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

Cyber Security Frameworks through the Lens of Foreign Direct Investment (FDI): A Systematic Literature Review

Vaidyanathan R. Iyer[1], Dr. Kishore Babu[2], Dr. Vignesh Ram Guruswamy[3]

Submitted: 05/09/2023 **Revised:** 21/10/2023 **Accepted:** 06/11/2023

Abstract: Cybersecurity is an essential aspect for businesses to safeguard themselves against cyber-attacks and ensure the protection, confidentiality, integrity, and availability of sensitive data. A strong cybersecurity posture can increase business resilience and minimize the risk of costly security breaches, thereby building trust with investors, customers, and partners. This, in turn, can create a competitive advantage that attracts foreign direct investment (FDI) and fuels business growth. Therefore, the interplay between cybersecurity frameworks and FDI is of paramount importance. This paper aims to explore the existing research on this interplay through a systematic literature review methodology and qualitative synthesis of data. The review found that a robust cybersecurity framework is crucial for building trust and confidence among investors, customers, and partners, which can help attract FDI and foster business growth across critical infrastructures and sectors. The review critically assessed different cybersecurity frameworks and their implementation strategies and identified potential research gaps while proposing possible solutions to address them. The study underscores the need for critical infrastructures to implement a comprehensive Cyber Assurance Framework that can help them identify and manage cybersecurity risks effectively. Additionally, the importance of adopting new cybersecurity technologies and practices that align with emerging technology-based threats due to the growth of Cloud, IoT, Artificial Intelligence, and Machine Learning was highlighted. Policymakers and regulatory bodies should also work together to establish a clear and robust Cyber Assurance Framework and Policy that provides guidance and support to businesses in their cybersecurity efforts. This paper is the first to provide valuable insights for businesses, policymakers, and regulatory bodies on the importance of a cybersecurity framework in attracting FDI and fostering long-term business growth. The findings of this review would aid policymakers and regulatory bodies in informing their policy decisions and providing guidance and support to businesses in their cybersecurity efforts.

Keywords: *cyber security frameworks (CSF), foreign direct investment (FDI), policy, governs, critical infrastructure*

1. Introduction:

Foreign Direct Investment (FDI) can be defined as an investment made by a company or entity based in one country into a company or entity situated in a different country. The factors that can influence a country's FDI level receives include economic stability and growth, market size, lawfulness and political stability, infrastructure, labor force, government policies and incentives, access to regional markets, natural resources, digital infrastructure, environmental and social policies, innovation and research and development, intellectual property rights, and cybersecurity. Recently, it has been observed that factors like digital infrastructure, intellectual property rights, and cybersecurity have a substantial impact on FDI.

The global FDI flows had a strong rebound in the first half of 2022, reaching USD 972 billion. However, during the second quarter of 2022, there was a substantial decrease of 22% in FDI compared to the previous quarter, primarily due to geopolitical factors. According to the Organization for Economic Co-operation and Development (OECD), the United States was the top recipient of FDI globally, followed by China and Brazil. FDI plays a crucial role in creating an open and efficient global economy and driving development. However, the advantages of FDI do not always reach all countries, industries, and regions equally. To increase FDI in developing countries and to completely benefit from it, it's essential for nations to have sound policies in place and for the global investment framework to be supportive. The main challenges lie with the host countries, which must have a clear and comprehensive policy environment that encourages investment and develop the necessary human and institutional resources to put these policies into action.

India has seen a steady increase in foreign direct investment (FD I) inflows in recent years, reaching a

[1]*Research Scholar, Department of Management, KL University, Guntur, Andhra Pradesh 522302, India*
[2]*Dean Management Humanities & Science, KL University, Guntur, Andhra Pradesh 522302, India*
[3]*Assistant Professor, Department of Geopolitics and International Relations, Manipal Academy of Higher Education (MAHE), Manipal, Karnataka 576104, India*
Correspondence should be addressed to Vaidyanathan R Iyer; vaidy20221@yahoo.com

historic high of $74.39 billion in 2020-2021. According to the Reserve Bank of India Governor Shaktikanta Das, the net foreign direct investment (FDI) in India reached USD 22.7 billion in the period between April and October 2022. This represents an increase from the USD 21.3 billion seen in the same period the previous year. This growth in FDI is a positive sign for India's economy. The government of India has implemented various measures to attract foreign investment, including liberalizing FDI rules in sectors such as retail, aviation, and insurance. Information Technology, Telecommunications, and Construction Development sector were the major sectors that attracted the highest foreign inflows. Some of the major contributors to FDI in India are Singapore, the United States, Japan, the United Kingdom, and the Netherlands. The main sectors that have attracted FDI in India include services, telecommunications, construction development, computer software and hardware, and power.

In recent years, advancements in digital technology have had an important effect on FDI. The expansion of digital infrastructure and the development of new technologies have facilitated companies' ability to reach new customers and expand into new markets, resulting in a growth of investment in these areas. Digitalization of business processes has made it easier for companies to operate remotely, meaning that investment decisions are increasingly based on factors such as access to talent and favorable regulatory environments. Digital technologies have increased competition in many industries and have led to an increase in cross-border M&A activity in digital and technology sectors. As the digitalization of business process and technology increases, so does the potential for cyber-attacks and data breaches, which can lead to increased concerns and investment in cybersecurity measures. According to data on cybersecurity, the total amount of damages inflicted by hackers is predicted to exceed $6 trillion in 2022. A worldwide cyberattack occurs every 39 seconds. In the entire world, a ransomware attack happens every 14 seconds (Barry, Görg, & Strobl, 2003).

The globalization era has seen a growing reliance on modern information networks for FDI carried out by multinational companies (Dunning, 1999). The network of a host nation infrastructure can offer advantages such as reduced international communication costs, reduced barriers to entry in foreign markets, and improved economic efficiency through enhanced social oversight and transparency, making it an attractive option for foreign investors (Narula, 2018). However, there is limited research on the role the internet plays in supporting FDI and, in particular, how internet security impacts FDI (Gorg and Strobl, 2020). Internet security is a crucial matter, especially for companies engaging in international business, as cyber threats like hacking, network fraud, and credit breaches can lead to significant financial losses and impact various industries. This is because cyber technologies have had a major impact on the way businesses operate in the internet era (Narula and Dunning, 2019).

Cybersecurity is a field concerned with safeguarding computer systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction (Kshetri, 2018). This can be accomplished through the implementation of technical and organizational measures to prevent cyberattacks and other malicious activities. The Cybersecurity Framework, also referred to as the NIST Cybersecurity Framework, is a collection of recommended procedures and standards formulated by the National Institute of Standards and Technology (NIST) in the United States. These guidelines aim to assist organizations in managing cybersecurity risks and enhancing the safety and robustness of their systems (National Institute of Standards and Technology, 2014). The NIST Cybersecurity Framework was developed as a reaction to Executive Order 13636 (The White House, 2013), which called for the development of a framework to improve critical infrastructure cybersecurity. The objective of this framework is to provide a common language and approach for managing cybersecurity risks and enhance the overall security and stability of critical infrastructure. The importance of cyber security is to provide Protection of sensitive information, Compliance with regulations, Avoidance of financial losses, Ensuring business continuity, Protection of national security (Kshetri, 2018).

This paper aims to achieve the following

- To critically review the literature on the cyber security frameworks and the implementation of various cyber security frameworks
- To identify existing research on the correlations between FDI and cyber security in various sectors.
- To identify gaps in knowledge and areas for future research on the relationship between cyber security and FDI.
- To provide insights into the interplay between cyber assurance and FDI that can inform policy and decision-making in the area of foreign investment and cyber security.
- To examine the studies from various disciplines such as computer science, business, economics and management to provide a comprehensive view of the literature

2. Related Works:

- Tissir, Kafhali, and Aboutabit (2021) introduced a methodology for handling and avoiding cyber threats in Cloud Computing that draws on ISO and NIST standards. The framework offers direction to

organizations on how to create or enhance their cyber risk management practices in the cloud computing environment. The study also outlines criteria for evaluating the development of organizations that adopt the framework.

- Krumay, Bernroider, and Walser (2018) found imbalances in the academic literature on cybersecurity metrics and controls and the NIST framework. The research suggested future academic research should focus more on incident detection, response, and recovery and NIST should expand into areas such as natural disasters, monetary considerations, and organizational culture. The European Union has established a directive for cybersecurity that adopts the principles of the NIST Cybersecurity Framework and mandates critical infrastructure organizations to frequently assess and report on their cybersecurity progress.
- Taherdoost (2022) analyzed various cybersecurity standards and frameworks to assist organizations in selecting the most suitable for their specific cybersecurity needs. The review offered a thorough understanding of the available options, drawing on existing research and real-world application in various industries, to help organizations make informed decisions.
- Azmi et al. (2018) streamlined various viewpoints on cybersecurity frameworks (CSFs) by comparing their different objectives and uncovering shared concepts. They divided the frameworks into four categories: promoted action, driver, framework environment, and audience and uncovered three common elements: shared actions, cyber pillars, and framework life cycle. Additionally, the study recognized three key processes for safeguarding cyberspace: profiling, delivering, and assuring.

There are numerous review papers published related to cybersecurity and cybersecurity frameworks, however there is not any paper relating to cybersecurity with FDI.

3. Review Methodology:

We conducted a systematic and thorough examination of existing literature on cyber security frameworks and FDI. We used a qualitative review methodology to identify and summarize the existing knowledge on a given topic.

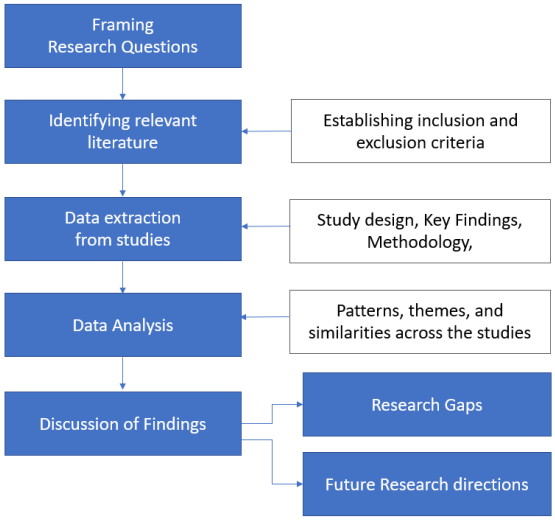

Fig 1: Workflow of the paper

The process typically begins with developing a research question and identifying relevant databases and sources to search for literature. Selection criteria have been established to ensure that only studies that are pertinent are included in the analysis. Once the studies are identified, they are critically evaluated for their quality, relevance, and applicability to the research question. The data is then extracted and analysed to identify patterns, trends, and gaps in the literature. The results are then reported and discussed in relation to the research question as shown below.

Research Questions:

1. How does the level of cyber security affect foreign direct investment (FDI) in different sectors, and what are the key factors that drive this relationship?
2. What are the existing cyber security frameworks, and what are the key elements and implementation strategies of these frameworks?
3. What are the key gaps in knowledge and areas for future research on the connection between cyber security and FDI, and how can these be addressed to inform policy and decision-making in this area?

Table 1: Search Keywords:

Terms	Search Strings
Cybersecurity frameworks + FDI	"Cybersecurity frameworks" & "FDI investment", "Cybersecurity" & "FDI investment", "Cybersecurity frameworks" & "FDI investment decisions"
NIST CSF	"Implementation of NIST CSF", "NIST CSF" & "Critical infrastructure"
ISO 27001	"Implementation of ISO 27001", "ISO 27001" & "Critical infrastructure"
COBIT, SOC, HIPAA and others	"Implementation of COBIT", "Implementation of SOC", "Implementation of HIPAA, "Implementation of others", "COBIT",

	"SOC", "HIPAA", "others" & "Critical infrastructure"

A total of 42 papers have been included in the final review and analysed.

4. Data Synthesis

4.1 **Cyber Security and FDI**:

The German Federal Ministry for Economic Affairs and Energy (FMEA) has recently increased its scrutiny of mergers and acquisitions (BLOMSTEIN, 2020), with a specific focus on cybersecurity, due to the implementation of the EU's FDI Screening Regulation and the strengthened FDI screening framework in Germany. This increased attention to the interplay between foreign investment and cybersecurity highlights the growing importance of finding a balance between the two in today's interconnected global economy. Studies have shown that various factors, including political, economic, legal, cultural, and infrastructure, can influence a country's ability to attract foreign investment (Hajdini, 2015). In order to strike a balance between national security and economic interests, researchers Graham and Marchick (2006) have suggested changes to the Exon-Florio provisions of US law.

In response to the increased demand for secure investments, organizations like FieldComm Group (2017) have taken steps to enhance cybersecurity measures, such as updating the FDI Technical Specifications to include UIP sandboxing and time stamping for device package signatures. Pearson (2019) has also emphasized the need for Sri Lanka to improve its cybersecurity environment in order to attract foreign investment, calling for increased funding, legislation, policy initiatives, and public awareness to address the issue. Governments around the world are placing greater importance on electronic security and national security risks in their evaluations of foreign investment, particularly in fields such as AI and cybersecurity. For example, the UK and Canada assess potential access to sensitive information and national security risks as part of their review process, while Germany has broadened its foreign investment evaluation to encompass new forms of electronic warfare (CAPOBIANCO, 2022).

Cristani (2019) conducted a comprehensive study of the cybersecurity challenges faced by foreign companies and their regulatory protection across the world, including in the EU, the Visegrad Four sub-region, and Slovakia. Cristani also evaluated the stakeholders involved in governing foreign investment's cybersecurity and assessed the feasibility of establishing a governance system at the EU and V4 levels. Due to the increased scrutiny of mergers and acquisitions, including cybersecurity, by the German Federal Ministry for Economic Affairs and Energy, reflects the growing global concern of balancing foreign investment with cyber security. As technology continues to advance and interconnected economies become increasingly reliant on secure investments, it is essential for governments and organizations to take steps to address and mitigate cyber risks. Some of the recent research efforts in relation to cyber security and FDI are discussed in the following Table. 2

Table 2: Relation to cyber security and FDI

Author	Key Findings
Huang et al. (2021)	The importance of internet security is substantial in the decision-making process of Chinese companies when investing abroad, as it significantly boosts Chinese foreign direct investment in the destination country.
Topping et al. (2021)	A comprehensive classification system and comprehensive, both general and industry-specific, guidelines are necessary for effective mitigation of supply chain risks in Cyber Supply Chain Risk Management (C-SCRM).
Kok and Ersoy (2009)	Attracting FDI brings significant domestic governance challenges that must be addressed
Contractor et al. (2020)	Examines the correlation between the country's regulations and business atmosphere and how it affects the inflow of FDI
Javorcik (2004)	Regions with stronger IPR protection tend to attract more FDI, particularly in the form of equity investments
Haudi et al. (2020)	Economic and political stability, market size, and availability of skilled labor are some of the most vital factors in attracting FDI
Brada et al. (2021)	On average, countries with stronger investor protection tend to attract more FDI
Bayar et al. (2021)	The presence of a shadow economy tends to decrease foreign investment
Hayakawa et al. (2021)	Certain risk factors in a country can negatively affect foreign direct investment
Nondo, Kahsai, and Hailu (2016)	A strong institutional structure can have a positive effect on attracting foreign investment.
Osemwengie and Oriakhi (2012)	The level of FDI in Nigeria is negatively impacted by the prevailing state of insecurity in the country.
Lee et al. (2017)	More investments from MNCs are made when the Internet infrastructure of the host nation is advanced.
Trope and Smedinghoff (2017)	Cybersecurity due diligence review to the start of any proposed M&A deal
Jeong et al. (2019)	Information security breaches can negatively impact competitiveness

Arcuri et al. (2018)	Stock returns are negatively impacted by breaches in information security.

The studies suggested that internet security and cyber supply chain risk management are important factors for attracting FDI, and that host countries should prioritize creating a secure and trustworthy business environment to attract FDI. Additionally, the studies suggest that regulations and policies play an essential role in attracting FDI and that it's important for countries to address issues that can impact foreign investors and society as a whole. It's also highlighted that protecting intellectual property rights can attract more FDI. The overall factors affecting FDI investment attraction (w.r.t cybersecurity frameworks) are illustrated in the following Fig.2

Fig 2: Cybersecurity related factors affecting FDI attraction

Evaluating the implementation and effectiveness of cybersecurity policies in different countries or different sectors and how they are relating to FDI is not given attention in the previous studies. The limk between FDI and cybersecurity in emerging economies: The studies provided focused on developed economies, however examining the relationship between FDI and cybersecurity in emerging economies has been ignored, which may have different regulatory environments and business practices.

4.2. **CYBER SECURITY FRAMEWORKS:**

Cyber threats have become increasingly sophisticated and severe in recent years. With the rise of the internet, IoT devices, cloud computing, mobile devices, and increase of remote working, cybercriminals have more opportunities to target organizations and individuals. Attacks using ransomware and other advanced persistent threats (APTs) have increased in frequency, and it is important for organizations to stay informed and proactive in protecting themselves by implementing a robust cybersecurity program and regularly reviewing and testing security controls.

There are several popular and widely-used cybersecurity standards that organizations can adopt to help protect their systems and data. This section reviews some of the widely used frameworks in relation to FDI investments.

Table 3: Cyber Security Frameworks

Framework Name	Description
NIST Cybersecurity Framework (NCSF)	Provides a risk-based approach for managing cyber security
ISO/IEC 27001	A global standard for information security management, providing a systematic approach for protecting sensitive information.
COBIT	IT governance system for managing enterprise IT
PCI DSS	Standard for ensuring secure credit card transactions
HIPAA	Health insurance industry's regulations for protecting patient data
COSO	Framework for managing and controlling enterprise risk
SOC 2	Standard for service organizations to report on controls ensuring information security, availability, accuracy, confidentiality and privacy.
NIST SP 800-53	Defines measures to ensure the security and privacy of information systems belonging to the government
FedRAMP	Offers a systematic method for evaluating the security of cloud products and services, including authorization and ongoing surveillance.
HITRUST	A common framework, Health Information Trust Alliance for ensuring information security in the healthcare industry, based on industry standards and regulations such as NIST and HIPAA.

4.3 NIST CSF

The significance of a unified and thorough system for overseeing cybersecurity, particularly for crucial infrastructure, is emphasized in this article. Recognizing this, the NIST created the NIST Cybersecurity Framework (NIST CSF) to address the issue. The NIST CSF provides organizations with a comprehensive set of recommendations and best practices for constructing and sustaining a robust cybersecurity program that can be customized to meet their unique requirements. The framework is divided into five key functions, namely Identify, Protect, Detect, Respond, and Recover, which offer a structured methodology for handling cybersecurity hazards and align with the typical cybersecurity lifecycle.

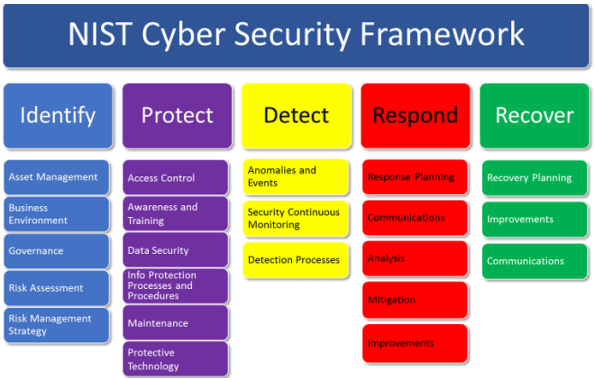

Fig 3: NIST CSF (IFSEC Global, 2020)

4.4 Review of NIST CSF:

Table 4: Review of NIST CSF

Author	Year	Key Findings	Methodology used
Gordon et al.	2020	The authors proposed integrating cost-benefit analysis using the Gordon-Loeb Model into the NIST Cybersecurity Framework as a way to make more informed decisions about cybersecurity investments	Quantitative (The Gordon-Loeb Model)
Delgado et al.	2021	The study found that a significant portion of government organizations were managing cybersecurity without a structured approach, leading to inefficiencies and a lack of metrics. Additionally, the research revealed that only a limited number of organizations surveyed utilized the NIST CSF, which could result in inadequate leadership in the implementation of cybersecurity measures.	Quantitative (Survey-based research)
Mbanaso et al.	2019	The article proposed a Cybersecurity Resilience Maturity Measurement framework for measuring the cybersecurity resilience maturity in organizations for cyber risk management, based on NIST CSF and other relevant frameworks, defining 4 Cybersecurity Resilience Quadrants to depict varying degrees of risk and resilience preparedness	Quantitative
Pavleska et al.	2020	The study outlines a method for incorporating robust security measures into the design and implementation of smart grids through the utilization of established guidelines like the NIST Cybersecurity Framework and ISO standards	goal-based methodology
Kandasamy et al.	2020	This proposed research identifies and analyzes cyberattacks in Asian healthcare, using the NIST framework and proposing a vulnerability priority score system to enhance security.	Mixed Methods
Armenia et al.	2021	The SMECRA system dynamics methodology and tool is proposed to help SMEs manage their cybersecurity risks by assessing the organization's risk profile and evaluating the impact of investments over time.	Case study
Boyson et al.	2022	The research in question analyzed the relationship between the NIST Cybersecurity Framework and breach types in cyber supply chain risk management, offering a data-driven approach for securing digital supply chains by pinpointing the NIST framework's policies that have the strongest impact on preventing specific breaches.	Quantitative

4.5 ISO/IEC 27001

According to Donaldson et al. (2015), ISO/IEC 27001 and 27002 are global standards that offer a structure for handling confidential information. These standards present a thorough framework for managing information security, from the essential needs for an Information Security Management System (ISMS) to instructions and principles for administering security within an organization. One of the strengths of these standards is that they are widely adopted globally, providing a common language and approach for information security management. Additionally, the standards are flexible, allowing organizations to adapt them to their specific needs and circumstances. However, one potential weakness of these standards is that they may require significant resources and effort to implement, especially for smaller organizations. Additionally, the standards are focused mainly on the management and technical controls of information security, and may not cover as much on administrative controls and governance as some other frameworks such as COBIT or NIST CSF.

4.6 Review of ISO/IEC 27001

Table 5: Review of ISO/IEC 27001

AUTHOR	YEAR	KEY FINDINGS	METHODOLOGY
Viet et al.,	2017	The article introduced a new cyber security architecture, referred to as ITI-GAF, that has been developed specifically for countries in need. The framework includes a unique evaluation tool, known as the Cyber Security Assessment Model (CSAM), to help organizations assess their vulnerabilities and develop plans to enhance their cyber security posture.	Mixed methods
Almuhammadi & Alsaleh	2019	The study presented a novel ISMM (Information Security Maturity Model) aimed at evaluating the progress of organizations that have adopted the NIST CSF for Critical Infrastructure.	Quantitative
Antunes et al.,	2021	The authors used a case study method to analyse the current state of SMEs in terms of their cybersecurity management, identify the main challenges they face and proposed a framework for managing information security and cybersecurity for SMEs based on international standards and best practices.	Mixed-methods
Alexei	2021	The research conducted a comparison between the mandatory cyber security regulations implemented by the government of the Republic of Moldova and the ISO 27001 international standard. Ensuring compliance with international cyber security requirements and to gain the trust of foreign partners is essential.	Quantitative
Alexei	2022	The study develop a comprehensive Conceptual Framework that could serve as a blueprint for Higher Education Institutions in the Republic of Moldova to improve their cybersecurity posture.	Qualitative
Borgman, Mubarak, & Choo	2015	The study presented the findings of an investigation aimed at determining the validity of the established processes and strategic direction of the government entities in South Australia with regards to implementing an Information Security Management System and classifying data.	Qualitative
Benoliel	2014	The article suggests key steps for establishing a national-level cybersecurity legal policy based on the example of the National Cyber Bureau in Israel.	Case study
Choraś et al.,	2015	The paper presented a practical framework for enhancing cybersecurity and privacy in ICT systems, specifically in systems that contain personal information and data.	Mixed-method
Jazri, & Jat	2016	The paper proposed a simplified framework for evaluating the profile of cyber security threats for important organisations facing daily cyber threats, and aims to help them detect and rectify vulnerabilities quickly.	Qualitative
Ozkan, & Spruit	2020	The study presented a method for SMEs to evaluate and enhance their cyber security readiness by incorporating essential components from current industry norms, considering the rising threat of cyber security and its impact on SMEs.	Quantitative

4.7 COBIT, SOC, HIPAA, and Others:

COBIT, PCI DSS, HIPAA, COSO, SOC 2, FedRAMP, and HITRUST are all frameworks and standards that help organizations to manage and protect sensitive information. COBIT provides guidance for IT management and governance, PCI DSS sets standards for protecting against credit card fraud, HIPAA is a federal law that sets standards for protecting personal health information, COSO provides guidance for internal control and risk management, SOC 2 is a set of standards for assessing and reporting on controls at a service organization, FedRAMP is a government-wide program for cloud products and services, and HITRUST focuses on improving the management of sensitive and regulated health information. These standards and frameworks are essential for ensuring the security and integrity of sensitive information in today's digital landscape.

4.8 Review of COBIT, SOC, HIPAA, and Others:

Table 6: Review of COBIT, SOC, HIPAA, and Others

AUTHOR	YEAR	KEY FINDINGS	METHODOLOGY
Wolden, Valverde and Talla	2015	The study found that implementing the COBIT 5 framework for information security in Supply Chain Management Systems (SCMS) reduced the likelihood of cyberattacks.	Qualitative
Zanzig and Francia III	2022	The Institute of Internal Auditors has defined ten steps for the successful implementation of technology change, which can be evaluated by the internal audit function.	Case study
Ahlstrom et al.,	2019	The paper discussed the evolution of HIPAA regulations and cyber security threats in the healthcare industry	Case study
Aliyu et al.,	2020	The article introduced a new approach in the form of the Holistic Cybersecurity Maturity Assessment Framework, a web-based model that can serve as a comprehensive evaluation tool for higher education institutions.	Quantitative
Lanz	2018	The article discussed the importance of the revised COSO Enterprise Risk Management-Integrated Framework for technology risk management	Quantitative
Al-Moshaigeh et al.,	2019	The article examined the System for Organization Controls for Cybersecurity (SOC-C), a recently developed technique by the American Institute of Certified Public Accountants (AICPA) for evaluating and managing cybersecurity threats in businesses.	Theoretical
Greer	2015	FITARA and FedRAMP helped government agencies become more comfortable with cloud-based systems by providing a standardized approach for security assessment and IT management.	Theoretical
Buresh	2022	The paper analyzed the potential effects of the Security and Exchange Commission's proposed modifications to its cyber regulations on the management of cyber security risks, with a specific focus on the Cybersecurity Maturity Model Certification framework.	Theoretical
Sulistyowati et al.,	2020	The study compared and designed a methodology for evaluating the maturity of an organization's cybersecurity measures using NIST CSF, ISO/IEC 27002, COBIT, and PCI DSS and presented a cybersecurity maturity framework.	Theoretical research
Hendriks et al.,	2021	The article compares the PCI-DSS framework and the ISO 27001/2 framework for information security management	Qualitative

4.9 Implementation Strategies:

The NIST CSF offers a comprehensive methodology for managing cyber security risk. It consists of five key elements that guide organizations through the process of identifying, protecting, detecting, responding to, and recovering from cyber threats. ISO/IEC 27001 offers a structured approach for the management of information security. It outlines a comprehensive set of policies, controls, and procedures for safeguarding sensitive information and encompasses aspects like risk assessment, incident handling, and contingency planning. Implementation strategies used in the existing researches for these frameworks typically involve conducting a risk assessment to identify potential threats and vulnerabilities, developing and implementing policies and procedures to address identified risks, and regularly monitoring and testing the effectiveness of the implemented controls.

Table 7: Implementation Strategy

Framework Name	Implementation Strategy
NIST Cybersecurity Framework (CSF)	A method of identifying and prioritizing cybersecurity threats and vulnerabilities based on their level of risk and implementing appropriate controls. Regular monitoring and adjustments are necessary to maintain an effective cybersecurity posture.
ISO/IEC 27001	Create an information security management system with policies, procedures, and controls, conduct risk assessments, and regularly monitor and review the effectiveness of the controls to manage sensitive information.
COBIT	Use a process-based approach to manage and govern IT. Identify and document IT processes. Implement controls to ensure the processes are carried out effectively and efficiently. Regularly monitor and assess the performance of the processes.
PCI DSS	To protect sensitive payment card information, use a set of security procedures. Identify and document the cardholder data environment. Regularly assess the effectiveness of the controls.
HITRUST	A risk-based approach to protect sensitive patient information. Perform a risk assessment, implement controls and monitor their effectiveness, and report compliance.
HIPAA	Conduct a risk assessment to identify potential threats and vulnerabilities to ePHI. Implement physical, administrative, and technical safeguards to protect ePHI. Regularly monitor and test the effectiveness of the safeguards. Have a comprehensive compliance program that includes regular employee training, regular risk assessment, and incident response planning and testing.

5. Important Sectors Identified In The Literature:

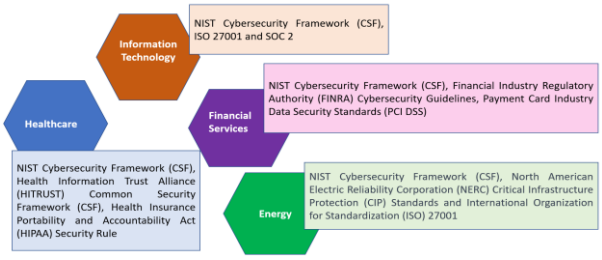

Figure 4: Important Sectors Identified in the Literature

6. Research Gaps:

Many frameworks provide general guidance on cyber security best practices, but may not provide enough detail or practical examples to help organizations actually implement these practices. Many frameworks were developed several years ago, and may not take into account newer technologies and emerging cyber threats. Many frameworks focus on preventing cyber incidents, but may not provide adequate guidance on how to respond to and recover from an incident. A number of approaches lack the proper guidance for assessing the effectiveness of their implementation and the organization's overall stance towards cyber security.

Table 8: Research gaps

Technology Based Gaps	• Security for emerging technologies is missing in the literature • The current security frameworks do not address Advance persistent threat (APT) detections
Sector Based Gaps	• Energy, IT, Financial, Healthcare were the only sectors given research focus in the literature • However, research in the implementation of cyber security frameworks in healthcare sector is very little • Developing countries often face unique cyber security challenges due to limited resources and infrastructure, this context is highly ignored in previous studies
Policy Based Gaps	• Lack of using maturity models to assess an organization's cyber security posture and identify areas for improvement • Not all organizations are effectively developing and implementing policies and governance structures to support cyber security • The function of government in supporting the implementation of cyber security policies in developing economies not studied enough

7. Growing Need:

Cyber threats are becoming more complex and sophisticated, and organizations of all kinds are starting to realize the importance of having a comprehensive framework for managing cybersecurity risk. Organizations require precise policies and procedures for compliance, incident response, and security hardening, but it's also critical to have a framework in place to direct the creation and upkeep of those policies. It's important to note that a framework provides a foundation to build on but it's not a one-time solution, organizations need to continually review, assess, and update their cybersecurity strategies and plans to keep up with the evolving threat landscape. Moreover, it's not only about the technology, but also the people and the processes, having a good cybersecurity culture is vital.

In addition, the growing dependence on technology has led to a heightened focus on cybersecurity, with foreign investors becoming increasingly interested in the cybersecurity measures and infrastructure of potential investment countries. Businesses need to be proactive in ensuring that their systems and data are secure and in compliance with regulations

8. Proposed Solution: Moving From Cybersecurity To Cyber Assurance Framework

An essential aspect of any cyber security program is a framework for assessing and managing risk. This framework acts as a benchmark for evaluating the effectiveness of the program and helps to increase awareness of the cyber threats faced by the organization. While there is no universally accepted framework that addresses all of the concerns of an audit committee, organizations can develop their own framework using relevant components from existing frameworks.

9. Future Research Direction

The ultimate aim is to solve the particular challenges faced by enterprises in critical infrastructure and sectors and to improve their cybersecurity posture. In particular, to address the cybersecurity challenges faced by developing economies and healthcare sector, this review proposes future research direction that is focused on developing a cyber assurance framework. The process of creating a new cyber assurance policy involves engaging stakeholders, defining objectives, gathering data, developing the framework, planning implementation, seeking feedback, obtaining approval, and monitoring effectiveness. The framework should be comprehensive and based on current trends and best practices in cybersecurity and should outline policies and procedures for securing systems and data. The framework should be updated based on feedback and monitored for effectiveness over time. The overall processes involved in future research are shown in the following Fig.5

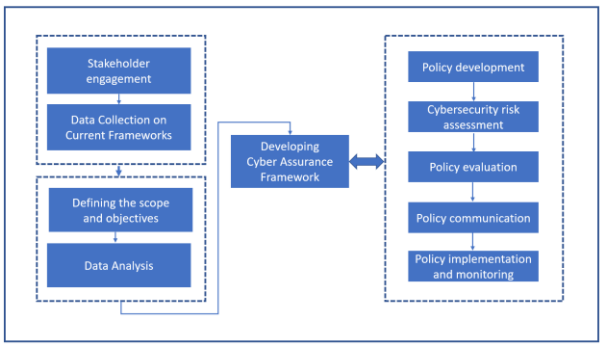

Fig 5: Future research directions

10. Conclusion:

The topic of Cybersecurity Framework and Foreign Direct Investment is a crucial one that is closely tied to the nation's economic development. The health sector is considered as the next economy powerhouse for India, as it is expected to be a major contributor to the country's GDP in the coming years. The findings of the review indicates the current state of research on the topic, highlighting areas where more research is needed and pointing to possible future research directions. It has also provided insights on how cyber security and FDI are related, and how the national regulations and policies play a role in attracting FDI.

Reference:

[1] Ahlstrom, J., Tait, C., & Zoline, K. (2019). Healthcare cyber security and HIPAA assurance with business associates. Cyber Security: A Peer-Reviewed Journal, 3(2), 145-158.

[2] Alexei, A. (2021). Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard.

[3] Alexei, L. A. (2022). Design & development of a cyber security conceptual framework for higher education institutions in the Republic of Moldova. Scientific and Practical Cyber Security Journal (SPCSJ), (1), 35-52.

[4] Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. Applied Sciences, 10(10), 3660.

[5] Al-Moshaigeh, A., Dickins, D., & Higgs, J. L. (2019). Cybersecurity Risks and Controls: Is the AICPA's SOC for Cybersecurity a Solution?. The CPA Journal, 89(6), 36-41.

[6] Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber

security framework. Computer Science & Information Technology (CS & IT), 7(3), 51-62.

[7] Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219-238.

[8] Arcuri, M. C., Brogi, M., & Gandolfi, G. (2018). The effect of cyber-attacks on stock returns. Corporate Ownership & Control, 15(2), 70-83. http://doi.org/10.22495/cocv15i2art6

[9] Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, 113580.

[10] Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: context and shared concepts. Journal of cyber policy, 3(2), 258-283.

[11] Barry, F., Görg, H., & Strobl, E. (2003). Foreign direct investment, agglomerations, and demonstration effects: An empirical investigation. Review of world economics, 139(4), 583-600.

[12] Bayar, Y., Remeikienė, R., Androniceanu, A., Gasparėnienė, L., & Jucevičius, R. (2020). The shadow economy, human development and foreign direct investment inflows.

[13] Benoliel, D. (2014). Towards a cybersecurity policy model: Israel national cyber bureau case study. NCJL & Tech., 16, 435.

[14] BLOMSTEIN. (2020). Cybersecurity and Foreign Direct Investment Controls, https://www.blomstein.com/en/news.php?n=cybersecurity-and-foreign-direct-investment-controls#:~:text=Cybersecurity%20considerations%20play%20a%20special,infrastructure%20or%20security%2Drelated%20sectors.

[15] Borgman, B., Mubarak, S., & Choo, K. K. R. (2015). Cyber security readiness in the South Australian government. Computer Standards & Interfaces, 37, 1-8.

[16] Boyson, S., Corsi, T. M., & Paraskevas, J. P. (2022). Defending digital supply chains: Evidence from a decade-long research program. Technovation, 118, 102380.

[17] Brada, J. C., Drabek, Z., & Iwasaki, I. (2021). Does investor protection increase foreign direct investment? A meta-analysis. Journal of Economic Surveys, 35(1), 34-70.

[18] Buresh, D. L. (2022, August). Given the SEC's 2022 Proposed Cyber Rule Amendments, is the DOD's CMMC Framework a Viable Cyber Framework? International Journal of Innovation Scientific Research and Review, 4(8), 3157-3165.

[19] CAPOBIANCO, A. (2022). The Relationship between FDI Screening and Merger Control Reviews – Note by BIAC, https://one.oecd.org/document/DAF/COMP/WD(2022)115/en/pdf

[20] Choraś, M., Kozik, R., Renk, R., & Hołubowicz, W. (2015, June). A practical framework and guidelines to enhance cyber security and privacy. In Computational Intelligence in Security for Information Systems Conference (pp. 485-495). Springer, Cham.

[21] Contractor, F. J., Dangol, R., Nuruzzaman, N., & Raghunath, S. (2020). How do country regulations and business environment impact foreign direct investment (FDI) inflows?. International Business Review, 29(2), 101640.

[22] Cristani, F. (2019). Cybersecurity of foreign investment in the Visegrád Four (V4) countries: designing a governance model with(in) Europe, Think Visegrad Non-V4 Expert Fellow at the Research Center of the Slovak Foreign Policy Association, Bratislava (Slovakia)

[23] Culot, G., Fattori, F., Podrecca, M., & Sartor, M. (2019). Addressing industry 4.0 cybersecurity challenges. IEEE Engineering Management Review, 47(3), 79-86.

[24] Delgado, M. F., Esenarro, D., Regalado, F. F. J., & Reátegui, M. D. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. 3 c TIC: cuadernos de desarrollo aplicados a las TIC, 10(2), 123-141.

[25] Donaldson, S.E., Siegel, S.G., Williams, C.K., Aslam, A. (2015). Cybersecurity Frameworks. In: Enterprise Cybersecurity. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4302-6083-7_17

[26] Dunning, J. H. (1999). The eclectic paradigm as an envelope for economic and business theories of MNE activity. International Business Review, 8(2), 163-190.

[27] FieldComm Group, Austin, TX, USA (9 November, 2017). FDI Now Supports Enhanced Cyber Security Measures & Additional Protocols!, https://www.fieldcommgroup.org/posts/press-release-fdi-now-supports-enhanced-cyber-security-measures-additional-protocols

[28] Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. Journal of Cybersecurity, 6(1), tyaa005.

[29] Gorg, H., & Strobl, E. (2020). The internet and foreign direct investment. Journal of International Business Studies, 51(3), 312-329.
[30] Graham, E. M., & Marchick, D. (2006). US national security and foreign direct investment. Peterson Institute Press: All Books.
[31] Greer, M. (2015). FITARA and FedRAMP: Accelerating federal cloud adoption. IEEE Cloud Computing, 2(5), 48-52.
[32] Hajdini, E. (2015). Cyber Security and FDI. International Journal of Scientific Engineering and Applied Science (IJSEAS), 1(8), 392-394.
[33] Haudi, H., Wijoyo, H., & Cahyono, Y. (2020). Analysis of Most Influential Factors to Attract Foreign Direct Investment. Journal of Critical Reviews, 7(13).
[34] Hayakawa, K., Kimura, F., & Lee, H. H. (2013). How does country risk matter for foreign direct investment?. The Developing Economies, 51(1), 60-78.
[35] Hendriks, J.M.A.M., Zuiderwijk, C.J.M., & Wieringa, R.J. (2021). A comparative study of the PCI-DSS framework and the ISO 27001/2 framework. Journal of Information Security and Applications, 50, 101935.
[36] https://www.oecd.org/investment/statistics.htm#:~:text=%E2%80%8CFDI%20in%20Figures%20October%202022,the%20first%20half%20of%202022.
[37] Huang, Y., Jiang, N., & Zhang, Y. (2021). Does internet security matter for foreign direct investment? A spatial econometric analysis. Telematics and Informatics, 59, 101559.
[38] Huang, Y., Jiang, N., & Zhang, Y. (2021). Does internet security matter for foreign direct investment? A spatial econometric analysis. Telematics and Informatics, 59, 101559.
[39] IFSEC Global. (2020, September 30). A Guide to the NIST Cybersecurity Framework. Retrieved from https://www.ifsecglobal.com/cyber-security/a-guide-to-the-nist-cybersecurity-framework/
[40] Javorcik, B. S. (2004). The composition of foreign direct investment and protection of intellectual property rights: Evidence from transition economies. European economic review, 48(1), 39-62.
[41] Jazri, H., & Jat, D. S. (2016, November). A quick cybersecurity wellness evaluation framework for critical organizations. In 2016 International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1-5). IEEE.
[42] Jeong, C.Y., Lee, S.-Y., Lim, J.-H., 2019. Information security breaches and IT security investments: Impacts on competitors. Inform. Manage. 56 (5), 681–695. https://doi.org/10.1016/j.im.2018.11.003
[43] Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital Healthcare-Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. IEEE Access, 10, 12345-12364.
[44] Kok, R., & Ersoy, B. A. (2009). Analyses of FDI determinants in developing countries. International Journal of Social Economics.
[45] Krumay, B., Bernroider, E. W., & Walser, R. (2018, November). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. In Nordic Conference on Secure IT Systems (pp. 369-384). Springer, Cham.
[46] Kshetri, N. (2018). The economics of cybersecurity. International Journal of Information Management, 37, 1-14.
[47] Kuhn, T. Heinrich, T. Wienke, T. Arhold, C. Kueper, S. (2021) Broadening the scope further – Latest revisions of German FDI rules go live. https://www.whitecase.com/insight-alert/broadening-scope-further-latest-revisions-german-fdi-rules-go-live
[48] Lanz, J. (2018). Enterprise Technology Risk in a New COSO ERM World: Eight Challenges Facing Management. The CPA Journal, 88(6), 6-10.
[49] Lee, S.-H., Oh, C.H., Lee, J.Y., 2017. The effect of host country Internet infrastructure on foreign expansion of Korean MNCs. Asia Pacific Business Rev. 23 (3), 396–419. https://doi.org/10.1080/13602381.2016.1156295
[50] Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework. The African Journal of Information and Communication, 23, 1-26.
[51] Narula, R. (2018). The role of institutions in foreign direct investment. Journal of World Business, 53(2), 195-208.
[52] Narula, R., & Dunning, J. H. (2019). The Oxford handbook of multinationals. Oxford University Press.
[53] National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.nist.gov/cybersecurity-framework
[54] Nondo, C., Kahsai, M. S., & Hailu, Y. G. (2016). Does institutional quality matter in foreign direct investment?: Evidence from Sub-Saharan African countries. African Journal of Economic and Sustainable Development, 5(1), 12-30.
[55] Osemwengie, D. O. P., & Oriakhi, D. E. (2012). The impact of national security on foreign direct

investment in Nigeria: An empirical analysis. Journal of Economics and Sustainable Development, 3(13), 89-95.

[56] Ozkan, B. Y., & Spruit, M. (2020). Assessing and improving cybersecurity maturity for SMEs: Standardization aspects. arXiv preprint arXiv:2007.01751.

[57] Ozkan, B. Y., & Spruit, M. (2020). Assessing and improving cybersecurity maturity for SMEs: Standardization aspects. arXiv preprint arXiv:2007.01751.

[58] Pavleska, T., Aranha, H., Masi, M., & Sellitto, G. P. (2020, September). Drafting a cybersecurity framework profile for smart grids in EU: a goal-based methodology. In European Dependable Computing Conference (pp. 143-155). Springer, Cham.

[59] Pearson, H. 2019. Strengthening cyber security can boost FDI, say experts, https://www.ft.lk/Front-Page/Strengthening-cyber-security-can-boost-FDI-say-experts/44-687887

[60] Shackelford, S. J., Proia, A. A., Martell, B., & Craig, A. N. (2015). Toward a global cybersecurity standard of care: Exploring the implications of the 2014 NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices. Tex. Int'l LJ, 50, 305.

[61] Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. JOIV: International Journal on Informatics Visualization, 4(4), 225-230.

[62] Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics, 11(14), 2181.

[63] The White House. (2013, February 12). Executive Order -- Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.whitehouse.gov/presidential-actions/executive-order-improving-critical-infrastructure-cybersecurity/

[64] Tissir, N., El Kafhali, S., & Aboutabit, N. (2021). Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal. Journal of Reliable Intelligent Environments, 7(2), 69-84.

[65] Topping, C., Dwyer, A., Michalec, O., Craggs, B., & Rashid, A. (2021). Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Security, 108, 102324.

[66] Trope, R., Smedinghoff, T., 2017. The Importance of Cybersecurity Due Diligence in M&A Transactions. Bus. L, Today, p. 1.

[67] Viet, N. A., Minh, L. Q., Hau, D. H., Tuan, N. N., Quang, N. N., Chinh, N. D., ... & Dat, P. T. (2017). Toward cyber-security architecture framework for developing countries: An assessment model. In International Conference on Advances in Information and Communication Technology (pp. 652-658). Springer, Cham.

[68] Viet, N. A., Minh, L. Q., Hau, D. H., Tuan, N. N., Quang, N. N., Chinh, N. D., ... & Dat, P. T. (2017). Toward cyber-security architecture framework for developing countries: An assessment model. In International Conference on Advances in Information and Communication Technology (pp. 652-658). Springer, Cham.

[69] Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. IFAC-PapersOnLine, 48(3), 1846-1852.

[70] World Economic Forum (2022). Discussing the role of Foreign Direct Investments (FDI) and Cyber Security in delivering the 2030 Agenda for Sustainable Development, https://www.aumun.org/assets/WEF%20AUMUN%202022%20BG.pdf.

[71] Zanzig, J. S., & Francia III, G. A. (2022). Assurance for Change Management With COBIT 2019 and CMMC Maturity Frameworks. In Achieving Organizational Agility, Intelligence, and Resilience Through Information Systems (pp. 163-196). IGI Global.

[72] Brian Moore, Peter Thomas, Giovanni Rossi, Anna Kowalska, Manuel López. Machine Learning for Decision Science in Energy and Sustainability. Kuwait Journal of Machine Learning, 2(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/220

[73] Rajan, S. ., & Joseph, L. . (2023). An Adaptable Optimal Network Topology Model for Efficient Data Centre Design in Storage Area Networks. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 43–50. https://doi.org/10.17762/ijritcc.v11i2s.6027

[74] Rajiv, A., Saxena, A.K., Singh, D., Awasthi, A., Dhabliya, D., Yadav, R.K., Gupta, A. IoT and machine learning on smart home-based data and a perspective on fog computing implementation (2023) Handbook of Research on Machine Learning-Enabled IoT for Smart Applications Across Industries, pp. 336-349.