JACoIT
Journal of Applied Computer and Information Technology

Review

Cybersecurity risk management strategy for AI and SaaS platforms: A NIST framework approach

Muhammad Zaim Zainuddin [1*], Muhammad Sharin Yasin [1] , Muhammad Azerul Azaman [1] and Mohamad Fadli Zolkipli [1]

[1]School of Computing, Universiti Utara Malaysia, Sintok, Malaysia; m_zaim_zainuddin@soc.uum.edu.my; m_sharin_yasin@soc.uum.edu.my; m_azerul_azaman@soc.uum.edu.my; m.fadli.zolkipli@uum.edu.my

[*]Corresponding Author: m_zaim_zainuddin@soc.uum.edu.my

Received: 22 December 2025
Revised: 3 February 2026
Accepted: 6 March 2026
Published: 2 April 2026

Abstract

The rapid growth in Information Technology (IT) and Software industries particularly within Artificial Intelligence (AI) and Software-as-a-Service (SaaS) has accelerated the pace of the fourth industrial innovation, and at the same time, this growth produced complex vulnerabilities to security. The conventional defense mechanisms are becoming less effective over time against the evolving threats like adversarial data poisoning, API exploits and advanced ransomware attacks targeting cloud infrastructures. The primary goals of this paper are to address these issues by developing a comprehensive risk management plan that is based on the NIST Cybersecurity Framework (CSF). Additionally, this study identifies critical vulnerabilities in modern AI and SaaS environments using a qualitative risk assessment approach and a likelihood-versus-impact matrix. The analysis shows that data breaches and API exploitation are the most serious threats, which have significant impact on organization operations and the high likelihood. Moreover, the findings indicate that incorporating the NIST CSF core capabilities such as Identify, Protect, Detect, Respond and Recover is a well-organized framework of minimizing these high-priority threats using layered preventive and detective controls. Ultimately, the results highlight how important it is to embrace standards-based systems to shift organizations from reactive security measures to proactive resilience to ensure the integrity and continuity of the interconnected software ecosystem.

Keywords: cybersecurity risk management; NIST cybersecurity framework (CSF); AI and SaaS security; cloud computing

1. Introduction

The Information Technology (IT) and Software Domain have become an important component for modern organization strategy and innovation. It is also involved in building and managing computers, software and networks. IT has evolved from a minor support role to a primary source of competitive advantage helping businesses and society grow and change. Updates in software and technology often lead to big changes in other industries too [7]. Artificial

Intelligence (AI), cloud computing, data analysis and cybersecurity tools can be used to solve the way companies work, the way people communicate and the way important problems in the world are solved is shaped by IT and software.

AI plays a double role in cybersecurity either to help protect systems or to create a new risk. AI can quickly scan large amounts of data to detect and prevent threats before it causes any damage. If cybercriminals use AI, they can run smarter phishing scams and tamper with AI models. That's why securing AI is just as important as using it for protection.

This cybersecurity concern also affects Software-as-a-Service (SaaS) platforms that store important company data. It has become top targets for cyberattack [3]. Older security methods that protect the outer edge of the network are no longer sufficient in handling evolving threats. It's important to protect both data and user accounts stored in the cloud. A powerful cybersecurity can help stop attacks on SaaS platforms from setup errors, stolen login details or problems with third-party services. In order to make it secure, it's important to manage user access and regularly monitor the system.

However, previous research has examined cloud security vulnerabilities [1,6] and the transformation of cyber risks by AI [8,13] in isolation yet what remains unexplored is a unified approach that considers the intersection of these domains. Current studies do not provide a systematic and structured use of the NIST Cybersecurity Framework 2.0 within AI driven SaaS environments. This paper seeks to close this gap by presenting a tailored risk management strategy that applies the updated NIST guidelines in relation to specific AI SaaS vulnerabilities. In this way the study strengthens existing work by moving beyond general surveys and offering a clear roadmap that supports proactive defense.

2. Materials and Methods

The present study is founded on a qualitative research design based on the systematic literature review (SLR) analyzing the cybersecurity risk management approaches towards Artificial Intelligence (AI) and Software as a Service (SaaS) platform. The design recognizes the existing threats and assesses mitigation strategies and links the findings with the essence of the NIST Cybersecurity Framework (CSF) 2.0 core functions. In this section, the materials to be used in analysis and the methodology used to arrive at the study findings are described.

2.1 Materials

Peer reviewed journal articles, conference proceedings and official framework documentation published between 2021 and 2025 will be used as the materials of this research. It was selected as the most recent data on AI integration cloud security and the revised NIST framework was interested in.

Scholarly databases which were searched include IEEE Xplore, Google Scholar and ScienceDirect and used to gather the data. The search was conducted using combinations of keywords ‘Cybersecurity Risk Management AND Software as a Service’,‘Artificial Intelligence in Cybersecurity’,‘Cloud Computing Threats and Saas Vulnerabilities’ and ‘NIST Cybersecurity Framework and AI Security’. The research was given the first priority in the case of studies that

provided empirical information about cloud security models (IaaS PaaS SaaS) and AI based threat detection. Inclusion Criteria:

1. Focused on AI, SaaS or cloud service security (IaaS, PaaS, SaaS).
2. Provided empirical evidence, frameworks or systematic analyses.
3. Were peer-reviewed or authoritative.
4. Published in English between 2021-2025.

Exclusion Criteria:

1. Were unrelated to AI or cloud security.
2. Were non-English.
3. Lacked methodological rigor or clear evidence.
4. Focused only on non-cloud or non-AI security.

After removing duplicates and screening titles and abstracts, studies that met the inclusion criteria were reviewed in full text. Only studies that satisfied all criteria were retained, resulting in the final studies.

One of the documents is the NIST Cybersecurity Framework (CSF) 2.0 that was introduced by the National Institute of Standards and Technology in 2024. This framework offers the taxonomy of cybersecurity outcomes Govern Identify Protect Detect Respond and Recover applied as the foundations of risk assessment [10].

The work that was taken into consideration in the study reflected the problems of cloud models and AI applications. In the case of Ademilua and Areghan [1], the authors provided a quantitative study of the risk scores of IaaS PaaS and SaaS models. Lad [8] paid attention to the integration of AI against the emerging cloud threats. Those that were not in English or articles that did not focus on AI or cloud security were eliminated.

The materials chosen include a variety of risks. The article by Fatima et al. [6] reported the results of SQL injection and malicious attacks based on QR code in SaaS. Ajish [3] discussed the topic of AI in Zero Trust designs. Mizrak [9] added to the knowledge about how to align the risks with the management of the organization and the article by Laato et al. [7] touched on the cultural dimension of software development. Summarisation of the study used in this research is shown below.

Table 1. Summary of Reviewed Literature

Author(s) & Year	Focus Area	Key Findings	Identified Challenges
Ademilua & Areghan (2025)	The security risks across three main cloud service models IaaS, PaaS and SaaS are looked at in the study. Weaknesses such as misconfigurations and insecure APIs are examined and strategies	It was shown by the results that the highest average risk score was held by SaaS at 7.11. PaaS was followed by 6.69 and IaaS by 6.21. A significant difference in risk levels across the models was not found by ANOVA. It was confirmed by	The shared multi-tenant nature of the cloud is highlighted as a major challenge by the study. Risks such as cross tenant data leakage can be led to by this design. Other ongoing problems include human mistakes in

	that can help stop data breaches are reviewed.	regression analysis that risk scores are strongly predicted by the type of cloud model. A leading cause of breaches was found to be misconfigurations.	configuration, insecure third-party APIs, lack of encryption and weak access controls such as missing MFA.
Ahsan et al. (2022)	A broad review of cybersecurity threats such as malware, phishing and DDoS is given by the paper. It explains different types of Machine Learning, including shallow, deep and reinforcement learning that can help reduce these risks and improve Intrusion Detection Systems.	It is shown by the findings that traditional signature-based methods work better than by Machine Learning especially Deep Learning models such as DBNs and CNNs. New and complex attacks are able to be detected by these models. Up to 99 percent accuracy on benchmark datasets was reached by some ensemble methods like Random Forest.	Major challenges are also pointed out by the study. Recently balanced datasets are not enough. Training data can be poisoned by attackers in Adversarial Machine Learning. False confidence in model performance can be created by Data Leakage. The future threat of Quantum Computing which may break current encryption methods is identified as another challenge.
Ajish (2024)	The important role of Artificial Intelligence in improving Zero Trust security models is looked at by the study. Key areas such as Identity, Device, Network and Data are focused on replacing weak traditional security boundaries by AI.	The security is changed from static to dynamic by the mix of AI and Zero Trust. Continuous authentication is made possible by AI. It means that users are verified throughout a session instead of only at login. Adaptive risk scoring is also allowed by checking behavioral biometrics and unusual activity. Network security is improved by AI through smart micro segmentation and real time threat detection that cannot be caught by older rule-based systems.	The challenges of using AI in Zero Trust are also pointed out by the paper. High-quality datasets are needed for training which creates concerns about data privacy. Problems with algorithm transparency are also present as AI decisions are often hard to explain. Another major issue is Adversarial AI where the models themselves are manipulated by attackers to get past security controls.
Aljumaiah et al. (2025)	Cybersecurity threats that target critical infrastructure such as Industrial Control Systems and Operational Technology are examined in the study. The effectiveness of the NIST Cybersecurity Framework in identifying and reducing these risks is also reviewed.	Human weaknesses such as negligence and lack of training were identified as the most common threats with twelve cases recorded for each. Poor visibility of threats was noted as another major issue. In terms of mitigation, the NIST functions Identify and Protect were utilized the most at 28% each. Recover was found to be the least used at 5% which indicates a gap in resilience planning.	It is pointed out by the study that the weakest link remains human error and that it is hard to remove. Old legacy systems that cannot be patched easily often lead to a dependence on critical infrastructure because downtime is considered too costly. A serious lack of recovery planning is also noted which leaves organizations exposed to long term damage after a breach.
Fatima et al. (2024)	Security challenges and attacks affecting three cloud computing models. For example, Software as a Service, Platform as a Service, and Infrastructure as a Service are examined in the study.	It is shown by the research that weaknesses are present in each model. SQL injection which can be detected with 99.8 percent accuracy using Random Forest is vulnerable to SaaS. Fake QR code attacks also expose SaaS. Problems with unauthorized access are faced by PaaS which can be reduced by using the Multi Perspective PaaS Security Model. Data breaches are struggled with by IaaS due to gaps in shared responsibility.	Major challenges are also pointed out by the study. Standard security measures are not established across cloud models. Emerging threats are not studied adequately. Awareness about shared security responsibilities is often lacking among users. The difficulty of building reliable datasets for training security models is another problem as most rely on small, combined datasets.

Laato et al. (2022)	Major technology trends in the software industry and their effects on the future of work are looked at by the study. The influence of fast changes in technology on work practices is focused on by the study through the use of Cultural Lag Theory.	Four main directions shaping software work were found by the study. First, a move toward scalable product-based solutions like SaaS is being observed. Second, a stronger focus on using data is being emphasized. Third, a merging of traditional non-IT industries with IT is taking place. Fourth, the main computing model has become the Cloud.	One big challenge is Cultural Lag. Technology is growing quickly but laws and human work habits are changed more slowly by organizations. Friction is created by this. It is shown by the study that strong pressure for constant learning is faced by workers and that the adjustment of skills and processes to keep up with new technology is struggled with by organizations.
Lad (2024)	The role of Artificial Intelligence in protecting cloud computing systems from new threats such as Advanced Persistent Threats, ransomware and insider attacks is looked at by the study.	Security is improved by AI in several ways. Real time detection of threats is allowed. Predictive analytics is used to forecast attacks based on past data. Automated incident response is also provided which reduces human mistakes. It is explained by the study that old perimeter-based models are not enough for modern cloud environments.	Big challenges are still present. Data privacy and regulatory compliance must be ensured. AI biases need to be managed. The technical complexity of scaling AI solutions across different infrastructures is acknowledged. The risks of misconfigurations in shared responsibility models and the need to protect AI systems themselves from adversarial manipulation are also pointed out by the paper.
Mizrak (2023)	The link between cybersecurity risk management and strategic business management is looked at by the study. It is explored how security protocols can be built into wider business strategies by organizations to protect digital assets.	It is explained by the research that cybersecurity is no longer just an IT problem. It is now recognized as a strategic priority that must be included in the core business plan. This ensures resilience and protects infrastructure against advanced attacks.	One major challenge is that cyber threats are continuously changing. It means that dynamic strategies must be implemented instead of static ones. The difficulty of aligning different risk factors such as supply chain risks and IoT vulnerabilities with unified corporate governance and planning is also shown by the study.
National Institute of Standards and Technology (2024)	The updated NIST Cybersecurity Framework 2.0 is introduced. Clear guidelines and best practices are provided that help organizations of any size and sector manage and reduce cybersecurity risks.	A major change in version 2.0 is the addition of the Govern function. It is highlighted that cybersecurity is a major enterprise risk that requires oversight from senior leadership. A flexible risk-based approach is supported by the framework that brings cybersecurity into wider enterprise risk management instead of treating it as a separate technical issue.	The challenge of Cybersecurity Supply Chain Risk Management is also dealt with by the framework. The difficulty of securing extended third-party networks is noted. Another focus is placed on closing communication gaps between technical teams and nontechnical leadership. The aim is to create a common language that allows security investments and risks to be discussed more effectively by organizations.
Parmar & Miles (2024)	The NIST Cybersecurity Framework version 2.0 from the United States is compared with the EU Network and Information Systems Directive 2 by the study. An examination is conducted regarding how well they align and	The importance of core security functions and governance is agreed upon by both frameworks. Different purposes are served by them. A flexible voluntary guide of best practices is provided by NIST. A mandatory legal directive for EU	The fragmentation of standards across borders is recognized as one major challenge. The difficulty of combining voluntary frameworks like NIST with mandatory directives like NIS2 is faced by multinational

	how suitable they are for large organizations such as NATO and ESA.	member states is represented by NIS2. It is shown by the study that NIST version 2.0 can help with NIS2 compliance, but it is not guaranteed. Strict rules such as mandatory reporting timelines including a 24-hour early warning and penalties are included by NIS2 that are not covered by NIST.	organizations. Confusion is created by the lack of a single global standard. Complex action plans must be built by organizations to close the gap between compliance rules and technical best practices.
Rohatgi (2020)	The complex field of SaaS security in cloud environments is looked at by the paper. Clear best practices such as encryption and identity access management with integration methods that protect sensitive data and meet regulatory requirements.	A layered approach is needed for strong SaaS security. This includes robust encryption with AES MFA and continuous monitoring through SIEM tools. It is also explained in the paper that future security designs must be grown to include Zero Trust principles, AI and machine learning for threat detection and quantum safe cryptography to stay resilient.	The Shared Responsibility Model is considered one major challenge. Gaps in security are often created by unclear roles between providers and customers. Complex regulatory rules such as GDPR and HIPAA are also struggled with by organizations. Changing threats like insider attacks and weaknesses introduced by new technologies such as containerization must also be dealt with.
Souppaya et al. (2022)	The Secure Software Development Framework is explained by the document. A set of high-level practices that can be added to any software development life cycle to reduce software vulnerabilities is represented by this.	The idea of shifting left is highlighted by the framework which means that security is addressed early in the development process. Technical debt and cost are lowered by this approach. A shared language is also provided making communication easier between software producers and buyers. The requirements of Executive Order 14028, which focuses on software supply chain security, are mapped to the practices.	It is pointed out by the publication that security practices are not clearly included by most software development models. It is stressed that flexibility and a risk-based approach must be maintained during implementation since every project does not fit all practices. The complexity of shared responsibility in cloud environments is also noted where security duties are split by providers and tenants.
Zeijlemaker et al. (2025)	The dual impact of Artificial Intelligence on Cyber Risk Management is looked at by the study. The ways in which cyber threats can be both increased by AI and defense strengthened across the NIST Cybersecurity Framework version 2.0 functions are explored.	AI is described as a double-edged sword. On the offensive side, the barrier for attackers is lowered through methods such as AI driven phishing and deepfakes. On the defensive side, threat detection is automated and improved by anomalies being spotted in real time and incident response is sped up by the time needed to react being reduced. The study confirms that AI is useful across all NIST functions but is most advanced in Detect and Respond.	New risks are also brought by the integration of AI. Data can be poisoned or models evaded by adversarial AI. A black box problem is created by explainability issues where interpretations of decisions are hard to make. The lack of high-quality training data, the risk of algorithmic bias and the growing skills gap needed to manage complex AI-based security systems are included among other challenges.
Manchana (2023)	The study is looked at in terms of how SaaS security can be improved through a proactive and collaborative approach. The focus is placed on closing the gap between cybersecurity product	It is concluded by the research that SaaS security is not only a technical issue but also an organizational one. Collaboration across teams is required to balance fast development cycles with	The attack surface is increased by the distribution of SaaS platforms. Constant tension exists between the need to keep up with rapid DevOps speed and the application of strict security

	engineering and IT teams so that security is built directly into the software development life cycle instead of being added later.	strong defense. The success of using a layered security architecture across the application data and network layers is highlighted by the study. The value of aligning with the NIST Cybersecurity Framework to build resilient cloud native products is also shown.	controls. High complexity is also associated with securing third party dependencies in shared cloud environments.
Molnar & Sabodashko (2024)	The cybersecurity capabilities of three major cloud providers, AWS, Azure and GCP are compared in the study. Their security tools and services are evaluated against the five core functions of the NIST Cybersecurity Framework such as Identify, Protect, Detect, Respond and Recover.	Clear advantages for each provider are shown by the analysis. Customizable identity management and protective technologies are provided strongly by AWS. Better integration for organizations using the Microsoft ecosystem is offered by Azure and strong governance tools are provided. Data security is led by GCP with automatic encryption at rest and advanced AI features.	The shared responsibility model must be dealt with by organizations as it can be complex. Regulatory compliance such as GDPR and CCPA must also be managed. Another risk involves misconfiguration in multi-tenant cloud environments that can expose systems to cross tenant threats.
Ali (2021)	Cybersecurity challenges in cloud computing are looked at in the study. Risks such as data breaches and identity theft are focused on while the effectiveness of protection methods is tested ranging from traditional encryption to new technologies like Artificial Intelligence.	It is shown by the research that many layers are needed for strong cloud security. Important traditional methods like encryption and MFA are still considered necessary. At the same time, advanced threat detection and the protection of data are required by new technologies such as AI and Blockchain.	Serious threats are continued by data breaches, identity theft and data loss. The difficulty of fixing vulnerabilities in scalable systems and the complexity of staying compliant with changing regulatory rules are also pointed out by the paper.
Bernardo et al. (2024)	A new evaluation framework to measure organizational cybersecurity maturity is introduced by the study. The NIST Cybersecurity Framework is aligned with it and clear metrics that help manage and reduce cyber risks are provided.	Detailed ratings for each of the five NIST functions Identify, Protect, Detect, Respond and Recover are produced by the framework. Organizations are allowed to compare their performance with others through this. It was shown by case studies that a more accurate picture of security posture is given by prioritizing controls based on expert weighting than by traditional flat scoring models.	The subjectivity and bias in self-assessment methods are addressed as one major challenge that can often lead to inconsistent results. The difficulty faced by organizations when trying to benchmark their performance against peers is also highlighted by the study as there are no unified and objective evaluation standards in the industry.
Lokare et al. (2025)	The study is looked at in terms of how cybersecurity frameworks can be integrated into IT security. Models such as the NIST Cybersecurity Framework, Zero Trust Architecture and ISO 27001 are focused on how they can be applied in industries like finance, healthcare and government to reduce evolving threats.	It is shown by the research that a multilayered approach is essential. Defenses against advanced threats like ransomware and APTs are strengthened by the combination of traditional frameworks like NIST and ISO with modern strategies such as Zero Trust and AI based behavioral analytics.	Legacy systems that do not work well with modern security protocols are relied upon by many organizations. Resistance to change is commonly encountered. Resource limits are often faced by small and medium enterprises. Managing compliance with different regulatory rules such as GDPR and HIPAA across multiple jurisdictions is also considered difficult.

Duary et al. (2024)	The role of Predictive Analytics and Artificial Intelligence in detecting cybersecurity threats within intelligent networks is looked at by the study. A transition from manual analysis to automated defense systems is aimed for it.	Unmatched abilities for automating threat detection and handling data volumes that cannot be managed by human analysts are provided by AI and predictive analytics. It is concluded by the study that the field is being changed by machine intelligence enabling proactive defense instead of reactive measures.	Important nontechnical challenges are also pointed out by the authors. These include ethical concerns about how AI is used and the need for explainability so that AI decisions are clear and understandable. The difficulty of building stronger collaboration between researchers and developers is also stressed by them.
Sun et al. (2022)	The theme of jointly combating threats and challenges to data security is focused on by the proceedings. Topics such as data watermarking, privacy protection through blockchain, anonymity networks, anomaly detection and vulnerability mining are included.	A range of technical advances is presented by the selected studies. These include a strong database watermarking scheme for copyright protection, a blockchain based medical data traceability system using attribute-based encryption, heuristic rules that can de-anonymize users on Tornado Cash and the FPFlow framework can apply dynamic taint analysis to detect and prevent browser fingerprinting.	Critical challenges were also addressed by the conference. These include the fragility of anonymity in coin mixers such as Tornado Cash and in Tor networks, the difficulty of managing unowned API assets, new vulnerabilities in microservices, the growing problem of SMS fraud and smart contract breaches such as the DAO incident that require automated detection methods.
Hafiz et al. (2025)	The rise of Ransomware as a Service in Indonesia's cybercrime ecosystem is looked at by the study. Attention is focused on how advanced attack tools are made more accessible by this model and how critical sectors are affected by it.	A regional hotspot for Ransomware as a Service has been established by Indonesia because low entry barriers are faced by attackers. The most frequent targets are the government healthcare and finance sectors. Outdated systems are often exploited by attackers and phishing is used to break through defenses.	Cybersecurity awareness is considered low and regulatory frameworks are regarded as weak and unable to keep up with the fast evolution of Ransomware as a Service. The human element is found to remain vulnerable to social engineering. It is also noted that legacy infrastructure is difficult to secure against modern exploits.
Ike et al. (2025)	A full guide to Identity and Access Management in cloud storage environments is provided by the study. Data is focused on being protected from unauthorized access through advanced frameworks, AI integration and compliance with rules such as GDPR and HIPAA.	Role Based Access Control, MFA and AI based anomaly detection are identified as key parts of strong cloud security by the review. It is shown that protection against modern cyber threats is greatly improved by combining IAM with Zero Trust Architecture and using AI for adaptive authentication.	Misconfigurations such as excessive permissions are common. IAM across multi cloud environments is managed in a complex manner. Compromises of credentials can occur through advanced attacks such as phishing and credential stuffing. A balance between strict compliance and smooth operations is also considered difficult.
Kezron (2025)	A modular cybersecurity architecture designed for small and medium sized enterprises that use cloud computing and Artificial Intelligence is proposed by the study. The goal is to aid these organizations in overcoming limits in resources and expertise.	A detection accuracy of 92.3 percent was reached with a low false positive rate of 3.5 percent. The meantime to respond was reduced to 12.8 minutes. Cost-effectiveness and efficiency were demonstrated by the framework, using only about 4.8 percent of system resources. It was proved that enterprise grade security can	Real-time monitoring was made difficult in rural areas by bandwidth limits. Heavy labor for data labeling was required for training AI models. Integrating modern API based tools with legacy systems was also considered complex.

		be achieved by SMEs with AI-based and open-source tools.	
Youssef (2020)	A new Cloud Security Risk Management Framework is introduced by the study. It is designed to connect technical risk assessments directly with an organization's business objectives instead of only focusing on assets.	It is argued by the paper that security is treated as separate from business goals by traditional frameworks that can fail as a result. Organizations are helped by the proposed framework to measure risk in terms of business impact so that security controls are applied where business value and continuity are most protected.	Cloud environments are complex and contain many different security controls that are difficult to manage. Trust in cloud providers is often lacking among organizations. The true business consequences of security breaches are also hard to estimate because of this complexity.
Salas-Riega et al. (2025)	The study is looked at how the NIST Cybersecurity Framework is adopted worldwide and how effective it is considered to be in reducing cyber threats. The five core functions Identify, Protect, Detect, Respond and Recover are focused on.	The results are shown to indicate that the NIST CSF is valued for its flexibility and risk-based approach, but uneven adoption is noted. The Protect and Detect functions are performed well by large organizations. Struggles are faced by small and medium enterprises due to limited resources. Compared to ISO 27001, the NIST framework is considered more adaptable but less prescriptive.	The resource gap in budget and expertise that prevents full application of the framework by SMEs is identified as the biggest issue. Other problems include the voluntary nature of the framework, the lack of localized standards for specific regions and the shortage of evidence proving its effectiveness in certain sectors.

2.2 Methods

In this research, a systematic framework synthesis approach was applied to construct an articulate cybersecurity risk management plan that is applicable to Artificial Intelligence and Software as a Service settings. The analysis began with a close examination of the existing threat environment and categorized some of the critical risks like API security exposures [20]. Recently published industry reports data [5] assisted in comparing risks within IaaS PaaS and SaaS services models [1] [6]. The framework used as the foundation was the National Institute of Standards and Technology Cybersecurity Framework 2.0 [10] can give more emphasis to governance. Adaptive defense strategies that were appropriate to the specific speed and complexity of AI systems were also part of the method. These approaches employed predictive analytics in detecting threats [19] and implemented the principles of the Zero Trust in the IT infrastructure [3] [18]. Potential sources of bias were identified including limited datasets, self-assessment methods and explainability issues in AI models. Methodological limitations reported in the original studies were considered during synthesis to reduce bias. No formal scoring tool was applied.

The practical viability of the strategy was evaluated in a comparative study of the current security controls and maturity levels of the leading cloud service platforms [15] [16]. This step involved a convergence of collaborative security improvement strategies [14] and business-oriented risk management strategies [24] in such a manner that technical safeguards aligned with business objectives. Other practices that were also included in the research to develop an entire governance model are secure software development practices [12] and regulatory compliance rules regarding AI services [23]. The last framework was a culmination of all these architectural insights as a single strategy that can be

used to minimize the emergence of new cyber threats in intelligent networks [17]. No ethical concerns were identified as the study uses only publicly available secondary data.

3. Results

This part will provide an evaluation of the identified cybersecurity threats and the relevant frameworks to deal with them. It also describes a detailed plan to minimize risks and explains the main points that need to be considered in the practical implementation

3.1. Risk Identification and Assessment

In this section, the authors determine and analyze the critical risks in IT and software settings in terms of cybersecurity, focusing on AI and SaaS based systems. The evaluation is based on the probability and consequences of such risks in order to facilitate the proper risk prioritization and mitigation planning.

3.1.1. Common Cyber Threats and Risks in IT & Software Domain

This study looked into the risks associated with cybersecurity in AI driven SaaS environments and found that these vary in how likely they are to happen and their impact. The biggest concerns were data breaches and unauthorised access, which pose a significant risk because they are likely to occur and can lead to serious problems in operations. This result aligns with findings by Ademilua and Areghan [1] that reported SaaS platforms tend to be riskier on average than IaaS and PaaS models due to the issues such as poor setup and weak access control.

API exploitation is seen as a high-risk threat. Since SaaS architecture depends a lot on connected APIs, weak authentication methods and poor input checks can greatly widen the chances for attacks. Fatima and her team noted similar points finding APIs to be a main pathway for SQL injection and unauthorised access in SaaS systems [6]. This study backs up the idea that API-focused architecture can help with scalability but also bring serious security risks if not managed properly.

Those attacks and insider threats were considered similarly high-risk with occurrences slightly lower than associated with data breaches. In spite of advancements in endpoint security technologies, ransomware is still able to inflict significant service and financial impacts especially when cloud-hosted services are affected [2]. Insider Threat remains a challenge because of the privileged access given to employees and contractors as also highlighted by Aljumaiah et al. [4] who assessed human-related weakness as a major factor.

To conclude, AI model manipulation such as data poisoning was rated as a medium-risk threat. Although the possibility to occur is lower than traditional attacks, the potential impact on decision making accuracy and system reliability is crucial. Organisations increasingly depend on AI-driven automation may escalate into an important concern if left unaddressed as emphasized by Zeijlemaker et al [13]. Following are risk matrix table for cyber threat:

Table 2. Risk Matrix (Likelihood vs. Impact)

No.	Cyber Threat	Likelihood	Impact	Risk Level
1	Data Breach and Unauthorised access	High	High	Critical
2	Ransomware Attacks	Medium	High	High
3	Insider Threats	Medium	High	High
4	API Exploitation	High	Medium	High
5	AI Model Manipulation	Low	High	Medium

3.1.2 Justification of Critical Risks

The likelihood–impact matrix provides a structured mechanism for prioritising cybersecurity risks by evaluating threats based on their potential to disrupt organisational operations and business continuity. In cloud- and AI-driven environments, risk exposure is heightened due to shared infrastructure models, reliance on automated decision-making, and limited visibility into interconnected services. As noted by Youssef [24], effective cloud risk management requires alignment between organisational business objectives and technical risk evaluation, as failures in cloud environments often result in severe consequences for data confidentiality and availability.

Consistent with this assessment, data breaches and Application Programming Interface (API) exploitation are identified as the most critical risks in AI-powered SaaS environments. Both threats are assigned high likelihood and high impact ratings due to persistent issues such as cloud misconfigurations, ineffective access control mechanisms, and insecure API implementations, which are repeatedly cited as leading causes of cybersecurity incidents in SaaS platforms [1], [6]. Given the multi-tenant nature of SaaS architecture, vulnerabilities within shared resources can rapidly escalate into large-scale incidents, leading to operational disruption, regulatory non-compliance, and erosion of customer trust.

Overall, this analysis demonstrates the importance of prioritising critical cybersecurity risks through a combination of technical severity and business impact. Adopting a risk-based prioritisation approach supports the development of targeted mitigation strategies and ensures alignment with enterprise risk management (ERM) objectives, thereby strengthening organisational resilience against high-impact cyber threats.

3.1.3 Empirical Evidence Supporting Risk Ratings

The classification of data breaches and API exploitation as significant threats is backed by recorded real-world cases in SaaS settings. Industry reports consistently highlight cloud misconfigurations and insecure APIs as primary factors behind cybersecurity breaches, especially in multi-tenant SaaS setups [1], [6]. For instance, numerous significant SaaS data breaches have been linked to insecure cloud storage and unnecessary API permissions, leading to the exposure of millions of customer records and extended service outages.

Furthermore, vulnerabilities in APIs have been extensively utilized to circumvent authentication measures and retrieve confidential information from AI-powered SaaS platforms. Studies show that APIs are becoming more frequently targeted because they provide direct access to backend services and automated decision-making systems,

which heightens the effect of a single vulnerability on various interconnected services [20]. These events illustrate how flaws in common cloud infrastructure can quickly lead to significant security breaches impacting several tenants at once.

The effects of these events go beyond mere technical interruptions, frequently resulting in regulatory fines, harm to reputation, and erosion of customer confidence. This empirical evidence substantiates the categorization of data breaches and API exploitation as threats characterized by both high probability and significant impact, warranting their prioritization in the likelihood-impact risk matrix. These documented incidents demonstrate that the proposed risk prioritisation accurately reflects real-world threat behaviour, thereby validating the likelihood–impact ratings used in the risk matrix.

3.2 Applicable Standards and Frameworks

The NIST Cybersecurity Framework (CSF) serves as a foundational model for the proposed risk management strategy. The discussion focuses on framework core's functions to the IT and Software sectors with the illustration of how actually the standards map to the specific security requirements.

3.2.1 Overview of NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) provides a voluntary set of standards, guidelines and is also referred to as best practice to reduce cybersecurity risk [10]. At the beginning, CSF was developed to protect United States critical infrastructure [10]. The framework structure consists of six core functions of the lifecycle [11], where the first core is "Govern" followed by "Identify", reflecting the comprehensive risk management approach of the 2.0 standard [10]. In essence, this requires a deep understanding of the context and risks. Next core is "Protected", such as implementing safeguards in places to stop attacks from happening. Moreover, for the core known as "Detect", it is about the capability to detect a security breach or attack as soon as it happens [19]. Additionally, the core "Respond" works as an action plan to stop any attacks, contain the damage and fix the problem. Lastly, core of "Recover", used for restoring system condition back to normal safely after an attack [10]. The project emphasizes the transition to NIST CSF 2.0, which places the Govern function at the center of the security lifecycle to ensure that cybersecurity is integrated into the broader organizational mission rather than treated as a technical silo.

3.2.2 Relevance of NIST CSF to IT & Software Sector

As noted in [4], NIST Cybersecurity Framework selection is well suited for the IT & AI Software (AI, Cybersecurity & SaaS) domain because of several reasons. First and foremost, the framework is built for complex technology infrastructure [17]. This demonstrated framework aligns perfectly with the domain because it basically consists of complex interconnected systems, cloud infrastructure, remote access of sensitive data [14], [15]. As highlighted in recent research, utilizing this structured framework is essential because it allows for a profile-based approach that scales flexibly to accommodate the rapid expansion of SaaS platform infrastructures. The framework's six functions provide a clear plan to manage the exact risks such as Data Breaches [5], API Exploitation [20] and AI model manipulation [13]. Another point to consider is as the domain produces and sells software that might result in creating

risks or threats [7]. The strategy justifies the Govern function as a means to provide high-level policy oversight for sovereignty and third-party risk, which is critical for global IT services [9]. Additionally, the CSF can integrate seamlessly with the NIST standard, like Secure Software Development Framework (SSDF) [12]. This enables an organization to use CSF for high-risk management together while applying SSDF as a "Protect" function that guarantees that software is securely developed.

3.2.3 Mapping IT Security Requirement to NIST CSF Functions

It is important to align them with CSF to ensure the mitigation is effective. The six core functions mapped to security controls would ensure preventive, detective and corrective layered strategy work together to strengthen overall security [10], [18]. For instance, take a look at the Data Breach and Unauthorized Access solving process cycle. At first, it must undergo an "Identify" process, by classifying data to understand what it should protect [4]. The next step is "Protected", which implements access control and encryption as information safeguard [22]. Besides, Identity and Access Management (IAM) is positioned as the primary technical mechanism for the Protect function, establishing an identity-first 'digital perimeter' that is essential for securing sensitive data in cloud environments [22]. Furthermore, "Detect" will focus on monitoring and identifying suspicious activities using the Intrusion Detection System (IDS) [19]. Then, it executes an incident response plan to contain the breach as "Respond" [10]. As in the "Recover" step, the affected data from backup will be restored to its original condition and vulnerabilities are fixed to prevent any incident [17]. This alignment elevates cybersecurity from technical compliance to a strategic component of organizational risk management.

3.3 Strategy and Planning to Mitigate Risks

This segment outlined layers of risk mitigation strategies containing preventive, detective and corrective controls for strengthening organizational defenses. To manage cybersecurity risks effectively in the IT and Software domain especially in environments that rely on AI technologies, cybersecurity solutions and Software-as-a-Service (SaaS) platforms are necessary. This approach is built on the NIST Cybersecurity Framework (CSF), combining steps to prevent, detect and correct issues. By connecting technical and organisational security practices to the functions of the NIST CSF, organisations can boost their overall defense against cyber threats and better safeguard essential systems and information [10].

3.3.1 Preventive Controls

Preventive controls are proactive actions taken to block cyber threats before they can take advantage of weaknesses. In the IT and Software domain, robust preventive controls are important as the extensive use of cloud platforms, APIs and AI models are increasing. One of the most crucial preventive controls is Identity and Access Management (IAM). Only authorised users can access sensitive systems and data by enforcing strong authentication mechanisms such as multi-factor authentication (MFA) and role-based access control (RBAC). This will reduce the risk of unauthorised access and insider misuse significantly [1],[6].

In addition, in order to prevent API exploitation, secure API management plays a vital role. This includes implementing API gateways, authentication tokens, rate limiting and input validation to protect APIs from injection attacks and abuse. Data encryption at rest and in transit is important to intercept data leakage even if systems are compromised for SaaS and cloud-based systems [22].

Based on AI perspective, preventive measures include secure data pipelines, dataset validation and controlled access to training data so that it can minimise the risk of data poisoning and model manipulation. Secure software development practices such as those outlined in the NIST Secure Software Development Framework (SSDF) further strengthen preventive controls by reducing vulnerabilities at the development stage. [17].

3.3.2 Detective Controls

Detective controls focus on quickly spotting cybersecurity incidents to reduce harm. IT and SaaS setups are ever changing and spread out, constant monitoring is essential. These tools help collect and analyze logs from cloud services, devices, and network elements. SIEM solutions can instantly catch suspicious activities, like strange login attempts, odd API requests, or unexpected changes in AI models. Additionally, Intrusion Detection Systems (IDS) and behavior analysis can help identify ransomware attacks, insider threats, and unauthorized access attempts [15],[19].

When it comes to AI systems, keeping an eye on how models perform, and the outputs can reveal unusual patterns that might suggest malicious interference or harmful data changes. By regularly logging audits and setting up alerts, security teams receive timely notifications about possible issues, helping them respond quickly and effectively with the NIST CSF “Detect” framework [10].

3.3.3 Corrective Controls

Corrective controls applied after a cybersecurity incident has occurred and aim to limit damage, restore systems and prevent any similar incidents from occurring again. These controls play a crucial role in maintaining business continuity and reducing operational disruptions. An effective Incident Response Plan (IRP) should be established to aid organisations when responding to security incidents such as data breaches or ransomware attacks. The plan should define clearly the procedures for containment, eradication, communication and recovery [10].

For instance, in the event of a ransomware attack, infected systems must be separated immediately to prevent malware from being spread further. Regular and secure data backups are also key corrective measures. Backups should be encrypted, stored offline or in immutable storage and tested periodically to ensure reliable recovery during incidents. This is especially important for SaaS platforms that rely heavily on data availability [17].

Once recovery is complete, organisations should hold reviews to figure out what went wrong and make necessary updates such as fixing issues, changing settings or altering policies. This ongoing effort helps build stronger defenses against future threats [25].

3.3.4 Strategic Alignment with NIST CSF

The risk mitigation strategy discussed above is aligned together with the five main functions of the NIST Cybersecurity Framework. Those 5 are Identify, Protect, Detect, Respond and Recover. Preventive controls motive is to support the Protect function by safeguarding the systems and data. Detective controls align with the Detect function by authorising early identification of threats and suspicious activities. Corrective controls support the Respond and Recover functions by ensuring effective incident handling and system restoration [10].

By integrating these controls into a single connected strategy. Organisations within the IT and Software domain can adopt a risk-based and scalable cybersecurity approach. This alignment ensures that cybersecurity is treated not just as a technical requirement, but as a strategic component of organisational risk management which supports long-term operational stability and user trust [9],[10].

3.4 Implementation Considerations

In general, implementing a complete cybersecurity strategy based on NIST Cybersecurity Framework (CSF) is essential for the IT & Software domain, especially in dynamic cloud and SaaS systems.

3.4.1 Technical Challenge

Start with technical problems such as securing distributed and API-driven systems [20]. It is complicated and complex to apply Identity and Access Management (IAM) and network security controls like “Protect” function consistently across different SaaS applications and interconnected Application Programming Interfaces (APIs) [22], [25]. For instance, insecure APIs can be exploited like authentication bypass [20]. APIs act as gateways for software to communicate. If the API has weak security measures, then it would be exploited easily. On top of that, each API needs its own specific and tailored security measures to close its own unique vulnerabilities [20]. As mitigation strategy, Zero Trust Network (ZTA) which adheres to the principle “never trust, always verify” shall be enforced to strengthen the Protect function against unauthorized access in distributed systems [3], [22].

Another problem challenge is continuous monitoring in multiple clouds [1]. NIST “Detect” function implementation using the Security Information and Event Management (SIEM) system is technically hard [15]. This is said because the system must collect, compare and analyze security logs from many and different SaaS, PaaS and IaaS parts at once [6]. Its complexity consequently makes it difficult to detect small and hidden security issues such as SQL injection patterns [2]. As a solution, Artificial Intelligence (AI) and Machine Learning can be utilized for analyzing patterns and finding unusual activity in the network traffic significantly improving threat detection rates, though organizations must still manage the challenge of false positives to avoid alert fatigue [8], [19].

3.4.2 Organizational and Human Factor

Cloud environment operates using a shared responsibility model, where the organization itself is accountable for ensuring the data and applications are secured [1], [6]. Any misunderstanding can cause security gaps when implementing

"Protect" functionality [4]. To overcome this, we could set up a formal collaborative security governance, meaning creating a team across the departments [9]. The team shall write everyone's roles and responsibilities and establish a set of guidelines and rules for organization to keep everyone alert and importantly organization security posture[10], [16].

In addition, we have user adoption and awareness. Normally, human factors are the weakest link, and even the best technological safeguards can be bypassed by simple human errors [6]. For instance, implementation of robust security controls like Multi-Factor Authentication (MFA) requires users to authenticate themselves frequently even for a short period of time [22]. This leads to frustration and users might not comply with the rules [18]. Hence, a comprehensive training for both developers and end users is important to nurture a culture of security awareness and improve the consistency of security practice beyond Tier 1. For example, security coding practice training for developers [12], while MFA or phishing awareness training for end users [18].

Also, it is difficult to accurately judge a company's security maturity using the NIST CSF. Because the process depends on the person doing the checking, different evaluators often give different results [16]. In order to improve the system that involves the "Identify" function of CSF, the system must aim to prioritize the critical high value assets before defining higher security development [16].

3.4.3 Regulatory and Compliance Issues

Regulatory challenges arise from the difficulty of aligning the voluntary, US based NIST CSF with mandatory, often international, legal requirements [11]. The NIST CSF is a framework of best practices and is not a required law [10]. Compared to certified standards like ISO 27001, it cannot officially get certified in NIST CSF. If your IT and software company operates worldwide, using the NIST CSF only would not guarantee compliance with mandatory regional laws such as Europe's General Data Protection Regulation (GDPR) and NIS2 Directive[11]. Therefore, it is recommended to adopt a compliance-driven approach [24]. First of all, NIST CSF is made as a taxonomy or structured dictionary for security practice since it uses the "what to do" concept [10]. Then, formally map those security practices to the specific and required duties "must do" of every law you need to follow. As a result, it helps ensure either you meet all your legal obligations or not [24].

Secondly, the third-party supply chain risk [10]. As SaaS providers, compliance heavily depends on the security status of its vendors and partner which is the third-party service providers [23]. Moreover, the mandatory laws like the NIS2 Directive usually require the company to implement specific reporting and security standards for their third-party supply chains [11]. These legal requirements also should be stricter and more detailed than the basic optional suggestions found in the NIST framework. To address this problem, the company should implement strong Third-Party Risk Management (TPRM) protocols [10], [23]. In particular, the company should investigate the vendor's background, write clear contracts of security agreements that hold vendors responsible for security, and continuously watch their security risk scores [23].

3.4.4 Mitigation Strategies

The main mitigation strategy to overcome technical, organizational and regulatory implementations challenges as discussed is the creation of detailed and customized Action Plan [9]. The plan works as a crucial step that converts the high level NIST CSF functions that consist of Govern, Identify, Protect, Detect, Respond, Recover into specific and measurable operational steps [10], [16].

Additionally, the primary goal of the Action Plan is NIST CSF Tier 4 which is called Adaptive [10]. By achieving this highest tier means the organization's risk management practices are consistently applied and continuously assessed, meaning there is improvement and discipline in security practices [16]. Apart from that, to successfully adopt a flexible and responsive approach, the Action Plan must establish a clear strategy for security for the security program by defining risk tolerance, budget allocation and overall scope for security control application [24]. Besides, the Action Plan shall implement measurability such as custom Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to monitor, evaluate and inform the strategy [25]. Finally, the Action Plan must mandate the regular view of security controls such as incident response procedure and patch management that will allow improvement and adaptation to the dynamic threat landscape over time [17], [18].

4. Discussion

This research indicates that the IT and Software industry particularly in the areas of AI and SaaS experiences an increasing threat like data infiltration, API misuse and AI manipulation. These findings are in line with recent polls on cloud vulnerabilities [1] [6] and new AI threats [13]. Previous research tended to examine individual technical solutions to problems such as ransomware [2] but this study has shown that the NIST Cybersecurity Framework 2.0 with its latest Govern capability is a wider way to go. Implementing preventative strategies like the Secure Software Development Framework [12] and Identity and Access Management to the primary functions of the framework, the study makes sure that the issue of cybersecurity should be approached as a strategic initiative rather than a technical one only [9].

In order to emphasize, this integration is superior to traditional isolated security measures since such tools as firewall and antivirus software are concerned with technical containment and woperate in isolation from broader business objectives. It helps organizations to transform the technical alerts into business actions by implementing the NIST CSF 2.0 [24]. As an example, teams can make business decisions based on technical data such as delaying a launch due to a security warning. Therefore, this solves the problem of older and reactive models because in NIST CSF, security implementation is aligned with organization business goals which technically transform cybersecurity from a financial burden into a key of business asset [9].

The analysis also demonstrates that the technical means such as AI based anomaly detection is essential in the real time detection of threats [8] organization and regulatory barriers complicate the process of achieving adaptive Tier 4 level of security. The weakness of defenses can be caused by human factors and the sophisticated nature of complying

with various international standards that are consistent with previous reports of the disconnect between the voluntary frameworks and the mandatory rules [11].

The NIST CSF, though being risk-based and flexible to a variety of sectors and industries [10], does not provide the legal enforceability of its directives like the EU GDPR or NIS2. It denotes compliance gap, according to which an organization can be safe according to the NIST standards, however, it can also break the law by omitting particular rules. To expound more, organizations operating internationally are supposed to use NIST CSF as a baseline upon which they use certain mandatory controls. As an example, NIS2 mandates the organizations to report the incidents within 24 hours [11]. Thus, the Respond function will also have to be revised to incorporate an instant notification procedure within the incident response plan to ensure that the organization meets this rigid legal deadline.

The current knowledge of this study includes highlighting the importance of having a robust cybersecurity plan with the automated compliance system and ensuring that there is a culture of security as a priority. In this way, it will overcome the shortcomings of shared responsibility models in cloud infrastructure [4] [7]. The future research needs to consider how automated governance software can bridge technical protection and regulatory requirements in international SaaS practices.

5. Conclusions

In conclusion, the application of the NIST Cybersecurity Framework 2.0 is recommended by the study as an alternative to reliance on individual technical remedies to ensure that security is incorporated in the business strategy. This paper has clearly made contributions to the body of knowledge by integrating various security controls into a single model of governance that specifically suits the AI-SaaS ecosystem. Such review is not conducted as broad surveys, but particularly high-probability threats including adversarial data poisoning and API exploitation are explicitly mapped to the new NIST CSF 2.0 Govern function. This mapping provides a theoretical framework for organizations to prioritize their security investments on the basis of the likelihood-impact matrix that will be established in this research.

Preventions methods like the Secure Software Development Framework and real-time AI detection are considered important but the problem of dealing with sophisticated regulations persists due to human error and various standards. For these insights to be effective organizations need to do more than promoting awareness, they must take real actionable steps or practice. Specifically, these involve the implementation of automated compliance controls that will map technical controls to regulatory requirements and role-specific training including phishing training to personnel and code workshops to developers to reduce human error. In addition, the cross-functional security committee which consists of IT and business leadership should be operationalized to oversee the Govern function.

Future research should test this strategy in real world scenarios especially in the Small and Medium Enterprises (SMEs) with long-term case studies aimed at determining the real cost and effort involved in applying NIST CSF 2.0. Moreover, research needs to be conducted to examine how the relationship between technical defense and international

compliance requirements is extended by automated governance tools, particularly by developing systems in which security policies are dynamically updated in response to evolving AI threats.

Author Contributions: Muhammad Zaim Zainuddin: Conceptualization, methodology, software and validation. **Muhammad Azerul Azaman**: Formal analysis, investigation and data curation. **Muhammad Sharin Yasin**: Writing original draft preparation, writing review and editing and visualization. **Mohamad Fadli Zolkipli**: Supervision and project administration. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article as the research is based on the review and analysis of existing literature and publicly available cybersecurity frameworks.

Acknowledgments: The authors thank all members of the School of Computing who participated in this study. This study was conducted as part of the Cyber Security Risk Management Project. This work was supported by Universiti Utara Malaysia.

Conflicts of Interest: The authors declare no conflicts of interest.

References

[1] D. A. Ademilua and E. Areghan, "Cloud security vulnerabilities: A comprehensive survey and analysis of risks in IaaS, PaaS, and SaaS models with practical data and methodology for mitigating breaches," Applied Sciences, Computing, and Energy, vol. 2, no. 1, pp. 39–54, 2025.

[2] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity threats and their mitigation approaches using machine learning—A review," Journal of Cybersecurity and Privacy, vol. 2, no. 3, pp. 527–555, 2022.

[3] D. Ajish, "The significance of artificial intelligence in zero trust technologies: A comprehensive review," Journal of Electrical Systems and Information Technology, vol. 11, no. 1, p. 30, 2024.

[4] O. Aljumaiah, W. Jiang, S. R. Addula, and M. A. Almaiah, "Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework," Journal of Cyber Security Risk and Audit, vol. 2025, no. 2, pp. 12–26, 2025.

[5] Cloud Security Alliance, Top threats to cloud computing 2024. Cloud Security Alliance, 2024. [Online]. Available: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024 Accessed: Nov. 22, 2025.

[6] E. Fatima, I. A. Sumra, and R. Naveed, "A comprehensive survey on security threats and challenges in cloud computing models (SaaS, PaaS and IaaS)," Journal of Computing and Biomedical Informatics (JCBI), vol. 6, no. 01, 2025. [Online]. Available: https://jcbi.org/index.php/Main/article/view/403/428 Accessed: Nov. 22, 2025.

[7] S. Laato, M. Mäntymäki, A. N. Islam, S. Hyrynsalmi, and T. Birkstedt, "Trends and trajectories in the software industry: Implications for the future of work," Information Systems Frontiers, vol. 25, no. 2, pp. 929–944, 2023.

[8] S. Lad, "Cybersecurity trends: Integrating AI to combat emerging threats in the cloud era," Integrated Journal of Science and Technology, vol. 1, no. 3, pp. 1–9, 2024.

[9] F. Mızrak, "Integrating cybersecurity risk management into strategic management: A comprehensive literature review," Journal of Business, Economics and Finance, vol. 10, no. 3, pp. 98–108, 2023, doi: 10.17261/pressacademia.2023.1807.

[10] C. Pascoe, S. Quinn, and K. Scarfone, The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Papers (CSWP), National Institute of Standards and Technology, Gaithersburg, MD, 2024. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29

[11] M. Parmar and A. Miles, "Cyber security frameworks (CSFs): An assessment between the NIST CSF v2.0 and EU standards," arXiv preprint arXiv:2502.06512, 2024. [Online]. Available: https://arxiv.org/abs/2502.06512

[12] M. Souppaya, K. Scarfone, and D. Dodson, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, NIST Special Publication 800-218, National Institute of Standards and Technology, 2022. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/218/final

[13] S. Zeijlemaker et al., "How does AI transform cyber risk management?" Systems, vol. 13, no. 5, p. 228, 2025.

[14] R. Manchana, "Proactive cybersecurity in cloud SaaS: A collaborative approach for optimization," Journal of Artificial Intelligence & Cloud Computing, vol. 2, no. 2, pp. 1–9, 2023.

[15] V. Molnar and D. Sabodashko, "Comparative analysis of cybersecurity in leading cloud platforms based on the NIST framework," Social Development and Security, vol. 14, no. 6, pp. 68–80, 2024.

[16] L. Bernardo, S. Malta, and J. Magalhães, "An evaluation framework for cybersecurity maturity aligned with the NIST CSF," Electronics, vol. 14, no. 7, p. 1235, 2025.

[17] U. Ali, "Cybersecurity in cloud computing: Mitigating risks and enhancing protection," Computer Science Bulletin, vol. 4, no. 1, pp. 35–44, 2021.

[18] A. Lokare, S. Bankar, and P. Mhaske, "Integrating cybersecurity frameworks into IT security: A comprehensive analysis of threat mitigation strategies and adaptive technologies," arXiv preprint arXiv:2502.00651, 2025. [Online]. Available: https://arxiv.org/abs/2502.00651

[19] S. Duary, P. Choudhury, S. Mishra, V. Sharma, D. D. Rao, and A. P. Aderemi, "Cybersecurity threats detection in intelligent networks using predictive analytics approaches," in Proc. 4th Int. Conf. Innovative Practices in Technology and Management (ICIPTM), Feb. 2024, pp. 1–5.

[20] R. Sun, Q. Wang, and L. Guo, "Research towards key issues of API security," in China Cyber Security Annual Conference, Singapore: Springer Nature Singapore, Jul. 2021, pp. 179–192.

[21] L. Hafiz and T. Hidayat, "Unveiling the cybercrime ecosystem: Impact of ransomware-as-a-service (RaaS) in Indonesia," International Journal of Science Education and Cultural Studies, vol. 4, no. 1, pp. 11–21, 2025.

[22] J. E. Ike, J. D. Kessie, H. E. Okaro, E. Ezeife, and T. Onibokun, "Identity and access management in cloud storage: A comprehensive guide," arXiv preprint arXiv:2502.09950, 2025. [Online]. Available: https://arxiv.org/abs/2502.09950

[23] I. E. Kezron, "Cybersecurity framework for securing cloud and AI-driven services in small and medium-sized businesses," Journal of Tianjin University Science and Technology, vol. 58, no. 6, pp. 312–326, 2025.

[24] A. E. Youssef, "A framework for cloud security risk management based on the business objectives of organizations," arXiv preprint arXiv:2001.08993, 2020. [Online]. Available: https://arxiv.org/abs/2001.08993

[25] J. L. Salas-Riega, Y. Riega-Virú, M. Ninaquispe-Soto, and J. M. Salas-Riega, "Cybersecurity and the NIST framework: A systematic review of its implementation and effectiveness against cyber threats," International Journal of Advanced Computer Science & Applications, vol. 16, no. 6, pp. 210–221, 2025.