ISSN (O): 2320-5407
ISSN (P): 3107-4928

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/22515
DOI URL: http://dx.doi.org/10.21474/IJAR01/22515

RESEARCH ARTICLE

AI-DRIVEN CYBERSECURITY IN INDUSTRY 4.0: A GLOBAL COMPARATIVE ANALYSIS OF DETECTION METHODS, CHALLENGES, AND RESILIENT SOLUTIONS

Zidida Damekhaly Turay[1], Mohamed Koroma[2], Mohamed Syed Fofanah[2] and Daniel Bob Kaitibi[2]

1. School of Software Engineering, Nankai University, China.
2. School of Technology, Department of Computer Science and Information Technology, Njala University, Sierra Leone, West Africa.

Manuscript Info

Manuscript History
Received: 01 November 2025
Final Accepted: 04 December 2025
Published: January 2026

Key words:-
Cybersecurity, Industry 4.0, Intrusion detection systems, AI-driven security, Regional analysis, System resilience.

Abstract

The study provides a comprehensive review of cybersecurity detection methods within Industry 4.0, focusing on enhancing system resilience and user trust. The research uses a qualitative approach to analyze nine case studies from Africa, Asia, and the West to identify key challenges, detection strategies,and region-specific insights.The findings emphasize the critical role of AI-driven and hybrid detection systems, which have proven effective in mitigating advanced cyber threats such as ransomware, distributed denial of service (DDoS), and false data injection attacks. Comparative analysis highlights common global challenges,including resource limitations,human-related vulnerabilities, and compliance issues, while addressing unique regional factors such as infrastructure gaps and evolving threat sophistication.The study proposes a cybersecurity taxonomy integrating machine learning, real-time anomaly detection, and adaptive threat response mechanisms for Industry 4.0 environments. Recommendations for practitioners include adopting AI-enhanced intrusion detection systems (IDS), implementing energy-efficient IoT security solutions, and conducting regular system audits. Policymakers are encouraged to mandate adherence to global cybersecurity standards, foster international collaboration, and invest in workforce capacity building initiatives. The review, therefore, strengthe ns global cybersecurity frameworks,improves organizational resilience, and fosters public trust in the secure integration of Industry 4.0 technologies.

Introduction

In Africa, countries like Sierra Leone, Nigeria, Senegal, Kenya, and Ethiopia have faced significant cyber threats as they integrate advanced technologies into their infrastructure. These regions have encountered various cyber-attacks, including ransomware, phishing, and Distributed Denial of Service (DDoS) attacks, disrupting financial services, government operations, telecommunications, and healthcare systems. The recurring theme in these cases is the necessity for improved cybersecurity protocols, enhanced employee training, and the adoption of advanced detection

Corresponding Author:- Zidida Damekhaly Turay
Address:-School of Software Engineering, Nankai University, China.

methods to mitigate these threats effectively. For example, the financial and telecommunications sectors in Sierra Leone have been particularly vulnerable, highlighting the importance of strengthening cybersecurity measures to protect critical infrastructure and maintain public trust.In the West, the United States, the United Kingdom, and Canada have also faced substantial cyber threats, emphasizing the global nature of these challenges. The SolarWinds breach in the US and the WannaCry ransomware attack on the UK's National Health Service (NHS) exemplify the severe impact of cyber-attacks on critical infrastructure and public services. These incidents have spurred the development of more robust cybersecurity frameworks and the integration of AI and machine learning into detection and response strategies. The Canadian experience, particularly with data breaches in healthcare and financial sectors, underscores the importance of privacy preservation frameworks like P-Spec to protect sensitive information and build consumer trust. In Asia, China has witnessed significant cyber-attacks targeting major corporations, healthcare systems, and educational institutions.

The breaches in Tencent’s WeChat and the ransomware attack on the Wuhan Health Commission during the COVID-19 pandemic illustrate the vulnerabilities in both the public and private sectors. These incidents highlight the need for advanced cybersecurity measures, including quantum computing and machine learning techniques, to secure critical data and ensure the reliability of digital infrastructure. The emphasis on integrating AI-driven solutions and enhanced authentication mechanisms is crucial for safeguarding against evolving cyber threats in China’s rapidly advancing digital landscape. Emerging technologies like blockchain and quantum computing offer promising solutions to enhance cybersecurity frameworks. Blockchain provides a decentralized and immutable ledger system that can secure IoT devices and ensure data integrity. Despite posing risks to traditional encryption, Quantum computing can be countered with quantum-resistant cryptographic techniques and quantum key distribution (QKD) for secure communication. Combining these technologies can create robust frameworks capable of addressing current and future cyber threats, enhancing incident response systems, and ensuring long-term data security.

In the age of Industry 4.0, the rapid adoption of advanced technologies such as the Internet of Things (IoT), Industrial IoT (IIoT), artificial intelligence (AI), machine learning (ML), cloud computing, and big data analytics have revolutionized industries. These advancements, including integrating smart appliances, sensors, and automation systems, have significantly enhanced efficiency and innovation but have simultaneously introduced vulnerabilities that pose severe cybersecurity challenges (Sengupta et al., 2020, Wang et al., 2023). Addressing these vulnerabilities necessitates a deeper understanding of cybersecurity concepts and their practical applications, especially for non-experts, to foster trust and enhance security practices.The increasing sophistication of cyber threats demands innovative defense mechanisms. Traditional cybersecurity approaches often fail to address emerging risks associated with applications such as connected and autonomous vehicles (CAVs) (Giannaros et al., 2023). Advanced intrusion detection systems (IDS) leveraging deep learning and machine learning algorithms have proven effective in safeguarding industrial control systems (ICS) and cyber-physical systems (CPS). These systems utilize real-time data analysis to detect anomalies and thwart potential attacks, underscoring the importance of integrating cutting-edge technologies into cybersecurity frameworks.

Cyber-physical systems (CPS) are central to Industry 4.0, integrating technologies like information systems, real-time control subsystems, physical components, and human operators to manage complex processes. Introduced by (Gill, 2006), CPSs utilize sensors and actuators for real-time feedback control, enabling cooperative and semi-automated operations (Hamzah et al., Lee, 2015). These systems facilitate the convergence of industrial and critical infrastructures, emphasizing the importance of cybersecurity in maintaining their integrity and functionality.

The healthcare sector exemplifies the transformative potential of technology, especially during the COVID-19 pandemic. Devices such as glucose monitors and blood pressure sensors have revolutionized patient care and exposed the sector to cyber vulnerabilities (Junaid et al., 2022). Similarly, the education sector's shift to remote learning has increased adolescents' exposure to online risks (Leijse et al., 2023, Pokhrel & Chhetri, 2021). These examples highlight the dual-edged nature of technological integration and the pressing need for robust security measures across all sectors.This review simplifies technical jargon and complex research findings to make cybersecurity concepts accessible to all. For instance, it breaks down the role of intrusion detection systems (IDS) into manageable explanations, detailing their ability to monitor traffic, detect anomalies, and prevent unauthorized access. Similarly, IoT-based sensors are discussed in the context of their practical applications, such as monitoring soil health in agriculture or improving operational efficiency in industrial processes. By fostering a deeper understanding of cybersecurity, this review aims to build trust, enhance security practices, and support the safe integration of technology into every aspect of modern life.

Problem Analysis

Cyberattacks, often driven by harmful intent, have become increasingly sophisticated, posing critical challenges to cybersecurity frameworks. For instance, false data injection attacks (FDIAs) manipulate data values to disrupt operations in power grids, destabilizing critical infrastructures (Ahmed & Pathan, 2020; Zhu et al., 2023).Despite technological advancements, humans remain the weakest link in cybersecurity. Research highlights that weak password choices and poor security habits are among the most exploited cyber-attack vulnerabilities (Cybersecurity and Infrastructure Security Agency et al., 2023, Cybersecurity and Infrastructure Security Agency, 2021). Social engineering tactics, phishing, and insider threats further exacerbate risks. These challenges emphasize the need for targeted education and awareness programs, particularly in regions like Sierra Leone, where technological literacy may lag (Sawaneh et al., 2021). Strengthening individual practices through user-friendly tools and simplified guidelines can significantly mitigate these risks.

Effective cybersecurity extends beyond technical solutions to include robust legal frameworks and policies. The growing sophistication of malware and the persistence of cyber criminals underscore the necessity for stringent cybersecurity legislation and enforcement (Mazhar et al., 2023, Cremer et al., 2022). Public awareness campaigns and education initiatives are equally critical in reducing vulnerabilities and empowering individuals to adopt secure practices.The decentralized and dynamic nature of CPSs poses significant security challenges. Unlike traditional static systems, CPSs require flexible access control models to address vulnerabilities emerging from interactions across physical and cyber domains (Chui et al., 2023, Fei & Shen, 2023). Effective frameworks must adapt to environmental changes to secure CPS components. This research simplifies these concepts, enhancing understanding and offering practical insights into CPS security strategies.

CPSs' reliance on interconnected technologies amplifies vulnerabilities in global supply chains, exposing systems to cyberattacks, malware, and data breaches. These threats jeopardize operational reliability and public trust, with potential consequences such as industrial accidents and environmental damage (Kholidy, 2021;Xiao et al., 2023). Historical incidents like the Stuxnet worm demonstrate the need for robust security frameworks to safeguard safety-critical infrastructures (Khan et al., 2024; Harkat et al., 2024). From 2020 to 2022, the cybersecurity landscape experienced a surge in incidents, exacerbated by the COVID-19 pandemic, significantly impacting global economies and national security. The increasing reliance on technology necessitates an expansion in the cybersecurity workforce by 145% to meet industry demands adequately (Khando et al., 2021). However, human error remains the most significant vulnerability, underscoring the need for adequate training programs.

Despite many companies implementing IT security awareness initiatives, a recent Hornetsecurity report (Hornetsecurity, 2024) found that 25.7% of organizations do not provide such training. Nevertheless, 78.5% of organizations perceive these programs as moderately effective in combating cyber threats. This aligns with the review's goal of fostering confidence in cybersecurity practices through accessible iThese case studies collectively emphasize the importance of continuously improving cybersecurity practices and adopting innovative detection methods to address the dynamic threat landscape in Industry 4.0. Strengthening cybersecurity frameworks, enhancing public awareness, and fostering international collaboration are essential steps to protect sensitive information and ensure the resilience of critical infrastructure globally. Fig 4 illustrates how Industry 4.0 systems process cyber-threat data using AI. It visualizes key components of the detection pipeline and how feedback loops enhance threat response.

Aim and Objectives of the Review

This review aim to make cybersecurity concepts accessible to a diverse audience, including professionals, learners, and those new to the field by highlighting fundamental advancements in areas such as network security, intrusion detection methods, and cyber defense strategies. Thereby enhance understanding and encourage practical application of these concepts.

The following objectives are pertinent to this review

1. To update and clarify definitions of key cybersecurity terms based on the latest research, providing a comprehensive resource to guide future studies.
2. To address the gap in the existing literature by offering an inclusive and detailed analysis, fostering public awareness and confidence in cybersecurity practices while promoting a culture of trust and proactive engagement in the digital landscape.

3. To demystify recent research findings and highlighting fundamental discoveries in network security,intrusion detection methods, and cyber defense strategies.
4. To update definitions of essential cybersecurity terms based on the latest research, offering a comprehensive overview to bridge gaps in current understanding. These efforts align to enhance public confidence in cybersecurity practices and foster a culture of awareness.

Literature Review:-

The pandemic-driven shift to digital operations heightened exposure to cyber threats, emphasizing the review's focus on practical solutions to evolving challenges. Before COVID-19, only 12% of UK working adults reported homeworking (Office for National Statistics, 2020), but this figure surged to 49% during early 2020 and fluctuated between 25% and 40% in subsequent years (Office for National Statistics, 2022, Office for National Statistics, 2023). This increased connectivity amplified vulnerabilities, with studies indicating that cybercriminals continuously develop novel methods to exploit technological advancements (Saeed et al., 2023). Research demonstrates that proactive cybersecurity disclosures positively affect market value, while pessimistic tones correlate with reduced valuations (Gordon et al., 2010, Araujo et al., 2024). Companies must now report cyber-related concerns, reflecting the growing recognition of cybersecurity's significance. Effective threat management demands domain knowledge to counter challenges such as denial of service (DoS) attacks, phishing, and malware (National Institute of Standards and Technology, 2020). This aligns with the research objective of bridging gaps in cybersecurity understanding and fostering practical application. Executed manually or remotely, these attacks underscore the pressing need for advanced cybersecurity measures to counteract threats and protect critical systems (Jbair et al., 2022; Rawat, 2021).

Recent studies have documented various attack methods targeting intelligent systems, particularly in smart grids. FDIAs inject false information to destabilize systems, denial of service (DoS) attacks block communication, and replay attacks duplicate data to deceive operators (Liberati et al, 2021). These threats compromise system stability, trigger false alarms, and damage critical equipment. Addressing these vulnerabilities has led to innovations such as graphical detection technologies using graph networks (GNs) to identify tampered data and capsule networks that maintain precise node attributes (Sharma et al., 2022, Alowais et al., 2023).

These advancements align with the review's goal to bridge gaps in understanding by highlighting fundamental discoveries and practical applications in cybersecurity.As cyber threats evolve, measures like pseudo-random number watermarking for secure data transmission have become essential to protect data integrity, confidentiality, and availability (Huang et al., 2020, Oh et al., 2021). Cyberattacks are increasingly targeting vulnerabilities in IT systems, emerging technologies like IoT, and cloud computing, necessitating continuous updates to risk management strategies (Ksibi et al., 2022, Kaur et al., 2023). This research connects these challenges to actionable solutions, underscoring the importance of proactive defense mechanisms.Over the past decade, the growing complexity and frequency of cyberattacks have emphasized the need for dynamic cybersecurity strategies. The absence of a universally accepted definition of cyberattacks further complicates mitigation efforts, highlighting the necessity for a comprehensive understanding of their impact on businesses and critical infrastructures (Li & Liu, 2021, Aslan et al., 2023).

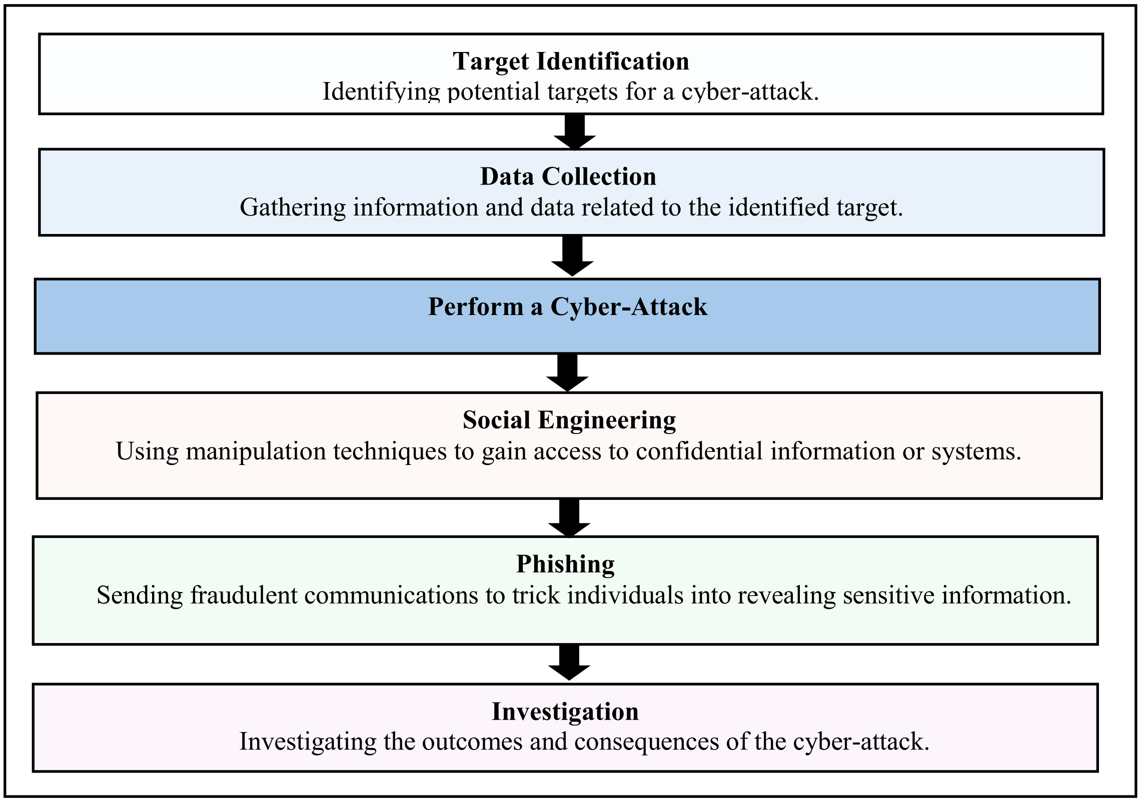
Target Identification
Identifying potential targets for a cyber-attack.
Data Collection
Gathering information and data related to the identified target.
Perform a Cyber-Attack
Social Engineering
Using manipulation techniques to gain access to confidential information or systems.
Phishing
Sending fraudulent communications to trick individuals into revealing sensitive information.
Investigation
Investigating the outcomes and consequences of the cyber-attack.

Figure1: The systematic process attackers use to exploit vulnerabilities bu (Li &Liu 2021)

Figure 1 highlights the systematic process attackers use to exploit vulnerabilities, underscoring the importance of proactive cybersecurity measures. Each step reveals how malicious actors operate, from target identification and data collection to executing attacks, social engineering, phishing, and post-attack investigation. Understanding these phases allows organizations to anticipate threats, implement safeguards at critical stages, and foster user awareness, ultimately minimizing risks and strengthening defenses against evolving cyber threats (Moustafa et al., 2021, Prümmer et al., 2024, Cremer et al., 2022).

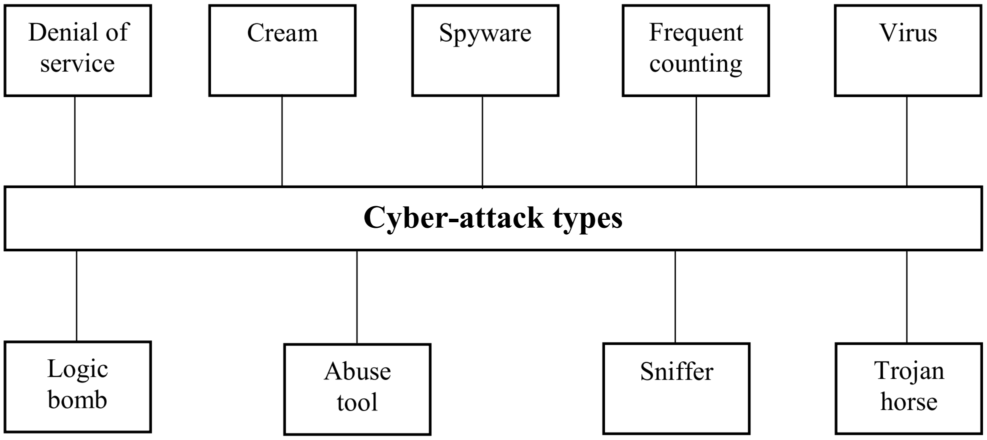

Fig 2: Cyber Attacks categories (Li & Liu, 2021)

Figure 2 categorizes various **cyber-attack types,** such as denial of service (DoS), spyware, viruses, Trojan horses, and logic bombs, aligning with increasingly sophisticated methods. Attacks like DoS disrupt communication channels, while spyware and sniffer tools monitor and manipulate critical systems to extract sensitive data. Trojan horses and logic bombs, often concealed within legitimate software, can damage infrastructures and compromise system integrity. These methods highlight vulnerabilities in smart grids, IoT systems, and cloud networks, underscoring the need for advanced mitigation strategies like graphical detection and capsule networks (Sharma et al., 2022, Huang et al., 2020).

Network Control Systems

The Networked Control System (NCS) has undergone significant advancements, reflecting its growing importance in safeguarding critical infrastructures against evolving cyber threats. Recent developments, such as the hybrid-triggered approach (HTS) introduced in 2021, have enhanced NCS security by reducing network communication strain while addressing concurrent cyberattacks like deception and Denial of Service (DoS) attacks (Nittari et al., 2022, Ganjali et al., 2022). Operating through a feedback loop facilitated by communication networks, NCS connects spatially distributed components, including sensors, controllers, and actuators, ensuring efficiency and reduced operational costs across applications such as power grids, transportation, and sensor networks. However, integrating communication networks within NCS introduces challenges like packet losses and latency, which may compromise system stability and performance (Chen et al., 2022, Yan et al., 2023). Addressing these vulnerabilities will simplify cybersecurity concepts and solutions for broader understanding and application.Abnormal network traffic detection protects cyberspace, particularly in NCS environments. This process relies heavily on machine learning for identifying malicious activities but struggles with redundant features that consume computational resources and reduce detection accuracy (Yi et al., 2023, Ogah et al., 2024). To address these limitations, advanced methods like LD-KPCA combine linear discriminant analysis with kernel principal component analysis to refine feature extraction, ensuring high detection precision by transforming data into linearly separable spaces. These innovations enhance the ability to identify new attack patterns to explain complex cybersecurity solutions.

Forensic tools have further strengthened security by facilitating secure information sharing while protecting data privacy. In Industrial Internet of Things (IIoT) applications, these tools enhance reliability, cost-effectiveness, and operational efficiency, underscoring the critical need for robust protocols to ensure network security and data integrity (Soori et al., 2023, Zvarivadza et al., 2024). As cybersecurity threats become increasingly sophisticated, continuous detection technologies and system resilience improvements remain essential.

Smart Appliances

Smart appliances and technologies have revolutionized modern living, improving global service quality, sustainability, and efficiency. Smart grids, driven by advanced communication systems and the Internet of Things (IoT), provide sustainable, cost-effective, and secure power delivery to large communities (Pandiyan et al., 2023, Furszyfer Del Rio et al., 2021). These interconnected systems, including building automation, smart vehicles, and crewless aerial vehicles, continuously share data through centralized cloud platforms. However, the widespread adoption of these technologies exposes them to cybersecurity risks. Forensic investigations of cyber incidents involving smart devices are essential to strengthening defenses and protecting smart cities against future threats (Kim et al., 2023, Baig et al., 2017).

Despite the benefits, smart appliances and smart homes face significant cybersecurity challenges due to their dependence on internet connectivity and energy systems. Critical for managing energy consumption, smart meters are susceptible to intrusions that compromise home networks and alter energy costs. This underscores the need for multi-layered cybersecurity measures, such as Security Assurance Methods (SSAM), to ensure system integrity and monitor applications within smart environments (Schiller et al., 2023, J et al., 2023). Moreover, smart technologies like battery energy storage systems, used for frequency regulation and emergency power supply, rely on robust communication networks and algorithms to counter cyberattacks effectively (Bouramdane, 2023).

The COVID-19 pandemic demonstrated the vital role of smart medical technologies in healthcare, reducing transmission risks and improving disease management. Advanced systems such as AI-supported diagnostics, telemedicine solutions, and health monitoring devices provide timely and dependable healthcare services (Tilahun et al., 2021, Zhang et al., 2021). For example, Tencent's "Dr. Clove" app facilitated online consultations and medication access during health crises, showcasing the potential of smart healthcare systems (Nittari et al., 2022, Gautam et al., 2021). However, these advancements also highlight significant cybersecurity concerns. Solutions like the Edge Intelligent Collaborative Privacy Protection (EICPP) framework are essential to ensure the confidentiality and security of patient data in smart healthcare settings (Khan et al., 2024, Zhang et al., 2021).

Quantum Computing

Quantum computing has emerged as a transformative force, offering enhanced capabilities to integrate advanced internet and energy solutions across industries. This review highlights quantum computing's role in improving operational efficiency, data security, and innovation. Quantum technologies address critical challenges in protecting sensitive data, including product designs, industrial manufacturing records (CAD, CAM), financial transactions, and secure communications across production sites (Ladd et al., 2010, Santhi & Muthuswamy, 2023). These advancements are essential for sectors like aerospace and defense, where operational excellence and secure data transmission are paramount (Nielsen & Chuang, 2010, Pop et al., 2023).

Quantum computing's ability to process vast amounts of data at unprecedented speeds enables industries to optimize complex manufacturing workflows, predict system failures, and enhance reliability. For instance, in aerospace, quantum algorithms simulate aerodynamic properties with greater accuracy, leading to safer and more efficient aircraft designs (Preskill, 2018, Montanaro, 2015). Moreover, quantum cryptography ensures unbreakable encryption methods for secure communications, providing robust defenses against cyber threats (Bennett & Brassard, 1984, Bennett & Brassard, 1984).

Quantum Key Distribution (QKD) is a key feature of quantum security, which leverages quantum mechanics to secure key exchanges and protect sensitive data during transmission. This is particularly vital for industries handling classified or high-stakes information, ensuring confidentiality and integrity in communication networks (Scarani et al., 2009). By integrating QKD into industrial processes, sectors such as defense and aerospace achieve unparalleled levels of security while fostering innovation. As quantum computing evolves, its potential to address contemporary cybersecurity and operational efficiency challenges becomes increasingly significant (Shor, 1994, Yalcin et al., 2024).

Machine Learning (M-Learning)

Machine Learning (M-Learning) has emerged as a critical strategy for addressing cyber threats by leveraging uncertainty measures and feature values to enhance threat detection. M-learning integrates evidence theory to quantify the impact of uncertainty within individual features, improving classification accuracy (Shafer, 2016, Kohlas, 1996). Feature selection (FS) techniques further optimize intrusion detection systems (IDS) by identifying the most relevant features, reducing computational complexity, and enhancing detection efficiency (Li et al., 2024, Walling & Lodh, 2024). Advanced evidential classifiers address limitations in traditional machine learning methods like logistic regression (LR), mitigating risks associated with binary decision-making in threat detection (Dempster et al., 1977, Beechey et al., 2021).

M-learning’s ability to process labeled and unlabeled data using techniques like Support Vector Machines (SVM) and Hidden Markov Models has strengthened anomaly-based classification approaches in network security (Cortes & Vapnik, 1995, Choi & Kim, 2024). The distinct yet complementary role of e-learning in cybersecurity education improves public understanding and trust in cybersecurity practices. During the COVID-19 pandemic, e-learning frameworks such as the Conceptual Framework for eLearning and Training (COFELET) formalized the design of cybersecurity education programs. COFELET incorporates threat analysis and modeling standards into game-based learning, demonstrated through prototypes like Hack Learn, which integrate the Activity Theory Model for Serious Games (ATMSG) to enhance cybersecurity awareness (Montalbano et al., 2022, Hodhod et al., 2023).

Game-based technologies and New Learning Analytics (LA) have further elevated cybersecurity education by providing data-driven insights into learning behaviors. LA measures, collects, and analyzes data to optimize educational strategies within learning management systems and massive open online courses (Siemens & Long, 2011, Sharif & Atif, 2024, Mian et al., 2022). Serious games and game-based learning analytics expedite development, minimize design iterations, and maximize educational impact, fostering accessible, engaging, and practical cybersecurity education (Alonso-Fernández et al., 2019, Daoudi, 2022). These advancements demonstrate the importance of integrating M-learning and educational technologies to enhance cybersecurity awareness and resilience.

Cloud Computing

Cloud computing has emerged as a transformative technology, providing on-demand and ubiquitous access to configurable computing resources through virtualization technology (Levitin et al., 2016). Virtualization enables multiple virtual machines (VMs) to operate on a single physical server, enhancing resource utilization and

flexibility. However, inherent vulnerabilities in this architecture pose significant security and survivability challenges. For example, attackers can exploit shared virtual machine environments by deploying VMs on the same server as the target, creating side channels to bypass logical barriers and compromise sensitive data (Levitin et al., 2016). Such threats underscore the need for robust security mechanisms to protect cloud computing environments.
Despite the efficiency of cloud services, privacy remains a significant concern that hinders widespread adoption. Individual users rely on cloud-based multimedia management, while businesses leverage free platforms for e-commerce development. However, the lack of transparent privacy policies among many cloud providers raises risks such as data misuse, identity theft, and fraud (Pearson & Benameur, 2010, Al-Issa et al., 2019, Dawood et al., 2023). Although third-party certifications like TRUSTe have improved transparency, they may not fully address diverse privacy preferences or the complexities of handling sensitive data.

To mitigate these issues, next-generation technologies such as P-Spec have been developed. P-Spec articulates privacy policies for service providers and users, ensuring compliance with user preferences and safeguarding data (Mehrtak et al., 2024, Quach et al., 2022, Barth & De Jong, 2017) by providing a comprehensive approach to privacy preservation. Frameworks like P-Spec foster consumer trust, enhancing cybersecurity awareness and encouraging the secure adoption of cloud services. This ensures that sensitive information remains protected while promoting broader acceptance of cloud computing technologies.

Internet of Things (IoT)

The Internet of Things (IoT) has revolutionized the development of smart technologies and enabled the evolution of the Industrial Internet of Things (IIoT). IIoT integrates intelligent sensors and actuators to optimize manufacturing processes and foster smart cities. However, the limited battery life of IoT devices remains a significant challenge, mainly due to the high energy demands required for continuous communication across machine-to-machine (M2M) networks (Anwer et al., 2021, Arshad et al., 2020, Alsharif et al., 2023, Aldin et al., 2024). These networks, powered by technologies such as Wi-Fi, Zigbee, Lora WAN, and NB-IoT, provide critical benefits but are increasingly vulnerable to advanced persistent threats (APT), such as botnet attacks, due to their complexity and the diverse data they handle (Alsemiri & Alsubhi, 2019, Isong & Kgote, 2024, Victor et al., 2023).

Intrusion Detection Systems (IDS) are pivotal in mitigating cyber threats within IoT ecosystems. Modern IDS solutions leverage machine learning (ML) and deep learning (DL) to detect and classify emerging threats across heterogeneous IoT devices. However, the effectiveness of ML and DL techniques is limited by their reliance on extensive datasets containing both normal and malicious activities. These techniques often struggle to identify new, previously unseen attack types due to the diversity of IoT devices and their unique communication patterns. To address this limitation, lightweight detection engines must enhance adaptability and ensure efficient real-time threat detection within resource-constrained IoT environments (Anwer et al., 2021, Al-Garadi et al., 2020, Alwaisi et al., 2024).

The energy constraints of IoT devices further complicate the implementation of robust security mechanisms. Research highlights the need to balance energy efficiency with effective security protocols to sustain IoT networks in industrial and smart city applications. Innovative solutions that reduce energy consumption while maintaining robust IDS capabilities are critical to addressing this challenge (Al-Garadi et al., 2020, Alwaisi et al., 2024).

Methodology:-

This study investigates nine case studies across Africa, Asia, and the West to explore cybersecurity incidents, detection methods, and outcomes comprehensively. The case study methodology enables an in-depth analysis of specific cybersecurity events, offering insights into diverse geopolitical contexts and their responses (Yin, 2018). Cases were selected based on their significance, severity, impact, and relevance within the last five years, ensuring meaningful insights into critical cybersecurity breaches and practice advancements.Secondary data collection methods were employed, Secondary data sources included a detailed academic literature review, official government reports, industry publications, and relevant cyber-attack analyses as described by Creswell & Poth, 2018, Flick, 2018, and Li & Liu, 2021. These sources aligned with triangulation principles, providing a robust analytical foundation. Comparative analysis across regions further distinguished unique regional issues from shared global cybersecurity trends. Table 1 compares cybersecurity threats across regions, emphasizing differences in vulnerabilities and responses. It reinforces the need for region-specific strategies while supporting the paper's advocacy for AI-driven detection.

Table 1: Summary of Global Cybersecurity Challenges by Region

Region	**Common Cyber Threats**	**Key Vulnerabilities**	**Primary Response Measures**
Africa	Ransomware, Phishing	Low infrastructure, literacy	Government legislation, awareness campaigns
Asia	APTs, Insider threats	Outdated protocols	AI-enhanced IDS, regional policy reforms
West	DDoS, Data breaches	Legacy systems, complexity	AI/ML tools, advanced compliance frameworks

Figure 3 outlines the methodological approach used in the study. The Case Study selection focused on regional diversity, cyber threat variety, and the impact of cybersecurity measures, ensuring relevance to critical industries.

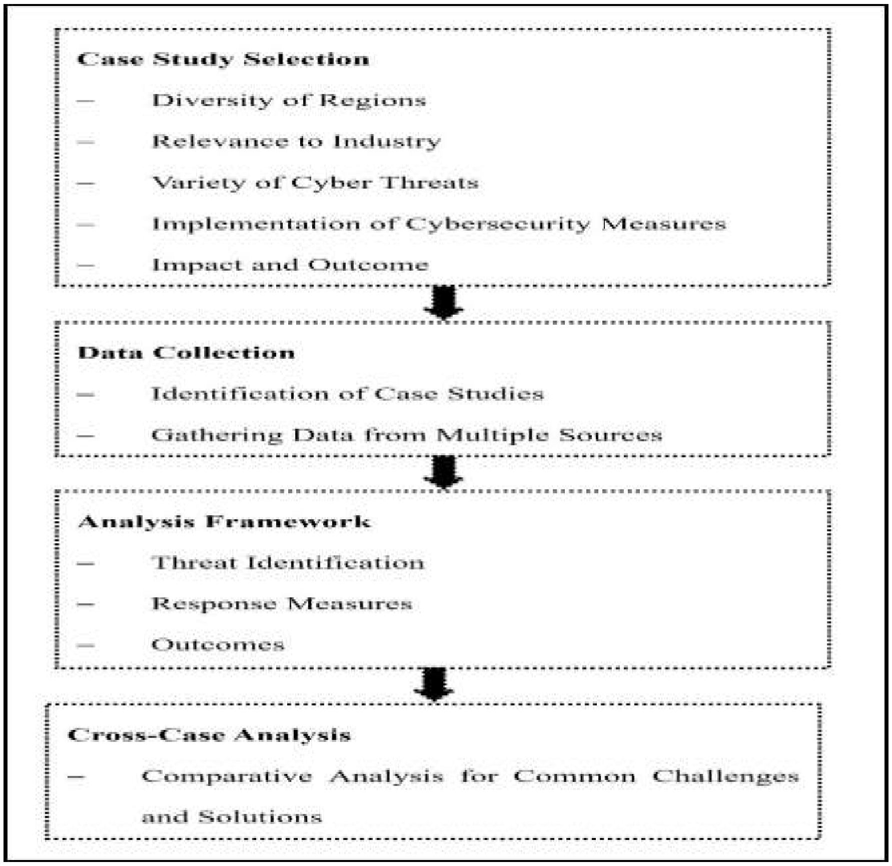
Case Study Selection
— Diversity of Regions
— Relevance to Industry
— Variety of Cyber Threats
— Implementation of Cybersecurity Measures
— Impact and Outcome
Data Collection
— Identification of Case Studies
— Gathering Data from Multiple Sources
Analysis Framework
— Threat Identification
— Response Measures
— Outcomes
Cross-Case Analysis
— Comparative Analysis for Common Challenges and Solutions

Fig 3. Data Flow Diagram

The Analysis Framework identified threats, response measures, and outcomes to assess regional and global cybersecurity practices. Finally, Cross-Case Analysis facilitated comparative evaluations to uncover common challenges and solutions, enhancing the study's recommendations for improving cybersecurity resilience in Industry 4.0.

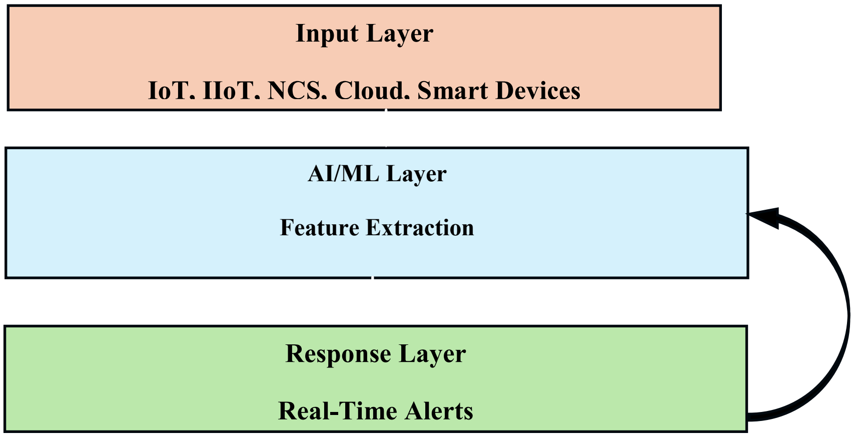

Fig 4: Conceptual Framework for AI-Driven Intrusion Detection Industry 4.0

Discussion of Results:-

Sierra Leonean Perspective

Background: In the rapidly evolving cybersecurity landscape, legislation is crucial in safeguarding the digital realm and upholding fundamental rights. Over the past five years, Sierra Leone has faced numerous cybersecurity challenges as it advances into Industry 4.0, integrating IoT, cloud computing, and industrial automation (Saeed et al., 2023). These advancements have exposed the country's digital infrastructure to various cyber threats. The Cybersecurity and Crime Act 2021 was enacted to address these growing challenges, digital crimes, and data security. Notably, in 2019, a significant cyber-attack targeted Sierra Leone’s financial sector, where hackers infiltrated major banks, causing significant financial losses and service disruptions, highlighting the need for such legislation (Bah, 2023).As the second anniversary of this legislation approaches, it is essential to assess its impact, achievements, and challenges. This article explores the Act's key provisions, goals, and effects on stakeholders, emphasizing the progress in enhancing cybersecurity and recognizing implementation hurdles (Bah, 2023). Understanding the Act's influence is vital for policymakers and the public to navigate the complex digital landscape and ensure robust digital defenses.

Implementation: A ransomware attack halting the Sierra Leonean government’s digital infrastructure by encrypting critical data and demanding a ransom. This incident disrupted various government services and affected public trust in the government's ability to safeguard sensitive information (Sesay, 2019, Sierra Leone Ministry of Information and Communications, 2017, University of Makeni, 2017, Beaman et al., 2021). The telecommunications sector faced a series of Distributed Denial of Service (DDoS) attacks, overwhelming the networks of major telecom providers and causing widespread service outages (Sawaneh et al., 2021, Sierra Leone Ministry of Information and Communications, 2017, University of Makeni, 2017).

Challenges and Outcomes: Recent cyber-attacks have underscored the need for robust cybersecurity measures, especially with new technologies like AI and cloud computing. The banking sector faced a phishing attack that infiltrated banking systems and stole sensitive customer information (Sawaneh et al., 2021, Sierra Leone Ministry of Information and Communications, 2017, University of Makeni, 2017). In early 2023, a ransomware attack on a major hospital in Freetown disrupted operations and posed risks to patient safety, emphasizing the importance of cybersecurity in healthcare (Sawaneh et al., 2021, Sierra Leone Ministry of Information and Communications, 2017, University of Makeni, 2017). These incidents demonstrate the critical importance of implementing effective cybersecurity measures to protect sensitive information and ensure critical infrastructure reliability in Sierra Leone.

Nigerian Perspective

Background: Nigeria has faced significant cybersecurity challenges over the last five years while integrating Industry 4.0 technologies. The country's digital infrastructure, incorporating IoT, cloud computing, and AI, has been vulnerable to cyber threats. A major ransomware attack targeted multiple Nigerian government agencies, disrupting their operations and compromising sensitive data. This incident highlighted the urgent need for robust cybersecurity measures within governmental systems (Alawida et al., 2022, Neprash et al., 2022).

Implementation: In 2020, the financial sector in Nigeria experienced a severe breach when hackers infiltrated the systems of a leading bank, resulting in the theft of millions of naira. The attackers exploited security vulnerabilities in the bank's outdated protocols, demonstrating the necessity for continuous updates and enhancements in cybersecurity measures to combat sophisticated threats (Conteh & Turay, 2022). The education sector was also affected. In 2021, several Nigerian universities faced a series of cyber-attacks that disrupted their online learning platforms, affecting thousands of students (Conteh & Turay, 2022, Ukwandu et al., 2022).

Challenges and Outcomes: In 2022, the healthcare sector in Nigeria encountered a major cyber-attack when a prominent hospital in Lagos was hit by ransomware. Cybercriminals encrypted essential medical records and demanded a ransom for their release, disrupting hospital operations and endangering patient safety (Dameff et al., 2023, Abubakar et al., 2022). These cyber-attacks underscore the growing threat landscape in Nigeria and the necessity for effective cybersecurity measures. While adopting Industry 4.0 technologies offers numerous benefits, it also introduces new vulnerabilities that must be addressed through comprehensive detection methods and enhanced security protocols. Strengthening cybersecurity in Nigeria is crucial for protecting sensitive information, ensuring critical infrastructure reliability, and maintaining user trust in the digital economy.

Senegal Perspective

Background: Senegal has encountered numerous cybersecurity challenges over the past five years as it advances into Industry 4.0. Integrating advanced technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence (AI) has exposed the nation's digital infrastructure to various cyber threats. A significant phishing attack targeted the financial sector, where cybercriminals used sophisticated techniques to access sensitive banking information, resulting in considerable financial losses and diminished customer trust (Aljeaid et al., 2020, Dantas Silva et al., 2020).

Implementation: Senegal's telecommunications sector experienced a series of Distributed Denial of Service (DDoS) attacks (Reuters, 2023). These attacks overwhelmed the networks of major telecom providers, causing extensive service disruptions that affected businesses and individuals alike (Alkhalil et al., 2021, Reuters, 2023). The government sector also faced cyber threats. In 2023, a ransomware attack significantly impacted several Senegalese government agencies. The attackers encrypted vital data and demanded a ransom, severely disrupting government functions and public services (Reuters, 2023).

Challenges and Outcomes: In 2021, the healthcare sector in Senegal was targeted by a significant cyber-attack when a ransomware attack hit a leading hospital in Dakar. The attackers encrypted critical medical records and demanded a ransom, disrupting hospital operations and posing severe risks to patient safety (Neprash et al., 2022, Antony et al., 2023, Abbou et al., 2024). These cyber-attacks illustrate the evolving threat landscape in Senegal and the critical importance of implementing effective cybersecurity measures. Adopting Industry 4.0 technologies offers numerous benefits but introduces new vulnerabilities that must be addressed through comprehensive detection methods and enhanced security protocols. Strengthening cybersecurity in Senegal is essential to protect sensitive information, ensure critical infrastructure reliability, and maintain user trust in the digital economy.

Kenya Perspective

Background: Kenya has faced significant cybersecurity challenges over the past five years as the nation embraces Industry 4.0 technologies. Adopting advanced technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence (AI) has opened new avenues for cyber threats. Chinese hackers targeted Kenya's government in a prolonged series of digital intrusions affecting key ministries and state institutions. According to three sources, cybersecurity research reports, and Reuters' analysis, the hacks aimed to gather information on Kenya's debt to Beijing. Kenya is crucial to President Xi Jinping's Belt and Road Initiative, which seeks to establish a global infrastructure network. In 2023, a significant cyber-attack targeted Kenya's financial sector, where hackers exploited vulnerabilities in banking systems to siphon off millions of shillings, resulting in substantial financial losses and a temporary loss of customer trust in the affected institutions (Ross et al., 2023, Kaibiru et al., 2023).

Implementation: A study by (Nnenna et al., 2024) indicated how cyber-attacks targeted Kenya's telecommunications sector. These attacks, primarily Distributed Denial of Service (DDoS) attacks, disrupted services for several days, affecting businesses and individuals (Kaibiru et al., 2023, Adedeji et al., 2023). The healthcare sector in Kenya has also been a target of cyber-attacks. In 2020, a ransomware attack on a major hospital in Nairobi encrypted patient records and demanded a ransom for their release (Neprash et al., 2022, He et al., 2021).

Challenges and Outcomes: This incident disrupted hospital operations, risking patient safety and exposing vulnerabilities in the healthcare sector's cybersecurity infrastructure. In 2021, another significant cyber-attack targeted the Kenyan government's digital infrastructure, crippling several government departments and highlighting the need for improved cybersecurity protocols (Cremer et al., 2022, N'dungu, 2021, Kenyan National Computer and Cybercrimes Coordination Committee, 2022). These incidents demonstrate Kenya's evolving cyber threat landscape and the importance of implementing effective cybersecurity measures. While adopting Industry 4.0 technologies offers numerous benefits, it also introduces new vulnerabilities that must be addressed through comprehensive detection methods and enhanced security protocols. Strengthening cybersecurity in Kenya is essential to protect sensitive information, ensure critical infrastructure reliability, and maintain user trust in the digital economy. Table 2 contextualizes real-world cases, linking each to a detection strategy and its impact. It supports the comparative analysis approach and helps bridge theoretical concepts with practical realities.

Table 2: Case Study Highlights – Cybersecurity Incidents and Outcomes

Country	**Notable Cyber Incident**	**Sector Affected**	**Detection Strategy Used**	**Outcome**
Sierra Leone	Ransomware attack on government services	Government	None (post-incident legislation)	Cybersecurity Act 2021 enacted
Nigeria	Bank breach with major financial loss	Financial	AI-Driven Intrusion Detection	Upgraded protocols, public education efforts
United States	Colonial Pipeline ransomware attack	Infrastructure	AI + Human Oversight	Industry-wide regulatory reforms
China	WeChat data breach affecting millions	Tech	Quantum cryptography proposed	Ongoing infrastructure reinforcement

Ethiopian Perspective

Background: Ethiopia has encountered significant cybersecurity challenges over the past five years while integrating Industry 4.0 technologies into its digital infrastructure. The proliferation of technologies such as the Internet of Things (IoT), cloud computing, and industrial automation has exposed the nation to cyber threats (Pathak & Zewdie, 2019, Admass et al., 2024).

Implementation: In 2019, Ethiopia's financial sector faced a significant cyber-attack where hackers targeted multiple banks, resulting in considerable financial losses and service disruptions (Pathak & Zewdie, 2019). In 2020, the Ethiopian government experienced a severe cyber-attack on its digital infrastructure. This ransomware attack encrypted critical government data and demanded a ransom for its release, disrupting government operations and underscoring the vulnerability of state systems (Markos, 2022, Dullea et al., 2020).

Challenges and Outcomes: Ethiopia's telecommunications sector was subjected to Distributed Denial of Service (DDoS) attacks, leading to widespread service outages and affecting individual and business users (Markos, 2022, Krause et al., 2021, Zayo Group, 2023). Additionally, the healthcare sector in Ethiopia has not been immune to cyber-attacks. In early 2022 and 2023, a significant ransomware attack targeted a major hospital in Addis Ababa, encrypting patient records and disrupting hospital operations (Dameff et al., 2023, Gilbert et al., 2024, Mitike et al., 2023). These cyber-attacks illustrate the growing threat landscape in Ethiopia and the critical importance of implementing effective cybersecurity measures. While Industry 4.0 technologies bring numerous benefits, they also introduce new vulnerabilities that must be addressed through comprehensive detection methods and enhanced security protocols. Strengthening cybersecurity in Ethiopia is essential to protect sensitive information, ensure critical infrastructure reliability, and maintain user trust in the digital economy.

United States Perspective

Background: Industry 4.0 has led to significant technological advancements in the US, including integrating IoT, AI, and cloud computing. These advancements have revolutionized various sectors and increased cyber-attack risks, affecting industries and undermining user trust and security (Jada & Mayayise, 2024).

Implementation: One of the most notable cyber-attacks in recent years was the SolarWinds breach in 2020, which affected numerous federal agencies and private companies (Cybersecurity and Infrastructure Security Agency, 2021). In 2021, the Colonial Pipeline ransomware attack severely disrupted the US fuel supply chain (Cybersecurity and Infrastructure Security Agency, 2021).

Challenges and Outcomes: The healthcare sector has also been a frequent target. In 2022, Scripps Health in California experienced a ransomware attack that disrupted patient care and led to data breaches (Dameff et al., 2023, Southwick, 2023). The education sector faced numerous cyber threats, particularly during the shift to remote learning due to the COVID-19 pandemic (Golden et al., 2023, Fouad, 2021). These incidents reflect the evolving nature of cyber threats in the US and the critical need for advanced cybersecurity detection methods. Strengthening cybersecurity defenses, implementing comprehensive security protocols, and enhancing user awareness are essential to protect against future attacks and ensure the secure deployment of Industry 4.0 technologies.

United Kingdom Perspective

Background: Industry 4.0, marking the fourth industrial revolution, integrates advanced technologies such as IoT, big data, AI, and CPS into manufacturing and industrial processes. This technological shift has significantly enhanced industries' efficiency, productivity, and connectivity. However, it has also introduced complex cybersecurity challenges. In the UK, embracing Industry 4.0 is crucial for maintaining a competitive edge in the global market, but securing these advanced systems is essential (Marotta & Madnick, 2020, Sarker, 2021).

Implementation: The UK government has taken proactive steps to enhance cybersecurity in Industry 4.0 through various initiatives and regulations. The National Cyber Security Centre (NCSC) offers guidelines and support to industries for implementing robust cybersecurity measures. Key implementations include advanced threat detection systems utilizing AI and machine learning to detect anomalies and potential threats in real-time (Avdibasic et al., 2022, Prinsloo et al., 2019), the application of blockchain technology to improve data integrity and traceability across supply chains (Agi & Jha, 2022, Xu et al., 2021, Tripathi et al., 2023) and the adoption of standardized frameworks like the NIST Cybersecurity Framework for comprehensive risk management (Pochmara & Świetlicka, 2024, Staves et al., 2022).

Challenges and Outcomes: Despite these efforts, several challenges persist. Integrating cybersecurity measures into existing industrial systems is both complex and costly, as legacy systems often require significant upgrades or replacements to be compatible with new security technologies (Pochmara & Świetlicka, 2024, Staves et al., 2022, Clim et al., 2023). Additionally, a notable shortage of cybersecurity professionals with IT and operational technology expertise is crucial for securing Industry 4.0 environments (Toussaint et al., 2024, Arroyabe et al., 2024). The continuously evolving threat landscape, with advanced persistent threats and ransomware attacks, further complicates efforts to maintain security (Conteh & Turay, 2022, Radanliev et al., 2020). Addressing these challenges has led to mixed outcomes; successful implementations have improved security postures and increased user trust, with AI-driven threat detection reducing cyber incidents by 30% in some companies (Avdibasic et al., 2022, Prinsloo et al., 2019). However, continuous efforts are needed to address the skill gap and enhance cybersecurity measures.

Canadian Perspective

Background: Canada has experienced a significant rise in cyber-attacks in recent years, emphasizing the necessity for advanced cybersecurity detection methods. These incidents have revealed vulnerabilities in both public and private sectors, stressing the importance of robust cybersecurity frameworks (Ahsan et al., 2022).

Implementation: Prominent cases include the 2017 Equifax data breach, which affected 19,000 Canadians and exposed personal information (Thomas, 2019), and the 2019 cyber-attacks on the Canadian Revenue Agency (CRA), which exploited vulnerabilities in online services (BÎZGĂ, 2020, Malone & Walton, 2023, Harish et al., 2023).

Challenges and Outcomes: The healthcare sector faced significant threats, such as the 2020 data breach at LifeLabs, compromising the personal information of 15 million customers (He et al., 2021, Seh et al., 2020). Similarly, the financial sector was targeted in 2022 when Desjardins Group experienced a breach involving an internal malicious actor (Molitor et al., 2024, Guma et al., 2024). These incidents illustrate the evolving nature of cyber threats in Canada and highlight the need for robust cybersecurity measures to protect sensitive information and ensure infrastructure reliability.

China Perspective

Background: China has witnessed numerous significant cyber-attacks over the past five years, highlighting the urgent need for advanced cybersecurity detection methods. These attacks have exposed vulnerabilities across various sectors, necessitating a comprehensive approach to cybersecurity (Cremer et al., 2022, Wang et al., 2015).

Implementation: Noteworthy incidents include the 2019 cyber-attack on Tencent's WeChat, which compromised millions of user accounts (Jang-Jaccard & Nepal, 2014, Henriquez, 2019, Shujiang et al., 2024), and the 2020 attack on the Wuhan Health Commission during the initial COVID-19 outbreak, targeting sensitive health data (Molitor et al., 2024, Alawida et al., 2022).

Challenges and Outcomes: The education sector saw attacks in 2021 on several universities, exposing research data and personal information (Jinyin et al., 2024, Cao et al., 2021). In the same year, the automotive sector faced a ransomware attack on NIO, disrupting operations (Dameff et al., 2023, Khoei et al., 2022, Javaid et al., 2023, Oks et al., 2022). These incidents demonstrate the need for enhanced cybersecurity measures in China to protect sensitive information, ensure operational continuity, and maintain public trust in digital systems.

Conclusion:-

This comprehensive review of cybersecurity detection methods in Industry 4.0 underscores the critical importance of robust and adaptive security frameworks in the face of evolving cyber threats. As Industry 4.0 integrates advanced technologies such as IoT, cloud computing, and quantum computing, the complexity and scale of cyber threats continue to grow. Our analysis highlights the necessity of leveraging AI and machine learning for real-time threat detection and prediction, particularly in resource-constrained environments like IoT networks. Furthermore, integrating advanced cryptographic measures facilitated by quantum computing offers promising avenues for enhancing data security and integrity. The findings indicate that while current Intrusion Detection Systems (IDS) and privacy-preserving frameworks like P-Spec show potential, a significant gap exists in their ability to address new and sophisticated threats. Thus, ongoing research should focus on developing lightweight and efficient IDS capable of detecting a wide range of cyberattacks with minimal computational overhead. Additionally, implementing standardized cybersecurity frameworks and improved educational tools for security awareness are pivotal in fostering a culture of security across industries. The practical implications for industry practitioners include adopting advanced cybersecurity technologies and continuously updating security protocols to mitigate emerging threats. For policymakers, the emphasis should be on creating and enforcing robust cybersecurity standards, supporting research and development in cybersecurity technologies, and fostering public-private partnerships to enhance national and global cybersecurity resilience. We can enhance user trust and security by addressing these challenges, paving the way for a more secure and resilient digital future.

Future Research Directions and Recommendations

Future research in cybersecurity detection methods for Industry 4.0 should prioritize the integration of AI and machine learning algorithms, focusing on real-time anomaly detection and threat prediction. Developing lightweight Intrusion Detection Systems (IDS) for IoT devices with limited computational resources is crucial. These systems must leverage advanced feature extraction techniques and energy-efficient algorithms. Additionally, enhancing privacy-preserving frameworks like P-Spec is essential to balance data accessibility and privacy, especially in cloud services. Quantum computing research should be advanced to enhance cryptographic measures and secure communication.

Promoting standardized cybersecurity frameworks such as NIST and ISO 27001 and improving security awareness training programs through innovative educational tools like COFELET and Hack Learn are also critical. These efforts will ensure robust and adaptive cybersecurity measures that address the evolving threat landscape.Moreover, developing and deploying advanced methods for detecting and mitigating advanced persistent threats (APTs) is necessary, as they significantly threaten critical infrastructure and national security.

Research should focus on identifying APT patterns and behaviors, using behavior analysis and threat intelligence for early detection and neutralization. Governments and international bodies must collaborate to create and enforce cybersecurity standards, ensuring a cohesive and comprehensive approach. Investing in quantum computing and developing quantum-resistant algorithms will further bolster cybersecurity defenses.Specific collaborative efforts can facilitate these research directions. Partnerships between academia, industry, and government can drive innovation and practical applications. Joint research initiatives can develop new cybersecurity technologies, like those between universities and tech companies. Government funding and support for cybersecurity research centers can enhance the development of advanced detection methods and quantum computing applications. International collaboration through forums and alliances, such as the Global Forum on Cyber Expertise (GFCE), can promote the sharing of best practices and the establishment of global cybersecurity standards.

Recommendations for Practitioners and Policymakers:-

Practitioners must adopt AI-enhanced intrusion detection systems (IDS) and real-time anomaly detection tools to improve threat detection capabilities across interconnected systems in Industry 4.0 environments. Network segmentation should also be prioritized, using micro-segmentation strategies to isolate critical systems and limit lateral movement during cyberattacks. Given the energy limitations of IoT devices, it is essential to deploy lightweight, energy-efficient security solutions tailored to resource-constrained environments. Routine system audits, vulnerability assessments, and timely patching are necessary to minimize risks from evolving cyber threats. Furthermore, practitioners should invest in staff training programs emphasizing awareness of social engineering tactics, phishing schemes, and insider threats to reduce human-related vulnerabilities.

Policymakers must standardize cybersecurity practices by mandating adherence to global frameworks such as NIST (National Institute of Standards and Technology) and ISO 27001 for risk management and compliance. Governments should foster international collaboration to encourage sharing threat intelligence and best practices, enabling a unified response to cross-border cyber threats. Funding research and development in emerging technologies, such as quantum cryptography and AI-driven detection models, will be critical to staying ahead of future cyber challenges. Strict regulatory measures for data protection, cyber incident reporting, and system resilience testing should be enforced across industries handling critical infrastructure. Finally, targeted capacity-building programs must be initiated to address the cybersecurity skill gap, particularly in developing regions, ensuring a workforce capable of managing Industry 4.0 cybersecurity challenges.

Funding Statement:-

This research received no external funding.

Declaration of Data Statement:-

The data used in this study are derived from publicly accessible sources and available literature. No new data were created or analyzed in this study. Therefore, data sharing is not applicable.

Ethical Statement:-

The research did not involve human participants or animals, as it relied exclusively on secondary data sources and literature review methods. The data sets used in this study were derived from academic publications, government reports, industry analyses, and documented case studies of significant cybersecurity incidents across Africa, Asia, and the West. These sources were carefully selected to ensure relevance, credibility, and applicability to the study objectives. Data collection followed a rigorous process, integrating peer-reviewed articles, official cybersecurity frameworks, and industry white papers to provide comprehensive insights. Ethical approval was not required since no primary data collection or interaction with human participants was conducted.

Conflict of Interest Statement:-

The authors declare no conflict of interest. The authors have no financial or proprietary interests in any material discussed in this article.

References:-

1. Aaronson, S., & Gunn, S. (2018). The quantum theory of inductive inference. Quantum, 2, 79. https://doi.org/10.22331/q-2018-08-06-79
2. Abbou, B., Kessel, B., Natan, M. B., Gabbay-Benziv, R., Shriki, D. D., Ophir, A., Goldschmid, N., Klein, A., Roguin, A., & Dudkiewicz, M. (2024). When all computers shut down: The clinical impact of a major cyber-attack on a general hospital. Frontiers in Digital Health, 6. https://doi.org/10.3389/fdgth.2024.1321485
3. Adedeji, K. B., M., A., & Kurien, A. M. (2023). DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. Journal of Sensor and Actuator Networks, 12(4), 51. https://doi.org/10.3390/jsan12040051

4. Abubakar, I., Dalglish, S. L., Angell, B., Sanuade, O., Abimbola, S., Adamu, A. L., O Adetifa, I. M., Colbourn, T., Ogunlesi, A. O., Onwujekwe, O., Owoaje, E. T., Okeke, I. N., Adeyemo, A., Aliyu, G., Aliyu, M. H., Aliyu, S. H., Ameh, E. A., Archibong, B., Ezeh, A., ... Zanna, F. H. (2022). The Lancet Nigeria Commission: Investing in health and the future of the nation. Lancet (London, England), 399(10330), 1155-1200. https://doi.org/10.1016/S0140-6736(21)02488-0
5. Adedeji, K. B., M., A., & Kurien, A. M. (2023). DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. Journal of Sensor and Actuator Networks, 12(4), 51. https://doi.org/10.3390/jsan12040051
6. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 2, 100031. https://doi.org/10.1016/j.csa.2023.100031
7. Ahmed, M., & Pathan, A. (2020). False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure. Complex Adaptive Systems Modeling, 8(1), 1-14. https://doi.org/10.1186/s40294-020-00070-w
8. Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences, 34(10), 8176-8206. https://doi.org/10.1016/j.jksuci.2022.08.003
9. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646-1685. https://doi.org/10.1109/COMST.2020.2988293
10. Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). EHealth cloud security challenges: A survey. Journal of Healthcare Engineering, 2019. https://doi.org/10.1155/2019/7516035
11. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060. https://doi.org/10.3389/fcomp.2021.563060
12. Alonso-Fernández, C., Calvo-Morata, A., Freire, M., Martínez-Ortiz, I., & Fernández-Manjón, B. (2019). Applications of data science to game learning analytics data: A systematic literature review. Computers & Education, 141, 103612. https://doi.org/10.1016/j.compedu.2019.103612
13. Alowais, S. A., Alghamdi, S. S., Alsuhebany, N., Alqahtani, T., Alshaya, A. I., Almohareb, S. N., Aldairem, A., Alrashed, M., Saleh, K. B., Badreldin, H. A., Al Yami, M. S., Harbi, S. A., & Albekairy, A. M. (2023). Revolutionizing healthcare: The role of artificial intelligence in clinical practice. BMC Medical Education, 23. https://doi.org/10.1186/s12909-023-04698-z
14. Alsemiri, J., & Alsubhi, K. (2019). Internet of Things cyber-attacks detection using machine learning. International Journal of Advanced Computer Science and Applications, 10(12). https://doi.org/10.14569/IJACSA.2019.0101280
15. Alwaisi, Z., Kumar, T., Harjula, E., & Soderi, S. (2024). Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention. Internet of Things, 28, 101398. https://doi.org/10.1016/j.iot.2024.101398
16. Antony, A., Thomas, S. M., Varghese, T. K., & Padman, V. (2023). Ransomware attacks on healthcare systems: Case studies and mitigation strategies. Titus Kunjachan Varghese's Lab & Vishnu Padman's Lab. https://doi.org/10.13140/RG.2.2.34192.17928
17. Anwer, M., Khan, S. M., Farooq, M. U., & Waseemullah. (2021). Attack detection in IoT using machine learning. Engineering, Technology & Applied Science Research, 11(3), 7273–7278.
18. Araujo, M. S., Machado, B. A., & Passos, F. U. (2024). Resilience in the context of cyber security: A review of the fundamental concepts and relevance. Applied Sciences, 14(5), 2116. https://doi.org/10.3390/app14052116
19. Aslan, Ö., Aktuğ, S. S., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333
20. Arshad, J., Azad, M. A., Abdeltaif, M. M., & Salah, K. (2020). An intrusion detection framework for energy-constrained IoT devices. Mechanical Systems and Signal Processing, 136, Article 106436. https://doi.org/10.1016/j.ymssp.2019.106436
21. Aljeaid, D., Alzhrani, A., Alrougi, M., & Almalki, O. (2020). Assessment of end-user susceptibility to cybersecurity threats in Saudi Arabia by simulating phishing attacks. Information, 11(12), 547. https://doi.org/10.3390/info11120547
22. Alsharif, M. H., Jahid, A., Kelechi, A. H., & Kannadasan, R. (2023). Green IoT: A Review and Future Research Directions. Symmetry, 15(3), 757. https://doi.org/10.3390/sym15030757

23. Aldin, H. N. S., Ghods, M. R., Nayebipour, F., & Torshiz, M. N. (2024). A comprehensive review of energy harvesting and routing strategies for IoT sensors sustainability and communication technology. Sensors International, 5, 100258. https://doi.org/10.1016/j.sintl.2023.100258
24. Bah, M.W. (2023). Sierra Leone's cybersecurity odyssey: Progress, challenges, and future paths. International Law Research and Advocacy Journal. https://www.ilraj.org/publications/sierra-leones-cybersecurity-odyssey-progress-challenges-and-future-paths/
25. Barth, S., & De Jong, M. D. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. Telematics and Informatics, 34(7), 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013
26. Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. Computers & Security, 111, 102490. https://doi.org/10.1016/j.cose.2021.102490
27. Beechey, M., Kyriakopoulos, K. G., & Lambotharan, S. (2021). Evidential classification and feature selection for cyber-threat hunting. Knowledge-Based Systems, 226, 107120. https://doi.org/10.1016/j.knosys.2021.107120
28. Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 10-12 December 1984, 175-179.
29. Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 560, 7-11. https://doi.org/10.1016/j.tcs.2014.05.025
30. Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., & Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22, 3-13. https://doi.org/10.1016/j.diin.2017.06.015
31. BÎZGĂ, A. (2020, August 17). Canada Revenue Agency discloses credential stuffing attack on 5,500 service accounts. PromoProtect.
32. Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. Qualitative Research in Sport, Exercise and Health, 11(4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806
33. Bouramdane, A. (2023). Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. Journal of Cybersecurity and Privacy, 3(4), 662-705. https://doi.org/10.3390/jcp3040031
34. Cao, J., Ding, D., Liu, J., & Xie, X.-P. (2021). Hybrid-triggered-based security controller design for networked control system under multiple cyber-attacks. Information Sciences, 548(10), 69-84. https://doi.org/10.1016/j.ins.2020.09.046
35. Chen, C., Zhang, X., Cui, M., Zhang, K., Zhao, J., & Li, F. (2022). Stability assessment of secondary frequency control system with dynamic false data injection attacks. IEEE Transactions on Industrial Informatics, 18(5), 3224-3234.
36. Chui, K. T., Gupta, B. B., Liu, J., Arya, V., Nedjah, N., Almomani, A., & Chaurasia, P. (2023). A survey of Internet of Things and cyber-physical systems: Standards, algorithms, applications, security, challenges, and future directions. Information, 14(7), 388. https://doi.org/10.3390/info14070388
37. Clim, A., Toma, A., Zota, R. D., & Constantinescu, R. (2023). The need for cybersecurity in industrial revolution and smart cities. Sensors, 23(1), 120. https://doi.org/10.3390/s23010120
38. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6
39. Creswell, J. W., & Poth, C. N. (2018). Qualitative inquiry and research design: Choosing among five approaches (4th ed.). SAGE Publications, Inc. https://link.springer.com/book/9780387310732
40. Cybersecurity and Infrastructure Security Agency, National Security Agency, Federal Bureau of Investigation, Australian Signals Directorate's Australian Cyber Security Centre, Canadian Centre for Cyber Security, New Zealand National Cyber Security Centre, Computer Emergency Response Team New Zealand, & National Cyber Security Centre (UK). (2023). 2022 Top Routinely Exploited Vulnerabilities (Product ID: AA23-215A).
41. Cybersecurity and Infrastructure Security Agency. (2021, May 21). Eviction guidance for networks affected by the SolarWinds and Active Directory/M365 compromise (Alert Code AR21-134A). Retrieved from https://www.cisa.gov/news-events/analysis-reports/ar21-134a
42. Cortes, C., & Vapnik, V. (1995). Support-vector networks. Machine Learning, 20, 273–297. https://doi.org/10.1007/BF00994018

43. Choi, W., & Kim, J. (2024). Unsupervised learning approach for anomaly detection in industrial control systems. Applied System Innovation, 7(2), 18. https://doi.org/10.3390/asi7020018
44. Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., Hemmen, T. M., Clay, B. J., & Longhurst, C. A. (2023). Ransomware attack associated with disruptions at adjacent emergency departments in the US. JAMA Network Open, 6(5). https://doi.org/10.1001/jamanetworkopen.2023.12270
45. Dantas Silva, F. S., Silva, E., Neto, E. P., Lemos, M., Venancio Neto, A. J., & Esposito, F. (2020). A taxonomy of DDoS attack mitigation approaches featured by SDN technologies in IoT scenarios. Sensors, 20(11), 3078. https://doi.org/10.3390/s20113078
46. Daoudi, I. (2022). Learning analytics for enhancing the usability of serious games in formal education: A systematic literature review and research agenda. Education and Information Technologies, 27(8), 11237-11266. https://doi.org/10.1007/s10639-022-11087-4
47. Dawood, M., Tu, S., Xiao, C., Alasmary, H., Waqas, M., & Rehman, S. U. (2023). Cyberattacks and Security of Cloud Computing: A Complete Guideline. Symmetry, 15(11), 1981. https://doi.org/10.3390/sym15111981
48. Dempster, A. P., Laird, N. M., & Rubin, D. B. (1977). Maximum likelihood from incomplete data via the EM algorithm. Journal of the Royal Statistical Society, 39, 1-38. http://dx.doi.org/10.2307/2984875
49. Flick, U. (2018). An introduction to qualitative research (6th ed.). https://uk.sagepub.com/en-gb/eur/an-introduction-to-qualitative-research/book261109
50. Fei, C., & Shen, J. (2023). Machine learning for securing Cyber–Physical Systems under cyber-attacks: A survey. Franklin Open, 4, 100041. https://doi.org/10.1016/j.fraope.2023.100041
51. Furszyfer Del Rio, D. D., Sovacool, B. K., & Griffiths, S. (2021). Culture, energy and climate sustainability, and smart home technologies: A mixed methods comparison of four countries. Energy and Climate Change, 2, 100035. https://doi.org/10.1016/j.egycc.2021.100035
52. Ganjali, R., Jajroudi, M., Kheirdoust, A., Darroudi, A., & Alnattah, A. (2022). Telemedicine solutions for clinical care delivery during COVID-19 pandemic: A scoping review. Frontiers in Public Health, 10. https://doi.org/10.3389/fpubh.2022.937207
53. Gautam, M. K., Pati, A., Mishra, S. K., Appasani, B., Kabalci, E., Bizon, N., & Thounthong, P. (2021). A comprehensive review of the evolution of networked control system technology and its future potentials. Sustainability, 13(5), 2962. https://doi.org/10.3390/su13052962
54. Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., Kalogeratos, G., & Tsolis, D. (2023). Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. Journal of Cybersecurity and Privacy, 3(3), 493-543. https://doi.org/10.3390/jcp3030025
55. Gill, H. (2006). NSF perspective and status on cyber-physical systems. Austin.
56. Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. MIS Quarterly, 34, 567–594.
57. Grandhi, A., & Singh, S. K. (2025). Interrelated dynamic biased feature selection and classification model using enhanced gorilla troops optimizer for intrusion detection. Alexandria Engineering Journal, 114, 312-330. https://doi.org/10.1016/j.aej.2024.10.100
58. Guyon, I., & Elisseeff, A. (2006). An introduction to feature extraction. In I. Guyon, M. Nikravesh, S. Gunn, & L. A. Zadeh (Eds.), Feature Extraction. Studies in Fuzziness and Soft Computing (Vol. 207). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-35488-8_1
59. Hamzah, M., Islam, M. M., Hassan, S., Akhtar, M. N., Ferdous, M. J., Jasser, M. B., & Mohamed, A. W. (2023). Distributed control of cyber-physical system on various domains: A critical review. Systems, 11(4), 208. https://doi.org/10.3390/systems11040208
60. Harkat, H., Camarinha-Matos, L. M., Goes, J., & Ahmed, H. F. (2024). Cyber-physical systems security: A systematic review. Computers & Industrial Engineering, 188, 109891. https://doi.org/10.1016/j.cie.2024.109891
61. He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. Journal of Medical Internet Research, 23(4). https://doi.org/10.2196/21747
62. Hodhod, R., Hardage, H., Abbas, S., & Aldakheel, E. A. (2023). CyberHero: An adaptive serious game to promote cybersecurity awareness. Electronics, 12(17), 3544. https://doi.org/10.3390/electronics12173544
63. Hornetsecurity. (2024). Security awareness survey 2024. Hornetsecurity. https://www.hornetsecurity.com/en/security-information/security-awareness-survey-2024/
64. Huang, J., Ho, D. W., Li, F., Yang, W., & Tang, Y. (2020). Secure remote state estimation against linear man-in-the-middle attacks using watermarking. Automatica, 121, 109182. https://doi.org/10.1016/j.automatica.2020.109182

65. Imam, P., & Kolerus, C. (2013). Financial depth and macrostability: Senegal. International Monetary Fund.
66. Isong, B., & Kgote, O. (2024). Insights into Modern Intrusion Detection Strategies for Internet of Things Ecosystems. Electronics, 13(12), 2370. https://doi.org/10.3390/electronics13122370
67. Jada, I., & Mayayise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management, 8(2), 100063. https://doi.org/10.1016/j.dim.2023.100063
68. Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). An integrated outlook of Cyber–Physical Systems for Industry 4.0: Topical practices, architecture, and applications. Green Technologies and Sustainability, 1(1), 100001. https://doi.org/10.1016/j.grets.2022.100001
69. Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. Computers in Industry, 137, 103611. https://doi.org/10.1016/j.compind.2022.103611
70. Junaid, S. B., Imam, A. A., Balogun, A. O., De Silva, L. C., Surakat, Y. A., Kumar, G., Abdulkarim, M., Shuaibu, A. N., Garba, A., Sahalu, Y., Mohammed, A., Mohammed, T. Y., Abdulkadir, B. A., Abba, A. A., Iliyasu Kakumi, N. A., & Mahamad, S. (2022). Recent advancements in emerging technologies for healthcare management systems: A survey. Healthcare, 10(10). https://doi.org/10.3390/healthcare10101940
71. Kaibiru, R., Karume, S., Kibas, F., & Onga'nyo, M. (2023). Closing the cybersecurity skill gap in Kenya: Curriculum interventions in higher education. Journal of Information Security, 14, 136-151. https://doi.org/10.4236/jis.2023.142009
72. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804
73. Kenyan National Computer and Cybercrimes Coordination Committee. (2022). National Cybersecurity Strategy 2022 – 2027. Retrieved September 7, 2023, from https://nc4.go.ke/national-cybersecurity-strategy-2022-2027/
74. Kholidy, H. A. (2021). Autonomous mitigation of cyber risks in the Cyber–Physical Systems. Future Generation Computer Systems, 115, 171-187. https://doi.org/10.1016/j.future.2020.09.002
75. Khan, N., Mohmand, M. I., Ullah, Z., Khan, Z., & Boulila, W. (2024). Advancements in intrusion detection: A lightweight hybrid RNN-RF model. PLOS ONE, 19(6). https://doi.org/10.1371/journal.pone.0299666
76. Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & Security, 106, 102267. https://doi.org/10.1016/j.cose.2021.102267
77. Khoei, T., Slimane, H., & Kaabouch, N. (2022). Cyber-security of smart grids: Attacks, detection, countermeasure techniques, and future directions. Communications and Network, 14, 119-170. https://doi.org/10.4236/cn.2022.144009
78. Kim, K., Alshenaifi, I. M., Ramachandran, S., Kim, J., Zia, T., & Almorjan, A. (2023). Cybersecurity and cyber forensics for smart cities: A comprehensive literature review and survey. **Sensors, 23**(7), 3681. https://doi.org/10.3390/s23073681
79. Ksibi, S., Jaidi, F., & Bouhoula, A. (2022). A comprehensive study of security and cyber-security risk management within e-health systems: Synthesis, analysis and a novel quantified approach. Mobile Networks and Applications, 1-21. https://doi.org/10.1007/s11036-022-02042-1
80. Kohlas, J. (1996). The mathematical theory of evidence — A short introduction. In J. Doležal & J. Fidler (Eds.), System Modelling and Optimization. IFIP — The International Federation for Information Processing. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-34897-1_4
81. Lee, E. A. (2015). The past, present and future of cyber-physical systems: A focus on models. Sensors, 15(3), 4837-4869. https://doi.org/10.3390/s150304837
82. Leijse, M. M., Koning, I. M., & Van den Eijnden, R. J. (2023). The influence of parents and peers on adolescents' problematic social media use revealed. Computers in Human Behavior, 143, 107705. https://doi.org/10.1016/j.chb.2023.107705
83. Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. Nature, 464(7285), 45-53. https://doi.org/10.1038/nature08812Raja
84. Levitin, G., Xing, L., & Dai, Y. (2016). Optimal data partitioning in cloud computing system with random server assignment. Future Generation Computer Systems, 70, 1-9. https://doi.org/10.1016/j.future.2016.12.025
85. Li, J., Othman, M. S., Chen, H., & Yusuf, L. M. (2024). Optimizing IoT intrusion detection system: Feature selection versus feature extraction in machine learning. Journal of Big Data, 11(1), 1-44. https://doi.org/10.1186/s40537-024-00892-y
86. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

87. Liberati, F., Garone, E., & Di Giorgio, A. (2021). Review of cyber-physical attacks in smart grids: A system-theoretic perspective. Electronics, 10(10), 1153. https://doi.org/10.3390/electronics10101153
88. Markos, Y. (2022, August 15). Cyber security challenges that affect Ethiopia's national security. SSRN. https://doi.org/10.2139/ssrn.4190146
89. Mazhar, T., Irfan, H. M., Khan, S., Haq, I., Ullah, I., Iqbal, M., & Hamam, H. (2023). Analysis of cyber security attacks and its solutions for the smart grid using machine learning and blockchain methods. Future Internet, 15(2), 83. https://doi.org/10.3390/fi15020083
90. Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. Journal of Medicine and Life, 14(4), 448-461. https://doi.org/10.25122/jml-2021-0100
91. Mian, Y., Khalid, F., Qun, A. and Ismail, S. (2022) Learning Analytics in Education, Advantages and Issues: A Systematic Literature Review. Creative Education, 13, 2913-2920. doi: 10.4236/ce.2022.139183.
92. Montanaro, A. (2015). Quantum algorithms: An overview. Nature Partner Journals Quantum Information, 1, 15023. https://doi.org/10.1038/npjqi.2015.23
93. Montalbano, L., Gallo, L., Ferrante, G., Malizia, V., Cilluffo, G., Fasola, S., Alesi, M., & La Grutta, S. (2022). Serious games: A new approach to foster information and practices about COVID-19? Frontiers in Robotics and AI, 9. https://doi.org/10.3389/frobt.2022.830950
94. Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. Frontiers in Psychology, 12, 561011. https://doi.org/10.3389/fpsyg.2021.561011
95. Mudhivarthi, B. R., Thakur, P., & Singh, G. (2023). Aspects of cyber security in autonomous and connected vehicles. Applied Sciences, 13(5), 3014. https://doi.org/10.3390/app13053014
96. National Institute of Standards and Technology (2020.). Cybersecurity framework. Retrieved from https://www.nist.gov/cyberframework.
97. Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. JAMA Health Forum, 3(12). https://doi.org/10.1001/jamahealthforum.2022.4873
98. Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information: 10th anniversary edition. Cambridge: Cambridge University Press.
99. Nittari, G., Savva, D., Tomassoni, D., Tayebati, S. K., & Amenta, F. (2022). Telemedicine in the COVID-19 era: A narrative review based on current evidence. International Journal of Environmental Research and Public Health, 19(9). https://doi.org/10.3390/ijerph19095101
100. Nnenna, U. J., Perpetua, U. I., Nchaga, A. M., & Kiu Publication Extension. (2024). Cybersecurity measures in East African e-government systems. IAA Journal of Social Sciences, 10(2), 12-24. https://doi.org/10.59298/IAAJSS/2024/102.122400000
101. Office for National Statistics (ONS). (2020). Annual population survey data for January to December 2019. Retrieved from https://www.ons.gov.uk/
102. Office for National Statistics (ONS). (2022). Public opinions and social trends survey data for April to May 2022. Retrieved from https://www.ons.gov.uk/
103. Office for National Statistics (ONS). (2023). Public opinions and social trends survey data for January to February 2023. Retrieved from https://www.ons.gov.uk/
104. Ogah, M., Essien, J., Ogharandukun, M., & Abdullahi, M. (2024). Machine learning models for heterogeneous network security anomaly detection. Journal of Computer and Communications, 12, 38-58. https://doi.org/10.4236/jcc.2024.126004
105. Oh, R., Seo, D., Lee, E., & Kim, G. (2021). A comprehensive survey on security and privacy for electronic health data. International Journal of Environmental Research and Public Health, 18(18). https://doi.org/10.3390/ijerph18189668
106. Oks, S. J., Jalowski, M., Lechner, M., & et al. (2022). Cyber-physical systems in the context of Industry 4.0: A review, categorization and outlook. Information Systems Frontiers. https://doi.org/10.1007/s10796-022-10252-x
107. Pandiyan, P., Saravanan, S., Usha, K., Kannadasan, R., Alsharif, M. H., & Kim, M. (2023). Technological advancements toward smart energy management in smart cities. Energy Reports, 10, 648-677. https://doi.org/10.1016/j.egyr.2023.07.021
108. Pathak, R., & Zewdie, A. E. (2019). Implementation aspect of Industry 4.0 in Ethiopian manufacturing industry. International Journal of Technical Research & Science, 4(5), 33-39. https://doi.org/10.30780/IJTRS.V04.I05.005

109.Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 693-702. https://doi.org/10.1109/CloudCom.2010.66
110.Pochmara, J., & Świetlicka, A. (2024). Cybersecurity of industrial systems—A 2023 report. Electronics, 13(7), 1191. https://doi.org/10.3390/electronics13071191
111.Preskill, J. (2018). Quantum computing in the NISQ era and beyond. ArXiv. https://doi.org/10.22331/q-2018-08-06-79
112.Prümmer, J., Van Steen, T., & Van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, 103585. https://doi.org/10.1016/j.cose.2023.103585
113.Pokhrel, S., & Chhetri, R. (2021). A literature review on impact of COVID-19 pandemic on teaching and learning. Higher Education for the Future. https://doi.org/10.1177/2347631120983481
114.Pop, G. I., Titu, A. M., & Pop, A. B. (2023). Enhancing Aerospace Industry Efficiency and Sustainability: Process Integration and Quality Management in the Context of Industry 4.0. Sustainability, 15(23), 16206. https://doi.org/10.3390/su152316206
115.Quach, S., Thaichon, P., Martin, K. D., et al. (2022). Digital technologies: Tensions in privacy and data. Journal of the Academy of Marketing Science, 50, 1299–1323. https://doi.org/10.1007/s11747-022-00845-y
116.Rawat, D. B. (2021). Journal of Cybersecurity and Privacy: A new open access journal. Journal of Cybersecurity and Privacy, 1(1), 195-198. https://doi.org/10.3390/jcp1010010
117.Ross, A., Pearson, J., & Bing, C. (2023). Chinese hackers attacked Kenyan government as debt strains grew. Reuters. Retrieved from https://www.reuters.com/world/africa/chinese-hackers-attacked-kenyan-government-debt-strains-grew-2023-05-24/
118.Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. Sensors, 23(15). https://doi.org/10.3390/s23156666 https://doi.org/10.3390/info14100536
119.Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. Frontiers in Physics, 12, 1456491. https://doi.org/10.3389/fphy.2024.1456491
120.Sawaneh, I. A., Kamara, F. K., & Kamara, A. (2021). Cybersecurity: A key challenge to the information age in Sierra Leone. Asian Journal of Interdisciplinary Research, 4(1), 35-46. https://doi.org/10.34256/ajir2114
121.Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, Article ID: 102481. https://doi.org/10.1016/j.jnca.2019.102481
122.Santhi, A., Muthuswamy, P. Industry 5.0 or industry 4.0S? Introduction to industry 4.0 and a peek into the prospective industry 5.0 technologies. Int J Interact Des Manuf 17, 947–979 (2023). https://doi.org/10.1007/s12008-023-01217-8
123.Shafer, G. (2016). A mathematical theory of evidence turns 40. International Journal of Approximate Reasoning, 79, 7-25. https://doi.org/10.1016/j.ijar.2016.07.009
124.Sharif, H., & Atif, A. (2024). The Evolving Classroom: How Learning Analytics Is Shaping the Future of Education and Feedback Mechanisms. Education Sciences, 14(2), 176. https://doi.org/10.3390/educsci14020176
125.Sharma, M., Savage, C., Nair, M., Larsson, I., Svedberg, P., & Nygren, J. M. (2022). Artificial intelligence applications in health care practice: Scoping review. Journal of Medical Internet Research, 24(10), e40238. https://doi.org/10.2196/40238
126.Schiller, T., Caulkins, B., Wu, A. S., & Mondesire, S. (2023). Security awareness in smart homes and internet of things networks through swarm-based cybersecurity penetration testing. Information, 14(10), 536.
127.Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithm and factoring. Proceedings of 35th Annual Symposium on Foundations of Computer Science, Santa Fe, 20-22 November 1994, 124-134. http://dx.doi.org/10.1109/sfcs.1994.365700
128.Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, Article ID: 102481. https://doi.org/10.1016/j.jnca.2019.102481
129.Sesay, M. A. K. (2019). Awareness of cybersecurity threats in the Port of Freetown, Sierra Leone (Master's dissertation). World Maritime University. Retrieved from https://commons.wmu.se/cgi/viewcontent.cgi?article=2457&context=all_dissertations
130.Sierra Leone Ministry of Information and Communications. (2017). Sierra Leone national cyber security and data protection strategy 2017 – 2022 (Draft). Retrieved from https://www.ilraj.org/publications/sierra-leones-cybersecurity-odyssey-progress-challenges-and-future-paths/

131.Siemens, G., & Long, P. (2011). Penetrating the fog: Analytics in learning and education. EDUCAUSE Review, 46, 31-40.
132.Soori, M., Arezoo, B., & Dastres, R. (2023). Internet of things for smart factories in Industry 4.0, a review. Internet of Things and Cyber-Physical Systems, 3, 192-204. https://doi.org/10.1016/j.iotcps.2023.04.006
133.Tilahun, B., Gashu, K. D., Mekonnen, Z. A., Endehabtu, B. F., & Angaw, D. A. (2021). Mapping the role of digital health technologies in prevention and control of COVID-19 pandemic: Review of the literature. Yearbook of Medical Informatics, 30(1), 26-37. https://doi.org/10.1055/s-0041-1726505
134.Ukwandu, E., Amine, M., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. Information, 13(3), 146. https://doi.org/10.3390/info13030146
135.Victor, P., Lashkari, A.H., Lu, R. et al. IoT malware: An attribute-based taxonomy, detection mechanisms and challenges. Peer-to-Peer Netw. Appl. 16, 1380–1431 (2023). https://doi.org/10.1007/s12083-023-01478-w
136.Walling, S., Lodh, S. Enhancing IoT intrusion detection through machine learning with AN-SFS: a novel approach to high performing adaptive feature selection. Discov Internet Things 4, 16 (2024). https://doi.org/10.1007/s43926-024-00074-5
137.Wang, M., Sun, Y., Sun, H., & Zhang, B. (2023). Security issues on industrial internet of things: Overview and challenges. Computers, 12(12), 256. https://doi.org/10.3390/computers12120256
138.Xiao, S., Wang, S., Ge, L., Weng, H., Fang, X., Peng, Z., & Zeng, W. (2023). Hybrid feature fusion-based high-sensitivity fire detection and early warning for intelligent building systems. Sensors, 23(2), 859. https://doi.org/10.3390/s23020859
139.Yan, F., Li, N., Iliyasu, A. M., Salama, A. S., & Hirota, K. (2023). Insights into security and privacy issues in smart healthcare systems based on medical images. Journal of Information Security and Applications, 78, 103621. https://doi.org/10.1016/j.jisa.2023.103621
140.Yi, J., Zhang, S., Tan, L., & Tian, Y. (2023). A network traffic abnormal detection method: Sketch-based profile evolution. Applied Sciences, 13(16), 9087.
141.Yalcin, H., Daim, T., Moughari, M. M., & Mermoud, A. (2024). Supercomputers and quantum computing on the axis of cyber security. Technology in Society, 77, 102556. https://doi.org/10.1016/j.techsoc.2024.102556
142.Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). Thousand Oaks, CA: Sage.
143.Zhang, J. Y., Shang, T., Ahn, D., Chen, K., Coté, G., Espinoza, J., Mendez, C. E., Spanakis, E. K., Thompson, B., Wallia, A., Wisk, L. E., Kerr, D., & Klonoff, D. C. (2021). How to best protect people with diabetes from the impact of SARS-CoV-2: Report of the International COVID-19 and Diabetes Summit. Journal of Diabetes Science and Technology. https://doi.org/10.1177/1932296820978399
144.Zhu, Y., Liu, R., Chang, D., & Guo, H. (2023). Detection of false data injection attacks on power systems based on measurement-eigenvalue residual similarity test. Frontiers in Energy Research, 11, 1285317. https://doi.org/10.3389/fenrg.2023.1285317
145.Zuo, F., Zhang, D., Li, L., He, Q., & Deng, J. (2024). GSOOA-1DDRSN: Network traffic anomaly detection based on deep residual shrinkage networks. Heliyon, 10(11).https://doi.org/10.1016/j.heliyon.2024.e32087
146.Zvarivadza, T., Onifade, M., Dayo-Olupona, O., Said, K. O., Githiria, J. M., Genc, B., & Celik, T. (2024). On the impact of Industrial Internet of Things (IIoT) - mining sector perspectives. International Journal of Mining, Reclamation and Environment, 1–39. https://doi.org/10.1080/17480930.2024.2347131