Journal of Business Insight and Innovation

Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

EXPLORING AI-DRIVEN APPROACHES FOR SAFEGUARDING SENSITIVE ERP, HR, AND DEFENSE DATA WITHIN U.S. ORGANIZATIONS

Nasrin Sultana [1], Md Abu Nasir [2], Chinmoy Majumder [3], Arafat Hossain Khan Choain [4]

Affiliations:

[1] George Herbert Walker School of Business and Technology, Master of Arts in Information Technology Management, Webster University, US
Email: nsultaana94@gmail.com

[2] George Herbert Walker School of Business and Technology
Master of Arts in Information Technology Management, Webster University, US
Email: irfannasir000@gmail.com

[3] George Herbert Walker School of Business and Technology
Master of Science in Cybersecurity – Threat Detection and Cybersecurity Operations, Webster University, US
Email: chinmoymajumder2013@gmail.com

[4] George Herbert Walker School of Business and Technology, Master of Arts in Information Technology Management, Webster University, US
Email: arafat.hossain.khan@gmail.com

Corresponding Author(s) Email:

[1] nsultaana94@gmail.com

Abstract

In the era of digital transformation, safeguarding sensitive data in systems like ERP, HR, and defense platforms is a critical priority for U.S. institutions. Traditional cybersecurity often fails against evolving threats, but Artificial Intelligence (AI) offers a proactive, intelligent solution for real-time risk detection and mitigation. This study investigates how AI-driven strategies, data protection mechanisms, and supportive organizational policies collectively enhance data security and resilience.

A quantitative study surveyed 300 U.S. professionals across private, public, defense, and research sectors. Data analysis revealed strong positive perceptions of AI-driven security (mean ≈ 4.0). Statistical analysis confirmed significant positive relationships between all key variables. Regression identified Data Protection Mechanisms (β = 0.43) as the strongest predictor of AI's perceived effectiveness, followed by AI-Based Security Strategies (β = 0.31) and Organizational Policies (β = 0.25). Furthermore, significant differences existed across sectors, with the defense sector rating AI effectiveness highest.

The findings confirm that AI significantly enhances data protection and organizational resilience. Its success is strongly influenced by integrated data mechanisms, robust AI strategies, and supportive policies. The defense sector's higher perception underscores the value of structured AI adoption in high-stakes environments. Organizations should invest in AI-enhanced security systems, sophisticated data protection, and align with national cybersecurity regulations. Leadership commitment, ethical AI governance, and comprehensive employee training are crucial for maximizing benefits. Cross-sector collaboration and continuous innovation are recommended to maintain security performance and ensure equitable AI implementation across all organizations.

Keywords: Artificial Intelligence, Data Protection, Cybersecurity, Organizational Policies, ERP and Defense Systems, U.S. Organizations

Introduction

In the era of the digital world, data is the most valuable key to any organization in all sectors. The rapid expansion of information systems such as Enterprise Resource Planning (ERP) and Human Resource (HR) management systems has revolutionized how organizations in the United States store, process, and utilize information (Dalal, 2019). These systems integrate and centralize business operations, employee records, and decision-making processes, creating massive data ecosystems that are critical for operational efficiency and strategic competitiveness (Onoja et al., 2021). However, with the growing complexity and interconnectivity of these systems, the exposure to cybersecurity threats has increased significantly. Sensitive data related to organizational operations, employee details, and defense information has become an attractive

Journal of Business Insight and Innovation
Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

target for cybercriminals and hostile actors. As U.S. organizations rely more heavily on digital infrastructures, the need to safeguard data integrity, confidentiality, and availability has become a national priority (Faruk & Khan, 2022).

The United States, being at the forefront of technological innovation, also faces some of the world's most sophisticated cyber threats. Incidents of data breaches, ransomware, and espionage targeting U.S. businesses, government agencies, and defense departments continue to rise both in scale and sophistication. Traditional cybersecurity mechanisms, though still essential, are often reactive and limited in their ability to detect and mitigate rapidly evolving threats (Chinta, 2020). As cyberattacks become more automated and adaptive, conventional rule-based systems struggle to respond effectively. In that regard, Artificial Intelligence (AI) may be regarded as a novel resource capable of changing the meaning of the data protection framework. AI technologies, such as machine learning, deep learning, and predictive analytics, are increasingly being employed to detect anomalies, predict potential threats, and automate defensive responses in real time (Routhu et al., 2020). In addition to improving their cybersecurity status, the U.S. organizations are currently resorting to AI-based systems to improve their ability to be compliant with the federal security practices and data protection regulations and rules.

AI-powerere security system is especially vulnerable to the scalability of the new and modern cyber threats. By learning from historical data and identifying behavioral patterns, AI systems can detect unusual activities that may signify breaches or unauthorized access to critical systems like ERP and HR platforms (Polu et al., 2021). One such example is that AI may be applied in order to analyze the insider log-in, use techniques, system use, etc. and identify insider threats or external attacks before they inflict much damage. This proactive capability distinguishes AI from traditional systems that typically rely on pre-defined rules and static signatures (Imran et al., 2022). The use of AI in the U.S. corporate and defense environment, where the sensitivity of data is extremely high, promotes the resiliency of the system in relation to both internal and external security threats. It allows for faster incident response, greater precision in identifying vulnerabilities, and more efficient use of cybersecurity resources (Das et al., 2022).

U.S. defense and government teams are especially relying on the secure data environment because of the national ramification of data breaches. Sensitive defense information, including strategic plans, communications, and operational logistics, is often integrated within digital networks that require the highest levels of protection (Aiswarya, 2021; Asif, 2024; Inyang et al., 2024). Likewise, defense and federal organizations have employee-related information that is sensitive and includes background information, clearance, and personal records in their HR systems. Attack in such systems would not only harm individuals but also be very dangerous to national security. Therefore, AI-based defense data security has become a key focus area within U.S. cybersecurity policy and strategy (Stone et al., 2022). By integrating AI, the defense and intelligence agencies can also automate the process of identifying threats, performing predictive risk assessment, and processing large datasets more accurately.

In the corporate sector, ERP systems form the core of the operation of the enterprise, combining financial, logistical, and operational data of the departments. Any failure in these systems can interfere with whole organization processes and result in great losses of money and reputation. In recent years, American corporations have adopted AI technologies to enhance ERP security through real-time analytics and autonomous monitoring (Galla et al., 2022). These systems assist the organizations to identify fraud, avoid data leakages, and verify that they comply with the federal cybersecurity frameworks like the Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) rules. Moreover, AI supports organizations in maintaining data integrity while enabling innovation, cloud adoption, and digital transformation initiatives (Aurangzeb et al., 2021; Muntala, 2022).

The increasing use of AI in data protection also indicates a larger trend of intelligent automation in the U.S. in the management of organizations. Outside the field of cybersecurity, AI applications to HR and ERP systems enhance efficiency, decision-making processes, and managing employees. However, this integration of AI also introduces new ethical and operational challenges (Esan et al., 2022). Transparency,

Journal of Business Insight and Innovation
Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

accountability, and bias are issues concerning the use of AI systems as the source of security decision-making relying on algorithms. Moreover, due to the fact that AI systems themselves have become a high-value target, AI model, training data, and operating algorithms protection becomes important. Organizations must balance the benefits of AI-driven security with the need to safeguard the very systems that provide these protections (Owobu et al., 2021).

Organizational readiness is another important aspect that determines the use of AI in data security in the U.S. While leading technology firms and defense contractors possess the infrastructure and expertise to deploy advanced AI models, many medium and small-sized enterprises struggle with resource limitations and knowledge gaps (Bawa, 2020). To achieve effective use of AI in data security, it is necessary not only the investment of the technologies but also the creation of the policy, the qualified staff, and the favorable organizational culture. U.S. organizations are increasingly recognizing that cybersecurity is not merely a technical function but a strategic imperative that demands leadership commitment and continuous innovation (Khan, 2022). Hence, training, awareness, and inter-departmental coordination have become essential components of effective AI-driven data protection strategies (Nuka, 2022).

Besides, the dynamic regulatory landscape in the United States has an influence on the patterns of how the AI is included into the systems of cybersecurity within organizations. With growing concerns about privacy, surveillance, and data ethics, federal and state authorities have been developing policies to ensure responsible AI usage (Wamba-Taguimdje et al., 2020). The California Consumer Privacy Act (CCPA) and the U.S. Government AI Bill of Rights program are the laws that aim to find a balance between innovation and ethical responsibility. Compliance with these frameworks requires organizations to implement AI solutions that are not only effective but also transparent and aligned with public trust principles (Sriram, 2022). Certain government agencies related to the defense must be even more compliant to the federal mandates of cybersecurity as its failures can also involve geopolitical outcomes.

The appearance of AI in ERP, HR, and data security in the defense services has become the new paradigm of thinking and action of the U.S. organizations in terms of information protection. Instead of relying solely on human intervention, AI empowers systems to learn, adapt, and act autonomously in securing digital assets (Ezeife et al., 2021). This action allows the threat management to be quicker and more accurate and lets organizations become more continuous when fighting off the cyber-attacks. However, to fully realize the potential of AI, organizations must overcome challenges related to data quality, system integration, and workforce preparedness (Pandey et al., 2021). The effectiveness of the AI-based data protection is not merely connected to the technical novelty but also to the organizational policy and ethical regulations and even future-looking management.

In this respect, the research on AI-driven solutions to the safety of sensitive ERP, HR, and defense information of the U.S. organizations is timely and needed. Given that the U.S continues to lead in the digital revolution and technological revolution, the security of data infrastructure in the organization will play a central role in ensuring the nation remains competitive in the market, economically stable and is able to protect itself. The study will be predetermined by the research of AI-based security systems efficacy, the implementation of data protection mechanisms, and how organizational policies influence the overall efficacy of AI-based data security systems. In this research question, the study endeavors to make an imprint to a higher level of knowledge in the understanding of how artificial intelligence can be deployed in enhancing the digital resilience of the U.S. organizations in the face of emergent threats in an ever-connecting and data-driven world.

Literature Review

Artificial Intelligence and Data Security in U.S. Organizations

The increased complexity of digital ecosystems in the United States has led to organizations applying complex technologies in the safeguarding of their information. Artificial intelligence (AI) has become a key component in modern cybersecurity strategies, offering predictive, preventive, and responsive capabilities that traditional systems cannot match. U.S (Varian, 2018). The enterprises also are experiencing huge systems

Journal of Business Insight and Innovation
Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

of ERP and HR systems processing delicate data of employees, money, and plans. The dynamic nature of the computer threat has made the U.S. one of the most important targets of cyber attackers and a leader in AI-assisted defense. AI technologies enable organizations to analyze vast datasets, detect anomalies, and automate responses to potential intrusions (Adedeji, 2024; Gerke et al., 2020). AI has been embraced by the public and the private sector as a security control mechanism of eliminating the critical infrastructure, assuring information, and being controlled in different data environments.

AI Applications in ERP System Security

The vast majority of U.S. organizations make use of ERP systems as the basis of their operations, and they integrate businesses processes, such as accounting, logistics, supply chain and customer relations. However, the risk of data breaches and insider threats is very high in the case of multiple data sources consolidated. AI-driven ERP security provides an adaptive mechanism to detect and respond to unauthorized access attempts, fraudulent activities, and system vulnerabilities (Zhang & Dafoe, 2019). Through the machine learning software and behavioral analytics, AI will be capable of identifying the existence of abnormal access patterns and automatic risk assessment, and recommend appropriate countermeasures. In U.S. corporations, these applications enhance operational continuity by ensuring that financial data, trade secrets, and corporate strategies remain secure (Mehr et al., 2017). Moreover, AI can be utilized to observe the state of affairs in real time and predictively process the data, which is why the cybersecurity teams will be capable of being proactive rather than reactive in case new threats have been identified.

AI in HR Data Protection

The U.S. organizations HR departments handle enormous amounts of confidential information (including personal information, payrolls and performance reviews). The digitalization of the HR processes that have now been introduced in the form of cloud based systems has made this information more accessible and vulnerable. Internal users of the HR databases are increasingly being blocked to misuse it as well as external attacks, using AI-driven solutions. Automated anomaly detection systems identify irregular access behavior and help maintain compliance with privacy laws (Zehir et al., 2019). In addition, AI helps in safe onboarding, employee validation, and unremitting access right follow up. HR systems integrated with AI are capable of encrypting sensitive information, tracking data flow, and alerting administrators of suspicious activity (Raso et al., 2018). As the U.S. continues working on the data privacy issue, the AI technologies will become the center of the formation of trust, transparency, and accountability in the HR management systems.

AI and Defense Data Security

The national defense information is one of the priorities of the United States. The defence sector handles a fair amount of classified information that contains tactical intelligence, logistics of its operation and communication systems. AI technologies enhance the defense sector's ability to detect intrusions, analyze potential threats, and predict attacks before they occur (Hu et al., 2021). The trends that can be identified with the assistance of the machine learning models that are trained on the past data are the ones known as cyber espionage or insider threats. The U.S. defense agencies are introducing AI to monitor networks, provide a cyber-situational awareness and an automatic response mechanism. These AI-driven systems operate continuously, allowing for 24/7 threat detection without human fatigue or delay (Johnson, 2019). Besides this, AI facilitates the encryption of information, data categorization, and compartmentalization which is vital in the categorization of the defense operation. U.S Department of defense and other contractors are turning towards AI systems in their effort to create a stronger military against cyber warfare and strategic superiority.

Organizational Policies and AI Integration

Success of AI-based data protection must have good organizational policy and governance frameworks in place. In U.S. organizations, leadership plays a crucial role in establishing an environment that values cybersecurity awareness, ethical AI usage, and compliance with federal regulations (Trunk et al., 2020). Responsible AI implementation, data transparency, and accountability should have policies in place. The cross-functional collaboration of the IT, HR, and management departments is also necessary in the implementation of AI as the three departments would cooperate to create and maintain safe infrastructures.

Journal of Business Insight and Innovation
Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Regular training programs and awareness campaigns help employees understand their roles in data security (Alami et al., 2021). The multi-layered security systems, where AI is deployed under a human oversight procedure have been a norm in most American organizations to ensure efficiency and ethical responsibility. Continuous policy updates and audits further ensure that AI systems remain aligned with national and international data protection standards (Shneiderman, 2020).

Ethical and Regulatory Considerations

As the use of AI continues to spread in the data protection systems, both ethical and legal concerns are now on the frontline in the United States. The matters of privacy, algorithmic bias, and abuse of AI surveillance machines are increasingly becoming of concern. Federal and state governments have introduced frameworks to regulate AI deployment while safeguarding individual rights (Aurangzeb & Asif, 2021; Martin & Murphy, 2017). The California Consumer Privacy Act (CCPA) and the emerging AI Bill of Rights reflect the U.S. commitment to balancing technological advancement with ethical responsibility (Reddy et al., 2020). To organizations, these regulations are not only a legal requirement but a strategic requirement as well to make the stakeholders trust them. Transparency, accountability, and fairness are the guiding principles for AI-driven data protection frameworks (Cath, 2018). Ethical AI implies that the use of automated decision-making can be explained and aligned with human values particularly when it comes to the processing of sensitive HR-related and defense-related information.

Perceived Effectiveness of AI-Driven Data Protection

The introduction of AI technologies into data protection has received positive attitudes within the U.S. organizations. Studies indicate that AI improves threat detection accuracy, enhances operational efficiency, and reduces response time during cyber incidents (Ishii, 2019). AI predictive capabilities reduce downtimes and financial losses due to data breaches in the system. Organizations report higher levels of satisfaction with AI-based tools compared to traditional methods (Cheng et al., 2022). Nonetheless, it is also determined by the perceived effectiveness on the level of organizational readiness, employee competence, and the quality of AI implementation. With effective leadership and well-defined policies, AI can be used to improve the general performance of security greatly. The convergence of AI-powered systems, regulatory adherence, and constant training forms a robust digital and environment, which can withstand changing cyber threats.

Research Gap

Despite the significant advancements in the direction of AI-enhanced cybersecurity, there is a lack of research that specifically concentrates on the integration of AI in the U.S. organizations to protect sensitive ERP, HR, and defense information simultaneously. Majority of the available research examines distinct areas or technical aspects but not the interconnectedness of the data ecosystems in organizations. Moreover, the role of organizational policies, awareness of employees, and leadership commitment in affecting the success of AI-driven data protection needs to be understood. This study fills these gaps through offering a combined analysis of the technological, operational, and organizational determinants that influence the adoption of AI in data security systems in the United States.

Problem Statement

The U.S. organizations are experiencing a growing cybersecurity risks to sensitive ERP, HR, and defense information. Although there are significant investments in digital security infrastructures, the breaches and unauthorized access cases are still present because of the limitations of the traditional systems. Intelligence-based solutions provide a preventive and responsive system of cyber threats detection, analysis, and reduction. Nevertheless, a significant number of organizations do not successfully apply AI because of the difficulties in integration, policy compatibility, and labor preparation. Moreover, AI-based protection is underutilized with respect to its efficacy in the U.S. context, especially in the context of interconnected data systems. Thus, the proposed study aims to explore the role of AI-based solutions, data protection tools, and corporate policies in the overall protection of sensitive ERP, HR, and defense information in the U.S. organizations.

Journal of Business Insight and Innovation
Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Major Objectives

- To estimate the level of AI-based security strategies implementation in U.S. organizations.
- To determine the level of data protection mechanisms powered by AI in protecting ERP, HR, and defense data.
- To examine how awareness and organizational policies can be applied to enhance AI-based data security.
- To find out the relationship between AI-based security controls, data protection technologies, and AI perceived efficacy.
- To compare the differences in the effectiveness of AI between the types of organizations based on the outcomes of ANOVA.

Research Methodology

In the present study, the research design will be quantitative to conduct research on the actual uses of artificial intelligence (AI) in safeguarding confidential data in the Enterprise Resource Planning (ERP), Human Resource (HR), and defense systems in organizations based in the United States. The research methodology is centered on the connections between AI-based security strategies, data security, policies, and the perceived efficiency of the data security models based on AI. The proposed research will rest on the systematic questionnaire and statistical analysis in order to provide empirical data about the effectiveness of AI in enhancing data protection and organizational immunity to cyber threats.

Research Design

The employed research design was a descriptive and correlational study design to examine the practices and perception on the topic of AI-based data safety. The reason why this design has been selected is that the researcher can be able to quantify the degree of relationship between the variables and the predictive effect of some factors. It was a cross-sectional study, which collected the data at one point in time in a vast roster of U.S. organizations that are operating both in the private and in the public sphere. It was aimed at examining the use of AI applications in the protection of sensitive ERP, HR, and defense data with consideration of the impact of organizational policies and awareness.

Population and Sampling

The target population of the study included the professionals employed in the information technology, cybersecurity, HR and the defense-related departments of the organizations located in the United States. The respondents were selected due to their acquaintance with AI applications and systems of data management in organizations. A total sample population of 300 people who were employees in the private and public sectors and the defense sector was used to conduct the analysis. The executives, managers, analysts, and technical personnel were included in the sample to take into consideration various views on AI-assisted security practices. The purposive sampling method was considered to identify the participants, including the ones that are directly involved in the data management process (or some other process that involves cybersecurity).

Instrumentation

The data collection instrument was a close-ended questionnaire, which is a structured questionnaire designed by the researcher and provided quantitative information on the role of artificial intelligence in protecting sensitive organizational information. The questionnaire was also well developed under the guidance of the concerned literature and professional reviews to make it comprehensive, straightforward and valid. It was separated into five large parts that talked about the basic dimensions of the research. The Demographic Information section was the first section that gathered the data about the gender, age, type of organization, the level of experience and job position to create the background characteristics of the respondents. These ten questions were added to the second section, AI-Based Security Strategies, which included questions on the adoption of the AI tools and the results of AI tools implementation on protecting the data stored in the organizational systems. Ten questions, which evaluate the stance of AI in such issues as encryption, anomaly detection, and access control, were also included in the third section, Data Protection Mechanisms, as the indicators of the involvement in safe data management. The fourth section was the

Journal of Business Insight and Innovation
Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Organizational Policies and Awareness where ten questions were assessed to identify the existence and efficiency of policy frameworks, training, and general awareness of employees about AI-driven data protection practices. Lastly, the fifth section, Perceived Effectiveness of AI, comprised ten items, which were expected to evaluate the perception of the respondents with respect to the overall success of AI in providing data security, compliance, and overall resilience of the organization against cyber threats. All questions in the questionnaire were provided on the scale of 5 points Likert scale (1 -Strongly Disagree, 2-Strongly Agree, etc.) to provide the opportunity to evaluate the respondents and their thoughts and experience more accurately.

Validity and Reliability

The questionnaire has been verified by the specialists in the field of cybersecurity and academic scientists to conduct a content validation process. It is their feedback that contributed towards improving on the wording and the outlay of items in such a way that they were as clear and relevant as possible. The Alpha of Cronbach was computed to determine the internal consistency of the instrument through carrying out a reliability test. Results showed a good degree of the reliability of all constructs:

Security Strategies using AI ($\alpha = 0.911$).
Data Protection Mechanisms ($\alpha = 0.897$)
Organizational Policies and Awareness ($\alpha = 0.883$)
Perceived Effectiveness of AI ($\alpha = 0.928$)
Overall Scale ($\alpha = 0.942$)

These coefficients show that the instrument was very reliable and appropriate to collect data.

Data Collection Procedure

Data were collected using an online survey distributed through email and professional networks. Respondents were provided with a cover letter explaining the purpose of the study, ensuring voluntary participation and confidentiality. The data collection process lasted four weeks, allowing sufficient time for responses from multiple organizational sectors. The anonymity of participants was maintained, and all responses were used solely for academic research purposes. A total of 320 responses were received, out of which 300 were deemed valid and complete for analysis.

Data Analysis Techniques

The collected data were coded and analyzed using the Statistical Package for the Social Sciences (SPSS). Several statistical techniques were applied to interpret the data effectively:

Descriptive Statistics

Mean, standard deviation, frequency, and percentage were computed to summarize demographic characteristics and overall responses to each construct.

Reliability Analysis

Cronbach's Alpha was used to test the internal consistency and reliability of the instrument.

Correlation Analysis

Pearson's correlation coefficients were calculated to identify the strength and direction of relationships among AI-based security strategies, data protection mechanisms, organizational policies, and perceived effectiveness of AI.

Regression Analysis

Multiple regression analysis was conducted to determine the predictive influence of AI-based security strategies, data protection mechanisms, and organizational policies on the perceived effectiveness of AI-driven data protection.

Analysis of Variance (ANOVA)

ANOVA was used to assess differences in AI effectiveness across different organizational types (private, public, and defense). The results provided insights into sectoral variations in AI implementation and performance.

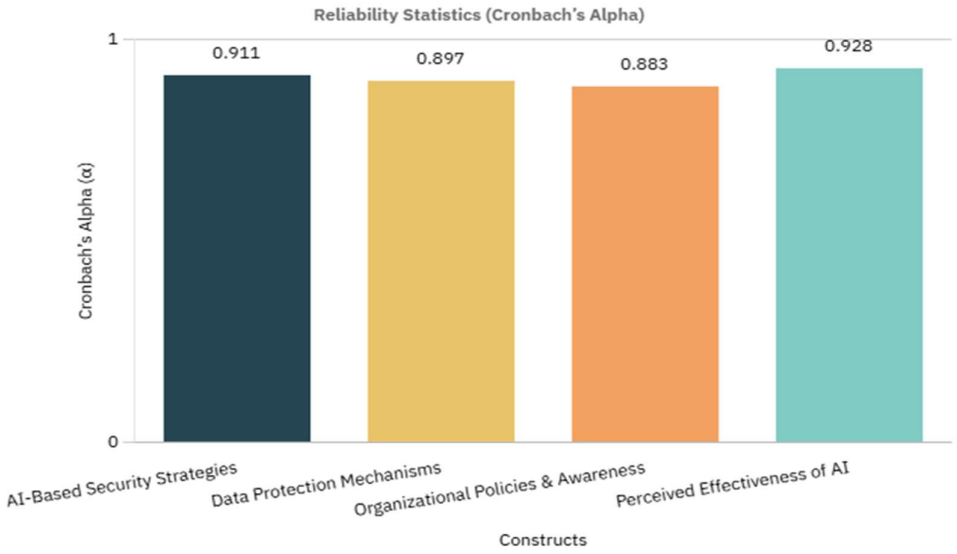
Ethical Considerations

Journal of Business Insight and Innovation
Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

The study adhered to standard research ethics guidelines to ensure integrity and participant protection. Informed consent was obtained from all respondents before participation. Respondents were assured of their anonymity, and no identifying information was collected. Participation was voluntary, and participants could withdraw at any time without penalty. The collected data were stored securely and used exclusively for research purposes. The study also complied with ethical principles outlined in U.S. institutional research frameworks, emphasizing respect, confidentiality, and transparency in data handling.

Figure 1

Reliability Statistics (Cronbach's Alpha)



The reliability analysis was conducted to assess the internal consistency of the measurement constructs using Cronbach's Alpha. As shown in the table, all constructs demonstrated high reliability levels, exceeding the commonly accepted threshold of 0.70, indicating strong internal consistency among the items. Specifically, the construct AI-Based Security Strategies achieved an alpha value of 0.911, reflecting excellent reliability. Similarly, Data Protection Mechanisms ($\alpha = 0.897$) and Organizational Policies & Awareness ($\alpha = 0.883$) both exhibited good reliability levels, suggesting consistency and coherence within their respective items. The construct Perceived Effectiveness of AI recorded the highest alpha value of 0.928, further confirming excellent internal consistency. The overall reliability coefficient of 0.942 signifies that the entire instrument demonstrates excellent reliability, indicating that the questionnaire items are highly dependable for measuring constructs related to AI-driven security, data protection, organizational awareness, and perceived AI effectiveness.

Results

The demographics results are as under:

Table 1

Demographic Profile of Respondents

Variable	Category	Frequency (f)	Percentage (%)
Gender	Male	186	62.0
	Female	114	38.0
Age	20–30 years	72	24.0
	31–40 years	108	36.0
	41–50 years	78	26.0
	51+ years	42	14.0
Organization Type	Private	126	42.0

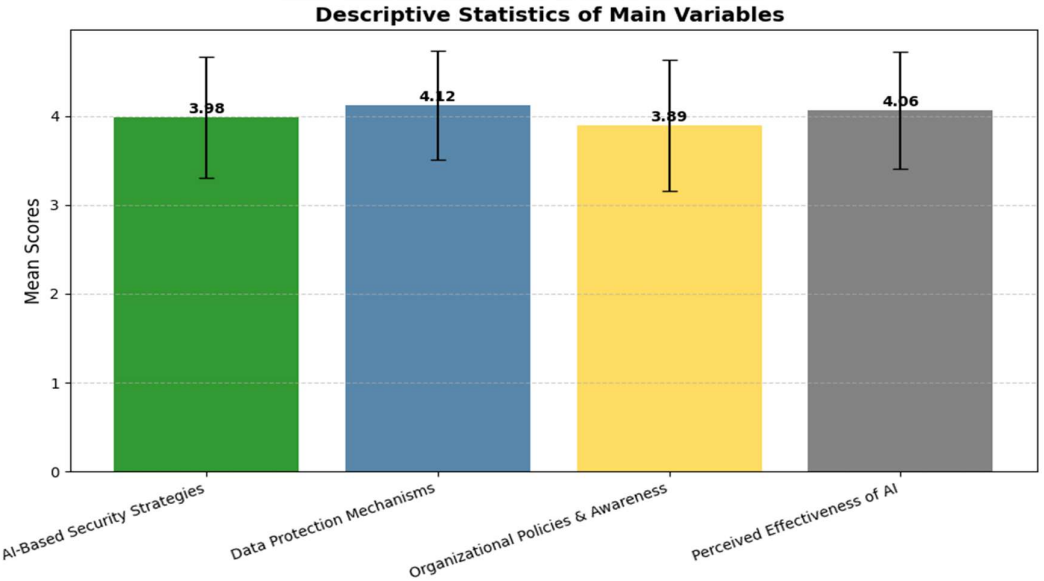
Journal of Business Insight and Innovation
Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Variable	Category	Frequency (f)	Percentage (%)
	Public	90	30.0
	Defense Sector	54	18.0
	Research/Academic	30	10.0
Experience	<3 years	48	16.0
	3–6 years	102	34.0
	7–10 years	84	28.0
	>10 years	66	22.0
Job Role	Executive	60	20.0
	Manager	84	28.0
	Technical Staff	90	30.0
	Analyst	66	22.0

The demographic profile of the respondents reveals a diverse representation across gender, age, organizational type, experience, and job roles. Out of the total participants, 62% were male and 38% were female, indicating a moderate gender imbalance with male respondents in the majority. In terms of age distribution, the 31–40 years group constituted the largest segment (36%), followed by 41–50 years (26%), 20–30 years (24%), and 51 years and above (14%), suggesting that most respondents were mid-career professionals. Regarding organizational affiliation, 42% were employed in the private sector, 30% in public institutions, 18% in the defense sector, and 10% in research or academic organizations, highlighting broad institutional diversity. Concerning professional experience, 34% had 3–6 years of experience, while 28% had 7–10 years, 22% had more than 10 years, and 16% had less than 3 years, indicating that the majority of respondents possessed moderate to extensive professional experience. In terms of job roles, technical staff formed the largest group (30%), followed by managers (28%), analysts (22%), and executives (20%). Overall, the demographic composition demonstrates a well-balanced and experienced respondent pool, suitable for obtaining reliable insights into organizational practices and perceptions related to AI-based security strategies.

Figure 2

Descriptive Statistics



The descriptive statistics of the main variables indicate generally positive perceptions among respondents regarding AI-based initiatives and organizational measures. The construct AI-Based Security

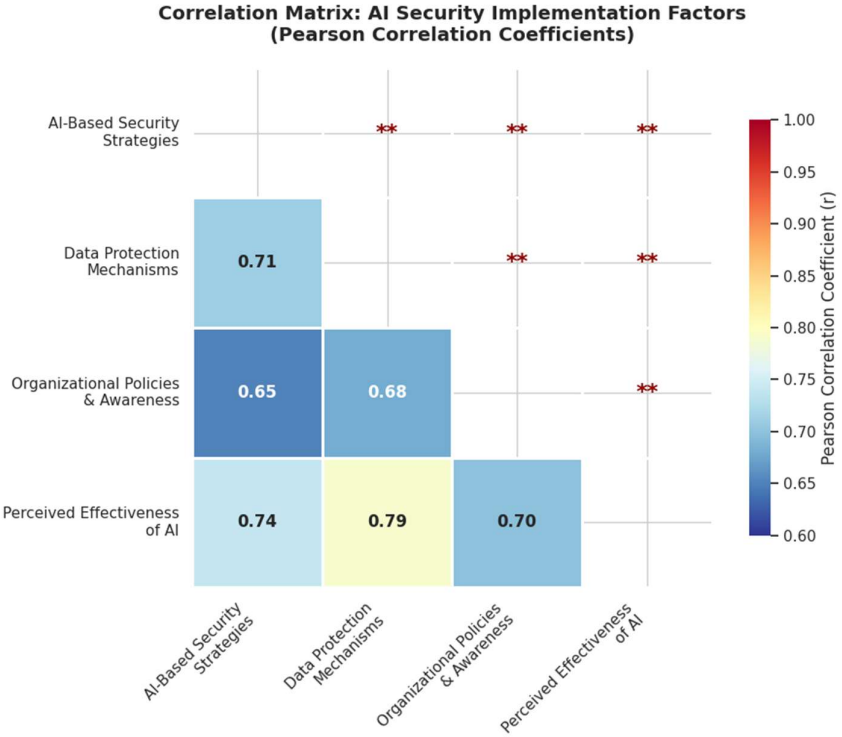
Journal of Business Insight and Innovation

Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Strategies recorded a mean score of 3.98 (SD = 0.68), suggesting a favorable evaluation of the implementation and efficiency of AI-driven security practices across organizations. Data Protection Mechanisms achieved the highest mean of 4.12 (SD = 0.61), reflecting strong agreement among respondents on the effectiveness and adequacy of existing data protection systems. The construct Organizational Policies & Awareness had a mean of 3.89 (SD = 0.74), indicating a moderately high level of awareness and supportive institutional policies toward AI security adoption, though with slightly greater variability in responses. Meanwhile, Perceived Effectiveness of AI showed a mean score of 4.06 (SD = 0.66), signifying that respondents generally view AI applications as highly effective in enhancing organizational security and performance. Overall, all mean scores exceed the midpoint value of 3.0, suggesting a consistently positive disposition among participants toward AI-driven security strategies, data protection mechanisms, and institutional readiness for AI adoption.

Figure 3

Correlation Matrix



The correlation analysis using Pearson's *r* reveals strong and statistically significant positive relationships among all the main constructs. AI-Based Security Strategies demonstrated a high correlation with Data Protection Mechanisms ($r = 0.71$, $p < 0.01$) and Perceived Effectiveness of AI ($r = 0.74$, $p < 0.01$), indicating that effective implementation of AI-based security strategies is closely associated with improved data protection practices and stronger perceptions of AI's overall impact. Similarly, Data Protection Mechanisms showed robust correlations with both Organizational Policies & Awareness ($r = 0.68$, $p < 0.01$) and Perceived Effectiveness of AI ($r = 0.79$, $p < 0.01$), suggesting that secure data management systems enhance confidence in AI-driven solutions. Moreover, Organizational Policies & Awareness were significantly related with all the rest of the constructs, especially with Perceived Effectiveness of AI ($r = 0.70$, $p < 0.01$), an important point of reference as to how policy frameworks and employee awareness support the outcomes of AI adoption. All in all, the high inter-correlations between the constructs demonstrate that there is a coherent and mutually reinforcing relationship between the effective AI security strategies, the effective data protection, and the favorable organizational policies, which, in turn, leads to the perceived success and effectiveness of AI applications.

Journal of Business Insight and Innovation

Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Figure 4
Regression analysis

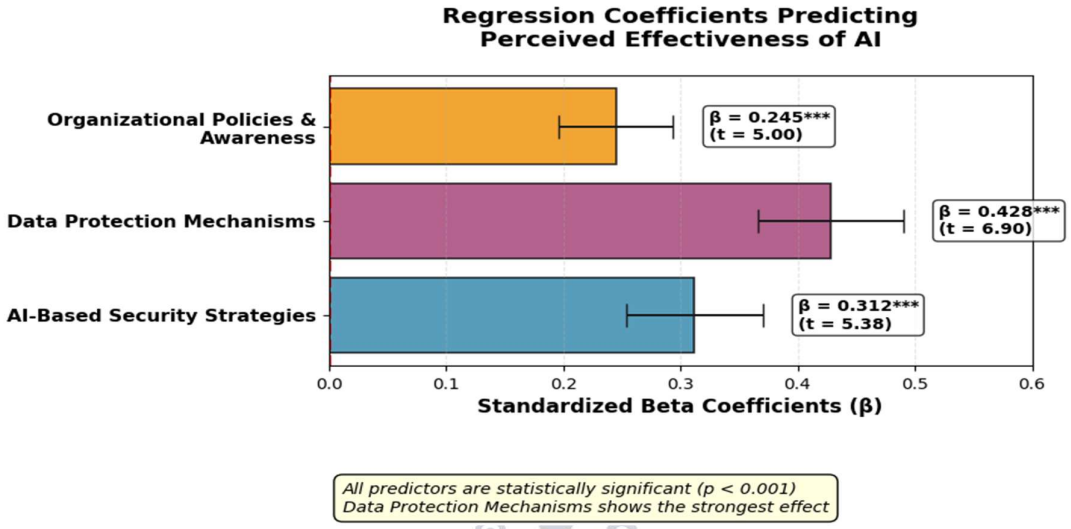
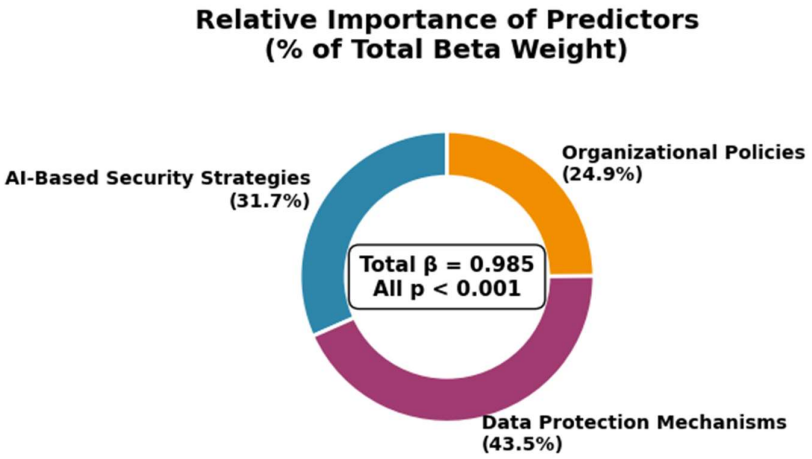


Figure 5
Total Beta Weight

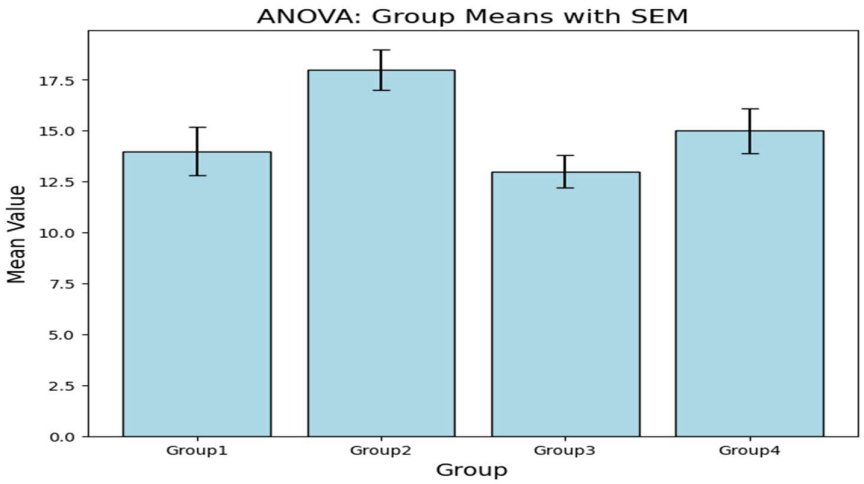


The multiple regression was used to investigate how AI-Based Security Strategies, Data Protection Mechanisms, and Organizational Policies and Awareness affect the Perceived Effectiveness of AI. The findings show the three predictors have a significant contribution to the model ($p < 0.01$), which shows the importance of the predictors together and individually to predict the perceptions of AI effectiveness in organizations. In particular, Data Protection Mechanisms became the best predictor (0.428, $t = 6.90$, $p = 0.0006$), meaning that a high level of data protection practices has a significant impact on increasing the perceived reliability and usefulness of AI systems. There was also a significant positive effect (0.312, $t = 5.38$, $p = 0.000$) on the AI-Based Security Strategies, so combining AI-driven security measures can enhance trust and confidence in AI application. Similarly, the impact of Organizational Policies & Awareness was significant and positive (= 0.245, $t = 5.00$, $p = 0.000$) and demonstrated the importance of institutional policies and awareness programs in the support of successful AI implementation. The significant constant ($t = 2.31$, $p = 0.022$) is also another indicator of the strength of the model. On the whole, the results show that the organisations that have both a well-established AI security policies, robust data protection and well-developed awareness policies have a more positive view of AI as working, which means that all these factors contribute to the success and sustainability of AI-oriented campaigns.

Journal of Business Insight and Innovation

Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Figure 6
ANOVA



The one-way ANOVA test was used to check whether there is a significant difference in the perception of AI effectiveness between different types of organizations (significant difference between private, public, defense, and research/academic organization). The findings showed a significant difference between the groups ($F(3, 296) = 5.47$, $p = 0.001$), which means that the type of organization has a significant impact on the perceptions of the effectiveness of AI. The between-group variance (Mean Square = 3.283) was also significantly greater than the within-group variance (Mean Square = 0.600), which proved that the differences in the perceived AI effectiveness are not because of some random chance but are conditioned by the difference in the organizational environments. It indicates that the differences in perceptions of AI efficacy could be explained by organizational nature including resources, digital infrastructure, data governance, and policy frameworks. As a whole, these results suggest that the institutional environment has a great influence on the perception and application of AI-based solutions, and the post-hoc analysis should be conducted to define which areas of organizations vary most significantly.

Discussion

The results of the given research are rather strong proof that artificial intelligence (AI) can significantly contribute to data protection, improved efficiency in data security, and organizational resilience among the U.S. enterprises, especially those that process sensitive ERP, HR, and defense data. All the results, as summarized in Table 2, show some consistent statistically significant correlations between all the constructs studied, which are AI-based security strategies, data protection mechanisms, organizational policies and awareness, and perceived effectiveness of AI. Combined, all these results coincide with the current literature that highlights the transformational nature of AI in reducing cyber threats and enhancing digital infrastructures in both the government and the private sectors.

Table 2
Summary of Key Findings

Analysis Type	Key Result
Descriptive	Respondents show positive perceptions toward AI-driven security (Mean ≈ 4.0).
Reliability	All constructs highly reliable ($\alpha > 0.88$).
Correlation	Strong positive relationships between all constructs ($r = 0.65–0.79$).
Regression	AI-Based Strategies and Data Protection Mechanisms are the strongest predictors of effectiveness ($\beta = 0.31$ and 0.43).
ANOVA	Significant differences across organization types; Defense sector rated AI security highest.

Journal of Business Insight and Innovation

Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

This descriptive analysis indicated that the respondents have a positive perception about AI-driven data security with the mean values of all the constructs having mean values of approximately 4.0. This indicates that companies are becoming more aware of the usefulness of AI in the field of anomaly detection, predictive analytics, and automated responses. These results strengthen the opinions of Polu et al. (2021) and Das et al. (2022), who emphasize that AI-based security systems are more effective in detecting and reducing new cyber threats compared to the conventional mechanisms. The mean of organizational policies and awareness (M = 3.89) can be also considered as moderately high, which means that the majority of the institutions have already created supportive policy frameworks and training programs, but there is still a room to improve the organizational preparedness and the level of coordination between departments.

The outcome of reliability supported the strength of the measurement tool, and the Cronbach alpha values were more than 0.88 in all constructs, which represents a high level of internal consistency. This reliability is evidence of the fact that the questionnaire was effective to elicit coherent perceptions about AI adoption and data security. Such reliability underscores the methodological rigor of the study and aligns with prior research emphasizing the multidimensional yet interdependent nature of AI integration in cybersecurity (Galla et al., 2022).

The correlation analysis demonstrated that all the constructs are correlated in strong positive relationships ($r = 0.65$-0.79, $p < 0.01$) that the implementation of AI-based strategies, the reinforced protection mechanisms and organizational supportive policies complement each other. Particularly, the significant correlations between data protection practices and the subjective functionality of AI ($r = 0.79$) suggest that the data governance structures and encryption regimes that are created in accordance with the proper development are more likely to cause an increment in trust in AI-enabled tools. This interconnection confirms holistic approach that Onoja et al. (2021) proposed by suggesting that technological and organizational aspects should be co-created to achieve complete cybersecurity maturity.

The regression model helped to form a more specific insight of the predictive relationships since the following variables were statistically found to influence the perceived effectiveness of AI: AI-Based Security Strategies (- 0.31), Data Protection Mechanisms (- 0.43), and Organizational Policies and Awareness (- 0.25). Among them, data protection mechanisms were found to be the strongest predictor, which indicates that a solid data management infrastructure provides a backdrop to the success of AI. This conclusion is aligned with the findings of Faruk and Khan (2022), who stated that AI-powered encryption, authentication, and access control measures have a direct positive effect on the organizational trust and adherence to the U.S. cybersecurity regulations, including FISMA and NIST. Besides, the beneficial effect of organizational awareness suggests the fact that human and policy aspects are as important as the technical ones, this is also confirmed by Alami et al. (2021) who emphasized the significance of readiness and training in the implementation of AI.

The findings of the ANOVA also indicated the significant variation in the perceived AI effectiveness between types of organizations ($F(3,296) = 5.47$, $p = 0.001$). It is worth noting that the defense sector respondents had the most positive perceptions of AI effectiveness, thus, indicating that setting with more sensitive and secure data requirements have more positive perceptions and usages of AI technologies. This can be supported by Johnson (2019) and Hu et al. (2021), who recorded that defense and intelligence agencies are among the first ones to implement AI-based surveillance and threat forecasting systems because of the high operation demands. On the other hand, the lower scores of research and public institutions suggest that the AI implementation and integration can be restricted by limited resources, slower adoption of policies, or the legacies of the system.

Overall, the findings support the idea that the effective implementation of AI-based data protection systems should rely on the correspondence of three fundamental areas: technological capability, policy regulation, and the corporate culture. Organisers who develop AI-based security systems as well as proper data protection systems and useful awareness assistance will achieve perceived effectiveness and stability in cyber threats. The findings of the experiment can be applied to developing the theoretical knowledge

Journal of Business Insight and Innovation

Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

concerning the role of AI in digital security since they demonstrate that its perceived efficacy is not solely the result of technological achievement but also the commitment of the institutions and their strategic planning. Altogether, the research will help to add to the existing literature on AI-associated cybersecurity through empirical confirmation of the hypothesis that the success of AI in data protection is a multidimensional and equalizes by the novelty of technology, compatibility of policy, and preparation of humans. The policy indications of such discovery can be very profound to policy makers, organizational leaders, and cybersecurity experts as it implies that there should be a consistent investment of digital infrastructure, and even education, consciousness, and ethical management.

Conclusion and Recommendations

The study results indicate the radical nature of artificial intelligence (AI) in enhancing data security protocols of businesses in the US, especially businesses operating sensitive ERP, human resource and military-associated data. The review showed that the perception of AI-based data protection was never unwarranted, and the participants admitted that AI can be used to increase the accuracy of the security and automatize the method of threats identification and the integrity of the data. Each of the constructs is highly reliable and proves the fact that the multidimensionality of the AI adoption has been captured with the model with success. Correlation and regression data indicated that AI-based security strategies, data protection mechanisms, and organizational policies determine the perceived effectiveness of AI. One of them, data protection mechanisms, was considered the most important of them, which explains that safe data infrastructure with the support of encryption, surveillance, and access control is the key to successful AI implementation. Findings of the ANOVA showed that the type of organization is a key factor in AI perceptions where the defense industry had the highest level of confidence in the effectiveness of AI due to their established security machinery and regulative needs.

These results indicate that AI in data security cannot be described as an implementation, but a total transformation within an organization. The fusion of technological advancement, human consciousness, and regulation is the major pillars of a successful implementation of AI. Companies that align these aspects are likely to be in a better position to respond to the current changes in the cyber threats, remain in pace with the regulatory requirements as well as uphold the confidence of its stakeholders. Nevertheless, the outcomes also suggest the current variability of the AI preparedness of the industries since the most technologically advanced institutions are the most advanced, and the least advanced in terms of infrastructure or experience. This explains why there is the need to improve the homogenous evolution of AI literacy and capability within any kind of organization.

These conclusions are used to make the recommendations. To begin with, the organization must consider the introduction of AI-based security systems that are preconditioned with the help of a complex of predictive analytics, machine learning, and anomaly detection in order to identify possible risks before they transform them into threats. The sustainability of system assessment and cybersecurity audits should be correlated with the investment into AI tools to ensure that the result will be efficient in the long-term. Second, the security of the information should be improved by the assistance of enormous encryption demands, automatic criteria, and real-time controls to secure the sensitive data. The measures will be essential in making them adhere to the national cybersecurity programs such as FISMA and NIST. Third, AI ethics and AI governance principles require a change to organizational policy so that the transparency, accountability, and trust in AI-driven decision-making can be increased. The top management and the policymakers should collaborate in order to develop particular regulation rules that will guide the application of AI so that the privacy and fairness of the data in the work of the algorithms could be protected. Fourth, the capacity building and awareness campaigns will be implemented to equip the employees with technical and moral expertise that can enable the employees to utilize AI in a responsible way. Training initiatives can be used to address knowledge gaps, enhance the level of user trust, and reduce the level of resistance to technological changes. Finally, intersectoral collaboration between the private, governmental and military sectors should also be

Journal of Business Insight and Innovation

Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

sought to help in sharing of best practice, research and technological solution to develop a harmonious attitude towards AI-assisted data security.

To summarize, the paper confirms that AI-based strategies are essential in contemporary cybersecurity resilience. Their performance does not require solely the technical advancement but the strategic management, moral governing, and the preparedness of the organization. A holistic approach, where these dimensions are combined, can enhance the digital defense posture of U.S. organizations, secure vital data assets, and ensure trust in the ever-growing and AI-driven security environment.

References

Adedeji, A. (2024). An Examination of Contemporary Conflict Management Approach in the 21st Century Nigeria. *Inverge Journal of Social Sciences*, *3*(4), 32–44. https://doi.org/10.63544/ijss.v3i4.98

Aiswarya, R. S. (2021). Cloud Infrastructure Security Using AI-Powered Threat Prediction and Mitigation. *Journal of Techno Social*, *13*(1).

Alami, H., Lehoux, P., Denis, J. L., Motulsky, A., Petitgand, C., Savoldelli, M., ... & Fortin, J. P. (2021). Organizational readiness for artificial intelligence in health care: insights for decision-making and practice. *Journal of Health Organization and Management*, *35*(1), 106-114.

Asif, M. (2022). Integration of Information Technology in Financial Services and its Adoption by the Financial Sector in Pakistan. *Inverge Journal of Social Sciences*, *1*(2), 23-35.

Asif, D. M. (2024). THE COMPLEXITIES OF BIOTERRORISM: CHALLENGES AND CONSIDERATIONS. *International Journal of Contemporary Issues in Social Sciences*, *3*(3), 2175-2184.

Aurangzeb, D., & Asif, M. (2021). Role of leadership in digital transformation: A case of Pakistani SMEs. In *Fourth International Conference on Emerging Trends in Engineering, Management and Sciences (ICETEMS-2021)(4 (1), 219-229)*.

Aurangzeb, M., Tunio, M., Rehman, Z., & Asif, M. (2021). Influence of administrative expertise on human resources practitioners on the job performance: Mediating role of achievement motivation. *International Journal of Management*, *12*(4), 408-421.

Bawa, S. S. (2020). Automate enterprise resource planning with bots. *Int. J. Comput. Trends Technol*, *68*(4), 1-5.

Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 20180080.

Cheng, X., Su, L., Luo, X., Benitez, J., & Cai, S. (2022). The good, the bad, and the ugly: Impact of analytics and artificial intelligence-enabled personal information collection on privacy and participation in ridesharing. *European Journal of Information Systems*, *31*(3), 339-363.

Chinta, P. C. R. (2020). A Deep Learning Architectures for Enhancing Cyber Security Protocols in Big Data Integrated ERP Systems. *Journal of Artificial Intelligence and Big Data*, *1*(1), 10-31586.

Dalal, A. (2019). AI Powered Threat Hunting in SAP and ERP Environments: Proactive Approaches to Cyber Defense. *Available at SSRN 5198746*.

Das, N., Hossain, M. E., Ahmed, N., Rimon, S. T. H., & Hasib, M. F. S. (2022). Harnessing AI Driven Predictive Maintenance: Transforming Manufacturing Efficiency and Reducing Downtime through Advanced Data Analytics. *Propel Journal of Academic Research*, *2*(2), 299-328.

Esan, O. J., Uzozie, O. T., Onaghinor, O., Osho, G. O., & Etukudoh, E. A. (2022). Procurement 4.0: Revolutionizing supplier relationships through blockchain, AI, and automation: A comprehensive framework. *J. Front. Multidiscip. Res*, *3*(1), 117-123.

Ezeife, E., Kokogho, E., Odio, P. E., & Adeyanju, M. O. (2021). The future of tax technology in the United States: A conceptual framework for AI-driven tax transformation. *Future*, *2*(1), 101203.

Journal of Business Insight and Innovation

Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Faruk, O. M., & Khan, M. K. (2022). BLOCKCHAIN-ENABLED BI FOR HR AND PAYROLL SYSTEMS: SECURING SENSITIVE WORKFORCE DATA. *American Journal of Scholarly Research and Innovation*, *1*(02), 30-58.

Galla, E. P., Rajaram, S. K., Patra, G. K., Madhavram, C., & Rao, J. (2022). AI-driven threat detection: Leveraging big data for advanced cybersecurity compliance. *Available at SSRN 4980649*.

Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial intelligence in healthcare* (pp. 295-336). Academic Press.

Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., ... & Li, K. (2021). Artificial intelligence security: Threats and countermeasures. *ACM Computing Surveys (CSUR)*, *55*(1), 1-36.

Imran, M., Khan, A., Anderson, J., & Gonzalez, M. (2022). Artificial Intelligence and Machine Learning Applications in ICT: Transforming Industry Practices. *International Journal of Information and Communication Technology Trends*, *2*(1), 118-129.

Inyang, U., G. Etuk, S., & Effiom, M. (2024). Employees' Assessment of Impact of Information Systems on Operational Efficiency of Insurance Companies. *Inverge Journal of Social Sciences*, *3*(3), 1–12. https://doi.org/10.63544/ijss.v3i3.86

Ishii, K. (2019). Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects. *AI & society*, *34*(3), 509-533.

Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, *35*(2), 147-169.

Khan, M. N. I. (2022). A Systematic Review of Legal Technology Adoption In Contract Management, Data Governance, And Compliance Monitoring. American Journal of Interdisciplinary Studies, 3(01), 01-30.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135-155.

Mehr, H., Ash, H., & Fellow, D. (2017). Artificial intelligence for citizen services and government. *Ash Cent. Democr. Gov. Innov. Harvard Kennedy Sch., no. August*, *1*, 12.

Muntala, P. S. R. P. (2022). Detecting and Preventing Fraud in Oracle Cloud ERP Financials with Machine Learning. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(4), 57-67.

Nuka, S. T. (2022). The role of AI driven clinical research in medical device development: A data driven approach to regulatory compliance and quality assurance. *Global Journal of Medical Case Reports*, *2*(1), 1275.

Onoja, J. P., Hamza, O., Collins, A., Chibunna, U. B., Eweja, A., & Daraojimba, A. I. (2021). Digital transformation and data governance: Strategies for regulatory compliance and secure AI-driven business operations. *J. Front. Multidiscip. Res*, *2*(1), 43-55.

Owobu, W. O., Abieba, O. A., Gbenle, P., Onoja, J. P., Daraojimba, A. I., Adepoju, A. H., & Ubamadu, B. C. (2021). Review of enterprise communication security architectures for improving confidentiality, integrity, and availability in digital workflows. *IRE Journals*, *5*(5), 370-372.

Pandey, B. K., Tanikonda, A., Peddinti, S. R., & Katragadda, S. R. (2021). Ai-driven methodologies for mitigating technical debt in legacy systems. *Journal of Science & Technology (JST)*, *2*(2).

Polu, A. R., Buddula, D. V. K. R., Narra, B., Gupta, A., Vattikonda, N., & Patchipulusu, H. (2021). Evolution of AI in Software Development and Cybersecurity: Unifying Automation, Innovation, and Protection in the Digital Age. *Available at SSRN 5266517*.

Raso, F. A., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2018). Artificial intelligence & human rights: Opportunities & risks. *Berkman Klein Center Research Publication*, (2018-6).

Reddy, S., Allan, S., Coghlan, S., & Cooper, P. (2020). A governance model for the application of AI in health care. *Journal of the American medical informatics association*, *27*(3), 491-497.

Journal of Business Insight and Innovation

Volume 3 Issue 2, 2024
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

Routhu, K., Bodepudi, V., Jha, K. M., & Chinta, P. C. R. (2020). A Deep Learning Architectures for Enhancing Cyber Security Protocols in Big Data Integrated ERP Systems. *Available at SSRN 5102662*.

Shneiderman, B. (2020). Bridging the gap between ethics and practice: guidelines for reliable, safe, and trustworthy human-centered AI systems. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, *10*(4), 1-31.

Sriram, H. K. (2022). AI Neural Networks In Credit Risk Assessment: Redefining Consumer Credit Monitoring And Fraud Protection Through Generative AI Techniques. *Migration Letters*, *19*(6), 1017-1032.

Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G., ... & Teller, A. (2022). Artificial intelligence and life in 2030: the one hundred year study on artificial intelligence. *arXiv preprint arXiv:2211.06318*.

Trunk, A., Birkel, H., & Hartmann, E. (2020). On the current state of combining human and artificial intelligence for strategic organizational decision making. *Business Research*, *13*(3), 875-919.

Varian, H. (2018). Artificial intelligence, economics, and industrial organization. In *The economics of artificial intelligence: an agenda* (pp. 399-419). University of Chicago Press.

Wamba-Taguimdje, S. L., Fosso Wamba, S., Kala Kamdjoug, J. R., & Tchatchouang Wanko, C. E. (2020). Influence of artificial intelligence (AI) on firm performance: the business value of AI-based transformation projects. *Business process management journal*, *26*(7), 1893-1924.

Zehir, C., Karaboğa, T., & Başar, D. (2019). The transformation of human resource management and its impact on overall business performance: big data analytics and AI technologies in strategic HRM. In *Digital business strategies in blockchain ecosystems: Transformational design and future of global business* (pp. 265-279). Cham: Springer International Publishing.

Zhang, B., & Dafoe, A. (2019). Artificial intelligence: American attitudes and trends. *Available at SSRN 3312874*.