Journal of Electrical & Electronics Engineering Research and Reviews

Academixs Open Access Publishers

Research Article

The Use of AI to Enhance Evaluation Model for Open-Source Software Adoption with a Focus on Cybersecurity Risks

Shahr Alazmi*

College of Business, Innovation, Leadership and Technology, Marymount University, USA

Corresponding Author:
Shahr Alazmi, College of Business, Innovation, Leadership and Technology, Marymount University, USA.

Received Date: 14.10.2025 **Accepted Date:** 23.10.2025 **Published Date:** 27.10.2025

Abstract

Modern digital ecosystems are driven by open-source software (OSS) used as a scalable, innovative, and cost-efficient option for organizations of all sizes. Nevertheless, cybersecurity dangers should also be inherent in the adoption of OSS: Vulnerabilities in dependencies, unorganized upkeep, and the plausible threat of conforming to legal requirements. This paper, therefore, proposes an AI-improved risk evaluation model that has been made of quantitative tools such as Snyk Advisor and OpenSSF Scorecard with qualitative aspects such as Software Development Life Cycle (SDLC) adherence, data sensitivity, and organizational fit. The model is intended to enable large organizations, government entities, and nonprofits to evaluate and reduce the risks of OSS adoption. This study shows, by way of an example, how this model can be used in practice to quantify risks and devise secure adoption strategies, applying it to a Microsoft OSS project, SignalR. The results emphasize the significance of joining together automated metrics with contextual adjustments to maintain adequate cybersecurity and operational alignment in OSS implementation.

Introduction

With open source software (OSS) revolution, the world of software has been turned upside down with freely available and modifiable codebases, which let developers get creative by innovating fast. With OSS, flexibility and scalability are sought-after vital resources for organizations, no matter how they power their essential web infrastructure or support the enabling of advanced machine learning frameworks. With organizations turning to OSS more than ever to propel innovation, organizations must also grapple with the inherent cybersecurity risks of the technology.

There are apparent benefits to OSS. Instead, it supports collaboration, lowers development costs, and increases the speed of development by using existing codebases. However, this is different in the OSS ecosystem. Organizations are susceptible to high risk of cybersecurity threats due to vulnerabilities in dependencies, lack of formalized support structures, and inconsistent updates [1]. Also, the OSS development being a decentralized affair can make it difficult to hold accountable and pose supply chain risks, as has been demonstrated in the SolarWinds attack.

These risks are magnified in the context of large organizations, government entities, and non-profits. For instance, government agencies usually have to keep sensitive data that needs strong security measures and strict due regulations. Unlike for-profits, non-profits are constrained in their resources but also need to keep their digital assets secure to continue to have their stakeholders' trust. As with large organizations having complex IT infrastructures, OSS adoption comes with unique integration challenges, which further amplify risks [2].

Awareness of these challenges has already been addressed by initiatives like OpenSSF Scorecard and tools such as Snyk Advisor, which provide automated assessments of OSS security and health. Projects are scored by OpenSSF Scorecard (2024) using metrics around branch protection and continuous integration [3]. Snyk Advisor (2023), an alternative vulnerability-checking tool that checks for known weaknesses in projects, shows popularity and maintenance activity [4]. Although these make significant progress, current evaluation frameworks are often context-insensate and lagging in the ability to accommodate organizational intricacies and particular use cases, leaving a gap in comprehensive risk management strategies.

This paper plugs this gap by introducing an AI-improved risk evaluation model combining quantitative and qualitative metrics. The model aims to create a more thorough OSS adoption risk evaluation framework by amalgamating automated tools like Snyk Advisor and OpenSSF Scorecard with factors such as Software Development Life Cycle (SDLC) adherence, Request for Information (RFI) availability, data sensitivity, organizational fit, and more. This model is applied to a Microsoft OSS project, SignalR, to show how the model can provide practical value when assessing and mitigating cybersecurity risks while considering organizational goals.

This research supports the objectives of the world's global cybersecurity policies, particularly emphasized by the White House's Executive Order on Improving the Nation's Cybersecurity including: increase of the Software Supply Chain Security using automated tools and secure development practices [5]. This study fulfills an urgent gap in the discourse on secure OSS adoption and the role operated OSS plays in supporting resilient digital ecosystems by offering a holistic approach to addressing the critical need for a unified risk evaluation framework.

Background

Open source software has long been seen as the fuel on the fire of innovation, offering organizations the ability to access quality code bases that have had such a decrease in development time and cost, enabling organizations to play very fast. OSS originated in collaborative programming initiatives that tried to level the playing field when it came to software development by making the source code free. In the past couple of years, OSS has become an integral part of modern software ecosystems — from cloud computing platforms to mobile applications [6].

OSS has become so widely adopted across industries that the way we work and our reliance on OSS continues to grow. Black Duck Software (2024) reports that more than 90% of current applications include open-source components showing the prevalence and significance [1]. However, there are high challenges to this reliability. OSS development is inherently decentralized, meaning projects tend not to have formalized structures for governance, security, and maintenance, so there are inherent risks and vulnerabilities, as well as supply chain risks. The SolarWinds attack is one example of how vulnerabilities in commonly used software components could be exploited to compromise the nation's critical infrastructure.

However, in response to these challenges, governments and organizations have seriously started to work to enhance the security and reliability of OSS. White House Executive Order on Improving the Nation's Cybersecurity places importance on having secure software development practices and robust supply chain security practices [5]. Similarly, industry driven efforts like the OpenSSF scorecard mechanistically rate OSS projects based upon metrics including branch protection, continuous integration, and license compliance [3]. While these advancements have simplified the evaluation and adoption of OSS, OSS evaluation and adoption for organizations that are unique with respect to their operational and regulatory requirements remain complex. While Snyk Advisor and OpenSSF Scorecard are both current evaluation tools that give some insight into a project's security and health, these tools are not invariant to context; e.g., they do not account for organizational fit or the sensitivity of the data in the OSS. This creates a gap that highlights the necessity of a complete risk evaluation framework that includes both quantitative and qualitative metrics for efficient and secure OSS adoption.

This paper further develops existing frameworks to propose an AI enhanced model to address these limitations. Using context time to automate the risks and benefits of OSS adoption to give organizations actionable insight to promote OSS adoption. This study demonstrates the model's applicability through its use in the context of OSS implementation, applying it to SignalR and origination work from Microsoft OSS.

Literature Review

Much research has been done on the adoption and evaluation of open-source software (OSS), and researchers and industry experts have noted the importance of striking a balance between the benefits and inherent risks. Unlike other top programs like Ruby and Python, OSS is at least partially decentralized and has many stakeholders that collaborate but, at the same time, can introduce challenges related to accountability and security. A multitude of frameworks and tools have been created to tackle these challenges, all with different points of view relating to how these risks should be assessed and mitigated.

OSS security evaluators today are also providing us with tools like OpenSSF Scorecard and Snyk Advisor, which are important advancements. OpenSSF Scorecard evaluates how projects rate on critical metrics like branch protection, dependency updates, and CI testing. The metrics according to OpenSSF (2024), 'these metrics can be used as a quantitative measure to assess the level of security for open source projects' (p. 8) [3]. If advisors have to be done, Snyk Advisor looks for vulnerabilities in a dependency while taking popularity, maintenance, and community engagement into account. "These tools are important," Black Duck Software (2024) points out, as their "comprehensive scanning and continuous monitoring are indispensables" (p. 14) [1].

Despite the availability of such tools, current frameworks are far from meeting the specific needs that organizations face. For example, although automated assessments are helpful in terms of the insights that they generate, they typically do not capture important qualitative issues like organizational fit and data sensitivity [2]. In particular, government entities and non-profits, which are constrained by limited resources and strict regulatory requirements, are most limited by this.

Additionally, in the literature, the importance of a secure software development life cycle (SDLC) on OSS projects has also been stressed. According to Checkmarx (2024), "integrating security touchpoints throughout the SDLC helps to significantly reduce vulnerabilities and ensure compliance to industry standards" (p. 5) [7]. On the other hand, despite this diversity, the adoption of secure SDLC practices is substantially inconsistent across OSS projects, something to be reflected by standardized models of evaluation that take into consideration imperfections. Factors from the context and organization have also received increasing attention beyond technical evaluations. Sharma (2024) states that 'for effective OSS adoption, a holistic approach, using automated tools in combination with qualitative assessment specific to the specific needs of the organization is required' (p. 10) [6]. In alignment with the goals of the global cybersecurity policy, including the White House's Executive Order on Improving the Nation's Cybersecurity, automating integrated organizational-specific risk management strategies is recommended [5].

Based on these insights, this paper proposes an AI-enhanced risk evaluation model to close the gap between where a single framework stands today and where more adequate risk frameworks need to be. To that end, the proposed model integrates these qualitative factors (such as adherence to SDLC processes, availability of RFI, and organizational fit of the OSS) with quantitative factors (such as incorporation of Snyk Advisor and OpenSSF Scorecard) as it integrates them with the qualitative factors. Finally, this model is demonstrated on SignalR to show its applicability to guiding secure and smart OSS implementation decisions.

Risk Evaluation Model

The integration framework proposed in this work combines quantitative OSS metrics obtained from automated tools Snyk Advisor and OpenSSF Scorecard with qualitative organizational specificOS Scoring, to create a holistic framework for evaluating the risks associated with the adoption of OSS. This model unites technical evaluations with contextual adjustments to address limitation of current frameworks, thus enabling secure OSS implementation.

Quantitative Metrics: Snyk Advisor and Openssf Scorecard

Snyk Advisor evaluates OSS projects based on four critical dimensions: Popularity, security, maintenance, and community. Collectively, these metrics help in gathering the general health and reliability of an OSS project. In its definition of the main objectives of the dependency management framework project, Snyk (2023) states that “a key aspect of secure software development is the ability to identify and address vulnerabilities in dependencies” (p. 12) [4]. Snyk Advisor is included in the model so that security risks are quantified and prioritized.

Openssf Scorecard (30%)

Where Snyk Advisor offers a thorough code intelligence experience related to vulnerabilities, the OpenSSF Scorecard completes that picture with a focus on secure development practices. For the long-term sustainability and security posture of an OSS project, metrics like branch protection, dependency updates and CI testing are critical [3]. That is consistent with the White House's Executive Order on Improving the Nation's Cybersecurity and its call to adopt secure software supply chain practices [5].

Qualitative Metrics

Software Development Life Cycle (SDLC) Adherence (10%)

SDLC practices ensure that security touchpoints are integrated into each stage of the development process. One of the points made by Checkmarx (2024) is that 'to reduce vulnerabilities and stay compliant to industry standards, an effective SDLC is needed' (p. 5) [7].

Request for Information (RFI) Availability (5%)

Transparency and quality of documentation are reflected in the availability of detailed RFIs. Hammes (2022) “observes that organizations that maintain an emphasis on transparency of their OSS projects can readily reduce implementation risks” (p. 18) [2].

Sensitivity of Data (15%)

The sensitive data risk of OSS must be evaluated to reach data protection regulations compliance. Sharma (2024) points out that “handling sensitive data means routine need of strict security measures to avoid risks” (p. 19) [6].

Organizational Fit (10%)

Successful implementation of OSS projects depends heavily on the alignment of OSS projects to organizational goals and infrastructure. Hammes (2022) highlights the notion of 'contextual factors' significantly influencing the risk profile of adopting OSS (contextual factors include process, intermediary, project, technology, and organization)— and the need to 'tailor OSS evaluations to specific contexts' (p. 15) [2].

Model Justification

First, their complementary focus areas justify the inclusion of the Snyk Advisor and OpenSSF Scorecard into the model. Snyk Advisor’s focus is on finding and fixing vulnerabilities, while OpenSSF Scorecard takes a more software development practice focused approach. All of these tools can give you a holistic view of OSS risks. The enhancement with qualitative metrics fulfils the gap of previous frameworks as organizational specific factors like data sensitivity and operational fit are addressed in integration into the risk evaluation process.

Case Study: Signalr

This study then validates the proposed model of risk evaluation, combining a case study application on SignalR, an open-source library developed by Microsoft for real-time web applications. SignalR is generally used in applications where live updates are required, such as collaborative tools, gaming platforms, and financial systems. SignalR is a perfect case to test the practical utility of the model because of its widespread implementation in sensitive environments.

Evaluation Using Quantitative Metrics

Snyk Advisor

Snyk Advisor metrics put SignalR in good stead; the Package Health score is an intense 94/100. This score reflects:

Security: Applications calling SignalR do not directly depend on SignalR dependencies, and no critical vulnerabilities were identified in SignalR’s dependencies. Key to the robust security of the project is the handling of real-time data streams, and such applications require robust security [4].

Popularity: SignalR is downloaded more than 460,000 times per week, so adoption and community trust are clearly widespread.

Maintenance: The library actively develops with release and patch releases to remedy possible issues.

Community: SignalR has a large and active community of contributors, and it is growing continuously improving and expanding with its actively maintained contributions.

OpenSSF Scorecard

SignalR also scores highly on OpenSSF Scorecard metrics, particularly in:

Branch Protection: Prevention of unauthorized change to the code base has strong safeguards implemented.

CI Testing: As with all big open source projects, continuous integration pipelines are setup to make sure all the changes are rigorously tested together before merging.

Dependency Updates: The OpenSSF (2024) states that dependencies are updated becoming updated regularly to fix vulnerabilities and maintain compatibility [3].

Evaluation Using Qualitative Metrics

Software Development Life Cycle (SDLC) Adherence

SignalR conforms not only to Microsoft's industry-standard SDLC but also to reviews and automated testing features, which are done throughout development. The result is less likelihood of undetected vulnerabilities [7].

Request for Information (RFI) Availability

SignalR API references, tutorials, and Best Practices are available for extensive documentation and resources. The transparency here ensures secure implementation and allows organizations to modify the library to suit the needs of their particular organization [2].

Sensitivity of Data

Out of all the deployment, SignalR is used to develop real time communication applications, so the data they contain might be very sensitive; for instance, financial transaction or personal information. Despite excellent security practices being widely exercised by the library itself, organizations need in place additional safeguards, like encryption as well as the security of the access control [6].

Organizational Fit

But because organizations often need real time communication capabilities, SignalR is a good fit. With extensive documentation, with active community support, and heartily integrated into the Microsoft ecosystem, it is a flexible suit option for different industries.

The Findings

According to the model’s evaluation, SignalR excels across quantitative and qualitative metrics, making it a good candidate for adoption by large organizations, government entities, and nonprofits. However, the applications of the data are sensitive and need additional organizational safeguards. The model presented in this case study shows how it can be used to gain actionable insights, both evaluating the technical side against the contextual considerations.

Existing Model Comparison

The existing OSS evaluation models are important and valid but do not give much flexibility to address both technical and organizational factors. For instance, the OpenSSF Scorecard is a tool focusing on mainly the technical security metrics: for example, branch protection and dependency updates are important but may not be enough for organizations with complicated operational needs [3]. Similar to Snyk Advisor, it highlights package health and vulnerability scanning and lacks qualitative thinking, such as the fit of an organization and the sensitivity of the data. Through this gap, the proposed model bridges by combining the rigor of technical tools like Snyk Advisor and OpenSSF Scorecard with qualitative metrics that are geared toward organizational contexts. Unlike the traditional frameworks, it builds upon the SDLC adherence and RFI documentation that reflects the transparency and ease of integration [2]. The model accommodates both technical and contextual dimensions for reviewing the current cybersecurity systems with organizational goals in mind and strives to mitigate those cybersecurity risks.

Discussion

In order to evaluate OSS adoption risks, the proposed model is shown through the SignalR case study findings to be practically helpful. Quantitative metrics show strong performance for SignalR, which gives reassurance to the reliability and security of the technology, while qualitative reviews reinforce that SignalR is in line with whether an organization has the need for SignalR and its services. Particularly in organizations seeking secure, scalable, and community-run software solutions, these insights are very pertinent.

Considering OSS adoption, the model is holistic and evaluates risks comprehensively so that organizations can make informed decisions about adopting the OSS. For instance, integrations of tools like Snyk Advisor and OpenSSF Scorecard provide actionable feedback on technical risks, and qualitative metrics such as data sensitivity give a pointer to operational issues. The dual focus is not only security-focused but also helps strengthen the organization's strategic alignment with the organizational objectives.

This could be a topic for future research – in which the scalability of the model is tested across different OSS projects and organizational contexts. In addition, so too could the integration of advanced AI techniques — like predictive analytics and machine learning — to further increase the model's ability to accurately and adaptively assess complex, dynamic risk landscapes.

Conclusion

Open source software is a critical part of modern digital strategy as it provides incredible opportunities to innovate and collaborate. Although the inherent cybersecurity risks presented by OSS must be considered in a comprehensive evaluation framework that encompasses both the technical and contextual aspects, at present a significant number of works focus only on the evaluation of functionality and operational characteristics provided by OSS. This is accomplished by combining quantitative measures like Snyk Advisor and OpenSSF Scorecard with qualitative measures like SDLC adherence and organizational fit through an AI-enhanced risk evaluation model. The SignalR case study demonstrates the effectiveness of the model in identifying and mitigating risk while also generating actionable insights for secure OSS adoption.

Together with relevant adjustments based on context, this model provides a robust support framework for compassing the complexities of OSS adoption by large organizations, government entities and by nonprofits organization in a comprehensive way, efficiently and securely. A future generation of AI and data analytics can take this approach even further and make it relevant.

References

1. Black Duck Software. (2024). 2024 Open Source Security and Risk Analysis Report. Black Duck Software.
2. Hammes, A. (2022). The Dangers of Open-Source Software Projects: Strategies for Approaching Open-Source Software as an Organization (Master's thesis, Utica University).
3. OpenSSF. (2024). OpenSSF Scorecard documentation.
4. Snyk. (2023). Accelerating open source security through AI and machine learning. Snyk Whitepaper.
5. Wu, J. J. X. (2025). Techno-Federalism: How Regulatory Fragmentation Shapes the US-China AI Race.
6. The White House.
7. Sharma, A. (2021). Software composition analysis explained, and how it identifies open-source software risks. CSO (Online).
8. Checkmarx. (2024). What is a secure software development life cycle (SSDLC)?

Citation: Shahr Alazmi., (2025). The Use of AI to Enhance Evaluation Model for Open-Source Software Adoption with a Focus on Cybersecurity Risks. *J. Electr. Electron. Eng. Res. Rev. 1*(1), 1-5.