Frontiers in Computer Science and Artificial Intelligence
ISSN: 2978-8048
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Autonomous Decision Intelligence for Secure and Resilient Digital Enterprises

Helal Murshed [1], Narmin Sayeed [2], and Subha Shamarukh*[3]

[1] RUDN University, Moscow, Russia, engr.helalmurshed@gmail.com, https://orcid.org/0009-0001-1806-2029
[2] The London School of Economics and Political Science, London. UK, narminsayeed@yahoo.com, https://orcid.org/0009-0008-7754-6614
[3] University of Rochester, Rochester, New York, USA, shamarukhsubha@gmai.com, https://orcid.org/0009-0000-2170-1541

Corresponding Author: Subha Shamarukh, **Email**: shamarukhsubha@gmail.com

| ABSTRACT

Few forces have reshaped organizational life as quickly as digital transformation. The way firms create value, manage risk, and hold their competitive ground now depends on systems that grow more entangled with one another every year. A typical enterprise sits at the center of a constant flow of data drawn from its operations, its cloud platforms, the sensors embedded in its products, its planning systems, and the many places where it meets its customers. Artificial intelligence (AI), machine learning, big data analytics, blockchain, and cybersecurity have each made it easier to turn that flow into useful judgment. Yet most organizations still adopt these tools one at a time, and the habit quietly erodes the strategic payoff that integration could deliver. This paper sets out an Autonomous Decision Intelligence (ADI) framework that gathers AI, cybersecurity, big data analytics, blockchain, and management information systems (MIS) into one coherent architecture built for resilient digital enterprises. The argument rests on a synthesis of recent work in decision intelligence, predictive analytics, business intelligence, federated learning, cloud computing, blockchain governance, cyber threat intelligence, and enterprise risk management. From that body of evidence, we construct a conceptual model for organizational decision-making that is trustworthy and capable of improving itself over time. The framework gives weight to secure data governance, explainable AI, privacy-preserving analytics, blockchain-based trust, cyber-resilience, and intelligent automation. It then asks how such a design might reinforce critical infrastructure protection, supply chain resilience, economic sustainability, IT project governance, and day-to-day agility. The contribution is at once theoretical and practical, because it shows how converging technologies can turn conventional decision-support systems into adaptive ecosystems that learn. Organizations that pair AI-driven analytics with strong security and decentralized trust look best placed to absorb uncertainty, keep operating under stress, and pursue digital transformation that lasts.

| KEYWORDS

Autonomous Decision Intelligence; Artificial Intelligence; Big Data Analytics; Blockchain; Cybersecurity; Management Information Systems; Digital Transformation; Business Intelligence; Enterprise Resilience

| ARTICLE INFORMATION

ACCEPTED: 01 May 2026 **PUBLISHED:** 03 June 2026 **DOI:** 10.32996/jcsts.2026.5.8.3

1. Introduction

The decade now underway has placed an unusual set of demands on business. Technology shifts faster than planning cycles, data accumulates faster than anyone can read it, adversaries grow more capable, and the economy refuses to settle. In almost every sector, firms lean on digital systems to keep operations moving, to make better calls, to serve customers well, and to stay a step ahead of rivals. Within that setting, management information systems (MIS) have quietly outgrown their origins as transaction-processing tools and become intelligent platforms that carry strategy, prediction, and resilience (Das et al., 2023). As

transformation programs mature, the joint use of AI, big data analytics (BDA), blockchain, and cybersecurity has turned into the hinge on which sustainable performance now swings (Chakraborty et al., 2024).

AI has changed the feel of decision-making more than any single technology. Managers can now question enormous datasets, notice patterns that would once have slipped past them, hand routine work to machines, and forecast with confidence that simply was not available a decade ago (Chakraborty et al., 2025a). Those abilities increasingly sit behind executive judgment, risk control, workforce planning, and customer analysis (Mahmud et al., 2024). They have also seeded a field of their own, decision intelligence, which knits together data science, analytics, and decision theory in pursuit of better outcomes (Haldar et al., 2025).

As big-data ecosystems have grown, so has the range of things a firm can sense and measure. Analytics now feeds economic forecasting, retention planning, credit-risk scoring, sustainability work, and market intelligence (Manik et al., 2025). The pattern is consistent: organizations that invest in advanced analytics tend to forecast more sharply and run more efficiently (Hossain et al., 2025). The reach extends well past finance into software quality, workforce management, and public policy (Joy et al., 2024). Studies of retention in the technology sector make the same point from a human-resources angle (Hossain et al., 2024a).

None of this comes without exposure. The more an organization stitches itself into shared infrastructure, the more inviting and more damaging an attack becomes. Today, the threat surface stretches across ransomware, insider abuse, advanced persistent threats, compromised IoT devices, poisoned supply chains, and offensive operations that themselves run on AI (Kaur et al., 2023). Risks of this kind have carried cybersecurity out of the server room and into the boardroom, where it now reads as a governance question rather than a purely technical one (Hasan et al., 2023). Even buildings show the strain, as smart-building deployments have opened fresh routes for IoT-borne intrusion (Siam et al., 2025b).

A substantial literature now shows that AI-enhanced security improves detection, response, and recovery through predictive modeling and automation (Das et al., 2025a). Architectures such as transformers and Long Short-Term Memory networks have done well at catching threats that keep mutating (Kaur et al., 2025). Reinforcement-learning agents push the idea further, yielding self-healing systems that adjust to changing conditions without waiting for a human hand (Hasan et al., 2025b). Continuous learning pipelines now make it realistic to flag insider risk as behavior drifts week by week (Nabi et al., 2026).

Blockchain, meanwhile, has matured into a serious answer to an old set of problems: trust, transparency, and the integrity of data once it leaves a single owner's control. Distributed ledger designs support secure identity, access control, compliance auditing, and fraud prevention in settings where no single party is in charge (Esa et al., 2025). Paired with federated learning and Lakehouse architecture, blockchain raises the trustworthiness of enterprise data without forcing everything into one central store (Chakraborty et al., 2025b). What once read as aspirational, privacy-preserving, and decentralized decision-making starts to look practical (Islam et al., 2025).

The meeting of AI, blockchain, and security has, in turn, sharpened interest in privacy-preserving analytics. Federated learning, homomorphic encryption, and decentralized governance let firms draw value from scattered data while still meeting their obligations under the law (Das et al., 2025b). Homomorphic methods are especially striking, since they allow computation to run directly on data that stays encrypted (Mohonta et al., 2026). The stakes are highest in healthcare, finance, and critical infrastructure, where sensitivity and compliance shape almost every design choice (Orthi et al., 2025c).

Cloud platforms and a new wave of communication technology supply the ground these intelligent enterprises stand on. Cloud-based MIS makes collaborative decisions, project governance, and large-scale analytics far easier to sustain (Mahmud et al., 2023). Out at the network edge, advances in 6G, semantic communication, and digital twins are carrying real-time support into highly distributed environments (Gangula et al., 2026). Secure edge intelligence is fast becoming a precondition for the digital twins that increasingly mirror physical operations (Varanasi et al., 2026). Zero-touch 6G frameworks point toward edge ecosystems that configure and defend themselves with little human oversight (Mahin et al., 2026).

Recent scholarship ties this intelligence directly to resilience. MIS-enabled analytics has been used to firm up supply chains, guard energy infrastructure, and steady economic activity (Goffer et al., 2024). National-scale studies extend the same reasoning to the defense of critical infrastructure and the stability of the wider economy (Das et al., 2026). Work on the energy sector shows how intelligent information management can underpin infrastructure resilience at a considerable scale (Barikdar et al., 2025). Read together, these threads send one message: enterprise intelligence has to reach past efficiency to take in security, resilience, and sustainability (Uddin et al., 2025).

The same turn appears in IT project management and software quality assurance. AI-driven project systems now fold predictive analytics, risk intelligence, and digital twins into the work of delivery (Siddiqa et al., 2024). On the quality side, predictive methods cut defects, hold down testing costs, and shorten development cycles (Bakhsh et al., 2024). Pipelines built for healthcare software show how predictive QA and digital twins raise safety and agility in tightly regulated settings (Rahman et al., 2025a). Agile teams have begun to treat digital twins as a routine part of sprint planning and validation rather than an experiment (Bakhsh et al., 2025).

For all this momentum, the literature remains scattered. Most studies advance one capability at a time, and very few explain how the pieces are supposed to fit together into a single, working architecture. Practitioners know the consequences well: brittle interoperability, governance that pulls in different directions, and transformation efforts that never quite cohere. A consolidating view is overdue (Ahsan et al., 2025).

This paper answers that gap with an Autonomous Decision Intelligence (ADI) framework that brings AI, big data analytics, blockchain, cybersecurity, and MIS into one ecosystem for resilient digital enterprises. The aim is to lay the groundwork for decision-making that is secure, explainable, adaptive, and trustworthy, and that can carry both resilience and sustainable growth. Five objectives organize the work (Uddin et al., 2026).

- Trace the changing role of AI, cybersecurity, blockchain, and big data analytics inside modern MIS environments.
- Pull together interdisciplinary evidence on enterprise intelligence, digital resilience, and decision support.
- Build a conceptual ADI framework that joins technological, organizational, and governance concerns.
- Examine what the framework means in practice for digital enterprises, critical-infrastructure systems, and future intelligent organizations.
- Mark out where research should go next on secure and autonomous enterprise decision-making.

Drawing on business analytics, cybersecurity, blockchain governance, federated learning, cloud computing, and decision intelligence, the study offers a single vision for the next generation of intelligent enterprises operating inside an unusually complex digital economy.

2. Literature Review

2.1 From Information Processing to Intelligent Enterprise Ecosystems

For decades, management information systems formed the quiet backbone of organizational information processing. They gathered data, produced reports, recorded transactions, and kept operations under control. Early designs leaned toward structured data and backward-looking reports, serving managers through central databases and a fixed menu of outputs. Rising complexity and the swift spread of digital technology have since recast MIS as a strategic platform for enterprise intelligence rather than a back-office utility.

Modern MIS environments are now bound up with AI, machine learning, cloud computing, and advanced analytics. Das et al. (2023) showed that careful MIS implementation lifts agile project outcomes by widening access to information and tightening strategic alignment. In a similar vein, Siddiqa et al. (2024) found that AI-driven project systems embedded in MIS sharpen efficiency, mitigate risk, and improve how quickly an organization can respond.

Placing AI inside MIS has hurried the move from systems that merely describe toward systems that predict and prescribe. Ahsan et al. (2025) named this shift the rise of "resilient intelligence," in which AI-enhanced MIS keeps adapting to changing business and cyber-economic conditions. Hossain et al. (2023) made a complementary case, arguing that the blend of AI, cloud, and analytics is rewriting the contribution MIS makes to resilience and digital sustainability.

Autonomous Decision Intelligence follows almost inevitably from this path. Where conventional decision support stops at recommendations, ADI frameworks weave together machine learning, predictive analytics, security intelligence, and automated governance so that decisions can be made continuously and adaptively. Chakraborty et al. (2024) proposed that modern MIS should grow toward autonomous decision intelligence by folding in explainable AI, scalable decision-support designs, and knowledge management.

Digital transformation has also widened the remit of MIS, pushing it beyond internal operations toward intelligence that spans an entire ecosystem. Hossin et al. (2025) showed how AI-enabled MIS platforms support post-pandemic transformation by improving agility, planning, and collaboration across the enterprise. Hassan et al. (2025c) drew attention to the part MIS plays in advancing national energy strategy through intelligent information management. Taken together, the literature reframes MIS not as a passive store of records but as an active platform for orchestrating decision intelligence, resilience, and innovation.

2.2 Artificial Intelligence and Decision Intelligence

Artificial intelligence has become one of the most consequential forces acting on enterprise decisions. Firms now lean on it to automate processes, sharpen forecasts, allocate resources, and pull insight out of very large datasets. Chakraborty et al. (2025a) examined AI and machine-learning applications across business management and found that AI-enhanced systems outperform traditional methods with some consistency once the decisions grow complex.

Decision intelligence marks a real step beyond ordinary business intelligence. It binds artificial intelligence, analytics, decision theory, and organizational learning into one framework aimed squarely at outcomes. As Chakraborty et al. (2024) put it,

decision-intelligence systems move the center of gravity from data-centric analysis toward outcome-oriented optimization, joining prediction to action.

The reach of AI-driven decision intelligence now spans a wide range of domains. Mahmud et al. (2024) showed that AI-powered workforce analytics can anticipate labor-market shifts and emerging skill gaps, which lets planners get ahead of the curve. Bhuiyan et al. (2025) turned advanced analytics on the economic costs of homelessness and used the results to shape sustainable policy. Haldar et al. (2025) linked AI-driven analytics to economic growth through better predictive accuracy and smarter use of resources.

Business-intelligence platforms increasingly run on machine learning when they support strategy and operations. Das et al. (2025c) reviewed the strategic impact of these tools and concluded that analytics-driven decisions strengthen an organization's ability to exploit and explore at once. Uddin et al. (2026) proposed AI-powered business-intelligence frameworks that reshape enterprise decisions through predictive analytics and big-data integration. The same logic has even been used to upskill the teams who run analysis and quality assurance (Alam et al., 2025a).

Finance offers some of the clearest evidence that the value is real. Manik et al. (2025) built big-data analytics models for credit-risk assessment that lifted predictive accuracy by a noticeable margin. Hassan et al. (2025a) proposed AI-driven environmental, social, and governance scoring to guide sustainable investment. Across these cases, explainability is the thread that holds adoption together, because transparency, fairness, and auditability increasingly decide whether a regulated enterprise will trust an AI system at all.

2.3 Big Data Analytics and Business Intelligence

The sheer growth of digital data has changed how organizations plan and decide. Big data analytics lets a firm work through large volumes of structured and unstructured information, expose patterns that were hidden, and turn raw records into a decision. None of this holds up without governance underneath it. Chy et al. (2024) studied the link between data governance and analytics success and found that strong governance lifts analytical effectiveness in measurable ways.

Predictive analytics has earned its place across many sectors. Goffer et al. (2024) showed that predictive analytics built into MIS strengthens supply chains and softens economic shocks. Sultana et al. (2024) demonstrated how well machine-learning algorithms handle sales forecasting, where they tighten operational response. To keep such pipelines reliable as they scale, automated, DataOps-style governance has begun to take hold (Orthi et al., 2025b).

Analytics has also moved to the center of sustainability work. Khair et al. (2024) traced how analytics-driven decisions advance green-energy initiatives and broader growth. Hossin et al. (2024) made a parallel argument for smart manufacturing and Industry 4.0, where analytics converts shop-floor signals into strategy. Hossain et al. (2025) framed the point more broadly, describing analytics as the route from raw data to evidence-based management.

Analytical methods themselves keep growing more capable. Rozario et al. (2026) proposed transformer-based generative models for dynamic big-data summarization, which help organizations distill meaning from sprawling information. Predictive sustainability analytics has been put to work optimizing resource use on the factory floor (Sizan et al., 2025). Deep-learning architectures, in turn, have forecast electric-vehicle adoption with attention-based designs (Rahaman et al., 2025).

In quality and risk settings, AI-enhanced analytics has become a fixture. Alam et al. (2025b) showed how predictive analytics supports defect prevention and quality optimization in enterprise software. Joy et al. (2024) found that predictive models trim testing costs while raising reliability. Explainable churn models that combine tabular machine learning with SHAP analysis show that interpretability and predictive power can travel together (Zerine et al., 2026). On the whole, the evidence places big data analytics among the load-bearing pillars of autonomous decision intelligence.

2.4 Blockchain and Decentralized Trust Architectures

Trust is a stubborn problem in digital ecosystems built from distributed data, many stakeholders, and a rising tide of threats. Blockchain offers a credible response by supplying decentralized, immutable, and transparent ways to verify and govern. Hassan et al. (2025b) showed that blockchain integration strengthens cybersecurity and data integrity inside MIS by removing the weaknesses that come with central control.

Blockchain also reshapes governance and privacy. Bauskar et al. (2025) introduced a privacy-aware big-data governance framework that pairs blockchain with stronger controls to improve transparency and accountability. Esa et al. (2025) proposed a blockchain-based digital identity management system that curbs fraud and reinforces trust in everyday transactions. Carbon-credit platforms tell a similar story, where the same properties improve traceability and compliance (Islam et al., 2025).

Applications now reach well beyond security and identity. Chakraborty et al. (2025b) proposed trustworthy data-Lakehouse architectures that combine blockchain with federated learning to support secure, decentralized data ecosystems. Rahaman et al.

(2024) singled out blockchain, alongside AI and analytics, as a key enabler of sustainable practice across industries. In federated cloud settings, Haldar et al. (2026) demonstrated blockchain-driven access control and compliance auditing that lift both security and accountability. Read as a body, these studies suggest that blockchain supplies the trust infrastructure on which autonomous decision intelligence can rest.

2.5 Cybersecurity as a Strategic Foundation for Resilience

Cybersecurity has graduated from a technical chore into a strategic capability. As threats grow more capable and digital dependence deepens, firms have little choice but to defend proactively and with intelligence. Kaur et al. (2023) traced the fast evolution of cyber threats and called for mechanisms able to meet new attack vectors head-on. Hasan et al. (2023) added to the picture by showing how big data analytics improves detection and response inside enterprise information systems.

AI-driven security frameworks count among the most important recent developments. Goffer et al. (2025a) proposed AI-enhanced detection and response aimed at protecting national security and critical infrastructure. Mahmud et al. (2025a) showed that AI-driven approaches sharpen risk mitigation and threat intelligence within IT-project environments. The idea of embedding cyber-risk management inside information-systems governance has been advanced as a national-scale strategy for resilience (Hasan et al., 2026).

Advanced learning architecture keeps pushing detection forward. Kaur et al. (2025) compared transformer- and LSTM-based models and reported clear gains in accuracy over older methods. Sultana et al. (2025) demonstrated AI-augmented analytics for real-time attack detection and proactive mitigation. The influence of AI on the underlying security of data systems has been examined alongside this line of work (Hasan et al., 2025a).

Increasingly, the research favors systems that adapt on their own. Hasan et al. (2025b) proposed reinforcement-learning self-healing architectures that detect, respond, and recover with little human involvement. Nabi et al. (2026) introduced continual-learning frameworks for catching insider threats across complex infrastructures. Adversarial-robustness mechanisms have also been designed to protect biometric verification in mobile financial applications (Raihan et al., 2026).

The stakes run well past any single firm, into society and the economy. Das et al. (2026) proposed AI-driven frameworks to shield critical infrastructure from large-scale attacks. Uddin et al. (2025) showed how AI-enabled security reinforces supply-chain integrity, energy resilience, and national security. National defense frameworks against evolving digital warfare make the point at the level of the state (Siam et al., 2025a). People matter as much as systems, and security training measurably shapes how employees behave in business settings (Shan-A-Alahi et al., 2024). All of these points to one conclusion: security belongs inside the decision-intelligence framework, not beside it.

2.6 Federated Learning, Privacy, Cloud, and Emerging Technologies

The future of autonomous decision intelligence will rest on technologies that hold access, privacy, scale, and security in balance. Federated learning, homomorphic encryption, cloud computing, edge intelligence, and next-generation networks are the chief enablers. Federated learning, in particular, lets organizations train models together without handing over sensitive records. Orthi et al. (2025c) demonstrated its value for distributed healthcare analytics.

Encryption advances strengthen the picture further. Das et al. (2025b) proposed privacy-preserving homomorphic federated models that raise protection in collaborative settings. Mohonta et al. (2026) showed how homomorphic techniques enable confidential big-data analytics on public cloud infrastructure without ever exposing the underlying data.

Cloud computing remains the scalable foundation under all of this. Mahmud et al. (2023) proposed cloud-based frameworks that improve IT-project management and decision-making. Mahmud et al. (2025b) drew attention to the role of cloud-based MIS in strengthening governance and stakeholder collaboration.

Edge AI, semantic communication, and 6G extend these capabilities to the periphery. Gangula et al. (2026) proposed a lightweight, secure semantic-communication architecture for edge–IoT–6G systems. Mahin et al. (2026) introduced an intelligent zero-touch 6G framework for autonomous edge-AI applications. Varanasi et al. (2026) demonstrated secure edge intelligence for real-time digital-twin deployments. Together these technologies give autonomous decision intelligence the technical ground it needs to be secure, scalable, and self-sustaining.

3. Conceptual Framework Development

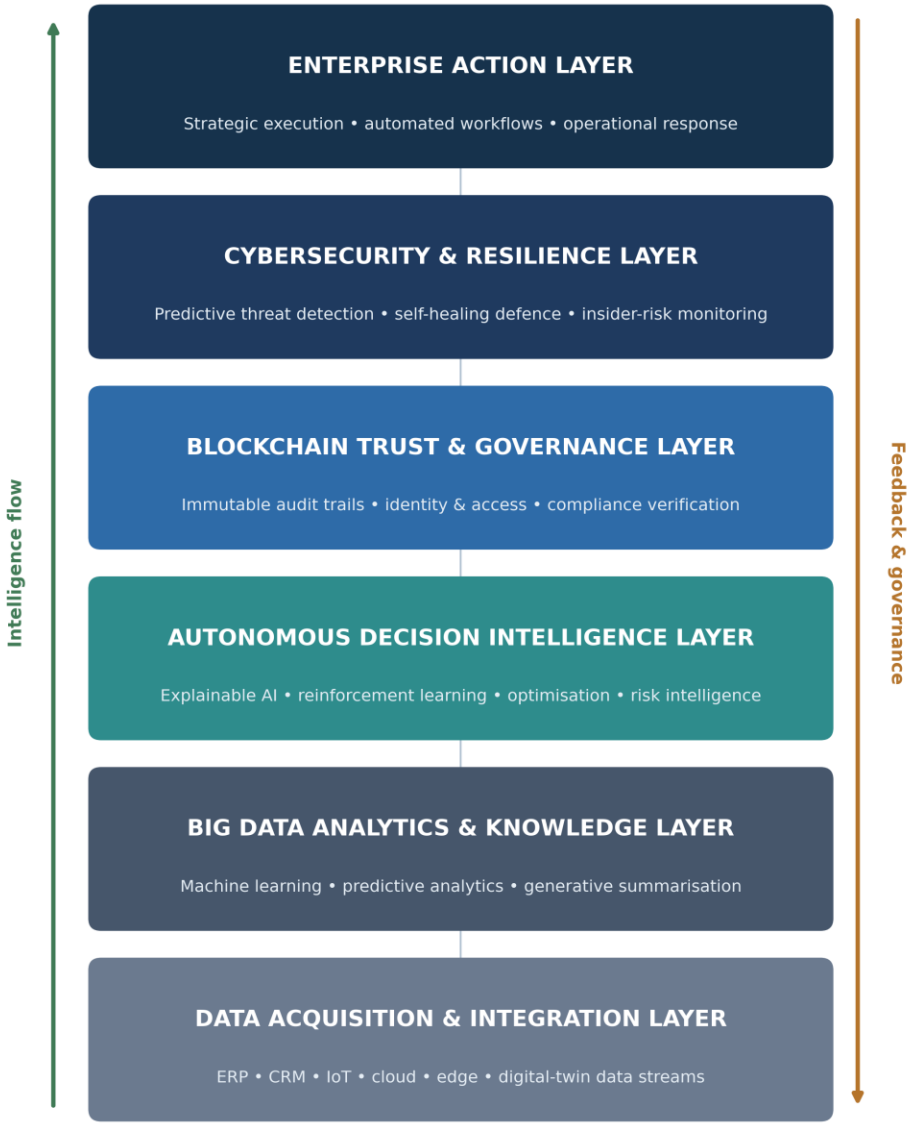
3.1 The Case for an Autonomous Decision Intelligence Framework

One pattern runs through the review above and is hard to miss. Artificial intelligence, big data analytics, cybersecurity, blockchain, cloud computing, federated learning, and MIS have each advanced enormously over the past decade, and yet

organizations keep adopting them one at a time. The result is a familiar set of ailments: data trapped in silos, governance that does not join up, analytical work done twice, and controls that drift out of step with one another.

Taken alone, each technology leaves a gap that another could close. AI generates predictions but rarely carries trustworthy governance around them. Blockchain offers trust and transparency, yet it usually sits off to one side of the analytics estate. Security systems catch threats competently enough, but they are seldom wired into the decisions the business actually makes. The net effect is that heavy investment in technology does not reliably add up to coherent enterprise intelligence.

Figure 1. The Autonomous Decision Intelligence (ADI) Framework



A layered architecture in which data ascends into intelligence while trust, security, and feedback descend through every tier.

Figure 1. The Autonomous Decision Intelligence (ADI) framework, showing intelligence flowing upward while trust, security, and feedback descend through every layer.

The Autonomous Decision Intelligence (ADI) framework meets this problem head-on by drawing these technologies into one architecture that collects, analyses, secures, validates, and acts on organizational intelligence without interruption. The design

begins from the autonomous-decision-intelligence architecture set out by Chakraborty et al. (2024). It also borrows from AI-driven business-intelligence designs (Uddin et al., 2026). The resilient-MIS perspective informs its overall logic (Ahsan et al., 2025). Blockchain-enabled governance supplies its trust layer (Hassan et al., 2025b). What we aim for is a secure, adaptive, and self-improving ecosystem that can carry resilient transformation. Figure 1 sets out the six-layer architecture that results.

3.2 Data Acquisition and Integration Layer

The first layer gathers and harmonizes data. A modern enterprise produces information from a sprawl of sources, among them ERP and CRM systems, IoT devices, cloud and edge environments, mobile applications, social platforms, and digital-twin ecosystems. Whether an organization thrives increasingly depends on how well it can braid these streams into a single analytical environment (Chy et al., 2024).

Cloud-based MIS makes that braiding feasible, offering scalable storage, distributed processing, and shared decision-making (Mahmud et al., 2025b). Transformation programs lean hard on such integrated ecosystems to keep their agility and planning intact (Hossin et al., 2025). At the edge, semantic-communication and 6G architectures improve how efficiently data moves across distributed environments (Gangula et al., 2026). Secure edge intelligence, for its part, sustains the real-time digital twins that mirror physical operations (Varanasi et al., 2026). This layer is therefore the bedrock on which everything else is built.

3.3 Big Data Analytics and Knowledge Generation Layer

Once data are gathered and integrated, they pass into the analytics layer, where raw records turn into organizational knowledge. This is the analytical core of the framework, and it draws on machine learning, deep learning, predictive analytics, data mining, natural-language processing, and generative AI. Through these methods, a firm can surface patterns, anticipate outcomes, and ground its decisions in evidence. The practical value shows up plainly in credit-risk assessment, where analytics sharpens financial judgment (Manik et al., 2025).

The same capability turns up in problems that look nothing alike. AI-powered workforce analytics anticipates labor-market shifts and skill shortages, which gives planners room to act early (Mahmud et al., 2024). Predictive techniques have proven effective in sales forecasting (Sultana et al., 2024). They have likewise informed economic-policy analysis aimed at sustainable solutions (Bhuiyan et al., 2025). The same family of methods supports sustainability-focused resource optimization in manufacturing (Sizan et al., 2025). They have even been applied to forecasting electric-vehicle adoption (Rahaman et al., 2025).

Automation is steadily lifting the manual burden of pulling knowledge out of data. AI-powered business-intelligence platforms now derive insight from massive, heterogeneous datasets at speed (Uddin et al., 2026). Transformer-based generative models push this further, summarizing and synthesizing information at scale and strengthening how organizations learn (Rozario et al., 2026). In short, this layer converts enterprise data into predictive signals, anomaly alerts, and strategic forecasts that adaptive decision-making depends on.

3.4 Autonomous Decision Intelligence Layer

The ADI layer is the framework's central innovation and the bridge between knowledge and action. Traditional decision support mostly describes or predicts; this layer goes further, weaving together explainable AI, reinforcement learning, optimization, decision theory, scenario analysis, and adaptive learning to produce recommendations and, where it makes sense, autonomous decisions. Its purpose is not simply to foresee what is coming but to find the best available course of action and keep getting better at it. Decision-intelligence systems tend to outperform ordinary analysis precisely because they tie prediction to what the organization is trying to achieve (Chakraborty et al., 2024).

Several specialized intelligence functions run inside this layer at the same time. Strategic intelligence supports long-term planning and growth through AI-driven analytics (Haldar et al., 2025). Project intelligence improves scheduling, resource allocation, and risk assessment in AI-enhanced project systems (Siddiqa et al., 2024). Workforce intelligence reads predictive analytics to map skill gaps and development needs (Mahmud et al., 2024). Quality intelligence brings down defects and development cost through advanced analytics (Joy et al., 2024). Risk intelligence applies machine-learning and neural-network models to weigh exposure and reinforce governance (Orthi et al., 2025a). With every feedback cycle, the layer grows more capable, carrying the organization toward decision-making that is genuinely adaptive.

3.5 Blockchain Trust and Governance Layer

Trustworthiness is not optional for any system that decides on its own, least of all where data are distributed and regulation is dense. The blockchain layer supplies the mechanisms for data integrity, transparency, auditability, compliance, and identity. Keeping immutable, tamper-resistant records raises confidence in enterprise data, transactions, and outcomes. As reliance on automated decisions grows, accountability becomes the hinge on which both effectiveness and acceptance turn.

A range of studies backs the idea of embedding blockchain in enterprise governance. Privacy-aware governance models show how it improves accountability in big-data settings (Bauskar et al., 2025). Decentralized identity systems cut fraud and shore up

digital trust (Esa et al., 2025). Inside MIS, blockchain integration strengthens security, integrity, and governance by removing single points of failure (Hassan et al., 2025b). In federated clouds, blockchain-driven auditing improves compliance monitoring and access control (Haldar et al., 2026). Carbon-credit platforms add evidence of better traceability in sustainability work (Islam et al., 2025). Beyond any single use, blockchain underpins trustworthy Lakehouse architectures that fuse decentralized governance with federated learning (Chakraborty et al., 2025b). Within ADI, then, blockchain works as an enterprise-wide trust fabric that validates decisions and records what the organization does.

3.6 Cybersecurity and Resilience Layer

Cybersecurity forms the protective backbone of the whole framework. The deeper an organization's dependence on interconnected infrastructure runs, the more it faces ransomware, insider abuse, supply-chain compromise, IoT attacks, AI-enabled offensives, and operations run by nation-states. These risks endanger more than information; they threaten continuity, economic stability, and national security. Security, therefore, belongs inside enterprise intelligence rather than alongside it. Big data analytics has already proven its worth in real-time threat detection within information systems (Hasan et al., 2023).

AI-enhanced frameworks deepen that defense by automating detection, anomaly identification, and response (Das et al., 2025a). Research on national infrastructure shows how AI-driven security raises resilience against attacks at scale (Das et al., 2026). Cybersecurity-governance models pull risk management and information-systems governance into a single strategy (Hasan et al., 2026). Cyber threat intelligence has itself been recast as a management-information-system function that ties governance to project delivery (Orthi et al., 2023).

The layer brings several concrete capabilities under one roof. Predictive detection uses machine learning to flag threats before an incident lands (Goffer et al., 2025a). Real-time monitoring applies analytics to surface suspicious activity the moment it appears (Sultana et al., 2025). Self-healing systems put reinforcement-learning agents to work responding and recovering on their own (Hasan et al., 2025b). Insider-threat detection leans on continual-learning algorithms to catch behavior that turns abnormal (Nabi et al., 2026). AI-driven defenses extend protection across supply chains and critical infrastructure (Uddin et al., 2025).

Resilience also rests on the architecture beneath it. Secure-by-design data centers show how energy efficiency and strong cyber controls can be balanced rather than traded against each other (Hossain et al., 2024b). Resilient distributed designs improve fault tolerance across large-scale ecosystems (Shan-A-Alahi et al., 2026b). Deep-learning threat prediction with autonomous response has been developed for containerized microservices in hybrid clouds (Shan-A-Alahi et al., 2026a). Survivability and importance analysis offer a complementary lens for networks that move intricate traffic flows (Siddiqa et al., 2025). Put together, these capabilities keep autonomous decision-making secure and adaptive even when an adversary is pressing hard. Table 1 maps each technology onto a primary function within the framework.

Table 1. Technology-to-function mapping within the ADI framework

Technology	Primary function	Representative study
Artificial intelligence	Prediction and decision optimisation	Chakraborty et al. (2025a)
Big data analytics	Knowledge discovery	Manik et al. (2025)
Management information systems	Enterprise coordination	Das et al. (2023)
Blockchain	Trust and governance	Hassan et al. (2025b)
Federated learning	Privacy preservation	Orthi et al. (2025c)
Homomorphic encryption	Confidential analytics	Mohonta et al. (2026)
Cybersecurity AI	Threat detection	Goffer et al. (2025a)
Reinforcement learning	Autonomous response	Hasan et al. (2025b)
Cloud computing	Scalability	Mahmud et al. (2025b)

Edge AI and 6G	Real-time intelligence	Gangula et al. (2026)

To make the architecture concrete, Table 2 distils the five thematic dimensions that surfaced during the literature synthesis, and Figure 2 shows how those themes converge on the autonomous-decision-intelligence core.

Table 2. Thematic dimensions identified during the literature synthesis

Thematic dimension	Core concern	Anchoring study
Intelligent decision support	Connecting prediction to action and strategy	Chakraborty et al. (2024)
Data governance and advanced analytics	Turning distributed data into reliable insight	Chy et al. (2024)
Cybersecurity and risk management	Proactive defence and organisational resilience	Hasan et al. (2026)
Blockchain-enabled trust	Transparency, auditability, and accountability	Bauskar et al. (2025)
Enterprise resilience and sustainability	Absorbing shocks and sustaining operations	Barikdar et al. (2025)

Figure 2. Five Thematic Dimensions Converging on Autonomous Decision Intelligence

Figure 2. Five thematic dimensions converging on autonomous decision intelligence.

3.7 Theoretical Contributions

The framework moves the literature forward in five ways. First, it unifies AI, MIS, blockchain, cybersecurity, and big data analytics within one architecture instead of leaving them as separate initiatives. Second, it carries decision-intelligence theory past prediction toward decision-making that is genuinely autonomous. Third, it brings blockchain-enabled trust directly into enterprise intelligence. Fourth, it builds cybersecurity into decision-support processes rather than bolting it on after the fact. Fifth, it offers a scalable foundation for resilient enterprises that operate across cloud, edge, IoT, and 6G environments. Table 3 summarizes the role each layer plays.

Table 3. Summary of the six ADI layers and their functions

ADI layer	Function within the framework	Illustrative capability
Data acquisition and integration	Ingests heterogeneous data streams	ERP, CRM, IoT, edge, digital twin
Big data analytics and knowledge	Transforms data into intelligence	ML, predictive analytics, generative summarisation
Autonomous decision intelligence	Recommends and optimises action	Explainable AI, reinforcement learning, risk intelligence
Blockchain trust and governance	Validates and records decisions	Immutable audit trails, identity, compliance
Cybersecurity and resilience	Protects the whole ecosystem	Predictive detection, self-healing defence
Enterprise action	Executes and feeds back outcomes	Automated workflows, operational response

I.

4. Research Methodology

This study takes a conceptual, integrative, theory-building approach to developing the ADI framework. The point is not to test a single hypothesis by experiment but to gather knowledge from several technical and managerial fields and to build one unified model that can guide later research and practice. An approach of this kind suits fast-moving areas where innovation outruns empirical validation. In fields such as AI, analytics, cybersecurity, blockchain, and MIS, conceptual frameworks often provide the scaffolding on which empirical work is later raised (Chakraborty et al., 2024).

The framework grew out of a systematic synthesis that ranged across information systems, artificial intelligence, cybersecurity, cloud computing, blockchain governance, business analytics, digital transformation, and enterprise resilience. The reasoning behind that breadth is simple. Earlier studies usually examine these technologies in isolation, even though enterprises deploy them together inside tangled ecosystems. What has been missing is a full account of how they work jointly (Ahsan et al., 2025).

The research moved through four stages, which Figure 3 sets out. The first stage was literature identification and domain mapping. We drew relevant studies from AI and machine learning, cybersecurity and digital resilience, blockchain and decentralized governance, big data analytics and business intelligence, and management information systems. The seventy-four references brought together here represent contemporary advances across those areas. Their breadth allowed the study to take in a wide range of perspectives and surface the challenges they hold in common.

The second stage was thematic analysis and knowledge synthesis. Working through the material in repeated passes, we found five themes returning again and again: intelligent decision support, data governance and advanced analytics, cybersecurity and risk management, blockchain-enabled trust, and enterprise resilience and sustainability. These themes exposed dependencies that isolated studies tend to hide. Predictive analytics, for one, leans on sound data governance, while AI-driven decisions need trustworthy security and governance if they are to stay transparent and accountable.

The third stage was framework construction. We folded the themes into a six-layer architecture made up of the data acquisition and integration layer, the big data analytics and knowledge generation layer, the autonomous decision intelligence layer, the blockchain trust and governance layer, the cybersecurity and resilience layer, and the enterprise action layer. This structure follows the logical flow of intelligence from data collection through to execution while threading security, governance, and resilience through every step. Where traditional models center on information processing, the framework keeps continuous learning and adaptive decision support in the foreground.

The fourth stage addressed theoretical validation and consistency. We checked the framework for fit with established theory in MIS, decision support, AI, enterprise architecture, cybersecurity governance, and digital transformation. A cross-domain analysis confirmed that the relationships among components were theoretically justified, and an interoperability assessment asked whether the integrated technologies could realistically run together. The framework that emerged shows strong conceptual coherence and matches the direction in which enterprises are already heading.

Figure 3. The Four-Stage Integrative Research Process

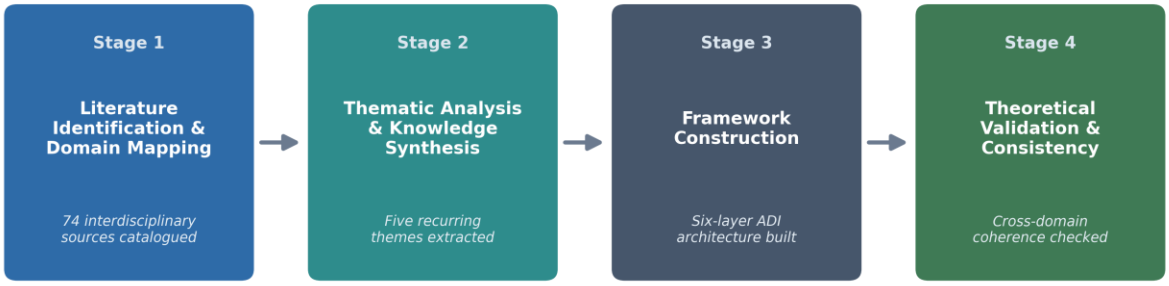


Figure 3. The four-stage integrative research process used to develop the ADI framework.

4.1 Research Propositions

The synthesis yields a set of propositions to steer future empirical work. AI-driven analytics should improve decision quality by raising prediction accuracy and adaptive responsiveness (Chakraborty et al., 2025a). Big data analytics should strengthen resilience by improving situational awareness and forecasting in volatile environments (Goffer et al., 2024). Blockchain-enabled governance should bolster trust, accountability, and regulatory compliance through decentralized verification (Hassan et al., 2025b).

AI-enhanced security should improve resilience through proactive detection and adaptive, automated defense (Das et al., 2025a). Federated and privacy-preserving analytics should enable collaboration while shielding sensitive data (Orthi et al., 2025c). Cloud-based MIS should improve agility through scalable collaboration and distributed decision-making (Mahmud et al., 2025b). Most of all, integrated ADI systems should outperform isolated deployments because they create synergies across analytics, governance, security, and intelligence (Chakraborty et al., 2024). Resilience, finally, should reach its peak when these capabilities behave as one ecosystem rather than a set of separate projects (Hasan et al., 2026). Table 4 brings these propositions together.

Table 4. Research propositions derived from the literature synthesis

No.	Research proposition	Support
P1	AI-driven analytics improves decision quality by raising prediction accuracy and adaptive responsiveness.	Chakraborty et al. (2025a)
P2	Big data analytics enhances resilience through better situational awareness and forecasting.	Goffer et al. (2024)

P3	Blockchain governance strengthens trust, accountability, and regulatory compliance.	Hassan et al. (2025b)
P4	AI-enhanced cybersecurity improves resilience via proactive detection and automated response.	Das et al. (2025a)
P5	Federated and privacy-preserving analytics enables collaboration while protecting sensitive data.	Orthi et al. (2025c)
P6	Cloud-based MIS improves agility through scalable collaboration and distributed decisions.	Mahmud et al. (2025b)
P7	Integrated ADI systems outperform isolated technology deployments through synergy.	Chakraborty et al. (2024)
P8	Resilience is maximised when AI, blockchain, security, analytics, and MIS act as one ecosystem.	Hasan et al. (2026)

5. Discussion

The analysis points to a deep change in what enterprise information systems are for. Historically, MIS existed to store data, run reports, process transactions, and watch over operations. Those jobs still matter, but organizations now need systems that predict, spot threats, learn from experience, recommend action, and adapt on their own. That is the shift from information-centric systems toward intelligent, adaptive ecosystems. The ADI framework adds to it by treating AI, analytics, cybersecurity, blockchain, and MIS as interconnected parts of one decision architecture rather than a drawer full of separate tools.

One of the clearest findings concerns the rise of cybersecurity as a strategic capability. For a long time, security was filed under technical matters, confined to protecting assets and networks. The contemporary evidence tells a different story, in which cyber risk bears directly on performance, supply-chain continuity, financial stability, and trust (Goffer et al., 2025b). Security has to live inside decision-making itself. The framework answers that demand by folding predictive detection, threat intelligence, self-healing mechanisms, and governance controls into its core.

Blockchain's role in building trust is a second theme worth dwelling on. As organizations lean more heavily on AI-driven decisions, stakeholders want some assurance that data, models, and outcomes stay transparent and open to audit. Blockchain meets that want through decentralized verification, immutable records, and transparent governance (Esa et al., 2025). Inside ADI, it works less as a narrow security tool and more as a foundational trust infrastructure that lends the organization legitimacy.

A third implication concerns autonomous learning. Traditional decision-support systems hand out static recommendations built on fixed models and historical data. The framework, by contrast, takes in adaptive mechanisms that refine decisions through feedback and reinforcement learning. That lets organizations move from reacting to anticipating, which matters most amid uncertainty and rapid change. Software quality assurance shows the idea vividly, as AI-driven predictive analytics and digital twins reshape practice across the development lifecycle (Rahman et al., 2025b).

The findings also push resilience to the center of digital transformation. Enterprises sit inside interconnected systems where disruption can begin in a cyberattack, an economic wobble, a geopolitical conflict, or a supply-chain failure. Resilience now depends not only on staying open but on the capacity to anticipate, adapt, and recover quickly (Barikdar et al., 2025). By joining intelligence generation, protection, trust, and adaptive decision-making, the framework offers a coherent footing for resilient enterprises. Figure 4 shows how the core technologies contribute to resilience in ways that complement rather than duplicate one another.

Figure 4. Complementary Contributions of Core Technologies to Enterprise Resilience

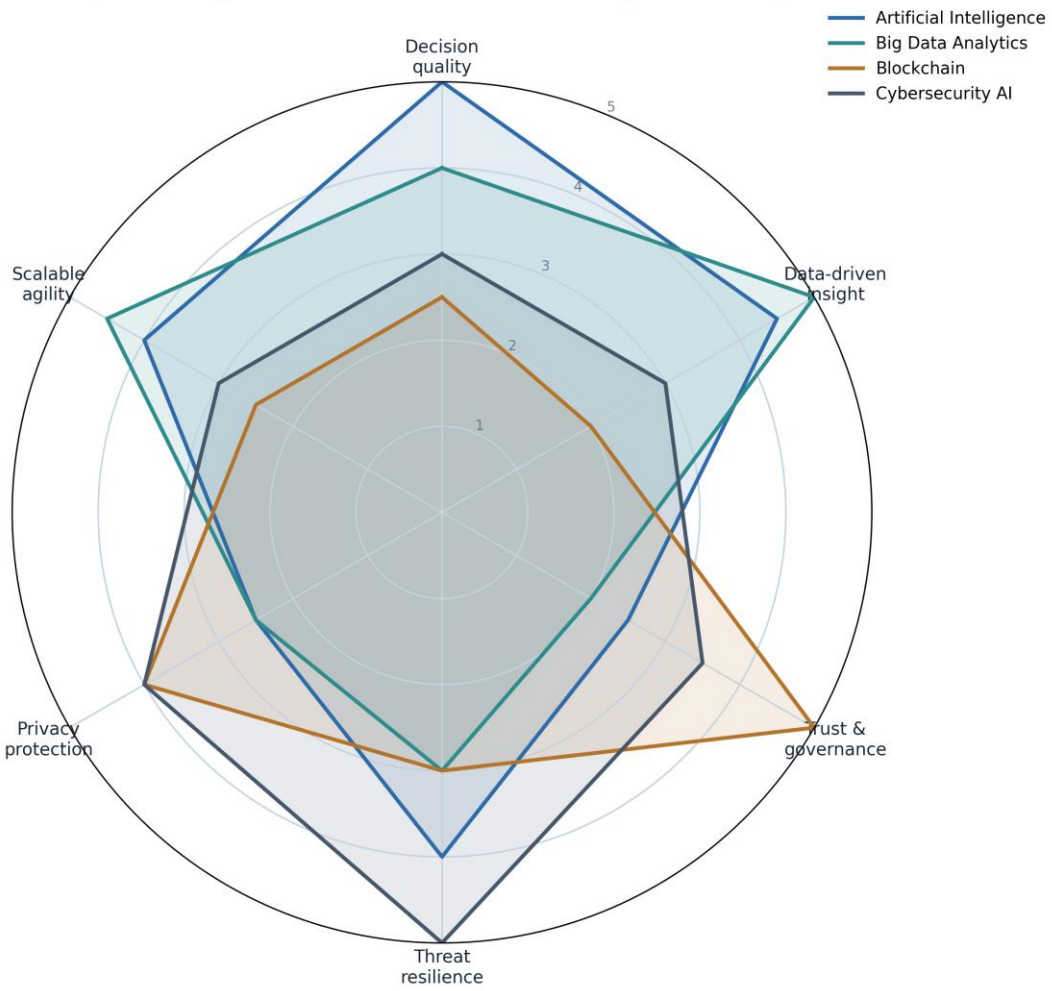


Figure 4. Complementary contributions of core technologies to enterprise resilience across six capability dimensions.

Read as a whole, the discussion underscores the cost of adopting technology piecemeal. Organizations that roll out AI, analytics, security, blockchain, and governance independently may never see the full return on their transformation. Those that bring them together inside one ADI ecosystem stand a better chance of making better decisions, stronger security, deeper trust, and durable resilience. The framework, therefore, offers both a theoretical contribution and a practical map for the cyber-economic era (Uddin et al., 2026).

6. Conclusion

The quickening convergence of AI, big data analytics, blockchain, cybersecurity, cloud computing, federated learning, and MIS is changing how organizations operate, compete, and create value. Systems built mainly for storage, transactions, and backward-looking reports increasingly fall short in environments defined by complexity and interdependence. As threats escalate, data swells, and regulators tighten their grip, a new generation of intelligent enterprise architecture has become a necessity rather than a luxury (Ahsan et al., 2025).

This study introduced Autonomous Decision Intelligence as a comprehensive framework for drawing these technologies into one ecosystem for adaptive, secure, and resilient decision-making. Where conventional decision support stops short, the framework presses on with continuous learning, predictive intelligence, trust-enabled governance, autonomous response, and resilience across the enterprise. Synthesizing a broad literature, it shows how the technologies can be orchestrated into an architecture that improves both performance and sustainability (Chakraborty et al., 2024).

Within that architecture, AI works as the analytical engine, enabling prediction, optimization, and adaptive decision-making. Big data analytics supply the informational ground by turning diverse data into knowledge. Blockchain contributes to trust, transparency, and governance. Cybersecurity safeguards confidentiality, integrity, availability, and resilience, while federated and

privacy-preserving methods make secure collaboration possible across distributed ecosystems (Orthi et al., 2025c). Together, these capabilities create an environment that senses, analyses, learns, and responds without pause.

A central contribution is the recognition that enterprise intelligence can no longer be treated as a pile of independent technologies. Organizations gain instead from a systems-minded view in which analytics, security, governance, and trust act as interdependent parts of one decision ecosystem. The framework offers a blueprint for integration, linking data acquisition, knowledge generation, autonomous decision-making, governance, resilience, and execution.

The study also lifts resilience to a strategic goal in its own right. In the cyber-economic era, success rests on the ability to anticipate disruption, withstand attack, hold stakeholder trust, and keep operating. Organizations that combine AI-driven intelligence with secure governance and resilient infrastructure will be better placed to handle whatever comes next (Uddin et al., 2025).

For practitioners, the framework offers concrete guidance to executives, chief information and security officers, and policymakers who are modernizing enterprise architecture. It supports better decisions, stronger security postures, sounder governance, and greater agility. For researchers, it lays a foundation for empirical work on decision-intelligence effectiveness, cyber resilience, and AI governance (Hasan et al., 2026).

Several limitations temper these contributions. Autonomous Decision Intelligence is still an emerging field, and the framework remains conceptual rather than empirically tested. Future work should put it to the test across industries and contexts, quantify how well it performs, weigh its ethical and regulatory implications, and trace the long-run impact of autonomous systems on performance. Adversarial robustness in sensitive applications such as mobile financial services is one priority worth pursuing early (Raihan et al., 2026).

In closing, the future of digital enterprises will turn more and more on their ability to fuse intelligence, security, trust, and governance into a single strategic capability. Autonomous Decision Intelligence offers a promising route toward that goal. By converging AI, cybersecurity, big data analytics, blockchain, and MIS into one coherent architecture, organizations can move past mere information processing toward intelligent, resilient, and adaptive ecosystems fit for a digital world that grows more complex by the day (Siam et al., 2025a).

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1]. Ahsan, R. M., Uddin, B., Hossen, T., & Das, S. (2025). Resilient intelligence: AI and MIS in the cyber-economic era. The Eastasouth Journal of Information System and Computer Science, 3(2), 151–163. https://doi.org/10.58812/esiscs.v3i02.758

[2]. Alam, G. T., Jobiullah, M. I., Suspee, A. S., Bakhsh, M. M., Saimon, A. S. M., & Uddin, S. M. M. (2025a). Creating a knowledge hub: AI-powered learning management systems for BA-QA training. International Journal of Innovative Science and Research Technology, 10(4), 3111–3118. https://doi.org/10.38124/ijisrt/25apr1081

[3]. Alam, G. T., Bakhsh, M. M., Nadia, N. Y., & Islam, S. A. M. (2025b). Predictive analytics in QA automation: Redefining defect prevention for U.S. enterprises. Journal of Knowledge Learning and Science Technology, 4(2), 55–66. https://doi.org/10.60087/jklst.v4.n2.005

[4]. Bakhsh, M. M., Joy, M. S. A., & Alam, G. T. (2024). Revolutionizing BA-QA team dynamics: AI-driven collaboration platforms for accelerated software quality in the U.S. market. Journal of Artificial Intelligence General Science, 7(1), 63–76. https://doi.org/10.60087/jaigs.v7i01.296

[5]. Bakhsh, M. M., Alam, G. T., & Nadia, N. Y. (2025). Adapting agile methodologies to incorporate digital twins in sprint planning, backlog refinement, and QA validation. Journal of Knowledge Learning and Science Technology, 4(2), 67–79. https://doi.org/10.60087/jklst.v4.n2.006

[6]. Barikdar, C. R., Siddiqa, K. B., Miah, M. A., Sultana, S., Haldar, U., Rahman, H., & Hassan, J. (2025). MIS frameworks for monitoring and enhancing U.S. energy infrastructure resilience. Journal of Posthumanism, 5(5), 4327–4342. https://doi.org/10.63332/joph.v5i5.1907

[7]. Bauskar, S., Sahoo, R. K., Boda, S. S., Singhai, H., Bakhsh, M. M., & Adnan, M. (2025). Privacy-aware big data governance framework using blockchain. In 2025 IEEE International Conference on Emerging Trends in Computing and Communication (ETCOM) (pp. 1–9). IEEE. https://doi.org/10.1109/ETCOM66606.2025.11436976

[8]. Bhuiyan, M. M. R., et al. (2025). Economic implications of homelessness in the U.S.: Applying advanced business analytics to forecast costs and develop sustainable solutions. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1–5). IEEE. https://doi.org/10.1109/ICECET63943.2025.11472202
[9]. Chakraborty, P., Rashed, R. A. M., Bashir, M., Imam, H., Siam, M. A., Miah, M. A., Siddiqa, K. B., & Islam, A. (2024). Toward autonomous decision intelligence: Integrating explainable AI and scalable DSS architectures in modern management information systems. Journal of Information Systems Engineering and Management, 9(4s). https://doi.org/10.52783/jisem.v9i4s.14591
[10]. Chakraborty, P., Siddiqa, K. B., Rahman, H., Miah, M. A., Das, N., Goffer, M. A., & Das, S. (2025a). Leveraging artificial intelligence and machine learning for decision-making in business management: A comprehensive analysis. Journal of Management World, 2025(2), 46–56. https://doi.org/10.53935/jomw.v2024i4.867
[11]. Chakraborty, P., et al. (2025b). Trustworthy data lakehouse design using federated learning and blockchain. In 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT) (pp. 1–8). IEEE. https://doi.org/10.1109/ICAFT66710.2025.11453041
[12]. Chy, M. A. R., Rozario, E., Rijvi, M. H., Uddin, S. M. M., Bakhsh, M. M., Hossain, E., Hossain, M. J., Saha, U. S., & Faruk, M. I. (2024). Understanding the relationship between data governance and business analytics success: A case study of global corporations. Journal of Information Systems Engineering and Management, 9(4s). https://doi.org/10.52783/jisem.v9i4s.14807
[13]. Das, N., Hassan, J., Rahman, H., Siddiqa, K. B., Orthi, S. M., Barikdar, C. R., & Miah, M. A. (2023). Leveraging management information systems for agile project management in information technology: A comparative analysis of organizational success factors. Journal of Business and Management Studies, 5(3), 161–168. https://doi.org/10.32996/jbms.2023.5.3.17
[14]. Das, N., et al. (2025a). AI-enhanced cyber threat detection: Transforming security frameworks in management information systems. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1–6). IEEE. https://doi.org/10.1109/ICECET63943.2025.11472511
[15]. Das, N., et al. (2025b). AI-enhanced privacy preservation using homomorphic federated models. In 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT) (pp. 1–8). IEEE. https://doi.org/10.1109/ICAFT66710.2025.11453096
[16]. Das, N., Rahman, H., Siddiqa, K. B., Barikdar, C. R., Hassan, J., Bhuiyan, M. M. R., & Mahmud, F. (2025c). The strategic impact of business intelligence tools: A review of decision-making and ambidexterity. Membrane Technology, 2025(1). https://doi.org/10.52710/mt.307
[17]. Das, N., Kaur, H., Siddiqa, K. B., Hasan, S. N., Chakraborty, P., Kaur, J., Rahman, H., Shan-A-Alahi, A., & Hasan, R. (2026). AI-driven threat detection and response framework for protecting U.S. critical infrastructure from cyberattacks. International Cybersecurity Law Review. https://doi.org/10.1365/s43439-026-00169-5
[18]. Esa, H., et al. (2025). Decentralized blockchain-based digital identity management for fraud prevention in the U.S. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1–6). IEEE. https://doi.org/10.1109/ICECET63943.2025.11472520
[19]. Gangula, U. K. R., Miah, M. A., Mula, K., Dhakan, M., Sadat, Q. T., & Nayak, S. (2026). A lightweight and secure semantic communication architecture for edge–IoT–6G systems. IEEE Communications Standards Magazine. https://doi.org/10.1109/MCOMSTD.2026.3677038
[20]. Goffer, M. A., Chakraborty, P., Rahman, H., Barikdar, C. R., Das, N., Hossain, S., & Hossin, M. E. (2024). Leveraging predictive analytics in management information systems to enhance supply chain resilience and mitigate economic disruptions. Educational Administration: Theory and Practice, 30(4), 11134–11144. https://doi.org/10.53555/kuey.v30i4.9641
[21]. Goffer, M. A., Uddin, M. S., Kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., & Hasan, R. (2025a). AI-enhanced cyber threat detection and response: Advancing national security in critical infrastructure. Journal of Posthumanism, 5(3), 1667–1689. https://doi.org/10.63332/joph.v5i3.965
[22]. Goffer, M. A., et al. (2025b). Cybersecurity and supply chain integrity: Evaluating the economic consequences of vulnerabilities in U.S. infrastructure. Journal of Management World, 2025(2), 233–243. https://doi.org/10.53935/jomw.v2024i4.907
[23]. Haldar, U., Alam, G. T., Rahman, H., Miah, M. A., Chakraborty, P., Saimon, A. S. M., & Manik, M. M. T. G. (2025). AI-driven business analytics for economic growth: Leveraging machine learning and MIS for data-driven decision-making in the U.S. economy. Journal of Posthumanism, 5(4), 932–957. https://doi.org/10.63332/joph.v5i4.1178
[24]. Haldar, U., Sultana, S., Siddiqa, K. B., Rozario, E., Miah, M. A., Rahman, H., & Chy, M. A. R. (2026). Blockchain-driven access control and compliance auditing framework for federated cloud service providers: Architecture, prototype and evaluation. In G. N. Nguyen, A. Swaroop, & P. Shukla (Eds.), Proceedings of Fifth International Conference on Computing and Communication Networks. ICCCN 2025 (Lecture Notes in Networks and Systems, Vol. 1773). Springer. https://doi.org/10.1007/978-3-032-14197-2_41

[25]. Hasan, S. N., Hassan, J., Barikdar, C. R., Chakraborty, P., Haldar, U., Chy, M. A. R., Rozario, E., Das, N., & Kaur, J. (2023). Enhancing cybersecurity threat detection and response through big data analytics in management information systems. Fuel Cells Bulletin, 2023(12). https://doi.org/10.52710/fcb.137

[26]. Hasan, S. N., Kaur, H., Mohonta, S. C., Siddiqa, K. B., Kaur, J., Haldar, U., & Manik, M. M. T. G. (2025a). The influence of artificial intelligence on data system security. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3476

[27]. Hasan, S. N., et al. (2025b). Self-healing cybersecurity systems using RL agents. In 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT) (pp. 1–8). IEEE. https://doi.org/10.1109/ICAFT66710.2025.11452866

[28]. Hasan, S. N., Chakraborty, P., Ansar, M. T. B., Tuhin, M. K., Siam, M. A., Kaur, J., Hassan, J., & Barikdar, C. R. (2026). Embedding cybersecurity risk management into information systems governance: A national-scale framework for organizational resilience, economic stability, and critical infrastructure protection. International Journal of Applied Mathematics, 39(1s). https://doi.org/10.12732/ijam.v39i1s.1623

[29]. Hassan, M., et al. (2025a). AI-driven ESG scoring for sustainable investment decisions. In 2025 International Conference on Advances in Machine Intelligence and Cybersecurity Technologies (AMICT) (pp. 239–244). IEEE. https://doi.org/10.1109/AMICT65811.2025.11402772

[30]. Hassan, J., et al. (2025b). Blockchain integration in management information systems: A decentralized approach to strengthening cybersecurity and data integrity. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1–7). IEEE. https://doi.org/10.1109/ICECET63943.2025.11472020

[31]. Hassan, J., Rahman, H., Haldar, U., Sultana, S., Rahman, M. M., Chakraborty, P., & Barikdar, C. R. (2025c). Implementing MIS solutions to support the national energy dominance strategy. Journal of Posthumanism, 5(5), 4343–4363. https://doi.org/10.63332/joph.v5i5.1908

[32]. Hossain, M. D., Sikder, M. S., Uddin, M. S., Ahsan, R. M., Uddin, B., & Hossen, T. (2023). Cognitive cyber defense: AI–MIS integration through big data and cloud frameworks for next-generation digital resilience. The Eastasouth Journal of Information System and Computer Science, 1(2), 140–152. https://doi.org/10.58812/esiscs.v1i02.764

[33]. Hossain, M., Manik, M. M. T. G., Tiwari, A., Ferdousmou, J., Vanu, N., & Debnath, A. (2024a). Data analytics for improving employee retention in the U.S. technology sector. In 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA) (pp. 344–349). IEEE. https://doi.org/10.1109/ICICYTA64807.2024.10913216

[34]. Hossain, M. D., Uddin, M. S., Sikder, M. S., Hossen, T., Uddin, B., & Ahsan, R. M. (2024b). Green and secure data centers: Balancing energy efficiency with advanced cybersecurity measures. Journal of Computer Science and Technology Studies, 6(5), 300–315. https://doi.org/10.32996/jcsts.2024.6.5.24

[35]. Hossain, S., Karim, F., Sultana, S., Uddin, M., Ahmed, M. K., Chy, M. A. R., & Manik, M. M. T. G. (2025). From data to value: Leveraging business analytics for sustainable management practices. Journal of Posthumanism, 5(5), 82–105. https://doi.org/10.63332/joph.v5i5.1309

[36]. Hossin, M. E., Hassan, J., Chy, M. A. R., Hossain, S., Rozario, E., Khair, F. B., & Goffer, M. A. (2024). Harnessing business analytics in management information systems to foster sustainable economic growth through smart manufacturing and Industry 4.0. Educational Administration: Theory and Practice, 30(10), 730–739. https://doi.org/10.53555/kuey.v30i10.9643

[37]. Hossin, M. E., Rahman, M. M., Hossain, S., Siddiqa, K. B., Rozario, E., Khair, F. B., & Mahmud, F. (2025). Digital transformation in the USA: Leveraging AI and business analytics for IT project success in the post-pandemic era. Journal of Posthumanism, 5(4), 958–976. https://doi.org/10.63332/joph.v5i4.1180

[38]. Islam, M. A., et al. (2025). Blockchain for transparent and efficient carbon credit trading. In 2025 International Conference on Advances in Machine Intelligence and Cybersecurity Technologies (AMICT) (pp. 215–220). IEEE. https://doi.org/10.1109/AMICT65811.2025.11402764

[39]. Joy, M. S. A., Alam, G. T., & Bakhsh, M. M. (2024). Transforming QA efficiency: Leveraging predictive analytics to minimize costs in business-critical software testing for the U.S. market. Journal of Artificial Intelligence General Science, 7(1), 77–89. https://doi.org/10.60087/jaigs.v7i01.297

[40]. Kaur, J., Hasan, S. N., Orthi, S. M., Miah, M. A., Goffer, M. A., Barikdar, C. R., & Hassan, J. (2023). Advanced cyber threats and cybersecurity innovation: Strategic approaches and emerging solutions. Journal of Computer Science and Technology Studies, 5(3), 112–121. https://doi.org/10.32996/jcsts.2023.5.3.9

[41]. Kaur, J., Prabha, M., Samiun, M., Hasan, S. N., Hasan, R., & Esa, H. (2025). Comparative analysis of transformer and LSTM architectures for cybersecurity threat detection using machine learning. EAI Endorsed Transactions on AI and Robotics, 4 https://publications.eai.eu/index.php/airo/article/view/9759

[42]. Khair, F. B., et al. (2024). Sustainable economic growth through data analytics: The impact of business analytics on U.S. energy markets and green initiatives. In 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS) (pp. 108–113). IEEE. https://doi.org/10.1109/ICPIDS65698.2024.00026

[43]. Mahin, M. R. H., Chakrborty, P., Das, N., Kaur, H., Himel, H. U., Kaur, J., & Mohapatra, A. G. (2026). Secured and standardized intelligent zero-touch 6G framework for edge-AI applications. IEEE Communications Standards Magazine https://doi.org/10.1109/MCOMSTD.2026.3660159

[44]. Mahmud, F., Orthi, S. M., Saimon, A. S. M., Moniruzzaman, M., Miah, M. A., Ahmed, M. K., Khair, F. B., Islam, M. S., & Manik, M. M. T. G. (2023). Big data and cloud computing in IT project management: A framework for enhancing performance and decision-making. Fuel Cells Bulletin, 2023(9). https://doi.org/10.52710/fcb.166

[45]. Mahmud, F., Goffer, M. A., Chakraborty, P., Sultana, S., Rozario, E., Miah, M. A., Chy, M. A. R., & Haldar, U. (2024). AI-powered workforce analytics: Forecasting labor market trends and skill gaps for U.S. economic competitiveness. Journal of Computer Science and Technology Studies, 6(5), 265–277. https://doi.org/10.32996/jcsts.2024.6.5.21

[46]. Mahmud, F., Barikdar, C. R., Hassan, J., Goffer, M. A., Das, N., Orthi, S. M., & Hasan, R. (2025a). AI-driven cybersecurity in IT project management: Enhancing threat detection and risk mitigation. Journal of Posthumanism, 5(4), 23–44. https://doi.org/10.63332/joph.v5i4.974

[47]. Mahmud, F., et al. (2025b). The role of cloud-based management information systems in enhancing IT project governance and stakeholder collaboration. In J. C. Bansal, P. Jamwal, & S. Hussain (Eds.), Proceedings of the International Conference on AI and Robotics (AIR 2025) (Lecture Notes in Networks and Systems, Vol. 1629). Springer. https://doi.org/10.1007/978-3-032-05548-4_1

[48]. Manik, M. M. T. G., Saimon, A. S. M., Islam, M. S., Moniruzzaman, M., Rozario, E., & Hossin, M. E. (2025). Big data analytics for credit risk assessment. In 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS) (pp. 1379–1390). IEEE. https://doi.org/10.1109/ICMLAS64557.2025.10967667

[49]. Mohonta, S. C., et al. (2026). Efficient homomorphic encryption techniques for confidential big-data analytics over public cloud infrastructures: Algorithms, performance, and trade-offs. In G. N. Nguyen, A. Swaroop, & P. Shukla (Eds.), Proceedings of Fifth International Conference on Computing and Communication Networks. ICCCN 2025 (Lecture Notes in Networks and Systems, Vol. 1859). Springer. https://doi.org/10.1007/978-3-032-21499-7_41

[50]. Nabi, N., Tuhin, M. K., Bashir, M., Lucky, K. Y., Raihan, M., & Imam, H. (2026). Continual learning pipelines for detecting insider threats across corporate cybersecurity infrastructures. In 2025 International Conference on Electrical Engineering and Informatics (ICEEI) (pp. 1–8). IEEE. https://doi.org/10.1109/ICEEI68459.2025.11330487

[51]. Orthi, S. M., Chakraborty, P., Siam, M. A., Shan-A-Alahi, A., Al Zaiem, A., Hasan, S. N., Kaur, J., Mahmud, F., & Goffer, M. A. (2023). AI-driven cyber threat intelligence as a management information system: Integrating cybersecurity governance and IT project management for organizational resilience. The Eastasouth Journal of Information System and Computer Science, 1(2), 194–214. https://doi.org/10.58812/esiscs.v1i02.873

[52]. Orthi, S. M., Siddiqa, K. B., Haldar, U., Siam, M. A., Das, N., Chakraborty, P., Hossain, E., & Mahmud, F. (2025a). AI-augmented risk intelligence in IT project management: An empirical MIS-driven evaluation using machine learning and neural networks. International Journal of Applied Mathematics, 38(12s). https://doi.org/10.12732/ijam.v38i12s.1594

[53]. Orthi, S. M., et al. (2025b). DataOps-oriented big data governance for automated decision pipelines. In 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT) (pp. 1–8). IEEE. https://doi.org/10.1109/ICAFT66710.2025.11452860

[54]. Orthi, S. M., Rahman, M. H., Siddiqa, K. B., Uddin, M., Hossain, S., Al Mamun, A., & Khan, M. N. (2025c). Federated learning with privacy-preserving big data analytics for distributed healthcare systems. Journal of Computer Science and Technology Studies, 7(8), 269–281. https://doi.org/10.32996/jcsts.2025.7.8.31

[55]. Rahaman, M. M., Islam, M. R., Bhuiyan, M. M. R., Aziz, M. M., Manik, M. M. T. G., & Noman, I. R. (2024). Empowering sustainable business practices through AI, data analytics and blockchain: A multi-industry perspective. European Journal of Science, Innovation and Technology, 4(2), 440–451. https://www.ejsit-journal.com/index.php/ejsit/article/view/550

[56]. Rahaman, M. M., Islam, M. R., Manik, M. M. T. G., Aziz, M. M., Noman, I. R., Bhuiyan, M. M. R., Bishnu, K. K., & Bortty, J. C. (2025). A novel data-driven multi-branch LSTM architecture with attention mechanisms for forecasting electric vehicle adoption. World Electric Vehicle Journal, 16(8), 432. https://doi.org/10.3390/wevj16080432

[57]. Rahman, M. H., Ansar, M. T. B., Hossain, S., Saha, U. S., Imam, H., & Ahsan, I. T. (2025a). AI-powered QA in healthcare software: Leveraging predictive analytics and digital twins for safe, cost-effective, and agile medical systems. Journal of Computer Science and Technology Studies, 7(9), 619–628. https://doi.org/10.32996/jcsts.2025.4.1.70

[58]. Rahman, H., Siddiqa, K. B., Sultana, S., Ahsan, I. T., Anwar, M. M., & Hossain, F. (2025b). Next-generation software quality assurance: Integrating AI-driven predictive analytics, digital twins, and agile methodologies for transformative research and practice. Journal of Computer Science and Technology Studies, 7(9), 453–463. https://doi.org/10.32996/jcsts.2025.7.9.52

[59]. Raihan, M., Adnan, M., Hossain, M. J., Siddiqa, K. B., Karim, F., & Mohonta, S. C. (2026). Adversarial robustness mechanism for safeguarding biometric verification across mobile financial applications. In 2025 International Conference on Electrical Engineering and Informatics (ICEEI) (pp. 1–7). IEEE. https://doi.org/10.1109/ICEEI68459.2025.11330502

[60]. Rozario, E., Nazmussakib, M., Alam, G. T., Roy, T., Adnan, M., & Faruk, M. I. (2026). Dynamic big data summarisation using transformer-based generative models. In 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON) (pp. 1–8). IEEE. https://doi.org/10.1109/I3CTCON68242.2026.11507387

[61]. Shan-A-Alahi, A., Mustafizur, M., Hossan, K. M. R., Al Zaiem, A., & Rahman, M. M. (2024). Cybersecurity training and its influence on employee behavior in business environments. Computer Fraud & Security, 2024(12). https://doi.org/10.52710/cfs.689

[62]. Shan-A-Alahi, A., et al. (2026a). Deep learning-based threat prediction and autonomous response mechanisms for containerized microservices in hybrid cloud deployments. In G. N. Nguyen, A. Swaroop, & P. Shukla (Eds.), Proceedings of Fifth International Conference on Computing and Communication Networks. ICCCN 2025 (Lecture Notes in Networks and Systems, Vol. 1859). Springer. https://doi.org/10.1007/978-3-032-21499-7_42

[63]. Shan-A-Alahi, A., Sikder, M. S., Himel, H. U., Ansar, M. T. B., Tuhin, M. K., & Kaur, H. (2026b). Resilient cybersecurity architectures for large-scale distributed systems. In 2026 IEEE International Conference for Convergence in Computing Technology (I3CTCON) (pp. 1–8). IEEE. https://doi.org/10.1109/I3CTCON68242.2026.11507768

[64]. Siam, M. A., Shan-A-Alahi, A., Tuhin, M. K., Hossain, E., Bashir, M., Lucky, K. Y., & Al Zaiem, A. (2025a). AI-driven cyber threat intelligence systems: A national framework for proactive defense against evolving digital warfare. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3793

[65]. Siam, M. A., Lucky, K. Y., Hasan, S. N., Kaur, J., Kaur, H., Uddin, M. S., & Manik, M. M. T. G. (2025b). Cybersecure intelligent sensor framework for smart buildings: AI-based intrusion detection and resilience against IoT attacks. Sensors, 25(24), 7680. https://doi.org/10.3390/s25247680

[66]. Siddiqa, K. B., Rahman, H., Barikdar, C. R., Orthi, S. M., Miah, M. A., & Rahman, R. (2024). AI-driven project management systems: Enhancing IT project efficiency through MIS integration. In 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS) (pp. 114–119). IEEE. https://doi.org/10.1109/ICPIDS65698.2024.00027

[67]. Siddiqa, K. B., Rahman, H., Imam, H., Ansar, M. T. B., Al Zaiem, A., Shan-A-Alahi, A., & Manik, M. M. T. G. (2025). Assessment of survivability and importance analysis for networks managing intricate traffic flows. IEEE Communications Standards Magazine https://doi.org/10.1109/MCOMSTD.2025.3638981

[68]. Sizan, A., et al. (2025). Leveraging machine learning for predictive sustainability analytics: Optimizing resource management in manufacturing. In 2025 International Conference on Advances in Machine Intelligence and Cybersecurity Technologies (AMICT) (pp. 245–250). IEEE. https://doi.org/10.1109/AMICT65811.2025.11402830

[69]. Sultana, S., Karim, F., Rahman, H., Chy, M. A. R., Uddin, M., Khan, M. N., Hossin, M. E., & Rozario, E. (2024). A comparative review of machine learning algorithms in supermarket sales forecasting with big data. Journal of Ecohumanism, 3(8), 14457. https://doi.org/10.62754/joe.v3i8.6762

[70]. Sultana, S., Uddin, M., Chy, M. A. R., Hasan, S. N., Hossain, E., Kaur, H., & Kaur, J. (2025). AI-augmented big data analytics for real-time cyber attack detection and proactive threat mitigation. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3564

[71]. Uddin, M. S., Sikder, M. S., Anwar, M. M., & Hossain, F. (2025). AI-driven cybersecurity and big data-enabled MIS frameworks: Strengthening supply chain integrity, energy resilience, and critical infrastructure protection. Journal of Computer Science and Technology Studies, 7(9), 223–232. https://doi.org/10.32996/jcsts.2025.7.9.26

[72]. Uddin, S. M. M., Nazmussakib, M., Mustafizur, M., Bakhsh, M. M., Islam, M. A., Saha, U. S., & Ahmed, M. K. (2026). AI-powered business intelligence: Enhancing decision-making through predictive analytics and big data. Journal of Posthumanism, 6(3), 218–237. https://doi.org/10.63332/joph.v6i3.4083

[73]. Varanasi, S. R., Valiveti, S. S. S., Adnan, M., Faruk, M. I., Hossain, M. J., & Manik, M. M. T. G. (2026). Cross-domain standardization and secure edge intelligence for real-time digital twin deployments in next-generation communication systems. IEEE Communications Standards Magazine. https://doi.org/10.1109/MCOMSTD.2026.3662187

[74]. Zerine, I., Islam, M. M., Khan, M. A. U., Chy, M. A. R., Saimon, A. S. M., Manik, M. M. T. G., & Wata, C. (2026). Explainable churn prediction in telecom with tabular ML: Five model benchmark and SHAP analysis. Discover Artificial Intelligence. https://doi.org/10.1007/s44163-026-00983-0