportunities and challenges. Public Administration Review, 80(6), 992-1002. DOI: 10.1111/puar.13255