Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 10
october 2025

Exploring the Landscape of Cybersecurity: A Comprehensive Survey of Standards and Frameworks for Effective Risk Management in the Digital Age

Dr. Aniket Satish Deshpande[1]

[1] Post-Doc. Researcher, Department of Computer Science and Engineering, Sunrise University, Alwar, India
Email Id: [1] anik.deshpande@gmail.com

Abstract

The cybersecurity landscape is becoming more complex, with a variety of threats and vulnerabilities that require strong protective measures. Therefore, cybersecurity involves different practices aimed at protecting data and systems from unauthorized access and attacks. Various organizations implement different cybersecurity standards and frameworks to safeguard data from attackers. These frameworks offer guidance for establishing security protocols and ensuring compliance with regulations. Reviewing several cybersecurity frameworks and standards, such as NIST (National Institute of Standards and Technology), GDPR, ISO/IEC 27000, COBIT, and others, is the main goal of this survey. But by methodically analyzing the junction of these well-established frameworks with Generative AI (GenAI) technologies, this review goes above and beyond other surveys in a unique way. It offers the first thorough examination the GenAI might be incorporated into conventional cybersecurity paradigms. Staying proactive is crucial in maintaining strong cybersecurity in a time where both attackers and defenders are using advanced technologies. The review also highlights the challenges faced by cybersecurity frameworks and technologies, and provides recommendations for overcoming these challenges in the future. The aim of the present survey is to offer a comprehensive overview of various cybersecurity frameworks while considering the impact of GenAI on enhancing security measures. Furthermore, this review provides valuable insights for strengthening organizational resilience against cyber threats in a complex digital environment.

Keywords: Cybersecurity, Frameworks, standards, Generative AI, Threats, Attacks.

1. Introduction

During the digital transformation era [1, 2], cybersecurity has shifted from being a minor concern in the field of information technology to a crucial guardian of digital assets and a fundamental element in upholding the integrity of data-driven societies [3]. This change is largely due to the growing reliance on digital technologies [4], which has amplified the importance of fortifying digital infrastructure [5]. The significance of cybersecurity in safeguarding sensitive information, maintaining privacy, and ensuring the smooth operation of crucial systems cannot be overstressed. Consequently, the introduction of cybersecurity frameworks and standards serves as vital tools intended to assist authorities in succeeding and reducing cybersecurity risks [6, 7]. These frameworks provide regulated instructions, best practices, and standards that organisations can implement to bolster their security stance and defend against cyber threats [8]. The necessity for cybersecurity frameworks arose in reaction to the increasing dangers and vulnerabilities posed by cyber-attacks experienced by organisations in various industries. As cyber threats become more advanced, there is a demand for more standardised methods for managing risks. The creation of these frameworks aims to establish a common dialogue for organisations to effectively discuss cybersecurity risks and strategies [9].

Typically, cybersecurity frameworks are categorized into three primary types, such as control frameworks, program frameworks and risk frameworks [10]. The application and effectiveness of conventional cybersecurity frameworks in a range of organizational scenarios have been well-documented in the literature. Frameworks like NIST, ISO/IEC 27000, COBIT, and FISMA have been extensively examined in studies,

which have shown their effectiveness in improving security posture, structured risk management, and regulatory compliance [11]. Additionally, studies have looked at the relative advantages and disadvantages of different frameworks, offering firms recommendations for choice depending on industry-specific needs and regulatory frameworks. Additionally, there is ample evidence of how these frameworks have changed in response to new threats; in fact, many articles have discussed how they have adjusted to problems like ransom ware, phishing, and advanced persistent threats [12]. Control frameworks focuses on establishing a baseline group of security controls necessary for an organization's cybersecurity strategy [7]. They assess the current state of technology and prioritize the implementation of security measures. Program frameworks evaluate an organization's existing security program and help construct a comprehensive cybersecurity strategy [13]. It facilitate communication between cybersecurity teams and management and risk frameworks are premeditated to describe procedures for assessing and supervision risks associated with cybersecurity threats. This aids organizations identify, measure and prioritize the security risks.

In recent years, the cybersecurity landscape has been shaped by a variety of factors including technological advancements, regulatory changes and emerging threats [8, 14]. The rise of sophisticated attack methods such as ransomware, phishing and DoS (Denial of Service Attacks) has necessitated a proactive approach to risk management [15]. Organizations are now compelled to adopt comprehensive frameworks and standards that guide their cybersecurity strategies [16]. Notable among these are, the NIST cybersecurity framework and ISO/IEC 27000s series frameworks and many more [17], which provide structured methodologies for assessing and mitigating risks associated with cyber threats. Moreover, the interplay between cybersecurity policies and societal factors cannot be overlooked. Effective risk management in the digital age requires not only technical solutions but also legal and policy considerations that encompasses user behaviour and awareness [18]. Some of the frameworks reviewed in the studies is demonstrated in figure 1.

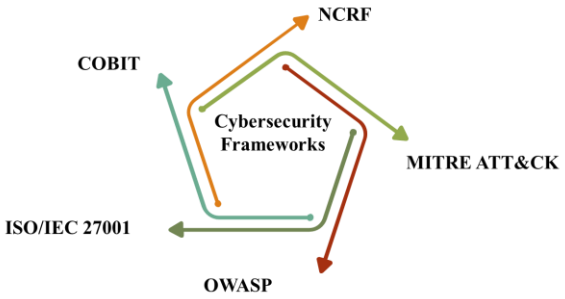

Figure 1. Some of the Cybersecurity Frameworks

The figure.1 illustrate an outer pentagonal shape with arrows pointing in various directions represents a cyclical process. Every arrow represents a phase or stage in the procedure, showing how the different parts flow and are connected to one another. The dynamic character of the process is highlighted by the arrows' varied colors, which could stand for various stages or priorities within the cycle. Since each step builds on the one before it, the overall structure suggests an iterative approach to reaching a goal and highlights the necessity of constant advancement and flexibility.

Though there are various existing papers which have discussed about cybersecurity frameworks and standards, the uniqueness of the present survey lies on the inclusion of GenAI technology, as it offers a transformative approach to enhancing cybersecurity measures. By integrating GenAI organizations can leverage advanced capabilities such as automated threat detection, real-time response strategies and improved vulnerabilities assessments. Besides, the study have explored and reviewed different types of cybersecurity frameworks highlighting the strengths and weakness in various organizational context. By examining these frameworks in details, the study identifies best practices and key performance indicators that can guide organizations in selecting and implementing the most suitable framework for the specific needs. Even with this extensive research on conventional cybersecurity frameworks, there are still a lot of unanswered questions about how new technologies in particular, GenAI, intersect and have the potential to change existing tried-and-true methods. The majority of the literature now in publication looks at GenAI applications and cybersecurity frameworks separately, with little investigation into how they perform together. The potential for GenAI capabilities to improve, challenge, or necessitate reconfiguration of conventional cybersecurity frameworks has not been thoroughly

examined in many studies. Furthermore, little study has been done on the particular security implications of GenAI technologies in relation to well-established risk management frameworks. There is an urgent need for new guidance that bridges the gap between traditional cybersecurity procedures and AI-enhanced capabilities, as both defenders and bad actors use AI technologies more and more. Additionally, the present review underscores the importance of adaptability within these frameworks to accommodate the rapid evolution of cyber threats, emphasizing that a one-size-fits-all approach is no longer viable. Gaps exist in cybersecurity literature regarding the integration of Generative AI into existing frameworks, particularly in terms of adaptability to evolving threats and specific best practices. There is limited exploration of the diverse applications of Generative AI in enhancing cybersecurity measures and the specific obstacles faced during implementation. Additionally, there is a need to identify technological gaps that hinder the effective use of advanced technologies within current frameworks. By highlighting the combined effect between cybersecurity standards and GenAI technologies, the work aims to provide practitioners, policymakers and researchers with actionable insights to develop more resilient security strategies in an increasingly complex cyber environment.

Paper objectives

The following are the main goals of this survey paper:

- To provide best practices to guarantee thorough risk management and regulatory compliance, as well as to thoroughly examine cybersecurity frameworks and standards for improving organisational resilience against cyber threats. The basis for comprehending how conventional methods might adapt to new technologies is this review.
- To methodically discuss generative artificial intelligence (AI) approaches for cybersecurity in order to investigate the technology's many uses and implications for improving security protocols, threat identification, and incident response. The crucial knowledge gap regarding the integration of AI technologies into current cybersecurity paradigms is filled by this analysis.
- To pinpoint and analyses the primary challenges that cybersecurity frameworks and standards face when incorporating GenAI capabilities, and to make recommendations for possible future paths that might close existing technology gaps and promote advancements in algorithm design and application scenarios. The necessity for advanced frameworks that can successfully integrate AI-enhanced security measures while addressing new vulnerabilities brought forth by these technologies is the specific focus of this purpose.

Paper organization

The paper is systematized in the resulting manner. In section 2 the paper cover the survey methodology part, section 3 focuses on significance of cybersecurity frameworks, section 4 deals with cybersecurity frameworks and policies, section 5 discusses about limitations of existing cybersecurity frameworks and current AI solutions in cybersecurity, section 6 deliberates on the boom of GenAI, section 7 reflects challenges and future recommendation and eventually section 8 summarize the entire work.

2. Survey Methodology

The process of collecting and fetching the right papers for survey is investigated in the subsequent section. Therefore, figure showcases the process involved in the papers effectively.

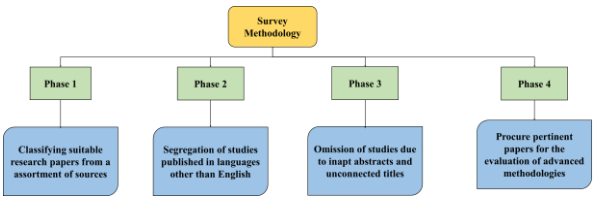

Figure 2. Survey Methodology

A four-phase survey process for methodically assessing research papers is shown in the figure 2. Phase 1 entails creating a foundational dataset by categorizing relevant research publications from multiple sources. In order to ensure a diverse inclusion of perspectives, phase two focusses on separating works published in languages other than English. Phase 3 refines the selection for quality by eliminating studies with poor abstracts or disjointed titles. Lastly, Phase 4 places a strong emphasis on obtaining relevant articles that will help assess sophisticated approaches, guaranteeing that the analysis that follows is thorough and applicable. The research review procedure is guaranteed to be comprehensive and rigorous with this staged method.

E-Sources Opted

A miscellaneous range of e-sources and DBs has been employed to retrieve papers apposite to the present survey work. The selected DBs for the current project feature an extensive collection of esteemed articles within the technical domain. Consequently, some of the key sources utilized for gathering these papers include,

- IEEE
- ACM
- Taylor and Francis
- Elsevier
- Scopus
- Web of Science (WoS)
- Springer
- Science Direct
- Wiley
- MDPI

Optimization of Keywords

Employing applicable keywords is vital for acquiring suitable content, as they facilitate the retrieval of apropos papers from numerous DB's. Accordingly, the following keywords were utilized to ensure effective paper fetching process- 'Cybersecurity', 'Cybersecurity frameworks and standards', 'Generative AI, 'Frameworks', 'Significance of cybersecurity' and many more.

Data sanitization

Inclusion Criteria

- The consideration of this review is solely on articles that specifically address cybersecurity frameworks and standards. Only papers published in English well be included for assessment and review.

Exclusion Criteria

- Paper deficient of titles and abstracts that are specifically applicable to the Cybersecurity frameworks will be excluded from this review and the studies that do not provide a clear and well defined methodology will be omitted from this analysis.

These strategies skeleton the methodologies employed in this survey paper to comportment a detailed and comprehensive review.

3. Significance of Cybersecurity Frameworks

Cybersecurity frameworks are indispensable tools for organizations aiming to cope and allay cyber risks effectively [19]. The structured guidelines afford a methodical tactic to categorizing, protecting, detecting, responding to, and recovering from cyber threats. The significance of these frameworks can be understood through various key aspects.

Table 1: Implications of cybersecurity frameworks

Implications	Description
Structured Risk Management	➢ Cybersecurity frameworks help organizations systematically identify and assess their vulnerabilities. By providing a clear set of guidelines and best practices, these frameworks enable organizations to conduct thorough risk assessments, prioritize vulnerabilities and allocate resources effectively to enhance security measures [20]. This structured approach reduces the likelihood of successful cyberattacks by ensuring that potential weakness are addressed proactively.
Regulatory compliance	➢ Many cybersecurity frameworks align with industry-specific regulations and standards such as GDPR, HIPPA or other frameworks [21]. This alignment simplifies compliance efforts for organizations by providing a roadmap to meet legal and regulatory requirements. Adopting a recognized framework helps organizations avoid legal penalties and maintaining operational integrity.
Steadiness across the organization	➢ Cybersecurity frameworks promote consistency in security practices across different departments and teams within

Implications	Description
	an organization [22]. This uniformity ensures that all employees adhere to the same protocols and standards, which is imperative for effective risk management. A consistent approach also facilitates better communication among stakeholders regarding cybersecurity matters [23].
Enhanced incident response capabilities	➢ Framework outlines clear protocols for detecting and retorting to security occurrences. Having pre-defined incident response plans permits organizations to minimize the impact of attacks, recover quickly from breaches and maintain business continuity. This preparedness demonstrates a commitment to protect data and maintain trust with clients and stakeholders [24].
Unceasing expansion and adaptation	➢ Cybersecurity frameworks are not static, they evolve as new threats emerge [25]. Organizations can adapt existing frameworks or develop their own tailored solutions while ensuring that it meet industry standards. This adaptability is crucial for maintaining resilience against evolving cyber threats.
Operational Efficiency	➢ By providing clear guidelines and best practices, cybersecurity frameworks help streamline operations within an organization. They enable teams to implement consistent security measures across departments, reducing redundancy and improving efficiency in managing cybersecurity task. Furthermore, frameworks can fill gaps in existing security models, enhancing the overall effectiveness of an organization's cybersecurity strategy [26].

4. Cybersecurity Frameworks and Policies

Frameworks Involved in Cybersecurity Environment

Frameworks involved in cybersecurity environment are essential structures that provide organizations with inclusive guidelines, standards and best practices for dealing and vindicating cybersecurity risks.

NIST (National Institute of Standards and Technology)

The cybersecurity framework was created by NIST framework following the signing of an executive order by President Obama in 2014 [27]. Additionally, the CEA (Cybersecurity enhancement Act) of 2014 revised NIST's responsibilities, expanding its focus to include the documentation and formulation of cybersecurity risk frameworks specifically for operators and owners of critical infrastructure. NIST framework address both current business operations and cybersecurity challenges. Consequently, it serves as a foundational tool for developing a new cybersecurity strategy or enhancing an existing program [28]. Organizations and private sector entities can adopt it as a set of best practices to safeguard the crucial infrastructure effectively.

NIST framework assists organizations in enhancing the cybersecurity efforts by providing a cohesive structure that integrates various cybersecurity strategies [29]. It complies best practices, standards and recommendations making it a valuable resource for detecting and addressing weakness in an organization's cybersecurity measures. Essentially, NIST framework serve as a tool for articulating cybersecurity requirements, enabling organizations to pinpoint deficiencies in its current practices effectively. Therefore, the core components of NIST framework

Figure 3. Components of NIST [30]

Figure 3 show that the five key functions of cybersecurity are identified, protected, detected, responded to, and recovered in this flowchart. The essential actions and factors required for efficient risk management are included in each section. Understanding assets, governance, and risk

management techniques are the main goals of the Identify phase. The Protect phase places a strong emphasis on using security and access control techniques to protect assets. Organizations keep an eye out for irregularities and security incidents during the Detect phase. While the Recovery phase places more of an emphasis on recovery planning and ongoing progress, the Respond phase deals with planning and communication for efficient event management. This methodical approach emphasizes how crucial it is to move through each stage in order to preserve and improve an organization's cybersecurity posture.

National Cybersecurity Reference Framework

NCRF is a framework designed to establish cybersecurity standards in India, with a particular emphasizes on critical sectors [26]. It offers a set of guidelines that assist organizations in building robust cybersecurity systems, The NCRF can act as a model for entities within the critical sectors to create their own governance and management frameworks. NCRFs serve as an essential guidelines for organizations to enhance the cybersecurity posture. Various countries have developed this framework to address unique challenges and requirements in the cybersecurity landscape. The NCRF supersedes the national cybersecurity policy of 2013, which was deemed outdated to its insufficient guidelines and lack of adaptability to the evolving cyber threat landscape. The previous policy failed to adequately protect critical sectors, prompting the need for a more robust framework that aligns with the contemporary cybersecurity challenges.

NCRF is built around several core components aimed at enhancing the cybersecurity across various sectors. Identification involves encouraging organizations to identify the assets and asses vulnerabilities. Protection focuses on establishing safeguards to secure critical infrastructure from potential threats. Detection phase emphasizes implementing measures to detect anomalies and potential breaches in real-time. Response is about developing incident response plans to mitigate damage from cyber incidents, while recovery ensures that organizations can effectively recover from incidents and restore normal operations. This structured approach is essential for improving the overall cybersecurity for improving the overall cybersecurity posture of organizations within critical sectors in India.

India's NCRF Framework

The NCRF in India is a significant policy document aimed at establishing cybersecurity standards and guidelines. Key aspects include:

- **Objectives:** The NCRF is designed to strengthen India's cybersecurity infrastructure by providing a structured approach to managing cyber threats.
- **Components:** It encompasses operational recommendations and outlines the legal and institutional framework necessary for effective cybersecurity governance.
- **Legal foundations:** NCRF framework is supported by the IT (Information Technology) act of 2000 and various regulations that guide cybersecurity practices within the country.
- **Institutional framework:** The key agencies involved includes the MeitY (Ministry of Electronic and Information Technology), the national cyber security coordinator and the ministry of home affairs and many more.

MITRE Framework

MITRE ATT&CK framework is an inclusive, open access knowledge base initiated in 2013 [31], that minutiae the TTP (Tactics, Techniques and Procedure) used for cyber adversaries. The acronym of ATT&CK stands for adversarial tactics, techniques and common knowledge, and it obliges as a critical source for organizations aiming to enhance the cybersecurity strategies [32]. This framework is developed by MITRE Corporation and offers valuable insights into behaviours of threat actors based on observations, making it invaluable for threat detection [33], incident response and security assessment. There are major two components of MITRE frameworks such as a tactics and techniques and the other one is matrices [34].

- **Tactics and Technique**

MITRE framework organizes adversarial behaviours into distinct tactics, which represent the goals of an attacker and techniques, which describes how these goals are achieved. Besides, as of version 9, the framework includes 14 tactics, encompassing 185 techniques and 367 sub-techniques, providing a detailed map of potential attack vectors [35].

- **Matrices**

The MITRE ATT&CK framework is structured into several matrices tailored to diverse environments such as Enterprise matrix, Mobile matrix and ICS matrix (Industrial Control System) [36]. Thus, MITRE ATT&CK framework is divided into several matrices, tailored to specific environment.

Enterprise Matrix: The Enterprise ATT&CK matrix focuses on tactics and techniques relevant to enterprise networks across various platforms, including operating systems like windows, macOS and Linux [37]. Likewise, cloud environment such as Azure AD, SaaS applications are covered in this setup and network infrastructure such as various network devices and configurations are enclosed under this realm of enterprise matrix. This specific matrix is the most widely utilized within the framework, providing detailed insights into how adversaries operate within enterprise settings [38]. It includes 14 tactics such as initial access, execution, persistence and more, with numerous associated techniques and sub-techniques that detail specific methods attackers may employ.

Mobile Matrix: The Mobile ATT&CK matrix is specifically designed to address threats targeting mobile devices and it covers platforms such as iOS and android [39]. Moreover for attack techniques, the methods that do not require physical access to devices, such as exploiting mobile applications or network services. This matrix highlights the unique challenges posed by mobile environments and provides guidance on detection and mitigation strategies tailored to mobile threats.

ICS Matrix: The ICS ATT&CK matrix focuses on tactics relevant to industrial control system commonly found in sectors such as energy, manufacturing and utilities [40]. Besides, the ICS ATT&CK matrix is tailored for industrial environments, focusing on tactics relevant to systems like SCADA (Supervisory Control and Data Acquisition). Hence, some of the common tactics involved in ICS matrix is initial access, command and control, impact and data manipulation. Hence, ICS matrix serves as a vital resource for security professionals working in critical infrastructure sectors, helping them develop effective strategies against cyber threats.

A case study has been explored in the work [41] for evaluating a comprehensive analysis of MITRE ATT&CK implementation. Here, the government agency which has been opted for the study has proven an overarching security policy for safeguarding the data, infrastructure and also systems. Thus, to establish a strong defense against cyber threats, the agency has adopted a wide-ranging suite of security technologies that encompasses both hardware and software solutions. Thus, by following the established industry standards, the agency carefully designed and executed it security strategy, employing technologies that conform to the guidelines set forth by NIST and MITRE. These frameworks have been instrumental in shaping the agency's security architecture, enhancing its capabilities to detect, protect against and respond to adversarial attacks. Hence, the SolarWinds incident highlights the intricate challenges of contemporary cyber espionage and the significant difficulties in safeguarding supply chains from sophisticated adversaries. The identification of this operation as being linked to SVR (Russia's Foreign Intelligence Service), as confirmed by both the US and UK governments in April 2021, emphasizes the involvement of state-sponsored elements in such campaigns. Impacting around 18,000 entities across both public and private sectors, with a smaller group facing actual system breaches due to follow-up actions by APT29, this incident serves as a stark illustration of the escalating threats in the cyber landscape. The MITRE ATT&CK framework offers a systematic approach to analyzing known tactics and techniques employed by adversaries, enabling organizations to foresee, prepare for, and effectively counteract advanced cyber threats. Consequently, the agency's integration of these framework is vital for sustaining a proactive and resilient security stance in a progressively stimulating cyber environment.

Open Web Application Security Project (OWASP)

OWASP is a nonprofit foundation, which is devoted to enhancing software security [42]. Founded in 2001, OWASP focuses on improving the security of web applications through community-driven projects. Thus, OWASP plays a decisive role in the cybersecurity landscape by offering actionable insights and tools that assist organizations defend against web-based threats [43]. By integrating OWASP guidelines into their development processes, organizations can significantly reduce vulnerabilities in varied applications, thereby enhancing overall security. Besides, OWASP Top 10 is an extensively renowned list classifies the most precarious web application security menaces. Updated

periodically, the list serves as a guideline for organizations to comprehend and mitigate vulnerabilities effectively and the latest version [44] was published in 2021 and include risks which is depicted in figure.

a) Broken Access Control: This happens when users act outside the envisioned consents. This vulnerability allows unauthorized users to access sensitive files or functions, potentially leading to data breaches. Common causes include missing or ineffective access controls and improper authentication mechanisms. Implementing robust role-based access controls and regularly testing for vulnerabilities can mitigate this risk.

b) Cryptographic Failures: Cryptographic Failures refers to weakness in the cryptographic mechanism that protect data. These can arise form weak encryption algorithms, poor key management, or flaws in implementation. Thus, to prevent failures, organizations should use strong encryption protocols, ensure proper key management and regularly update cryptographic libraries.

c) Injection: Injection susceptibilities arise when an attacker can direct untrusted data to a transcriber as part of a command or query. This results to various attacks, including SQL injection and command injection. Preemptive measures include using parameterized queries, input validation and employing web application firewalls.

d) Insecure Design: Insecure design pertains to inherent vulnerabilities within an application's architecture that overlook essential security considerations. This can encompass of insufficient threat modeling or suboptimal architectural choices that expand the attack surface. To mitigate these issues, security measures should be integrated by developers during the design phase and perform regular threat assessments.

e) Security Misconfiguration: Security misconfiguration occurs due to the inadequate setup of security controls across multiple components, including servers, databases and applications. Common problems include the use of default configurations, open ports and weak passwords. To tackle these challenges, it is essential to conduct regular audits and follow secure configuration checklist.

f) Vulnerability and outdated components: This vulnerability arises from the use of outdated software components or those known to contain vulnerabilities. Neglecting to update these components can leave applications susceptible to attacks. Organizations should establish regular scanning procedure and maintain an inventory of all software components to ensure the components are up-to-date and secure.

g) Identification and Authentication Failures: Failures in identification and authentication can enable attackers to exploit inadequate password policies or vulnerabilities in session management, allowing them to impersonate users. The implementation of MFA (Multi-factor authentication) and robust session management practices can substantially alleviate this risk.

h) Software and data integrity failures: This category addresses issues pertaining to the integrity of software updates and data management processes. Attacks involves the alteration of code or data during transmission or while stored. Implementing secure coding practices and validating software integrity through checksums or digital signatures can effectively protect against these vulnerabilities.

i) Security logging and Monitoring Failures: Insufficient logging and monitoring can hamper an organization's capacity to sense and retort to security occurrences effectively. It is essential for applications to comprehensively log security-relevant events and to actively monitor these logs for any unusual activity.

j) Server-Side Request Forgery: SSRF occurs when an attacker manipulates a server to make request on its behalf, potentially gaining access to internal resources that should remain protected from external access. Therefore, to confront the risk of SSRF attacks, developers should validate all incoming requests and limit server-side request to trusted domains.

As OWASP top 10 is a framework for web application security testing that aims to identify vulnerabilities within websites, the study [45] has focused on employing OWASP cybersecurity architecture on assessing web application security to uncover the weakness that could be exploited. Besides, the study has analyzed and tested the security of the web along with 6 sub domain in order to know and gauge the security level of the website. Correspondingly, a MobileNet based OWASP [46] vulnerabilities scanner tool has been employed in the work, with the aim to safeguard the web pages of the cloud. With the intention of achieving this process, data collected from

OWASP has been pre-processed for ignoring the recurrent values and null words. Implementation of MobileNet model offered security on the web pages and the simulation outcome were generated in order to ensure the security of the model by obtaining accuracy rate of 96.40%. Besides, study [47] has explored web application security in education platform based on OWASP API security project. Therefore, this technique introduced a model for creating a legal and secure environment for learning API security, grounded in the OWASP API security project. Therefore, implementation of the framework addressed various security risks, including resource limitations, improper asset management, and mass assignment vulnerabilities that are often overlooked in existing security training applications.

International Organization for standardization /IEC 27000 Series

ISO/ICE 27000 focuses on the management of information security within the information systems and is jointly published by the ISO and IEC. This series of standards, originally known as BS7799, transitioned into ISO standards once they were integrated into the ISMS (Information Security Management System) framework [48]. ISO 27001 series emphasizes on the secure and reliable data exchange and communication channels. The standard prioritize a risk based approach to achieve both managerial and organization goals, including sub-objectives. However, the ISO 27000 series has not proven to be a complete solution for integration ISM into a broader systems effectively. ISO 27001, the inaugural standard in the ISO/ICE 27000 series, was established in 2005. At present 4 standards such as ISO 27001, 27002, 27005 and 27006 have been published and are commonly utilized by organizations.

a) ISO/IEC 27001- 2013

ISO/ICE 27001 is an internationally recognized standard for information security management systems, developed by the ISO (International Organization for Standardization) and the ICE (International Electrochemical Commission) [49]. This standard provides a structured framework to protect the sensitive information assets from various cybersecurity threats. There are 11 sections with 36 objectives which are further fragmented into sub-objectives.

Therefore, ISO/IEC 27001 is built around three fundamental principles known as CIA trait:

- **Confidentiality:** This ensures that sensitive information is accessible only to authorized individuals.
- **Integrity:** Upholding the accuracy and completeness of data, preventing unauthorized alterations.
- **Availability:** Assuring that information is accessible when required by authorized users.

Besides, structure of ISO/IEC 27001 employs a top-down, risk- based approach to information security and table demonstrates the various requirements and controls necessary for compliance or operational effectiveness.

b) ISO/IEC 27002- 2013

ISO/IEC 27002 serves as a code of practice for information security controls, providing a comprehensive framework of controls designed to align with ISO/IEC 27001[50] . It is important to note that organizations are not required to implement security control that are not explicitly included in this framework. ISO/IEC 27002 offers best practice guidelines for individual tasked with implementing information security management within organizations. These recommendations aim to enhance the effectiveness of security measures and ensure robust protection of information assets.

c) ISO/IEC 27005- 2018

ISO/IEC 27005 provides guidelines for implementing a risk based approach to cybersecurity risk management. This standard reinforces the concepts and requirements outlined in ISO/IEC 27001, ensuring that organizations can effectively manage their information security risks [51]. To fully grasp ISO/IEC 27005, organizations must comprehend the processes and principles outlined in ISO/IEC 27001, as well as those in ISO/IEC 27002. This standard is applicable for establishing a robust, risk based information system across various organization masses and divisions. ISO/IEC 27005 outlines an information risk management process that comprises 7 essential elements [52, 53]: establishing context, consulting menaces, measuring perils, handling risks, tolerating hazards, communicating risks, reviewing the risks as well as monitoring risks. This structured approach is designed to assist organizations effectively manage their information security risks.

d) ISO/IEC 27006- 2015

ISO/IEC 27006 aims to establish official procedures and criteria that must be followed by third party organizations offering information security auditing and certification services to other companies [54]. Utilizing ISO/IEC 27006 enables organizations to be acknowledged as credible and dependable entities for conducting certifications of ISMS. This standard enhances the reputation and assure clients of a certain caliber to provide trustworthy certification services.

Control Objectives for Information and Related Technologies (COBIT)

COBIT is a comprehensive framework urbanized by ISACA (Information Systems Audit and Control Association) aimed at improving IT governance and management practices [55]. COBIT framework offers organizations with guidelines and best practices to align with the IT strategies with business goals, ensuring effective risk management and compliance with regulatory requirements [56]. Typically, COBIT framework offers a common language and reference model for IT processes, delineating responsibilities across planning, building, running and monitoring activities. It also establishes a high level requirements necessary for effective control of each IT process, serving as measurable targets for organization. Hence, COBIT is widely used in the US to comply with regulations such as SOX (SarbanesOxley Act), which aims to deter fraudulent financial reporting. Additionally, COBIT standard has recently introduced a draft for its latest version, known as COBIT 5. This new version significantly enhances the focus on security objectives and outlines methods for organizations to effectively achieve these goals. Therefore, the key components of COBIT 5 framework is depicted in figure,

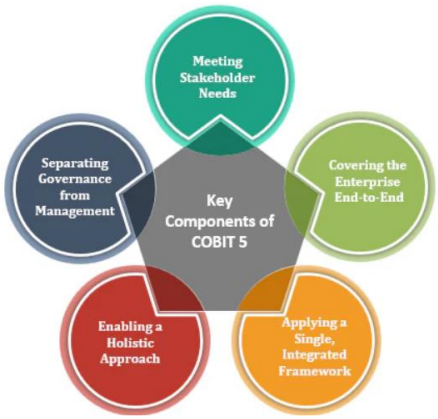

Figure 4. Components of COBIT 5 Framework

Therefore, figure underscores the critical importance for organizations to address and prioritize the diverse needs of other stakeholders, which include customers, regulators and shareholders, ensuring that IT initiatives are aligned with these expectations. The framework promotes a comprehensive approach that encompasses the entire organization, from strategic planning to value generation and risk management. By advocating for a unified governance and management framework, COBIT 5 framework seeks to eliminate redundancies and inconsistences in IT processes, thereby fostering a cohesive operational strategy. Furthermore, it encourages organizations to consider all dimensions of IT governance to develop a well-rounded governance model. Eventually, COBIT 5 framework emphasized the necessity of distinguishing between governance, focused on strategic decision making and management concerned with operational execution to ensure that IT activities effectively support overarching business objectives.

Implementation Enterprise Governance of It- COBIT Implementation Approach

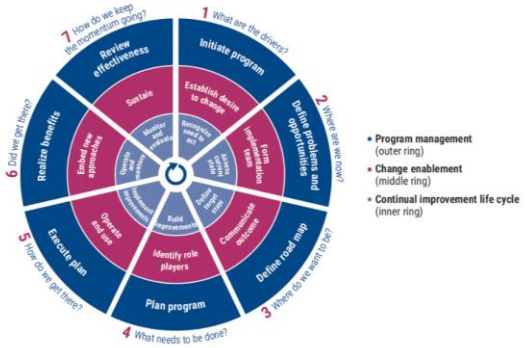

Figure 5. Process Involved in COBIT framework

a) Level 1- what are the drivers?

The initial phase of the implementation strategy focuses on identifying the factors driving change that are currently active within the organization. It aims to foster a desire to change among top management, which is then outlined in a business case. A change driver refers to any interior or exterior event, situation or urgent concern that prompts the need for change. Various elements can trigger change, including trends in the industry and market, technological advancements, specific events, performance gaps and software rollouts and even the strategic goals of the organization. The business case is instrumental in identifying and managing the risks associated with program implementation, which exist throughout the

entire lifecycle of the program. ®Developing, maintaining and monitoring a business case are vital practices that support, justify and ensure the success of any initiative including improvements to the governance framework.

b) Level 2 – Where are the users now?

Level 2 establishes priorities for corporate objectives, alignment goals, and processes, while ensuring that I&T (information and technology) objectives are in sync with risk management and enterprise strategies. The COBIT ® 2019 design guide offers various design parameters to facilitate the selection process. The organization needs to establish key governance and management objectives along with the necessary procedures, to achieve effective outcomes aligned with the selected enterprise and IT related goals as well as other design consideration. The management should be cognizant of its current capabilities and any potential vulnerabilities. This can be accomplished through a process capability assessment that evaluates the current state of selected process.

c) Level 3- Where do the users want to be?

Level 3 involves setting an improvement target and performing a gap analysis to identify potential solutions. Some issues may have short term fixes, while other require more complex, long term solutions. Projects that are expected to deliver the greatest benefits and can be completed with relative ease should be prioritized. Additionally, longer term initiatives should be broken down into smaller, more adaptable tasks.

d) Level 4 – what needs to be done?

Level 4 outlines the process for describing projects reinforced by compelling business cases and a change implementation plan, aimed at creating practical and effective solutions. A well-structured business case can aid in detecting and unceasingly monitoring the benefits of the project.

e) Level 5 – How do the users get there?

In phase 5, the solutions are implemented through standard procedures. Systems for measurement and monitoring are established to ensure alignment with business objectives and to enable performance assessment. Success in this phase relies on engagement, knowledge sharing, and effective communication, understanding as well as ownership by the business and IT process owners affected by the changes.

f) Level 6 – Did the users get there?

The primary aim of level 6 is to ensure the lasting incorporation of improved governance and management practices into the organization's routine operations. Additionally, this phase emphasizes the use of performance metrics and expected benefits to monitor the success of these improvements,

g) Level 7 – How do the users keep the momentum going?

Level 7 assesses the overall effectiveness of the COBIT framework, identifies any additional governance or management needs and highlights the significance of continuous improvements. Furthermore, it prioritizes new opportunities to strengthen the governance framework.

Each of the seven levels of program and project management includes built-in check points. These checkpoints help ensure that the program is performing as expected, keep the business case and risk assessments current, and allow for adjustments in planning for the next phase as necessary. Program and project management relies on best practices and incorporates these checkpoints throughout all 7 phases. It is expected that the organization will follow its established methodology.

Federal Information Security Management Act

FISMA is a critical section of legislation that establishes an ample framework for protecting government information and information system from different threats [57]. Originally enacted in 2002 and updated in 2014, FISMA aims to boost the security deportment of federal agencies and their contractors by mandating development, documentation and implementation of robust information security programs. FISMA's primary purpose is to defend complex information from unauthorized access, practice, confession and even destruction [58]. This particular framework not only applies to federal agencies, but also extends to state agencies administering federal programs and private sector organizations that contract with the government. The compliance steps under FISMA

To comply with FISMA, organizations must follow a structured approach that includes several key steps:

- **Categorization:** This step focuses on identifying and sorting information systems depending on the potential impact of a security breach.
- **Control selection:** Selection of minimum baseline security controls from NIST guidelines that are appropriate for the system's configuration.
- **Implementation:** Executing the selected controls within the organization's information system
- **Assessment:** Frequently measure the efficiency of these controls through testing and evaluation.
- **Authorization:** Approve the system for processing based on its compliance with security requirements.
- **Continuous Monitoring:** Unceasingly monitor the system's security posture and make the necessary adjustments depending on emerging threats or vulnerabilities.

Moreover, in recent years, there have been discussions regarding updates to FISMA to enhance its effectiveness in addressing evolving cybersecurity challenges. Additionally, there is an ongoing effort to align FISMA with other cybersecurity frameworks like the CMMC (Cybersecurity maturity model certification) and FedRAMP (Federal Risk and Authorization Management Program) to ensure comprehensive protection of federal information systems. [59]

GDPR - General Data Protection Regulation

The GDPR is a comprehensive privacy and security law enacted by the EU that governs how private data of individuals within the EU can be administered and reassigned [60]. It was adopted on April 2016, and become enforceable on May 25, 2018 replacing the preceding data protection directive from 1995. The GDPR aims to augment the individual's control over their personal information and abridge the regulatory environment for international business by standardizing data protection laws across members states [61]. The GDPR outlines 6 specific principles required of companies when processing data.

- Lawfulness, Fairness and transparency
- Purpose limitation
- Storage limitation
- Data minimization
- Overarching accountability
- Integrity and confidentiality

i) Lawfulness, Fairness and transparency

Lawfulness: This principle entails that personal data dispensation is steered based on a legitimate legal ground as specified in Article 6 of the GDPR. Common grounds includes consent, legal obligations, vital welfares, contractual necessity pursued by the data controller or a third party [62]. Fairness implies that processing should not be detrimental or misleading to the data subjects. The processing must respect their rights and expectations, ensuring that it does not exploit or disadvantage them. For transparency, the organizations must deliver clear and accessible information about how personal data is administered. This includes informing individuals about the purposes of data collection and their rights regarding the data. Transparency foster trust and allows individuals to make informed decisions about their personal information.

ii) Purpose limitation

This principle statuses that private data should only be obtained for definite, obvious and genuine purposes. Once collected, organization cannot use this data for purpose incompatible with those originally specified. This limitation helps prevent misuse of personal data and ensures that individuals are aware of how their information will be used.

iii) Data minimization & storage limitation

Data minimization mandates that organizations only gather personal data that is satisfactory, applicable and restricted to what is necessary for the intended purposes [63]. This principle encourages organizations to critically assess their data collection practices and avoid unnecessary accumulation of personal information.

According to this principle of storage limitation, personal data must be retained only for as long as necessary to fulfill the purpose for which it was collected. Organizations are required to establish retention periods and securely delete or anonymize data once it is no longer needed. This practice helps mitigate risks associated with prolonged storage of sensitive information.

iv) Overarching Accountability

Accountability requires organizations to validate compliance with all GDPR principles. This comprises

preserving records of dispensation actions and being prepared to display how they meet their obligations under the regulation [64]. Organizations must employ suitable mechanical and administrative measured to ensure compliance.

v) Integrity and Confidentiality

This principle emphasizes the need for organizations to secure personal data against unauthorized access, loss or damage. It requires implementing appropriate security measures to protect the integrity and confidentiality of personal information throughout its lifecycle. This principle is particularly important of sensitive categorizes of data.

These principles form the foundation of GDPR compliance, guiding organizations in their handling of personal data while safeguarding individual rights and freedom. Therefore, the table 2 summarize the cybersecurity frameworks with varied indicators.

Table 2: Cybersecurity Frameworks

Framework	Scope	Focus	Core Components	Applicability	Key Features
NIST cybersecurity Framework	U.S. framework for cybersecurity risk management	Cybersecurity practices and risk management	Core Functions, Implementation Tiers, Profiles	Widely applicable across industries in the U.S. and beyond	Emphasizes a flexible approach to managing cybersecurity risks through five core functions: Identify, Protect, Detect, Respond, Recover.
ISO 27000 Series	International standards for information security management	Information security management systems (ISMS)	ISMS requirements, Risk assessment, Continuous improvement	Organizations of all sizes globally	Provides a systematic approach to managing sensitive company information, including risk management.
OWASP	Open Web Application Security Project	Web application security	Top Ten risks, Security practices, Tools and resources	Developers and organizations building web applications	Focuses on the top 10 web application security risks and best practices for mitigation.
FISMA	U.S. federal law	Information security for federal agencies	Security standards, Risk management framework, Continuous monitoring	Federal agencies and contractors	Mandates the development of information security programs, risk assessments, and annual audits.
HIPAA	U.S. federal law	Health information privacy and security	Privacy Rule, Security Rule, Breach Notification Rule	Healthcare providers, insurers, and business associates	Protects patient health information with strict rules on data use and sharing.
COBIT	IT governance framework	IT management and governance	Governance framework, Management objectives, Performance metrics	Organizations needing strong IT governance practices	Aligns IT goals with business objectives, focusing on risk management and performance.
MITRE ATT&CK	Knowledge base of adversary tactics and techniques	Cyber threat intelligence and defense strategies	Tactics and techniques matrix, Threat modeling guidelines	Organizations seeking to enhance their cybersecurity posture	Provides a comprehensive matrix of known attack vectors to aid in defense planning.

Framework	Scope	Focus	Core Components	Applicability	Key Features
CIS Controls	Best practices for cybersecurity controls	Technical cybersecurity measures	20 Critical Security Controls (Basic, Foundational, Organizational), Implementation best practices	Organizations seeking practical guidance on implementation	Consists of 20 prioritized actions grouped into Basic, Foundational, and Organizational controls aimed at reducing risk.
GDPR	European Union regulation	Data protection and privacy	Principles, Rights of individuals, Obligations of controllers and processors	All organizations processing personal data of EU citizens	Emphasizes individual rights, data protection by design, and breach notification.

The frameworks present in the table, showcased that NIST CSF is broad and adaptable across industries, OWASP specifically targets web application security concerns. Likewise, regulatory compliance plays a crucial role in frameworks such as HIPAA and FISMA, which are legally mandated for specific sectors, whereas others like NIST CSF provide voluntary guidelines that can enhance overall cybersecurity posture without formal certification requirements. The core components highlight the structured approaches each framework takes towards cybersecurity. For instance, NIST's five core functions provide a comprehensive method to address cybersecurity risks systematically. Besides, the applicability of these frameworks ranges from specific industry needs (like HIPAA for healthcare) to more general uses (like ISO 27000 Series), making it essential for organizations to select frameworks that align with their operational context. Eventually, understanding these frameworks allows organizations to tailor their cybersecurity strategies effectively while ensuring compliance with relevant regulations and addressing specific security challenges within their operational environments.

Influence of regulatory bodies

i) Role of Regulatory Bodies

The influence of regulatory bodies in shaping cybersecurity frameworks is increasingly significant, particularly as organization face evolving cyber threats and the need for robust defenses. Here, the regulatory bodies, including agencies like CISA (Cybersecurity and Infrastructure Security Agent) and the NIST (National Institute of Standards And Technology) [65], play a momentous role in developing guidelines that govern cybersecurity practices. This collaboration with industry stakeholders ensures that frameworks are not only comprehensive but also adaptable to changing technological landscape and emerging threats. This collective effort is vital for fortifying defenses against cyber risk.

Framework Development: Regulatory framework serve as foundational structures that guide organizations in enhancing the cybersecurity posture. In 2024, NIST introduced cybersecurity framework 2.0, which expands its applicability beyond critical infrastructure to a broader range of entities, emphasizing governance and risk management as integral components of cybersecurity strategies.

ii) Compliance and Enforcement

*Mandatory Regulations vs. Frameworks***:** Regulatory compliance is legally enforced, requiring organizations to adhere to specific cybersecurity standards set by regulatory bodies. Non-compliance can lead to severe penalties, making it essential for organizations to comprehend the regulations applicable to the industry such as HIPAA for healthcare or be it GDPR for data protection in Europe [66]. In contrast, cybersecurity frameworks provide voluntary guidelines that help organizations enhance the security measures without the same level of legal obligation.

Industry-specific regulations: As cyber threats vary across sectors, regulatory bodies are increasingly tailoring frameworks to address specific vulnerabilities within industries. This targeted approach not only enhances compliance but also fosters a more effective defense against sector-specific risks.

iii) International Collaboration

Global standards and information sharing: The interconnected nature of cyber threats demands international collaboration among regulatory bodies, by sharing intelligence and best practices, countries can

develop cohesive strategies that bolster global cybersecurity defenses. This collaborative framework is crucial for addressing cross border cyber risks effectively.

Performance based regulation: Some regulatory tactics virtuously emphases on performance based metrics rather than perspective guidelines. Regulators define security objectives and allow organizations the flexibility to determine how best to meet these goals [67]. This method encourages innovation while ensuring accountability trough audits and compliance checks. Hence, the influence of regulatory bodies in cybersecurity frameworks is profound and multifaceted. Therefore, by nurturing collaboration, tailoring regulations and promoting international cooperation, these entities play a key role in enhancing organizational resilience against cyber threats.

5. Limitations of Existing Cybersecurity Frameworks and Current AI Solutions in Cybersecurity

While cybersecurity standards and frameworks aim to provide guidance for organizations to enhance the security posture, there exist few notable drawbacks such as High level guidance as many frameworks is too general making it challenging for organizations to apply effectively in real world scenarios. Inflexibility and slow updates as these regulations and frameworks are often slow to adapt to emerging threats and technologies. Moreover, establishing cybersecurity frameworks can be resource intensive and time consuming, potentially affecting productivity. Therefore, to overcome these drawbacks, AI based approaches have been opted. In the ever-evolving landscape of cybersecurity, AI has significantly streamlined the identification and resolution of security issues. According to the author [68], advanced AI techniques such as DL and ML analyze vast amount of data effectively to detect harmful patterns. These sophisticated systems are gradually replacing traditional rule based methods that reply o established threat signatures. Authors [68] have highlighted that anomaly detection system represent a major advancement in defensive AI, designed to identify unusual behaviors that maybe indicate potential security breaches. The algorithms employed in behavioral analytics enable organizations to detect user's exhibiting usual behavior. Systems powdered by DL father threat intelligence from a wide array of data sources, allowing them to uncover new vulnerabilities and potential attack vectors.

Despite the potential benefits of defense AI models, it faces numerous challenges. Accuracy remains a critical concern, as highlighted by the author, even though AI has the capacity to reduce false positive rates [69]. Poor labeling can hinder the detection of threats or trigger alerts when security personnel are already overwhelmed. Likewise, author [70] has examined whether AI models can effectively adapt to emerging threats, given that hackers continuously evolve their tactics, AI systems must be capable of recognizing patterns and deriving insights from limited datasets. Adaptability is essential for discovering novel methods to combat previously unknown threats, as noted by study [71]. Furthermore, the explain ability of AI models complicates defense efforts, making it challenging it fully truest the output. In critical scenarios, understanding the decision making processes of a model is essential, as inaccurate interpretations can result in severe consequences [72]. AI models and DL systems frequently function as "black boxes" creating challenges in comprehending the rationale behind the actions. Thus, to overcome these limitations, Generative AI is needed in cybersecurity. Therefore, figure 6 shows the growth of GenAI and it is noted that, there has been significant growth of GenAI in the realm of security domain.

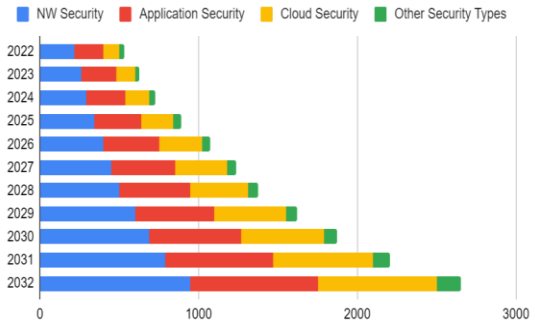

Figure 6. Projected growth of Generative AI in the security market 2022- 2032 (USD millions)[73]

6. Introduction to Generative AI in Cybersecurity

Generative AI is a transformative subset of AI that focuses on creating new content based on existing data. GenAI has emerged as a powerful tool for enhancing security measures, threat detection and incident response. These GenAI utilizes AI techniques such as GAN (generative adversarial networks) or transformer models to analyze massive amount of datasets and generate novel outputs. By learning underlying patterns and relationships within the data, GenAI can produce insights automate processes, and

even simulate attacks to test security systems. Therefore, some of the studies employed GenAI models are discussed. Present work have opted GenAI approaches for detecting cybersecurity attacks such as usage of GAN, SVM (support vector machine), AE (auto encoder), DAE (denoising autoencoder) [74] using NSL-KDD dataset, in which the outcome of the study has projected, that GenAI based GAN model has delivered better accuracy of 91.12% when compared to other models. Likewise, Attention-GAN [75]based GenAI model has adopted for detecting the cyber threats using CICIDS 2017 and KDDCup1999 datasets. Finally, the accuracy gained by attention-GAN model for CICIDS 2017 dataset is 99.69% and KDD dataset is 97.93%. Similarly, four different datasets have been explored in the study for capturing the attacks in the network using GAN model in which, better accuracy has been obtained by NSL-KDD dataset and UNSW-NB15 dataset.

Table 3: Comparing the existing models and datasets

References	Objectives	Dataset	Accuracy
[74]	Detecting cybersecurity attacks using GenAI models	NSL-KDD	91.12%
[75]	Detecting cyber threats using Attention-GAN	CICIDS 2017 and KDD	99.69% and 97.93%
[76]	The effectiveness of ML algorithms in intrusion detection	NSL-KDD and UNSW-NB15	98.6% and 97.8%
[77]	To develop and evaluate an optimized DL based IDS	NSL-KDD	84.19%
[78]	To developed an optimized AI - based Gen	NSL-KDD and UNSW-NB15	99.78% and 99.70%

Applications of GenAI in cybersecurity

GenAI has several critical applications in cybersecurity, enhancing various aspects of threat management.

- **Threat intelligence and detection:** GenAI improves threat intelligence by analyzing vast amounts of data to identify patterns indicative of potential attacks [79]. It can prioritize alerts based in an organization's specific risk profile, enabling security teams to focus on the most pressing threats.
- **Automated incident response:** By generating dynamic incident response playbooks, GenAI helps automate responses to security incidents. This capability reduces the burden on human analysts and allows for quicker reaction times during an attack.
- **Vulnerability management:** GenAI can analyze software code for vulnerabilities and suggest or apply patches automatically. This automation streamlines security processes and enhances overall system resilience [73].
- **Training simulations:** GenAI creates realistic training scenarios for cybersecurity professionals, allowing them to practice decision making in simulated environments that mimic real world attacks. This immersive training enhances the preparedness against actual threats.

Advantages of GenAI in Cybersecurity

The integration of GenAI into cybersecurity frameworks offers numerous benefits

- **Enhanced threat detection:** GenAI's ability to process large datasets allows for rapid identification of anomalies that might indicate cyber threats. This capability enables organization to detect zero-day attacks more effectively than traditional models.
- **Proactive risk management:** By simulating potential attacks scenarios, organizations can identify vulnerabilities before they are exploited. This proactive stance is crucial in maintaining robust defense mechanism against evolving threats.
- **Improved efficiency:** Automating routine tasks such as log analysis and incident response frees up cybersecurity professionals to focus ion more complex challenges [80]. This efficiency leads to better resource allocation within security teams.

7. Challenges and Future Recommendation

Findings of the Survey from Cybersecurity Frameworks

Findings of the work has demonstrated that, NIST cybersecurity framework has been used by the

organizations frequently due to its adaptability and comprehensive nature, making it suitable for a wide range of organizations.

Challenges Faced by Existing Genai Models

Though there are various positives of employing GenAI for cybersecurity identification process, there are certain pitfalls which needs to be addressed such as,

- **Vulnerability to malicious manipulation**: A major concern regarding GenAI system is the potential to be misused by malicious individuals. When wielded irresponsibility, these technologies can be exploited to uncover security weakness, create sophisticated malware and execute highly convincing phishing attacks, thereby jeopardizing the integrity of systems.
- **Struggle with long range dependencies:** Ensuring coherence and consistency in the generation of lengthy sequences presets significant challenges for GenAI models. Key features subsidizing to these difficulties include inadequate short-term memory, the reliance on fixed-length token sequence and the existence of vanishing gradient issues during the process of training, these limitations can ultimately hinder the effectiveness of system security measures.
- **Time exhaustive Setup**: GenAI require extensive training periods, often lasting from several weeks to months. This lengthy preparation time can pose challenges for organizations that need to respond quickly to security demands, potentially affecting the overall agility and responsiveness.
- **Lack of control:** Users have limited influence over the outputs of GenAI models, particularly, when these models produce content independently without explicit user guidance, this diminished control makes it challenging to detect, categorize and address nuanced threats, highlighting the need for careful examination by security professionals.
- **Risk of Unethical and Inappropriate Output:** Due to the innovative nature of GenAI models, their long term effects remain largely uncertain. As a result using GenAI models such as GAN, LLMs carries inherent risks that encompass both recognized and ye-to-be discovered factors.

Future Recommendation

Real time Analysis

Therefore, to overcome these challenges encountered by existing GenAI, real time data analysis can be opted in future, as implementation of GenAI models are capable of analyzing large datasets in real time to identify attacks and suspicious activities quickly. This proactive approach allows cybersecurity teams to respond faster to potential threats, minimizing damage and reducing response times. Moreover, implementation of continuous feedback mechanism is significant, since GenAI systems learn from new data inputs and adapt their threat detection algorithms accordingly. This ensures that security measures evolve alongside emerging threats. Besides, regularly update cybersecurity frameworks to adapt to emerging threats facilitated by advancements in technology. This includes monitoring trends in cyberattacks that utilize GenAI, ensuring that security measures are always current and effective.

By integrating GenAI's capabilities for real-time threat detection and response with the advanced encryption techniques afforded by quantum technology, organizations can create a multi-layered defense strategy that not only anticipates but also mitigates potential attacks before they materialize. The synergy between these technologies allows for the development of adaptive security protocols that evolve alongside emerging threats, thereby maintaining efficacy against sophisticated cyber adversaries who increasingly utilize AI-driven tactics.

Adaptive Learning Algorithms

Future GenAI systems should incorporate continuous learning mechanisms that allow them to evolve with new data inputs. This adaptability will help maintain the effectiveness against novel cyber threats and tactics employed by malicious actors, ensuring that these systems can respond dynamically to an ever-changing landscape of risks. By leveraging techniques such as reinforcement learning and continual learning algorithms, GenAI can continuously update its knowledge base, thereby minimizing the risk of catastrophic forgetting, where the model loses previously acquired knowledge when trained on new data.

Quantum Computing Integration

Furthermore, quantum technology along with GenAI can be inherited in future as a part of future recommendation. Quantum technology has the potential to revolutionize cybersecurity by providing unprecedented computational power and enhanced encryption methods. This holistic approach can ultimately transform how organizations defend against cyber threats, ensuring robust protection in an increasingly complex landscape.

Moreover, as cybercriminals become more adept at leveraging AI tools for malicious purposes, the combination of GenAI and quantum technology will empower organizations to stay one step ahead. This integration will facilitate automated risk assessments and continuous monitoring, allowing for proactive identification of vulnerabilities across digital infrastructures.

Automating Compliance Monitoring

Future advancements could include automating the monitoring of compliance with cybersecurity regulations. GenAI can help organizations ensure they meet legal requirements while minimizing the administrative burden associated with compliance tasks

8. Conclusion

The present survey makes a distinctive contribution to the cybersecurity literature by providing the first comprehensive analysis of the intersection between established cybersecurity frameworks and emerging Generative AI technologies. While previous studies have examined cybersecurity frameworks and AI applications separately, this work uniquely bridges these domains, offering novel insights into how traditional risk management approaches must evolve to accommodate AI-enhanced security capabilities and address AI-specific vulnerabilities. By systematically reviewing the applicability of frameworks such as NIST, ISO/IEC 27000, and COBIT in the context of GenAI, this survey identifies critical gaps in current approaches and proposes specific adaptations required for effective cybersecurity in the AI era. Furthermore, it explored the interplay between these frameworks and emerging technologies, particularly GenAI (Generative AI), which presented both opportunities and challenges in the realm of cybersecurity this multifaceted approach not only highlighted the importance of compliance with regulatory standards but also addressed the evolving nature of cyber threats that obliged continuous adaptation and improvement of security measures. Ultimately, the current survey pursued to contribute valuable insights into best practices for safeguarding sensitive information against increasingly sophisticated cyberattacks. The findings demonstrate that leveraging GenAI along with the existing cybersecurity frameworks provides a promising pathway for organizations worldwide to improve real-time threat analysis, proactive defence mechanisms and long-term resilience making this knowledge valuable for a broad readership committed to advancing cybersecurity practices in diverse organizational contexts.

References

[1] O. Renuka, N. RadhaKrishnan, B. S. Priya, A. Jhansy, S. J. E. T. Ezekiel, and C. i. Cybersecurity, "Data Privacy and Protection: Legal and Ethical Challenges," pp. 433-465, 2025.

[2] B. Firmansyah, "Cybersecurity Fundamentals," in *Challenges in Large Language Model Development and AI Ethics*: IGI Global, 2024, pp. 280-320.

[3] D. I. EKWUNIFE, O. T. PRECIOUS, O. A. RASUL, O. F. AKINLADE, T. O. NWOKORO, and V. I. IKPE, "Cyber threat and information shortage: The immediate risk of supply chain technology and how to tackle them," 2024.

[4] D. Ayaz and J. Elsa, "Cloud Security in a Connected World: Safeguarding Data and Privacy," EasyChair, 2516-2314, 2024.

[5] H. Jamal, N. A. Algeelani, N. J. C. S. Al-Sammarraie, and I. Technologies, "Safeguarding data privacy: strategies to counteract internal and external hacking threats," vol. 5, no. 1, pp. 46-54, 2024.

[6] M. O. Akinsanya, C. C. Ekechi, C. D. J. C. S. Okeke, and I. R. Journal, "The evolution of cyber resilience frameworks in network security: a conceptual analysis," vol. 5, no. 4, pp. 926-949, 2024.

[7] S. AlDaajeh, S. J. C. Alrabaee, and Security, "Strategic cybersecurity," vol. 141, p. 103845, 2024.

[8] O. C. Obi *et al.*, "Comprehensive review on cybersecurity: modern threats and advanced defense strategies," vol. 5, no. 2, pp. 293-310, 2024.

[9] W. S. Admass, Y. Y. Munaye, A. A. J. C. S. Diro, and Applications, "Cyber security: State of the art, challenges and future directions," vol. 2, p. 100031, 2024.

[10] M. Toussaint, S. Krima, and H. J. J. o. I. I. I. Panetto, "Industry 4.0 data security: A cybersecurity frameworks review," p. 100604, 2024.
[11] S. K. Gupta and V. K. Dwivedi, "Evaluation of hydraulic jump characteristics in rough sloping surfaces for sustainable environment: A laboratory investigation," *Sigma Journal of Engineering and Natural Sciences,* vol. 43, no. 1, pp. 148-159, 2025.
[12] A. Kıral and Z. Tonyalı, "The effect of LRB stiffness changes with and without supplemental viscous dampers on seismic responses of an experimentally verified mdof building," *Sigma Journal of Engineering and Natural Sciences,* vol. 43, no. 1, pp. 301-315, 2025.
[13] T. O. Abrahams, S. K. Ewuga, S. O. Dawodu, A. O. Adegbite, A. O. J. C. S. Hassan, and I. R. Journal, "A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection," vol. 5, no. 1, pp. 1-25, 2024.
[14] M. Ibrar, S. Yin, H. Li, S. Karim, A. A. J. I. J. o. E. S. Laghari, and D. Forensics, "Comprehensive review of emerging cybersecurity trends and developments," vol. 16, no. 5, pp. 633-647, 2024.
[15] A. J. I. J. o. C. AL-Hawamleh and D. Systems, "Cyber resilience framework: Strengthening defenses and enhancing continuity in business security," vol. 15, no. 1, pp. 1315-1331, 2024.
[16] I. A. Barbhuiya, S. Laroiya, and R. J. A. a. S. Singh, "Holistic Cybersecurity Risk Management Framework," 2024.
[17] H. Boyes and M. D. J. J. o. I. S. Higgins, "An Overview of Information and Cyber Security Standards," vol. 12, no. 1, pp. 95-134, 2024.
[18] K. J. I. J. o. A. I. R. Patel and Development, "Ethical reflections on data-centric AI: balancing benefits and risks," vol. 2, no. 1, pp. 1-17, 2024.
[19] R. H. Chowdhury, N. U. Prince, S. M. Abdullah, L. J. W. J. o. A. R. Mim, and Reviews, "The role of predictive analytics in cybersecurity: Detecting and preventing threats," vol. 23, no. 2, pp. 1615-1623, 2024.
[20] A. J. R. E. d. D. C. Damaraju, "Mitigating Phishing Attacks: Tools, Techniques, and User Education," vol. 18, no. 02, pp. 356-385, 2024.
[21] W. Wang, S. M. Sadjadi, and N. Rishe, "A Survey of Major Cybersecurity Compliance Frameworks," 2024: IEEE, pp. 23-34.
[22] S. Jawhar, J. Miller, and Z. Bitar, "AI-based cybersecurity policies and procedures," 2024: IEEE, pp. 1-5.
[23] S. Jawhar, J. Miller, and Z. Bitar, "AI-based cybersecurity policies and procedures," in *2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC)*, 2024: IEEE, pp. 1-5.
[24] O. Badmus, S. A. Rajput, J. B. Arogundade, and M. J. R. Williams, October, "AI-driven business analytics and decision making," 2024.
[25] S. J. J. o. A. R. i. L. Rawat and I. Science, "Navigating the Cybersecurity Landscape: Current Trends and Emerging Threats," vol. 10, no. 3, pp. 13-19, 2023.
[26] S. AlDaajeh *et al.*, "The role of national cybersecurity strategies on the improvement of cybersecurity education," vol. 119, p. 102754, 2022.
[27] H. J. E. Taherdoost, "Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview," vol. 11, no. 14, p. 2181, 2022.
[28] D. P. Möller, "NIST cybersecurity framework and MITRE cybersecurity criteria," in *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*: Springer, 2023, pp. 231-271.
[29] G. Beuchelt, "Information Technology Security Management," in *Computer and Information Security Handbook*: Elsevier, 2025, pp. 475-508.
[30] M. Syafrizal, S. R. Selamat, N. A. J. I. J. o. C. N. Zakaria, and I. Security, "Analysis of cybersecurity standard and framework components," vol. 12, no. 3, pp. 417-432, 2020.
[31] A. Oruc, A. Amro, and V. J. S. Gkioulos, "Assessing cyber risks of an INS using the MITRE ATT&CK framework," vol. 22, no. 22, p. 8745, 2022.
[32] J. Kinnunen, "Threat Detection Gap Analysis Using MITRE ATT&CK Framework," 2022.
[33] S. Suominen, "Cyber Threat Intelligence Management in Technical Cybersecurity Operations," 2024.
[34] W. Xiong, E. Legrand, O. Åberg, R. J. S. Lagerström, and S. Modeling, "Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix," vol. 21, no. 1, pp. 157-177, 2022.
[35] Y.-J. J. A. S. Lee, "A Study on a Scenario-Based Security Incident Prediction System for Cybersecurity," vol. 14, no. 24, p. 11836, 2024.
[36] S. Roy, E. Panaousis, C. Noakes, A. Laszka, S. Panda, and G. J. a. p. a. Loukas, "Sok: The mitre att&ck framework in research and practice," 2023.
[37] B. Al-Sada, A. Sadighian, and G. J. A. C. S. Oligeri, "MITRE ATT&CK: State of the art and way forward," vol. 57, no. 1, pp. 1-37, 2024.

[38] A. Bolla and F. Talentino, "Threat Hunting driven by Cyber Threat Intelligence," Politecnico di Torino, 2022.

[39] S. Zhang *et al.*, "An automatic assessment method of cyber threat intelligence combined with ATT&CK matrix," vol. 2022, no. 1, p. 7875910, 2022.

[40] I. H. Sarker, "Cybersecurity Background Knowledge: Terminologies, Attack Frameworks, and Security Life Cycle," in *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability*: Springer, 2024, pp. 21-39.

[41] M. F. Abo El Rob, M. A. Islam, S. Gondi, and O. J. I. i. I. S. Mansour, "The application of MITRE ATT&CK framework in mitigating cybersecurity threats in the public sector," vol. 25, no. 3, 2024.

[42] D. Upadhyay and N. R. Ware, "Evolving Trends in Web Application Vulnerabilities: A Comparative Study of OWASP Top 10 2017 and OWASP Top 10."

[43] S. Patil, M. Rao, L. Misal, D. Phaldesai, and K. Shivsharan, "A Review of the OW ASP Top 10 Web Application Security Risks and Best Practices for Mitigating These Risks," 2023: IEEE, pp. 1-8.

[44] S. K. Sahu, "Security Standards and Best Practices," in *Building Secure PHP Applications: A Comprehensive Guide to Protecting Your Web Applications from Threats*: Springer, 2024, pp. 249-313.

[45] M. A. Helmiawan, E. Firmansyah, I. Fadil, Y. Sofivan, F. Mahardika, and A. Guntara, "Analysis of web security using open web application security project 10," 2020: IEEE, pp. 1-5.

[46] R. Vallabhaneni, S. A. Vaddadi, S. Pillai, S. R. Addula, B. J. I. J. o. E. E. Ananthan, and C. Science, "MobileNet based secured compliance through open web application security projects in cloud system," vol. 35, no. 3, pp. 1661-1669, 2024.

[47] M. Idris, I. Syarif, and I. J. E. i. j. o. e. t. Winarno, "Web application security education platform based on OWASP API security project," pp. 246-261, 2022.

[48] E. J. M. E. T. Koza, "Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in the context of operational and strategic information security," vol. 2, pp. 26-39, 2022.

[49] A. Qusef and H. J. P. C. S. Alkilani, "The effect of ISO/IEC 27001 standard over open-source intelligence," vol. 8, p. e810, 2022.

[50] O. Vakhula, Y. Kurii, I. Opirskyy, and V. Susukailo, "Security as Code Concept for Fulfilling ISO/IEC 27001: 2022 Requirements," in *CPITS*, 2024, pp. 59-72.

[51] A. S. C. Junior and C. H. J. R. F. Arima, "Cyber risk management and iso 27005 applied in organizations: A systematic literature review," vol. 16, no. 02, pp. e1188-e1188, 2023.

[52] G. B. Mateus, "ISO/IEC 27005."

[53] F. Kitsios, E. Chatzidimitriou, and M. J. S. Kamariotou, "The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector," vol. 15, no. 7, p. 5828, 2023.

[54] S. Peltonen, "ISO27000 implementation handbook," 2024.

[55] H. M. J. J. o. C. Melaku and Privacy, "A dynamic and adaptive cybersecurity governance framework," vol. 3, no. 3, pp. 327-350, 2023.

[56] A. J. D. v. G. H. D. Efe, "A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT," vol. 3, no. 2, pp. 185-205, 2023.

[57] E. Oluomachi, A. Ahmed, W. Ahmed, and E. J. a. p. a. Samson, "Assessing The Effectiveness Of Current Cybersecurity Regulations And Policies In The US," 2024.

[58] D. P. Sharma, A. Habibi Lashkari, and M. Parizadeh, "The Basic of Cybersecurity Concept," in *Understanding Cybersecurity Management in Healthcare: Challenges, Strategies and Trends*: Springer, 2024, pp. 19-34.

[59] T. Kavitha, M. Sandhya, V. Subashini, and P. Srikanth, "Secure Communication in Internet of Things: Emerging Technologies, Challenges, and Mitigation," 2024.

[60] Ž. Spalević and K. J. T. E. J. o. A. E. Vićentijević, "GDPR and challenges of personal data protection," vol. 19, no. 1, pp. 55-65, 2022.

[61] V. Wylde *et al.*, "Cybersecurity, data privacy and blockchain: A review," vol. 3, no. 2, p. 127, 2022.

[62] P. Voigt and A. von dem Bussche, "Scope of application of the GDPR," in *The EU General Data Protection Regulation (GDPR) A Practical Guide*: Springer, 2024, pp. 9-36.

[63] D. J. J. N. D. L. R. Solove, "The limitations of privacy rights," vol. 98, p. 975, 2022.

[64] C. P. Efunniyi *et al.*, "Strengthening corporate governance and financial compliance: Enhancing accountability and transparency," vol. 6, no. 8, pp. 1597-1616, 2024.

[65] Z. Ciekanowski, J. Nowicka, M. Czternastek, S. Żurawski, and P. Mikosik, "How cybersecurity

shapes effective organizational management," 2024.
[66] S. A. Oyetunji, "Investigating Data Protection Compliance Challenges."
[67] J. R. Biden, "Executive order on the safe, secure, and trustworthy development and use of artificial intelligence," 2023.
[68] I. Jada, T. O. J. D. Mayayise, and I. Management, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," vol. 8, no. 2, p. 100063, 2024.
[69] R. Kaur, D. Gabrijelčič, and T. J. I. F. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," vol. 97, p. 101804, 2023.
[70] T. S. Oyinloye, M. O. Arowolo, R. J. D. S. Prasad, and Management, "Enhancing Cyber Threat Detection with an Improved Artificial Neural Network Model," 2024.
[71] O. C. Bordeanu, "From Data to Insights: Unraveling Spatio-Temporal Patterns of Cybercrime using NLP and Deep Learning," UCL (University College London), 2024.
[72] S. R. Sindiramutty *et al.*, "Explainable AI for Cybersecurity," in *Advances in Explainable AI Applications for Smart Cities*: IGI Global, 2024, pp. 31-97.
[73] K. Palani, J. Kethar, S. Prasad, and V. J. J. o. S. R. Torremocha, "Impact of AI and Generative AI in transforming Cybersecurity," vol. 13, no. 2, 2024.
[74] H. J. J. o. W. A. Sinha and C. Security, "The identification of network intrusions with generative artificial intelligence approach for cybersecurity," vol. 2, no. 2, pp. 20-29, 2024.
[75] M. A. J. a. p. a. Sen, "Attention-GAN for Anomaly Detection: A Cutting-Edge Approach to Cybersecurity Threat Management," 2024.
[76] F. Türk, "Analysis of intrusion detection systems in UNSW-NB15 and NSL-KDD datasets with machine learning algorithms," *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi,* vol. 12, no. 2, pp. 465-477, 2023.
[77] N. M. Eldakhly, "Optimized intrusion detection with deep learning classification models," *Neural Computing and Applications,* pp. 1-29, 2025.
[78] S. Siva Shankar, B. T. Hung, P. Chakrabarti, T. Chakrabarti, and G. Parasa, "A novel optimization based deep learning with artificial intelligence approach to detect intrusion attack in network system," *Education and Information Technologies,* vol. 29, no. 4, pp. 3859-3883, 2024.
[79] L. R. J. I. B. O. L. Easton Jameson and LITERATURE, "Advancing GenAI for Real-Time Cybersecurity: Applications in Threat Detection and Adaptive Response," vol. 7, no. 3, pp. 77-85, 2024.
[80] H. Hayagreevan and S. J. a. p. a. Khamaru, "Security of and by Generative AI platforms," 2024.