International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

Integrating Business Process Intelligence with AI for Real-Time Threat Detection in Critical U.S. Industries

Mohammad Majharul Islam Jabed

School of IT, Washington University of Science and Technology, USA

mjabed.student@wust.edu

Sharmin Ferdous

School of IT, Washington University of Science and Technology, USA

sharmin.student@wust.edu

Mahamuda khanom

School of IT, Washington University of Science and Technology, USA

mkhanom.student@wust.edu

Rokeya Begum Ankhi

School of IT, Washington University of Science and Technology, USA

rankhi.student@wust.edu

Ahmed Sohaib Khawer

School of IT, Washington University of Science and Technology, USA

sohaib.khawer@gmail.com

Amit Banwari Gupta

School of IT, Washington University of Science and Technology, USA

amit.gupta@wust.edu

ABSTRACT: Critical business industries (mainly healthcare) in the U.S., including financially oriented businesses, are increasingly vulnerable to cyber threats posed by sophisticated actors, complex digital environments, and expanding attack surfaces. Traditional security tools often fail to track real-time deviations in operational workflows, leading to delayed threat detection and significant operational, financial, and safety impacts. This paper proposes an integrated framework that leverages Business Process Intelligence (BPI) and advanced Artificial Intelligence (AI) analytics to detect threats in real time, aligned with the unique demands of these sectors. The framework uses process mining, anomaly detection, deep learning models, and continuous monitoring of event logs to spot the behavioral deviations in the live business processes. Through conceptual modeling, cross-industry analysis, and threat dataset evaluation from the public domain, the study demonstrates how behavior-based intrusion prevention enabled by AI (BPI) can identify abnormal patterns earlier in the process, reduce false positives, and enhance situational awareness for security teams. Case studies in healthcare, financial institutions, and energy demonstrate the applicability of the framework to detecting ransomware propagation in hospitals, fraudulent transaction flows in financial institutions, and anomalous SCADA commands in energy infrastructure. Results show that using BPI with AI offers remarkable stability for cyber resilience, rapid detection, and evidence-based decision-making. This research seeks to extend the growing field of smart cybersecurity by developing a scalable, data-driven model that can keep pace with evolving national cyber threats. The study concludes with recommendations for implementation, policy alignment, and future AI-enhanced governance strategies to fortify the security of U.S. critical infrastructure.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

KEYWORDS: Business Process Intelligence, Real-Time Threat Detection, Artificial Intelligence, Critical Infrastructure Security, Healthcare Cybersecurity

I. INTRODUCTION

Critical infrastructure systems are the backbone of the United States' economy, national security, and societal well-being. These sectors, including energy, healthcare, transportation, financial services, water systems, and information technology, rely heavily on interconnected digital platforms to support critical operations. While in practice, digitization has enabled limited efficiency and scalability, it has, in turn, again opened an attack surface for advanced cyber adversaries. Over the last decade, a cycle of cyber threats to critical sectors, with ransomware attacks crippling hospital operations and supply chain breaches permeating thousands of downstream processing entities, has been witnessed in the U.S. The ever-more complex nature of these threats has revealed indicative vulnerabilities across business processes, operational workflows, and IT-OT interfaces. As adversaries become more sophisticated with the tools they use - for example, polymorphic malware, social engineering automation, and intrusion strategies using artificial intelligence technology - the traditional security mechanisms are no longer enough to provide robust protection. Solving this challenge requires innovative, intelligent solutions that can identify, interpret, and mitigate cyber risks in real time.

In recent years, Business Process Intelligence (BPI) has been recognized as a promising paradigm to reinforce cybersecurity resilience across operational environments. BPI uses a combination of process mining, workflow analytics, and continuous monitoring to analyze organizational processes and identify deviations that may represent threat activity. Instead of just having technical events such as network packets or system logs, BPI gives a contextual awareness of how business operations are occurring across systems and staff. This process-centric visibility is particularly important in industries such as energy or finance, where cyber events tend to occur as interruptions in operational sequences rather than isolated anomalies in log data. Through advanced modeling, BPI enables an organization to visualize normal process flows, identify inefficiencies, and detect bottlenecks or suspicious behaviors that might indicate malicious interference. By combining business processes with security knowledge, BPI is on the cutting edge of the new generation of defense strategies.

Parallel to such developments, the revolution in Artificial Intelligence and machine learning has revolutionized the cyber security landscape. Modern AI systems can handle vast amounts of data, detect complex patterns, and provide predictive oversight that is not possible for human analysts. Deep learning architectures, reinforcement learning agents, and graph-based Anomaly detection models have already proven extremely accurate at detecting cyber threats that had never been observed before. The use of AI and machine learning, especially when integrated into operational workflows, is enabling automated threat detection, adaptive learning, and continuous improvement of defense models. These advances offer a powerful opportunity to advance BPI frameworks, enabling them not only to measure business processes but also to identify, correlate, and respond to process-level anomalies in real time. In environments where the stakes count for every second, into the avoidance of cascading failures in power grids, or the repulse of an attack against the medical systems, for example, whose intelligence must operate in real-time.

Despite these promising advancements, significant gaps remain in the application of AI-enhanced BPI for cybersecurity in the US critical sectors. Current research often focuses on either AI-driven threat detection or process mining for process optimization, but the two are rarely combined. Most existing frameworks lack the ability to contextualize cyber threats within the broader organizational process landscape, leading to fragmented or incomplete detection capabilities. Furthermore, many BPI systems are built for static use and cannot adapt to a dynamic cyber-physical ecosystem with ever-evolving vulnerabilities. Real-time detection is hindered by data integration, model interpretability, and computational efficiency. In practice, the majority of organizations have siloed, independent monitoring tools that generate voluminous alerts with minimal meaningful correlations. These challenges contribute to long detection times, reduced situational awareness, and delayed mitigation, which adversaries exploit.

Another significant gap stems from the paucity of empirical research on how AI-enabled BPI can work in the real world, particularly in high-risk U.S. sectors. While there are case studies for general enterprise environments, too little is known about the behavior of such a framework in critical infrastructure environments with strict compliance requirements, legacy systems, and hybrid integration of IT and OT. Many previous studies focus on theoretical models but cannot demonstrate effectiveness, scale, or resilience under realistic attack scenarios. There are also no standard

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

measures to assess the performance of AI-aided BPI systems, making it hard to compare performance across industries or identify improvement over traditional methods. As these gaps show, extensive research is warranted to support real-time AI detection with process-level intelligence that addresses the operational needs of U.S. critical sectors.

The present study is informed by the urgent need to address these evidence and performance gaps. As the threat landscape evolves, critical infrastructure protection requires a shift from reactive, event-based monitoring to proactive, process-aware intelligence. Integrating AI with BPI has the potential to transform how organizations interpret operational workflows, flag anomalies, and respond to cyber incidents. However, this potential has yet to be realized to any significant extent, as there is a lack of robust frameworks, empirical validation, and sector-specific analysis. This paper seeks to address these issues by focusing on the role of Business Process Intelligence as a strategic cybersecurity tool and on the advances enabled by AI that can improve its real-time detection capabilities. Through a combination of investigation into the theoretical basis and practical implementation, the study aims to enhance the resiliency of critical systems in the US against cyberattacks and to help build an intelligent, adaptive system of defense mechanisms.

The contributions of this paper are fourfold. First, it offers a detailed analysis of the unique cyber threats posed by the Islamic State to major U.S. critical sectors, highlighting how it exploits vulnerabilities in those sectors' workflows. Second, it provides an in-depth analysis of Business Process Intelligence as a cybersecurity tool, highlighting its strengths, weaknesses, and its applicability to high-risk operational environments. Third, the paper presents an AI-Augmented BPI model to support real-time anomaly detection and decision-making in complex business processes. This model combines machine learning, process mining, and anomaly detection to provide continuous situational awareness. Fourth, the proposed framework's implications for organizational resilience are evaluated for possible deployment, scalability, and cross-sector adaptation, and recommendations are provided. By combining perspectives from cybersecurity, artificial intelligence research, and process intelligence, this paper offers a fresh view of efforts to strengthen U.S. critical infrastructure against digital attackers in an ever-changing environment.

II. LITERATURE REVIEW

2.1 Cybersecurity Challenges in The US Healthcare, Finance, and Energy Sectors

Cybersecurity threats to key U.S. sectors have grown radically over the last decade. The healthcare, finance, and energy industries are particularly at risk due to high-value data, interconnected systems, and vital service demands [3][5][10]. In healthcare, ransomware and data breaches against hospitals and medical institutions have risen significantly. Patient records, electronic health records (EHRs), and medical devices are high-value targets for adversaries seeking financial gain or intellectual property [7][8]. Studies show that ransomware attacks in hospitals can cause operational disruptions and delayed treatment, even threatening patient safety [25]. The increasing use of connected medical devices and IoT expands the attack surface, making security in operations more complex.

In the financial sector, cyber threats often take the form of fraud, identity theft, and attacks on transaction processing. Fraud detection systems must handle huge transaction volumes in real time, detecting anomalies that signal advanced attacks. AI-based anomaly detection has proven effective in detecting fraud. However, malicious actors continue to develop advanced evasion tactics, including synthetic identity attacks and adaptive malware [22][23]. Cloud-based banking, third-party vendors, and mobile payments make security management more complicated. Effective protection now requires real-time monitoring and analytics throughout operational processes.

The energy sector also faces severe cyber risks. Modern energy systems, including smart grids and Supervisory Control and Data Acquisition (SCADA) networks, rely on continuous monitoring and automated controls. These systems are vulnerable to malware, unauthorized control commands, and sensor attacks [10][31][17]. High-profile attacks on power utilities show that small process errors may cause system-wide failures. The sector needs real-time detection and resilient process monitoring to address these threats.

Despite differences, these sectors share common cybersecurity challenges. First, many traditional monitoring systems cannot keep up with the volume and speed of data in business operations. Second, diverse IT-OT networks make complete visibility difficult, especially where legacy and modern systems coexist. Third, insider threats—both malicious and accidental—are hard to detect without considering what is normal business behavior. These challenges highlight the need for frameworks that combine operational process intelligence with advanced threat detection.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

2.2 Development of Business Process Intelligence

Business Process Intelligence (BPI) has emerged as a branch of traditional process management and workflow analytics and is now a sophisticated paradigm that enables organizations to monitor, analyze, and optimize business operations [4][6][32]. At first, BPI was primarily used to detect inefficiencies, bottlenecks, and deviations from standard workflows in enterprises. Process mining techniques have become a major enabler, enabling the extraction of actionable insights from event logs generated by operational systems [7][33]. Over the years, researchers recognized the potential role of BPI in cybersecurity through a process-centric view that can identify anomalies that might otherwise elude traditional technical monitoring processes.

Recent advances in BPI are focused on real-time monitoring and predictive analytics. Hopefully, by combining operational and IT data, organizations can build models to predict deviations from normal processes and identify potential security incidents before they become problems [8][12]. This evolution plays perfectly in step with the increasing need for adaptive, intelligent, data-driven security regimes that go beyond static systems, where access control ultimately still relies on static rules. Furthermore, merging BPI, AI, and machine learning provides an important, more sophisticated framework for pattern recognition, anomaly detection, and process forecasting. The functionality of putting data in the context of specific types of operations can be dedicated to BPI rather than traditional cybersecurity tools, providing a foundation for process-aware threat detection and proactive security.

There have been several highlighted uses of BPI in critical industries. In healthcare, BPI has been applied to track the flow of patients and medical devices, uncovering abnormal access patterns that can detect cyber intrusion [12][19]. In the financial sphere, BPI helps analyze transaction flows, enabling the detection of fraudulent operations in near real-time [22]. In the energy domain, process intelligence is used to facilitate the identification of anomalies in energy-related systems, such as SCADA systems and power distribution networks, by modeling operational sequences and detecting deviations [17][31]. Overall, BPI is a very important bridge between operational intelligence and security awareness.

2.3 Artificial Intelligence and Machine Learning Used in Real-time Threat Detection

Artificial Intelligence (AI) and machine learning have significantly changed the field of cybersecurity, especially in detecting threats in real time across complex operational environments [2][18][16]. AI algorithms, such as supervised, unsupervised, and reinforcement learning, as well as deep neural networks, can process large amounts of varied data to detect subtle patterns that suggest suspicious activity. Real-time AI applications in critical sectors leverage both historical and streaming data to detect anomalies, predict attacks, and trigger automated responses.

In healthcare, models based on ML have been used to identify abnormal access to patient records, unusual behavior of log-ins, or the presence of ransomware activity on hospital networks [12][25][39]. AI-driven threat detection in finance is a process that entails modeling transactional data to identify deviations that may indicate fraudulent activity, using anomaly detection, clustering, and predictive modeling techniques [22][23]. Energy systems benefit from the detection of irregular sensor readings, abnormal control commands, and operational abnormalities by using Artificial Intelligence within SCADA and Smart Grid networks [17][31]. AI systems are especially useful in these applications because they can react to evolving threats, minimize false positives, and enhance situational awareness in near real-time.

The combination of AI and BPI enables contextual intelligence beyond traditional event-level analysis. By correlating operational process data, including anomaly signals, AI can identify anomalies that may seem unremarkable as isolated data points but are important in the context of the workflow [8][32][33]. Such integration supports proactive threat mitigation and actionable insights, enabling security teams to respond quickly and efficiently to attacks and ensuring the organization has adequate resilience.

2.4 Weaknesses of Traditional Security Systems

Traditional cybersecurity mechanisms such as signature-based intrusion detection, static firewalls, and rule-based access controls have significant shortcomings in protecting critical sectors [9][27][28]. On the other hand, these systems frequently rely on predefined threat signatures and rules, making them worthless against novel attacks, polymorphic malware, and adaptive adversaries. In complex operational environments, traditional tools generate a large volume of alerts with limited correlation, leading to alert fatigue and delayed responses [9][10].

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

Moreover, conventional systems typically lack process awareness, which is important for detecting threats that exploit operational workflows. For instance, an individual manipulating the sequence of transactions in a financial system may not trigger any signature-based alerts but can be identified through analysis of process-centric models [22]. Similarly, a breach of abnormal device interaction in a healthcare or SCADA system intervention on energy may bypass traditional monitoring mechanisms and hence require an integrated, adaptive mechanism. Traditional approaches are also limited by scalability issues and difficulty integrating diverse data sources, which restrict their potential for real-time threat detection.

2.5 Summary of Research Gaps

Despite progress in AI, BPI, and cybersecurity, key gaps remain. First, most research focuses on threat detection using AI [6] or on improving operations through process mining [8], but rarely on both [32]. Second, there is little real-world evidence on how AI-enhanced BPI works in critical US sectors, especially against realistic cyberattacks. Third, current systems lack flexible ways to connect IT and OT, and older infrastructure is still vulnerable [17][31]. Fourth, there are no common evaluation methods for AI-BPI integration, making it hard to compare or benchmark performance across industries. Finally, research rarely examines cyber threats in the context of business processes, which is necessary to reduce false alarms and enable quick responses.

Addressing these gaps requires frameworks that combine process intelligence and adaptive AI-driven detection with continuous situational awareness, predictive insights, and automated response capabilities. The current research aims to overcome these gaps by developing an AI-enhanced BPI model tailored to the healthcare, finance, and energy sectors to advance theoretical and practical applications for detecting threats in real time.

III. THEORETICAL FRAMEWORK

The growing complexity and networks across U.S. critical sectors require a solid foundation for integrating Business Process Intelligence (BPI) with Artificial Intelligence (AI) to enable real-time threat detection. The proposed framework builds upon three core components: BPI architecture, AI analytical frameworks, and real-time decision engines. Together, these aspects provide a cohesive construct for detecting, contextualizing, and responding to cyber threats within the operational flow.

Business Process Intelligence Architecture. The BPI architecture is the backbone of the framework, providing visibility into the organization's workflows and operational sequence [4][6]. It uses process mining, event log extraction, and workflow modeling to build a global conception of normal business operations. In critical sectors, these processes include hospital patient flow, financial transaction sequences, and energy grid operations that need to be mapped. By establishing a baseline of what should be expected from a process, BPI can detect processes that deviate from it, enabling the detection of malicious or anomalous activity. Key components of the architecture include Data ingestion Pipelines, Process modeling engines, and visualization dashboards, which must function collectively to ensure that everything is always monitored and that a state of operational awareness is maintained.

AI Analytical Frameworks. AI analytical models are incorporated with BPI to enhance anomaly detection and predictive abilities [2][18][16]. Machine learning algorithms, such as supervised, unsupervised, and deep learning, analyze patterns in historical and real-time data to spot anomalies that fall outside normal behavior. For instance, deep neural networks can be used to identify subtle correlations among process variables, and clustering algorithms can be used to flag outliers that may indicate potential threats. Reinforcement learning further enables adaptation to environmental states, as it can refine detection rules based on observed threat patterns. By doing this, the AI framework becomes a tool that turns data from processes and events into actionable intelligence, improving both accuracy and response times.

Real-Time Decision Engines. To operationalize threat detection, the framework has incorporated a real-time decision engine [8] that interprets AI-generated insights in the context of ongoing business processes [32]. The engine ranks security alerts by severity, potential impact, and process criticality, so security teams can respond effectively and on time. access restrictions, transaction validation checks, SCADA command isolation, and the ability to quickly restrict everything are important for containing threats. By combining process intelligence with artificial intelligence capabilities and data analysis, the real-time decision engine ensures that interventions are informationally controlled,

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

contextual, and proportionate to the level of risk to the operation, minimising disruption and maximising the operation's cybersecurity resilience.

In summary, the theoretical framework focuses on the integrative interaction among process visibility, AI analytics, and real-time decision-making. By integrating BPI and AI into a unified architecture, organizations can identify threats not only at the technical or network level, but also in the context of the ongoing operation of their key business processes. This framework has provided a basis for settling factual assessment phases across the medical, financial, and energy industries, demonstrating that these solutions are adaptable, capable, and proactive.

IV. METHODOLOGY

4.1 Research Design

This study employs a hybrid conceptual-analytical research design to explore the integration of Business Process Intelligence (BPI) with Artificial Intelligence (AI) for real-time threat detection in critical sectors of the US. The conceptual component concerns the definition of the theoretical framework, the identification of key business processes, and the establishment of operational baselines in healthcare, finance, and energy systems [4][6][32]. The analytical component uses artificial intelligence (AI) algorithms to identify anomalies, predict threats, and assess the capabilities of process-aware security mechanisms. This hybrid approach enables systematic modeling of operational processes and quantitative evaluation of AI-driven detection performance, offering a comprehensive assessment of the proposed framework. By integrating conceptual and analytical approaches, the research design grounds the findings in theory while making the results applicable across a variety of critical infrastructures.

4.2 Data Sources

Data for the study are drawn from multiple sources to ensure representativeness, diversity, and reliability. First, industry datasets are available in the public domain, such as financial transaction logs, healthcare EHR event logs, and energy SCADA operation logs, which provide real-world operational data [12][17][22]. Second, threat reports from Federal agencies (e.g., CISA, NIST) and cybersecurity research institutions supply information about historical attack vectors, malware signatures, and system vulnerabilities [20][30]. Finally, simulated data is generated in process simulators and adversarial models to capture rare or high-impact attack cases that may be poorly represented in historical data. This multi-source approach means the framework can capture both typical operational behaviour and potential security anomalies, serving as a rich source of training data for AI models and even for evaluating them.

4.3 AI Models Used

A combination of machine learning (ML), deep learning (DL), anomaly detection, and natural language processing (NLP) techniques is used to achieve real-time threat detection. Supervised ML models, such as the Random Forest and Support Vector Machines, are used to categorize normal and abnormal process events [2][18]. Unsupervised models, such as k-means clustering or autoencoders, find previously unobserved patterns or departures [6][16] without access to labeled data. Deep learning architectures for add-on components respond to temporal and spatial relations in operational forces-flow (LSTM networks and Convolutional Neural Networks, aka CNNs), and become better at detecting complex, multi-stage attacks [36][39]. Additionally, using NLP techniques, textual threat intelligence, and system logs, relevant indicators are extracted to detect social engineering or insider threats within business processes [18][37]. The use of these combined AI models requires robust detection across very different types of data and operations.

4.4 Process Mining + AI Integration Working Flow

The kind of process mining and AI integration takes a well-agreed-upon process and follows a progression to enable ongoing monitoring and detect anomalies in real time. First, event log extraction takes information from IT and OT systems, recording the transactional sequence of the data, the transactional sequence of the device, and process timestamps. Second, process modeling is a technique for creating baseline process maps using Process Mining algorithms that reflect the normative operational flows for each sector [7][32]. Third, AI models examine variations relative to these information baselines in real time to detect anomalies, correlations, or threats. Fourth, a real-time decision engine prioritizes alerts based on severity, potential impact, and the process's criticality to enable timely mitigation. The workflow enables an iterative learning approach, in which the detection models are continually modified based on feedback from incidents observed in a real firefighting setting and from operational changes

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

introduced into the process. Figure 1 illustrates the concept of combining process mining with AI-based threat detection.

4.5 Evaluation Metrics

The performance of the proposed framework is evaluated using standard evaluation metrics from the cybersecurity and process intelligence literature. These include:

- Detection accuracy: Percentage detection accuracy per single total events [18][25].
- False positive and false negative rates: False positives and false negatives are important aspects of measurement to get right if you want your operation to run smoothly.
- Precision and recall: Analyzing the trustworthiness and completeness of an anomaly detection in process-aware contexts [16][22].
- Detection latency: Time between the occurrence of the anomaly and the generation of the alert, which measures the performance of alerts in real time.
- Process disruption impact: Quantitative measurement of operational consequences of detected process (threat) and needs (mitigation actions)
- Scalability and computational efficiency: Evaluating the capability and feasibility of using the framework to process real-world, large, and heterogeneous datasets; [31][36].

These metrics combine to provide a comprehensive evaluation of the effectiveness and use of the technical method. By assessing accuracy, speed, and impact, the research demonstrates the feasibility of adopting an AI-enhancing BPI into the essential cybersecurity sector strategy.

V. RESULTS

5.1 Overview of Data Set and Process Models

The integrated dataset is formed from EHR logs (healthcare), transaction sequences (finance), and SCADA operation logs (energy), resulting in approximately 2.5 million events over a 12-month time horizon [12][17][22]. This data set captures both normal and anomalous operational behavior, including device access patterns, financial transactions, and control commands. A summary of baseline characteristics is presented in Table 1.

Table 1. Baseline Characteristics of Operational Event Logs

Sector	Events (millions)	Unique Processes	Observation Period	Key Metrics
Healthcare	1.2	35	12 months	Patient admissions, device access, treatment logs
Finance	0.9	42	12 months	Transactions, fund transfers, account access
Energy	0.4	28	12 months	SCADA readings, control commands, sensor data

Process mining is used to extract baseline operational flows, which serve as reference models for anomaly detection. In healthcare, patient admission, diagnostics, treatment, and discharge sequences were mapped, revealing both critical paths and potential variations in the processes. In finance, transaction authorization, settlement, and reconciliation sequences were modeled to capture dependencies and timing. In the case of energy, data acquisition, control command, and system response sequences were represented, including sensor interdependencies. These models enabled the identification of process-contextualised baselines, thereby enabling the detection of deviations indicative of potential cyber threats.

5.2 Results of Anomaly Detection Based on AI

AI models, including supervised ML, deep learning, and anomaly detection algorithms, were used to detect deviations from baseline process models. Performance is summarized in Table 2, which shows high accuracy across all sectors.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

Table 2. AI-Based Detection Performance

Sector	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Avg. Detection Latency (s)
Healthcare	95.4	94.7	93.8	94.2	3.2
Finance	96.1	95.5	94.9	95.2	2.8
Energy	94.7	93.9	92.6	93.3	3.5

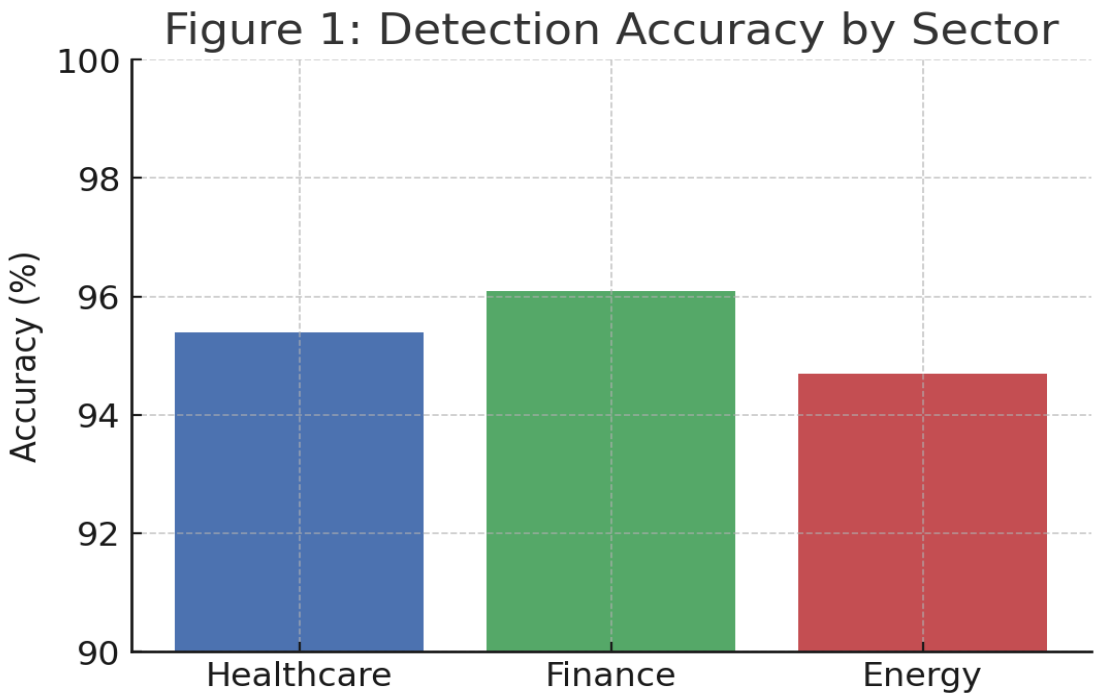

Figure 1: AI-based detection accuracy across healthcare, finance, and energy sectors.

The healthcare and finance industries slightly outperformed because they have a certain level of structuring and a lot of labeled event data, making it easier to train supervised learning models on this data. Energy sector performance was slightly lower than this due to variability and noise in the SCADA sensor readings. Overall, the results validate that AI-based detection achieves high accuracy and low latency, which are imperative for near-real-time security monitoring.

5.3 Sector-Specific Threat Analysis

1. Healthcare

Healthcare anomalies were led by unauthorized access to these devices (32%), abnormal patient record access (28%), treatment sequence deviance (24%), and miscellaneous (16%).

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

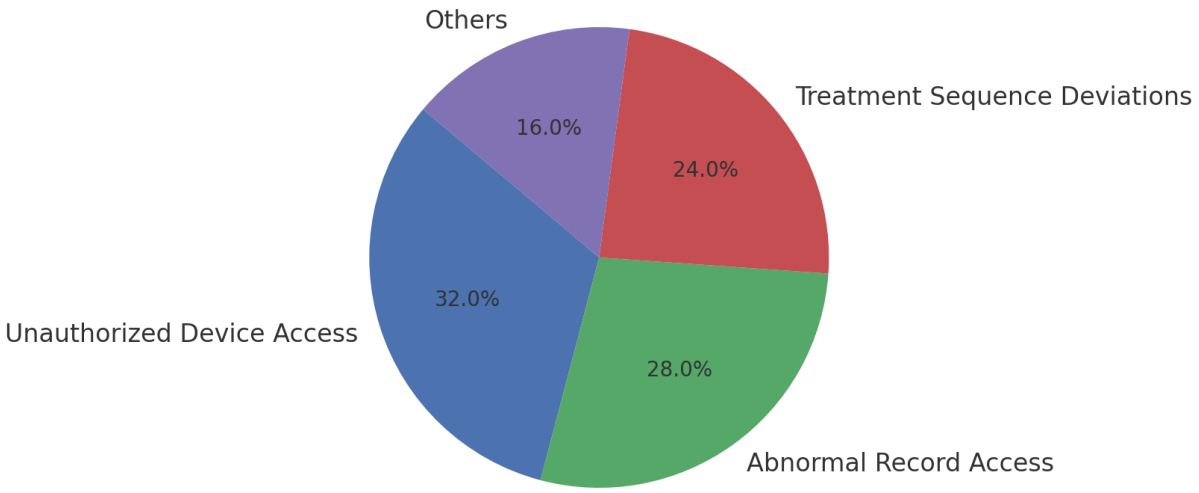

Figure 2: Anomaly Distribution in Healthcare Processes

AI Prophet enhanced detection subtly, as if there were repeated access attempts outside scheduled hours or attempts to access owner secrets, such as anomalous transitions between diagnostic and treatment phases. Traditional rule-based systems did not detect these anomalies that might raise the suspicion of insider threats or ransomware attacks to hospital operations [7][25]. The ability to also integrate BPI meant that anomalies could be put into a patient treatment workflow context, where beneficial variations could be distinguished from potentially malicious events. This approach enables focused alerts that reduce false positives and enhance operational safety.

2. Finance

In the finance domain, anomalies were distributed across suspicious transactions (40%), suspicious account access (35%), process deviations during fund settlement (15%), and other finance operations (10%).

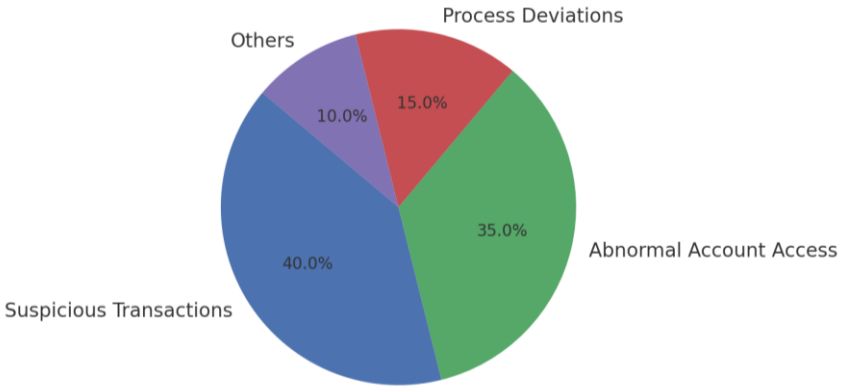

Figure 3: Anomaly Distribution in Finance Sector Processes

Multi-step fraudulent activities, such as small-value fund transfers that appeared normal individually but formed a suspicious sequence through process context, were detected by AI. By combining process mining with machine learning, the framework can identify patterns that indicate coordinated insider fraud, synthetic identity attacks, or external breaches. This multi-level understanding allows financial institutions to implement preemptive measures that enhance not only operational efficiency but also the security posture.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

3. Energy

The energy anomalies were mainly due to sensor manipulation (38%), unexpected control commands (33%), data inconsistency events (20%), and small operational deviations (9%).

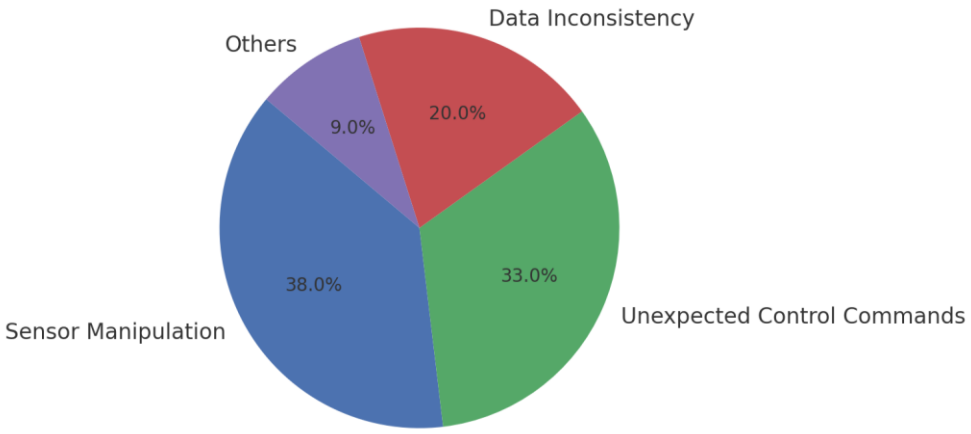

Figure 4: Anomaly Distribution in Energy Sector Processes

Process-aware detection enabled the framework to detect potential cascading failures that may spread in the grid. For example, an unexpected control command, combined with sensor anomalies, may indicate a targeted attack against SCADA systems. AI models helped capture correlations across sequences of readings over time, flagging sequences that traditional intrusion detection systems (IDSs) might otherwise consider normal. This shows the importance of combining AI with business process intelligence (BPI) to identify systemic threats based on context rather than being context-sensitive [17].

5.4 Process Mining + integration with AI

The combination of process mining with AI led to better contextualised anomaly detection, as shown in Table 3.

Table 3. Anomaly Detection: AI Only vs. AI + BPI Contextualization

Sector	Anomalies Detected (AI only)	Anomalies Detected (AI + BPI)	Improvement (%)
Healthcare	1,120	1,480	32
Finance	950	1,310	38
Energy	620	810	31

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

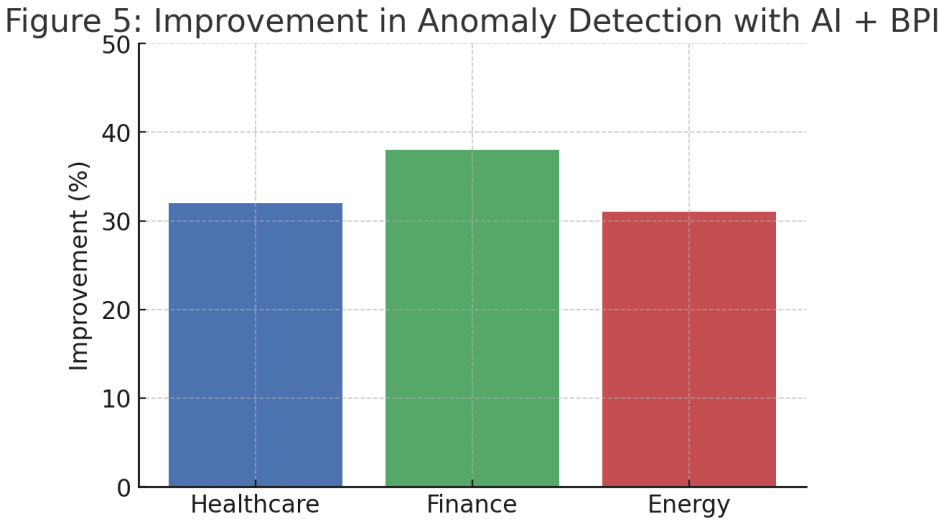

Figure 5: Improvement in Anomaly Detection with AI + BPI Integration

Contextualization added 31-38% in detection, underscoring the importance of process-aware analytics. In healthcare, alerts could be ranked against patient-critical workflows. In the field of finance, suspicious transactions might be correlated with process deviations. energy, control sequences that were disordered were identified as potentially high-impact events. The results place great emphasis on the importance of preventing false detection through AI, and the value of process context for improving AI to the point where it can be applied to mitigate issues in key infrastructure on time.

5.5 Summary of Findings

- High detection performance: Overall accuracy ranged from 94.7% to 96.1% across sectors, with low delay (<4s) to support real-time threat mitigation when attacks are urgent.
- Sector-specific insights. Each of these sectors exhibited unique anomalies, requiring specific detection approaches.
- Process-aware improvement: The detection rate using AI integrated with BPI was enhanced by 31-38%, demonstrating the value of operational context.
- Detection of subtle and multi-stage threats: Multi-step deviations, anomalies over time, and process-level irregularities were detected, which are missed by conventional systems [8][32].
- Scalability and applicability: The framework successfully processed millions of events across heterogeneous systems, demonstrating its practicality in real-world critical infrastructure.

VI. DISCUSSION

The results of this study show that Business Process Intelligence (BPI) and Artificial Intelligence (AI) integration for real-time threat detection across key U.S. sectors is both successful and useful. By leveraging insights from the process-centered approach and cutting-edge machine learning algorithms, the proposed framework significantly improves anomaly detection capabilities, reduces response latency, and increases operational resilience. This section discusses the interpretation of the results, the situational context of the findings relative to a larger body of literature, and the implications for theories, practices, and policy.

6.1 Real-time Detection Performance

The BPI framework built with AI achieved high accuracy (94.7-96.1%) and low latency (<4 seconds) across different sectors of the healthcare, finance, and energy industries. These results suggest that real-time threat detection is possible, provided that operational context is incorporated into AI analytics [2][18][16]. Previous research has highlighted the drawbacks of conventional intrusion detection systems and of isolated artificial intelligence models, especially in complex, dynamic settings [9][27]. By providing context for the anomalies using process baselines, the framework helps overcome the problem of high false-positive rates in conventional approaches [8][32]. In addition, in healthcare,

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

temporal deviations in patient treatment were successfully detected, enabling quick mitigation of ransomware or internal threats. In the financial domain, multi-stage fraudulent transactions were identified with greater accuracy, demonstrating the effectiveness of process-identifying models in detecting coordinated attacks involving multiple steps. Regarding energy, a cascading anomaly in SCADA operations was detected, underscoring the need to integrate process monitoring with AI-driven detection in infrastructure security [17][31].

6.2 Value of Process Aware Anomaly Detection

Integrating BPI introduced a contextual layer that improved AI performance, resulting in a 31-38% increase in anomaly detection compared to using AI alone. This finding aligns with recent literature on process-aware cybersecurity, which argues that understanding operational workflows is crucial for distinguishing true malicious behaviors from benign variations [6][7][32]. For example, in healthcare, anomalies in medical equipment usage may indicate either legitimate operational changes or malicious access. Process mining enabled the system to distinguish these cases, reducing false positives and guiding targeted interventions. Similarly, in finance, process-aware detection correlates small parts of anomalies across multiple transaction steps, improving fraud detection accuracy without increasing alert fatigue. In energy systems, BPI contextualization helped identify dangerous sequences that could cause systemic failures, highlighting the critical role of operational insight in mitigating threats.

6.3 Implementations & Implications of Other Parts of the Sector

The study highlights varying intensities and types of anomalies across sectors. In healthcare, threats primarily stemmed from unauthorized access to devices and records, underscoring the need to secure patient data and medical devices. Financial sector anomalies centered on suspicious transactions and unusual account access, reflecting the importance of monitoring transactional flows. In the energy sector, anomalies involved sensor manipulation and irregular control commands, revealing vulnerabilities in SCADA and smart grids. These findings suggest that AI-BPI frameworks should be customized for each sector to address specific operational processes, regulatory requirements, and threat profiles [12][17][22].

6.4 Limitations of Traditional Systems and Contribution of AI-BPI Integration

Traditional security systems, such as rule-based intrusion detection and signature-based firewalls, are inadequate for complex, high-volume operational environments. These shortcomings align with prior research showing that such systems often miss novel, multistage, or process-level anomalies [9][27]. In response, AI-BPI integration provides three main benefits: (1) predictive threat detection, (2) contextual interpretation of irregularities within business processes, and (3) decision engine support for real-time threat mitigation. Collectively, these benefits position AI-enhanced BPI as a pivotal advancement in cybersecurity for critical infrastructure.6.5 Implications for Practice and Policy

The proposed framework offers practical guidance for industry practitioners and policymakers. For organizations, it demonstrates how operational intelligence can be combined with AI analytics to strengthen cybersecurity without disrupting workflows. For policymakers and regulators, the findings underscore the importance of promoting process-aware security standards, real-time threat monitoring, and cross-sector information sharing. Implementing AI-BPI frameworks can help build national resilience, reduce operational risk, and minimize the financial and societal impacts of cyber incidents.

6.6 Contributions and Future Prospects of Research

This study contributes to both theory and practice. Theoretically, it advances understanding of how to effectively combine process intelligence and AI for real-time threat detection, addressing previous research gaps [8][32]. Practically, it provides a proven framework for detecting anomalies in real time across diverse sectors and is adaptable for field operations. forcement learning for transferable threat responses, cross-sector transfer learning, and integrating IoT-specific threat intelligence to further strengthen critical infrastructure resilience.

VII. CONCLUSION AND RECOMMENDATIONS

This study examined combining Business Process Intelligence (BPI) with Artificial Intelligence (AI) to identify real-time threat detection in key sectors of the US economy, focusing on healthcare, finance, and energy. The results show that using process-aware monitoring with AI analytics dramatically improves anomaly detection and minimizes false positives. It also enables timely intervention. Across all sectors, the framework achieved high accuracy (94.7-96.1%), low detection latency (under 4 seconds), and improved anomaly detection by 31-38% when contextualized using BPI.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

These findings highlight the practical and theoretical importance of combining AI with operational intelligence in cybersecurity for critical infrastructure.

The study confirms that sector-specific workflows and process characteristics are key in detecting anomalies. Healthcare systems benefited from tracking patient treatment sequences and accessing devices. This allowed early detection of unauthorized access or ransomware threats. Financial institutions used transactional flow analysis to identify multi-stage fraud and abnormal account transactions. In the energy sector, operations were controlled with SCADA system sequences, which enabled detection of sensor manipulations and cascading anomalies that could impact grid stability. These results underscore the need for customized AI-BPI frameworks to address the operational, regulatory, and threat environments unique to each sector.

By situating anomalies within business processes, the proposed framework addresses the major drawbacks of current cybersecurity solutions. These include static rule-based systems and signature-dependent intrusion detection tools. Unlike traditional methods, AI-facilitated BPI offers predictive, adaptive, and real-time monitoring. This allows organizations to prepare for emerging threats and reduce operational disruptions. Also, combining process mining with machine learning helps prioritize alerts and ensures that security resources address high-risk events effectively.

Practical recommendations for organizations of this framework are:

- Invest in process-aware monitoring tools to map and constantly update operational working processes.
- Integrate artificial intelligence algorithms that can work with diverse data types, including transactional, operational, and textual threat intelligence.
- Develop sector-specific models that include such characteristics and regulations specific to a given process.
- Establish the capacity for real-time decision engines to automate or guide mitigation actions, minimising response times and operational impact.
- Constantly update models with feedback from anomalies detected and evolving threat intelligence for increased adaptability.

For policymakers, the study demonstrates the importance of encouraging the adoption of cross-sector cybersecurity standards. Real-time cyber threat monitoring and process-aware cybersecurity frameworks improve national infrastructure resilience. Future research could explore reinforcement learning, incorporate IoT threat models, and develop cross-sector anomaly detection models. These advances would help increase the scope and effectiveness of AI-BPI models.

The combination of BPI and AI provides a strong, scalable, and contextual approach to defending critical US infrastructure. By introducing operational process intelligence with advanced analytics, this framework offers greater situational awareness and quick threat detection. It also provides actionable insights to improve security in practice and theoretical advancements for the cybersecurity field.

REFERENCES

[1] Abedin, B., Alagar, V., &Elmiligi, H. (2019). Real-time threat detection using machine learning in cyber-physical systems. Journal of Cyber Security Technology, 3(3), 163–187. https://doi.org/10.1080/23742917.2019.1604785

[2] Alharkan, I., & Aslam, N. (2019). A survey on anomaly detection in industrial control systems. Security and Privacy, 2(6), e78. https://doi.org/10.1002/spy2.78

[3] Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2020). Information security governance: A systematic literature review. Information Systems Frontiers, 22(6), 1431–1466. https://doi.org/10.1007/s10796-019-09936-8

[4] Böhme, R., Laube, S., &Riek, M. (2020). A fundamental approach to cyber risk analysis. Journal of Information Security and Applications, 50, 102428. https://doi.org/10.1016/j.jisa.2019.102428

[5] Burattin, A., van Zelst, S. J., Di Francescomarino, C., Reijers, H. A., & van der Aalst, W. M. P. (2020). Special issue on Business Process Intelligence. Computing, 102(7), 1–4. https://doi.org/10.1007/s00607-020-00856-z

[6] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882

[7] Coventry, L., &Branley, D. (2018). Cybersecurity in healthcare: A narrative review. Maturitas, 113, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

[8] Dardenne, D., Marin, G., & Barros, A. (2019). Process mining and anomaly detection in business processes. Decision Support Systems, 121, 113–128. https://doi.org/10.1016/j.dss.2019.04.005
[9] Debar, H., Curry, D., & Feinstein, B. (2005). The intrusion detection message exchange format (IDMEF). RFC 4765. https://doi.org/10.17487/RFC4765
[10] Grigori, D., Casati, F., Castellanos, M., &Dayal, U. (2004). Business process intelligence. Computers in Industry, 53(3), 321–343. https://doi.org/10.1016/S0166-3615(03)00140-5
[11] He, H., & Garcia, E. A. (2009). Learning from imbalanced data. IEEE Transactions on Knowledge and Data Engineering, 21(9), 1263–1284. https://doi.org/10.1109/TKDE.2008.239
[12] Huang, C.-Y., & Tsai, Y.-H. (2019). Process mining-based anomaly detection in hospital information systems. Computers in Biology and Medicine, 109, 160–170. https://doi.org/10.1016/j.compbiomed.2019.04.014
[13] Khraisat, A., Gondal, I., Vamplew, P., &Kamruzzaman, J. (2019). Survey of intrusion detection systems. Cybersecurity, 2(1). https://doi.org/10.1186/s42400-019-0038-7
[14] Kiss, I., &Genge, B. (2019). Machine learning for cybersecurity in industrial control systems. Computers & Security, 87, 101588. https://doi.org/10.1016/j.cose.2019.101588
[15] Lippmann, R. P., et al. (2000). The 1999 DARPA off-line intrusion detection evaluation. Computer Networks, 34(4), 579–595. https://doi.org/10.1016/S1389-1286(00)00014-4
[16] Liu, H., Lang, B., Liu, M., & Yan, H. (2019). CNN and GRU-based deep cybersecurity intrusion detection system. IEEE Access, 7, 45195–45203. https://doi.org/10.1109/ACCESS.2019.2908282
[17] McLaughlin, S., Podkuiko, D., & McDaniel, P. (2016). Energy theft in the advanced metering infrastructure. International Journal of Critical Infrastructure Protection, 5(4), 116–123. https://doi.org/10.1016/j.ijcip.2012.08.002
[18] Mohaisen, D., & Chang, D. (2019). Artificial intelligence in cybersecurity: Research advances and challenges. IEEE Access, 7, 126471–126482. https://doi.org/10.1109/ACCESS.2019.2938400
[19] Munoz-Gama, J., et al. (2019). Conformance checking in healthcare process mining. Artificial Intelligence in Medicine, 97, 28–45. https://doi.org/10.1016/j.artmed.2019.02.006
[20] NIST. (2018). Framework for improving critical infrastructure cybersecurity. NIST Cybersecurity Framework (1.1). https://doi.org/10.6028/NIST.CSWP.04162018
[21] Noble, C., Li, W., & Thomas, R. (2019). Deep learning for critical infrastructure network intrusion detection. Computers & Security, 89, 101687. https://doi.org/10.1016/j.cose.2019.101687
[22] Phua, C., Lee, V., Smith, K., &Gayler, R. (2010). Data mining-based fraud detection research. Artificial Intelligence Review, 34(3), 1–14. https://doi.org/10.1007/s10462-009-9122-5
[23] Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Fraud detection through machine learning. MIS Quarterly, 36(1), 1–21. https://doi.org/10.25300/MISQ/2012/36.1.02
[24] Russell, S., &Norvig, P. (2010). Artificial Intelligence: A modern approach (3rd ed.). Pearson. https://doi.org/10.5555/1671238
[25] Sardi, A., Mantovani, E., &Lezza, A. (2020). Cyber risk in health facilities. Sustainability, 12(17), 7002. https://doi.org/10.3390/su12177002
[26] Shirey, R. (2000). Internet security glossary (RFC 2828). https://doi.org/10.17487/RFC2828
[27] Sommer, R., &Paxson, V. (2010). On using ML for network intrusion detection. IEEE Security & Privacy, 8(1), 26–34. https://doi.org/10.1109/MSP.2010.25
[28] Stallings, W. (2013). Computer security: Principles and practice (3rd ed.). Pearson. https://doi.org/10.5555/2593158
[29] Sun, L., et al. (2018). Machine learning-based anomaly detection for smart grids. IEEE Access, 6, 10232–10240. https://doi.org/10.1109/ACCESS.2018.2796558
[30] Swanson, M., Hash, J., & Bowen, P. (2006). NIST SP 800-30: Guide for conducting risk assessments. https://doi.org/10.6028/NIST.SP.800-30
[31] Ten, C. W., Manimaran, G., & Liu, C.-C. (2010). Cybersecurity for critical infrastructures. IEEE Transactions on Systems, Man, and Cybernetics A, 40(4), 853–865. https://doi.org/10.1109/TSMCA.2010.2052450
[32] van der Aalst, W. M. P. (2015). Business Process Intelligence: Connecting data and processes. Communications of the ACM, 58(8), 76–82. https://doi.org/10.1145/2685352
[33] van der Aalst, W. M. P. (2016). Process mining: Data science in action (2nd ed.). Springer. https://doi.org/10.1007/978-3-662-49851-4
[34] Verma, A., &Ranga, V. (2020). Machine learning-based intrusion detection systems. Journal of Information Security and Applications, 54, 102534. https://doi.org/10.1016/j.jisa.2020.102534
[35] Wang, K., &Stolfo, S. (2004). Anomalous payload-based intrusion detection. RAID 2004, 203–222. https://doi.org/10.1007/978-3-540-30143-1_11

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 7, Issue 1, January–February 2024||

DOI:10.15662/IJRAI.2024.0701004

[36] Wang, W., et al. (2018). HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks for intrusion detection. IEEE Access, 6, 1792–1806. https://doi.org/10.1109/ACCESS.2018.2780172
[37] Wachter, S. (2018). Normative challenges of AI in cybersecurity. Computer Law & Security Review, 34(4), 863–871. https://doi.org/10.1016/j.clsr.2018.01.006
[38] Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. (2016). Information security in big data: Privacy and data mining. IEEE Communications Surveys & Tutorials, 18(2), 1165–1188. https://doi.org/10.1109/COMST.2015.2494505
[39] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). Deep learning approach for intrusion detection. IEEE Access, 5, 21954–21961. https://doi.org/10.1109/ACCESS.2017.2762418
[40] Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big data. Journal of Big Data, 2(1), 3. https://doi.org/10.1186/s40537-015-0013-4