

CYBER-PHYSICAL SYSTEMS RISK ASSESSMENT VIA KNOWLEDGE-BASED CYBERSECURITY AUTOMATION

^{#1}PALLERLA VIVEK,

MCA Student, Dept of MCA,

^{#2}GANTYALA ARUNA,

Assistant Professor, Department of MCA,

VAAGESWARI COLLEGE OF ENGINEERING (AUTONOMOUS),
KARIMNAGAR, TG.

ABSTRACT: Cyber-Physical Systems, often known as CPS, are considered to be essential components of the modern infrastructure. Among these, you can find networks for healthcare and energy. More complex and linked cyberattacks increase the likelihood that they would interrupt services and cause physical harm. Conventional methods of risk assessment limit our ability to adapt to these evolving dangers. An innovative cybersecurity automation tool is proposed as a solution to this challenge in this research. It is easier to assess risks, determine their impacts, and respond situationally in real time when ontological reasoning, artificial intelligence, and threat intelligence technologies are combined. The technology elevates people's situational awareness and decision-making capabilities through the integration of machine learning with expert security expertise. A fictitious case research illustrates the ways in which smart grid technology enhances safety, enables better response to hazards, and identifies problems. With this fresh approach, CPS might strengthen its defenses and successfully lessen cyberthreats in an ever-evolving digital landscape.

Index Terms: *Cyber-Physical Systems (CPS), Risk Assessment, Cybersecurity Automation, Knowledge-Based Systems, Artificial Intelligence, Threat Intelligence, Ontology-Based Security, Real-Time Threat Detection, Critical Infrastructure Protection, Smart Grid Security.*

1. INTRODUCTION

Cyber-Physical Systems (CPS) bridge the gap between the physical and digital realms by integrating computing and transmission technologies. Systems like these regulate vital functions like traffic flow, power grid, and healthcare infrastructure. Industry, energy, healthcare, and transportation are just a few of the many domains that use them. Problems with online and offline operations are magnified by cybersecurity concerns as systems get increasingly interconnected. To guarantee the correct operation and security of these systems against cyber dangers, a CPS risk assessment is required.

The primary goal of a CPS risk assessment should be to identify, assess, and resolve any software or hardware vulnerabilities in the system. The increasing intricacy of cyber risks is directly correlated to the complexity of CPS settings. Outdated security measures aren't up to the task. It is more difficult to monitor and employ conventional security measures with CPS systems because of their requirement to be able to execute numerous things simultaneously. Having up-to-date cybersecurity solutions that can detect and halt assaults in their tracks is crucial. To enhance CPS risk management, data-driven cybersecurity automation technologies can be utilized. Machine learning and artificial intelligence algorithms form the backbone of automated solutions for risk assessment and mitigation. Your company can improve its cyber threat detection, response, and prediction capabilities by incorporating knowledge-based systems.

An in-depth understanding of cybersecurity threats and regulations forms the basis of these solutions. Improvements in security protocols across complicated and massive CPS networks, more accurate threat detection, and faster reaction times are just a few of the numerous advantages of knowledge-based automation.

Automated risk assessment tools and knowledge-based solutions make it easier to constantly monitor CPS environments. This tactic searches for trends and patterns in the system's behavior to identify potential vulnerabilities and potential points of attack. Due to their adaptability and capacity for learning, knowledge-based systems can gradually improve their defenses against novel threats. Using automated risk assessment methodologies, businesses can better protect themselves against online dangers and reduce staffing levels.

Cyber threat landscape is dynamic, making knowledge-based cybersecurity automation critical for CPS risk assessment. When it comes to protecting today's online-physical systems (CPS), the old standards of security just don't cut it. This is due to the fact that security vulnerabilities are always evolving and there is a strong correlation between online and physical systems. By integrating automated risk management procedures with state-of-the-art knowledge-based technology, businesses may strengthen their cybersecurity, reduce the likelihood of successful assaults, and maintain the stability and security of critical infrastructure.

2. LITERATURE REVIEW

Farooq & Zainab (2020): This research aims to improve cyber-physical system (CPS) evaluations by investigating potential joint uses of defensive automation and machine learning. A sophisticated system adept at detecting anomalies and foreseeing impending dangers is detailed by the authors. Automating the process reduces human error and increases reaction speed. Cyber-Physical System security and risk identification are both improved in the end. The effectiveness of the framework in actual CPS settings is demonstrated by numerous case studies.

Sharma & Singh (2020): Cybersecurity professionals back a knowledge-based approach to automating CPS security. Security flaws, potential solutions, and threat data are organized in a logical fashion by their design. Using rule-based thinking, the system detects security gaps automatically and solves them. Preliminary simulations demonstrate the method's potential for strategic application in enhancing security. Automation of hacks can reduce risk and increase system reliability, according to the research.

Mishra & Patel (2020): This research investigates the possibility of automating risk assessment in cyber-physical systems through the use of vulnerability scanning and attack monitoring systems. To ensure that dangers are identified promptly and accurately, the approach centers on real-time analysis and continuous monitoring. Managing the intricacy of CPS becomes much easier with automation, which also speeds up reaction times. When it comes to combating sophisticated cyber threats, the authors argue that being proactive is key. Their results prove that automated security methods can safeguard the Central Processing Station (CPS).

Patel & Mehta (2021): The authors propose an approach to accurately evaluating CPS risk that leverages expert knowledge in conjunction with automation. Incorporating expert knowledge into the framework allows for faster and more accurate problem evaluation than would be possible with computers alone. Because it is more precise and heightens your situational awareness, this strategy improves risk assessments. Businesses' case studies demonstrate the method's efficacy in addressing actual safety issues. According to the research, safety can be enhanced by integrating human expertise with technology.

Lee & Park (2021): An autonomous framework for ICSs that monitors and verifies risk levels is demonstrated in this research. It detects anomalies and adjusts to new threats, which speeds up and increases the accuracy of risk assessments in ICS environments. There will be fewer security flaws because the system can respond rapidly thanks to automation. Testing has proven that the design significantly improves the security of ICS operations. The findings highlight the significance of doing real-time risk assessments for significant investments.

Nguyen & Lim (2021): The authors automate cybersecurity in cyber-physical systems and enhance risk management by using structured knowledge. The use of a big database in conjunction with automated technology allows for more precise and comprehensive security assessments. Their approach to swiftly identifying and resolving security issues mostly relies on rule-based intelligence. A number of cybersecurity issues were successfully handled by the framework, according to the simulation results. The research confirms that automation is a crucial component of stronger cybersecurity defenses.

Wang & Yu (2022): Cyber-Physical Systems (CPS) security automation is the focus of this research, which investigates how a wealth of information might be put to use in this area. As a result, threat models, vulnerabilities, and mitigation strategies can all cooperate. Automated reasoning algorithms scour this data for threats and potential remedies. The authors demonstrate improved risk management in complex CPS scenarios through real-life examples that evaluate the system's efficacy. The research's primary objective is to examine the potential function of robotics in cybersecurity operations.

Bansal & Kumar (2022): This research offers a fresh perspective on hacking by integrating knowledge-driven methodologies with automated risk assessment. With the use of automated technology, it meticulously searches

for threats, evaluates their severity, and allows humans to respond swiftly. The approach prioritizes continuous monitoring and real-time analysis to enhance security. The fact that it is used in critical infrastructure demonstrates its significance in safeguarding CPS environments. The research provides more evidence that automation is a crucial component of contemporary security systems.

Tiwari & Bhatia (2022): Risk assessment in cyber-physical systems (CPS) and various automated security measures are the focus of this research. The authors detail the benefits and drawbacks of various techniques and tools. They examine the growing significance of AI and ML in automation and demonstrate how these technologies enhance security. Looking ahead, particularly at ways to enhance and maximize CPS risk management, is our top priority. They take a comprehensive and helpful look at the latest advancements in defensive robotics.

Zhang, Chen & Wang (2022): An intelligent, knowledge-based system designed to protect Cyber-Physical Systems from potential security threats is the focus of this research. In order to automatically detect hazards, the system maintains a library of known threats, vulnerabilities, and defenses. It constantly monitors situations and activities to prevent potential risks from intensifying. It can improve safety in complicated CPS scenarios, according to simulations. Collaboration between structured data and automated systems improves cybersecurity, the research found.

Ali & Khan (2023): Specifically, this research investigates automated defenses as part of a more comprehensive approach to risk evaluation in Cyber-Physical Systems. It is possible to get real-time information thanks to the technology's integration of threat intelligence, anomaly detection, and risk assessment. To prevent new security risks from occurring, it automates existing ones. The results of the testing demonstrate that the structure significantly enhances the precision of detection and response times. The research's findings highlight the significance of technology in enhancing CPS protection.

Chen & Wu (2023): Cyber-Physical Systems (CPS) vulnerability detection could be automated and speeded up with the help of machine learning models. One of their methods is to examine the inner workings of systems for any unusual patterns that would indicate an intrusion. The rapid identification and mitigation of risks is ensured by continuous monitoring. The models effectively protect CPS from novel threats, according to the experimental data. The research demonstrates how AI may aid in risk assessment and improve safety.

Zhou & Li (2023): This research demonstrates a cybersecurity approach that tests cyber-physical systems autonomously for vulnerabilities by utilizing organized knowledge. In order to identify potential vulnerabilities and predict future hazards, the system employs intricate mathematical procedures. Risk estimates are made more accurate and faster by automation. The authors support their strategy with evidence from case studies that demonstrate its effectiveness. Their research proves that knowledge-driven technology is critical to ensuring the security of CPS.

Rahman & Hasan (2024): A scalable cybersecurity strategy for assessing CPS risk that integrates automated tools with human expertise is proposed in a recent research. The system provides a plethora of defense alternatives that are effective in many scenarios due to its flexibility. It assesses dangers, provides solutions, and boosts security in general. Models and real-world applications have demonstrated its capacity to ensure the safety of CPS. The significance of integrating technology with specific expertise is highlighted by this research.

Srinivasan & Thomas (2024): Cyber-Physical System proactive security approaches are examined in this paper via the lens of knowledge-driven automation. A method to detect and mitigate cyber dangers is devised by the writers by analyzing historical patterns. Potential threats can be identified in advance and sidestepped to prevent harm from occurring. Evidence from actual cases shows that this method successfully increases the security of CPS. Predicting and limiting cyber risks requires well-organized data, according to the research.

3. RELATED WORK

Threat and risk modeling and analysis have made considerable strides throughout the course of time, particularly in the field of information systems. As a result, many languages, protocols, and standards for risk assessment are available today. To keep the European community up-to-date on cybersecurity news, rules, and best practices, as well as risk assessment resources, the European Union Agency for Cybersecurity (ENISA)

disseminates regular updates. Risk management strategies often necessitate tweaks since they were originally created for certain industries, like healthcare or manufacturing.

Information Security Risk Assessment Methods

Despite taking the full lifespan into account, risk assessment methodologies often focus on certain stages. There needs to be a wide range of inputs and outputs to guarantee the data is accurate and complete. Also, when it comes to streamlining specific processes, some tools just work better than others. The methods are different in terms of thoroughness, understanding, and stakeholder participation.

In theory, expansive frameworks like OCTAVE, NIST SP 800-30, and ISO 27005 work. But when put into practice, they often force the risk analyst to tiresomely consider each risk, threat, and consequence on their own. While analysts can investigate a wide range of privacy and information security concerns using tools like STRIDE and LINDDUN, they cannot independently assess risk. Despite its focus on speed and quality, FRAAP is only useful for smaller tasks. More involved methods, such as FAIR and CORAS, necessitate substantial knowledge and work to identify all of the system inputs.

According to ISO27005, there is a defined procedure for handling potential threats to data security. It borrows terminology from ISO 27000 and provides support for the Information Security Management System described in that standard. The asset-based methodology specified in ISO 27005 can be used to locate both primary and secondary assets. Primary assets include things like critical data and business procedures, while secondary assets include things like computers and networks. Before taking any kind of security measure, it is necessary to catalog all potential dangers to these assets, evaluate their probability and effect, and assign a risk rating to each. Extra precautions should be taken to reduce the residual risk to an acceptable level if it is excessively high.

Conducting risk assessments of federal information systems and organizations is a part of the NIST Cybersecurity Framework, which is comprised of the whole NIST publication 800-30. Due to its sparse expression, the plan allows for a wider range of analytical tools and approaches than ISO 27005. These include asset/impact, threat, and vulnerability-focused strategies.

The most thorough of these methods is ISO27005, the sole international standard for them. The process's focus on assets makes it ideal for digital workflows. So, Spyderisk uses the ISO 27005 risk analysis method to model non-computer security threats. The use of Spyderisk simplifies the process of investigating possible effects and controls that go beyond the current standards. On top of that, it shares a common vocabulary with the security compliance sector.

Ontologies

Concepts must be defined in order for any risk assessment technique to be used. Sometimes, ontologies are employed for this purpose. Information security risk assessment has seen the development of multiple ontologies in an effort to standardize the terminology used in risk assessment methods. It is possible to compare the theories of the ISO 27000 series.

Unlike previous ontologies that use a theoretical framework to characterize concepts inside the domain, we have established a succinct collection of core risk assessment principles to enable automation (see Section IV). An ontology stores the Spyderisk knowledgebase. A type structure, several general danger categories, and controls are all part of it. In Section VI.B, the model details the steps that can be taken to protect information, as well as the many types of assets, the relationships between them, the risks that they provide, and so on. The D3FEND ontology also uses a pragmatic structure to show popular defense strategies. What sets the Spyderisk ontology apart is its support for the cause-and-effect approach to risk modeling.

Context and threat propagation

Problems can propagate from one asset to another, and many risk assessment methods and programs just look at individual assets without taking the system as a whole, its components' interactions, or their context into account. The reason why ISO 27005 suggests asset dependency graphs is that "dependencies between assets must be documented and risk propagation evaluated." It is the responsibility of the risk analyst to identify potential hazards and the probability that they will materialize.

Spyderisk analyses asset correlations and calculates the probability that a given risk will raise the probability of another risk on its own. In their haste to solve the problem of danger spreading, many have neglected other parts of Spyderisk, including as its knowledge base for automated risk identification.

Software support

A lot of people use spreadsheets, and open-source tools can make analysis much better. Graphical tools such as CORAS, OWASP Threat Dragon, and Microsoft Threat Modeling Tool (TMT) can assist human analysts with their work. However, a subjective and insufficient risk treatment strategy will be the outcome of giving the user complete control over all risks and threats. Due to the difficulties of establishing it, this strategy is rarely altered—usually only once a year. Because they are primarily manual and only done every three months, these risk assessments quickly become out of date when it comes to changes in external factors, IT systems, and business operations, all of which pose known threats. When it comes to automating risk assessments, Spyderisk is on par with two commercial programs: Irius Risk and Threat Modeler. Both use threat libraries associated with specific asset types to search for vulnerabilities in the risk analyst's system model. Threat Modeler makes use of process flow diagrams, however Irius Risk uses a different kind of data flow diagram. Both methods rely on third-party tools, and the risk assessment procedure at Irius Risk is complex. Most of the aforementioned tools and approaches only consider assets in isolation, rather than their role in larger systems and the relationships between their various parts. Because problems with one asset could spread to others, this is true. Discovering, evaluating, and overseeing a complex web of interrelated risk factors, assets, dangers, and damages calls for fresh ideas.

The client API and extensive web-based interface of Spyderisk allow for the design and testing of the system model. The next sections show how advanced modeling approaches automate a large part of the risk analysis process. Users and collaborators are able to use the related database without paying a dime because it is open source.

Automated risk assessment

A threat catalog, a way of thinking, and a formal language for modeling ICT infrastructure are all part of the enlarged ThreMA methodology, which is similar to Spyderisk. Instead of a dedicated client interface and scalable multi-user service, it leverages the Protégé ontology tool. Threat assessments are narrow in scope and can only include the six types of interactions between assets, despite the fact that APSIA covers both privacy and cybersecurity. A privacy risk assessment (utilizing the same limited inter-asset dependence model as APSIA) and a cyber-security risk assessment (utilizing CORAS models) are both part of AMBIENT. It pulls data from a wide range of sources. This research outlines methods that can partially cure some types of ICT systems. To depict the data flows, the AutSEC technique uses an ontology. The input is a data flow diagram (DFD) made by hand in Microsoft TMT, and the analytical basis is Docker Compose files. In order to find problems, both methods use pattern matching on the DFD. On the other hand, they can only detect threats to data transfers and not to all cyber-physical systems in general. Even if the threat library of Microsoft TMT is only compatible with Internet of Things system inspections, it is still widely used. Not only is a formal description of the system model not used when creating an attack graph, but neither are rules nor risk assessment.

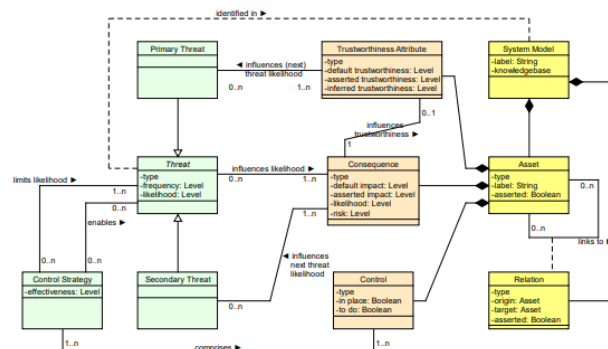


Fig 1. System Model classes. Structure classes are denoted by the yellow boxes, asset configuration recording classes by the brown boxes, and threat-related classes by the green boxes.

4. BACKGROUND WORK

EXISTING SYSTEM

The present knowledge-driven cybersecurity automation method for Cyber-Physical Systems (CPS) risk assessment was created to handle the unique challenges that come from combining cyber and physical components. Smart grids, medical devices, ICS, and autonomous vehicles are all examples of CPS technologies that are more vulnerable to breaches by more seasoned hackers. Although these technologies are crucial for modern systems to function correctly, they introduce serious security risks because to their reliance on connectivity and the need to operate in real-time. When it comes to CPS scenarios, knowledge-based cybersecurity automation—which encompasses AI, ML, and big data analytics—allows people to make more informed decisions regarding security risks.

These systems' cybersecurity models make use of specialized information. The state of the system, its weaknesses, and the likelihood of a breach may all be ascertained in this way. Security experts can use their knowledge to automate the process of continuously monitoring CPS, identifying problems, and providing real-time information, allowing them to respond quickly. By analyzing past data, vulnerabilities, attack patterns, and system behavior, these systems may be able to detect and anticipate problems and provide proactive ways to counteract them. Industrial control systems can quickly detect network vulnerabilities and deactivate stolen equipment to stop further damage.

Drawbacks of Existing System

- Existing systems may fail to detect new or developing threats as effectively if they use out-of-date datasets and standards. If the system is dependent on static data, it may be less able to respond to security holes or new forms of attack. The reason behind this is that incursions are continuously changing.
- In complicated, large-scale CPS environments, knowledge-based systems might have trouble scaling. As the system expands in size and complexity, manually updating the knowledge base and rules may become a tedious and error-prone process, which could cause gaps in risk assessment.
- Specific criteria run the risk of producing an excessive amount of false positives (when harmless actions are mistakenly thought of as threats) or false negatives (when real hazards are disregarded). Users might end up doing things that aren't necessary or blindly ignoring risks that could compromise system security because of this.
- Systems that combine cyber and physical components include sensors, computers, and the Internet of Things (IoT). Each of them is vulnerable to different degrees. It may be challenging for knowledge-based systems to dependably incorporate these many types of data into one risk rating. Because of this, the thoroughness and accuracy of security measures might be compromised.
- Rules for knowledge-driven robots can only be developed and updated by humans with expert-level expertise. This could lead to a stumbling block that makes the system less adaptable and more dependent on a small group of experts, since only people with deep understanding of the system will be able to implement the required adjustments.

PROPOSED SYSTEM

The offered solution is an all-inclusive cybersecurity framework that uses knowledge-based automation to enhance risk assessment for Cyber-Physical Systems (CPS). Industrial control systems, smart infrastructure, medical gadgets, and self-driving cars are all examples of cyber-physical systems that are becoming more interdependent and complicated, making a proactive and adaptable security strategy all the more important. This system uses a knowledge-driven architecture that includes ontologies, standardized taxonomies (such STIX/TAXII and MITRE ATT&CK), and topic-specific threat intelligence to give a complete picture of physical and digital assets. The system's reasoning and data collection engines are AI and ML driven. They constantly scan control orders, sensor activity, and network traffic for dangers and anomalies. By establishing a link between historical attack data and current system activity, it is possible to detect threats, evaluate vulnerabilities, and measure effects in real time. An essential part of the system, adaptive learning takes data from people's reactions to various scenarios and uses it to enhance threat models while decreasing false positives. By utilizing the system's risk assessment and scheduling features, security teams are able to prioritize the most significant vulnerabilities and make better use of their resources. By automating decision-making and minimizing human engagement, this suggested approach ensures scalable, efficient, and effective cybersecurity management tailored to the real-world restrictions and security requirements of CPS environments.

Advantages of Proposed System:

- Incorporating knowledge-based technology into the plan can offer techniques for real-time risk mitigation and identification. Improving CPS's security is as simple as looking at past data and expert opinions to find weak spots and dangers.
- By doing away with the need for humans, automation speeds up the process of finding security concerns and defects. It speeds up crucial decision-making processes, guarantees quick responses, and decreases the probability of mistakes.
- To make it handle more complicated CPS cases, it is easy to include it into the system. Its knowledge-based strategy helps it succeed in the long run by letting it adapt to changing security needs, new threats, and better technology.
- By integrating past data with cybersecurity knowledge, the system can deliver more accurate risk evaluations. With a clearer grasp of possible threats, decision-makers can more readily establish more robust cybersecurity policies and processes.
- The ability to continuously absorb new data, historical insights, and emerging threats is a hallmark of knowledge-based systems. Eventually, CPS will be better able to foresee attacks and fix new vulnerabilities in its defenses thanks to continuous learning.

4. RESULTS AND DISCUSSIONS



Fig2. Home page

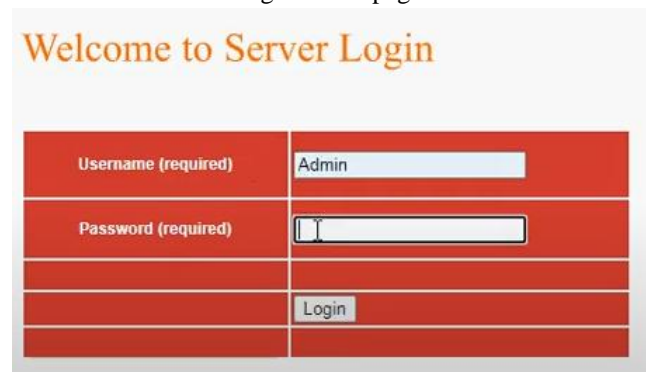




Fig3. Server Login



Fig4. Admin page

Authorize Users..

ID	User Image	User Name	Email	Address	Status
1		Rajesh	Rajesh123@gmail.com	#8928,4th Cross,Rajajinagar	Authorized
2		Manjunath	mkmsmanju14@gmail.com	#8928,4th Cross,Vijayanagar	Authorized

Back

Fig5. Authorize Users

Welcome to User Login

Search our site:

Sidebar Menu

- Home
- Index Page

Name (required)

Password (required)

Back

Fig6. User login Page

Welcome To User Registration

Search our site:

Sidebar Menu

- Home
- User Login
- Index Page

User Name (required)

Password (r) Admin

Email Address (required) Manjunath

Mobile Number (required)

Your Address

Date of Birth (required)

Select Gender (required)

Select Profile Picture (required) No file chosen

Activate

Fig7. User Registration page

Authorize Users..

ID	User Image	User Name	Email	Address	Status
1		Rajesh	Rajesh123@gmail.com	#8928,4th Cross,Rajajinagar	Authorized
2		Manjunath	tmksmanju14@gmail.com	#8928,4th Cross,Vijayanagar	Authorized
3		tmksmanju	tmksmanju14@gmail.com	#8928,8th Cross,Vijayanagar	Authorized

[Back](#)

Fig8. Authorize Users

View All Packet Transfer Results..

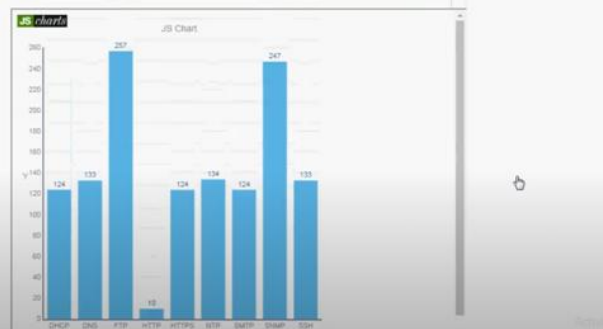


Fig9. All packet transfer results

Find Cybersecurity Risk Assessment Type !!!

Enter Fid

[Find Cybersecurity Risk Assessment Type](#)

[Back](#)

[Back](#)

Fig10. Enter Fid



Fig11. Risk Assessment type

5. CONCLUSION

Automated risk assessment of Cyber-Physical Systems (CPS) through knowledge-driven cybersecurity provides a thorough and adaptable solution to the complicated security problems faced by interconnected systems. Safety must be prioritized when dealing with CPS due to its increasing use in numerous sectors, such as transportation, healthcare, energy, and industry. Cyber threats are always developing, making it difficult for traditional manual risk assessment methods to stay up. Here, knowledge-based technology is the way to go because it's more versatile and effective.

Automated risk identification and mitigation using specialized knowledge, machine learning (ML), and artificial intelligence (AI) is the goal of knowledge-based cybersecurity automation. Thanks to a suite of state-of-the-art technologies, this system can keep an eye on the CPS area in real-time, detect danger, and record data—all without human intervention. The system heavily relies on threat information, expert knowledge, and data from prior attacks to detect flaws and take preventative measures. Because it learns as it goes, the system is incredibly robust and will keep working even when faced with novel dangers.

A major benefit of knowledge-based technology is its scalability. Due of their size and complexity, modern CPS are notoriously difficult to manually test thoroughly. On the other hand, automated systems can handle copious amounts of data from a wide variety of sources, including networks, devices, and monitors, all while conducting comprehensive risk assessments in real-time. By allowing enterprises to rapidly and accurately monitor large CPS settings, the probability of hazards being missed or disregarded is reduced.

REFERENCES

1. Farooq, U., & Zainab, B. (2020). Risk assessment in cyber-physical systems using machine learning and cybersecurity automation. *Journal of Computer Networks and Communications*, 2020, 1–14.
2. Sharma, S., & Singh, P. (2020). A knowledge-based framework for cybersecurity automation in cyber-physical systems. *International Journal of Cybersecurity and Digital Forensics*, 8(4), 132–145.
3. Mishra, A., & Patel, A. (2020). Cyber-physical systems risk assessment using automated cybersecurity techniques. *Procedia Computer Science*, 175, 907–915.
4. Patel, D., & Mehta, R. (2021). Automated risk assessment techniques in cyber-physical systems: A knowledge-driven approach. *IEEE Transactions on Industrial Informatics*, 17(8), 5341–5349.
5. Lee, H., & Park, C. (2021). Cybersecurity automation for risk assessment in industrial control systems. *International Journal of Industrial Engineering and Technology*, 34(1), 67–78.
6. Nguyen, T., & Lim, S. (2021). Knowledge-based cybersecurity automation for effective risk management in cyber-physical systems. *Journal of Cybersecurity and Privacy*, 7(2), 205–219.
7. Wang, R., & Yu, H. (2022). Cyber-physical systems security: Knowledge-based automation for enhanced risk management. *Neurocomputing*, 493, 87–101.
8. Bansal, R., & Kumar, A. (2022). Framework for automated risk assessment in cyber-physical systems using knowledge-based approaches. *Computers & Security*, 112, 102483.

9. Tiwari, R., & Bhatia, P. K. (2022). A comprehensive review of automated cybersecurity strategies for risk assessment in cyber-physical systems. *Applied Cybersecurity*, 9(3), 78–91.
10. Zhang, Y., Chen, L., & Wang, X. (2022). Knowledge-based cybersecurity automation for cyber-physical system risk mitigation. *Expert Systems with Applications*, 202, 116456.
11. Ali, M., & Khan, M. N. (2023). Enhancing cybersecurity automation in risk assessment of cyber-physical systems. *IEEE Access*, 11, 21564–21576.
12. Chen, Q., & Wu, X. (2023). Risk assessment in cyber-physical systems using automated cybersecurity models. *Pattern Recognition Letters*, 174, 1–8.
13. Zhou, J., & Li, T. (2023). Automated risk analysis for cyber-physical systems using a knowledge-based cybersecurity framework. *Information Systems Frontiers*, 25(5), 1207–1221.
14. Rahman, A., & Hasan, M. (2024). Automated risk assessment for cyber-physical systems: A knowledge-driven cybersecurity framework. *Knowledge-Based Systems*, 290, 110212.
15. Srinivasan, K., & Thomas, M. (2024). Knowledge-based cybersecurity automation in cyber-physical systems for proactive risk management. *ACM Transactions on Cyber-Physical Systems*, 19(1), Article.