Advances in Nonlinear Variational Inequalities
ISSN: 1092-910X
Vol 27 No. 2 (2024)

Rule-Based Threat Analysis Methodology for Cyber-Physical Systems in Healthcare

Piyush P. Gawali[1], Parikshit N. Mahalle[2], Gitanjali R. Shinde[3], Nilesh P. Sable[4]

[1]Ph.D Scholar, Department of Computer Engineering, Vishwakarma Institute of Information Technology, SPPU, Pune, India

e-mail: piyush.gawali@viit.ac.in

[2]Professor, Dean R&D, Artificial Intelligence & Data Science, Vishwakarma Institute of Technology, SPPU, Pune, India

e-mail: aalborg.pnm@gmail.com

[3]Associate Professor, Department of Computer Science & Engineering(Artificial Intelligence & Machine Learning), Vishwakarma Institute of Information Technology, SPPU, Pune, India

e-mail: gitanjali.shinde@viit.ac.in

[4]Associate Professor, Department of Computer Science & Engineering (Artificial Intelligence), Vishwakarma Institute of Information Technology, SPPU, Pune, India

e-mail: nilesh.sable@viit.ac.in

Article History:

***Received**: 12-02-2024*

***Revised**: 26-04-2024*

***Accepted**: 12-05-2024*

Abstract:

Cyber-physical system (CPS) integration in the field of contemporary healthcare has completely changed patient monitoring and management. But because these systems are linked, they are vulnerable to different kinds of cyber attacks, which calls for strong security protocols. This work aims to proactively identify and reduce possible security risks by proposing a Rule-Based Threat Analysis Methodology (RBTAM) specifically designed for CPS in healthcare environments. RBTAM uses formalized rules to methodically evaluate threats in the physical and cyberspaces. Its foundations are in discrete mathematics. The process starts with identifying the parts and vulnerabilities of the system, then rules capturing possible threat scenarios are formulated. Among the many things covered by these regulations are denial of service, hardware malfunctions, data tampering, and unauthorized access. By means of an extensive analysis process, RBTAM assesses the probability and consequences of threats found on the availability, confidentiality, and integrity of healthcare systems. Through the facilitation of the prioritization of mitigation measures, this analysis helps healthcare professionals to efficiently distribute resources and reduce possible hazards to data security and patient safety. Important elements of RBTAM are the creation of threat scenarios specific to healthcare settings, the development of security rules based on system architecture, and the incorporation of real-time monitoring systems to identify and address new threats. Furthermore, the approach stresses feedback loops for ongoing improvement, which guarantees flexibility to changing cyberthreats and technology developments. We provide a case study of RBTAM application in a simulated CPS healthcare setting to illustrate its effectiveness. Results show that by efficiently identifying and reducing possible security risks, RBTAM improves the general resistance of healthcare systems to cyberattacks. In the ever-connected healthcare environment,

RBTAM provides healthcare professionals and system administrators the tools and insights they need to protect patient well-being and data integrity through a proactive and methodical approach to threat analysis in CPS healthcare.

Keywords: Cyber-Physical Systems (CPS), Healthcare Security, Threat Analysis, Rule- Based Methodology, Vulnerability Assessment, Risk Mitigation

1. Introduction

Cyber-Physical Systems (CPS) integration into healthcare environments in recent years has revolutionized patient monitoring, diagnosis, and treatment. CPS systems are those in which networked sensors and computational algorithms monitor, control, and coordinate physical processes. CPS shows up in the medical field as hospital information systems, smart medical devices, and remote patient monitoring systems. These systems provide hitherto unheard-of chances to enhance patient outcomes and healthcare delivery by means of real-time data collecting, analysis, and decision- making[1], [2].

Benefits of CPS in healthcare include better patient care, better treatment results, and more effective healthcare operations. But with these developments also come new difficulties, especially with cybersecurity. Healthcare systems are more susceptible to cyberattacks and threats the more dependent they are on digital technologies and linked devices[3], [4]. Malicious actors looking to take advantage of weaknesses in these systems for financial gain, data theft, or service interruption now especially target the healthcare sector.

Patient safety, data integrity, and the general integrity of healthcare operations are all profoundly impacted by the growing cybersecurity issues that healthcare organizations face. Breach of security can jeopardize sensitive information and patient medical records, so violating trust and privacy. Furthermore, misdiagnoses, treatment delays, or even patient injury can all be disastrous effects of disruptions to healthcare systems. For this reason, maintaining the integrity and security of healthcare systems is critical to guaranteeing the provision of patient care that is both safe and efficient[5], [6].

Threat analysis is at the core of healthcare cybersecurity management that works. In threat analysis, possible security risks and vulnerabilities inside a system are methodically found, evaluated, and mitigated. Healthcare organizations can take preventative action to stop security breaches and lessen their effects by being aware of the threat environment and risk profile. Threat analysis helps companies to stay ahead of new cyberthreats, foresee possible weaknesses, and put focused mitigation plans into place to lower risk exposure[7], [8].

Healthcare threat analysis done traditionally frequently relies on reactive strategies like incident response and post-breach mitigation. Even while these methods are very important for handling security problems right away, they might not be able to deal with the systemic risks and underlying vulnerabilities that are present in CPS environments. Moreover, established approaches might find it difficult to keep up with the quickly changing threat environment,

which would expose healthcare institutions to new cyberthreats and attack channels[9], [10].

Threat analysis in healthcare is becoming more and more recognized to require a proactive and methodical approach in response to these issues. Using a rule-based methodology to threat analysis is one promising strategy. Within CPS settings, rule- based threat analysis provides a formalized framework for methodically recognizing, evaluating, and reducing security risks. Using preset algorithms and rules, this method helps healthcare companies to prioritize security measures, carry out thorough threat assessments, and react to new cyber threats with effectiveness.

The ability of a rule-based method to threat analysis to offer a structured and flexible framework for cybersecurity management in healthcare is the justification for its use. Rule-based approaches provide a methodical and scalable approach to threat analysis, in contrast to conventional approaches that could depend on ad hoc or manual procedures[11], [12]. Healthcare organizations can do more effective and efficient threat assessments, find possible vulnerabilities, and put into place focused mitigation plans by codifying domain-specific knowledge and expertise into rules and algorithms.

In this work, a Rule-Based Threat Analysis Methodology (RBTAM) designed especially for CPS settings in healthcare is proposed and evaluated. We shall start by giving a general summary of the organization and substance of the paper and describing the contribution of each part to the study issue. We shall next go into great length about RBTAM, covering its main elements, approach, and implementation issues. The outcomes of a case study assessing RBTAM's efficacy in a simulated CPS healthcare setting will next be covered. We shall finally summarize the main conclusions, their ramifications for healthcare cybersecurity, and possible directions for future study.

This paper attempts to address the urgent need for a proactive and methodical approach to cybersecurity management in healthcare. Our goal in putting out and assessing a Rule-Based Threat Analysis Methodology is to give healthcare organizations a workable structure for recognizing, evaluating, and reducing security risks in CPS environments. By means of this research, we intend to support the continuous initiatives to improve the integrity and security of healthcare systems and protect patient care in a world growing more digital and networked.

2. Literature review

When one looks over the literature on cybersecurity in healthcare, a few main themes come to light that show how threats are changing and how difficult healthcare organizations have it. The need of proactive security measures is highlighted by studies that highlight the growing frequency and sophistication of cyber threats aimed at medical cyber-physical systems. With an eye toward safeguarding patient data and guaranteeing the continuity of care, researchers have looked into threat modeling, vulnerability assessment, and mitigation techniques among other areas of cybersecurity. The literature now in publication still has gaps, especially in the creation of thorough frameworks for risk management and systematic threat analysis. Healthcare cybersecurity literature offers insightful information about the changing threat environment and difficulties that healthcare institutions must overcome. Multiple research have

shown how common and advanced cyberthreats are that target medical cyber-physical systems. Priyadarshini et al.[13] suggested an improved cyber security architecture for medical CPS, emphasizing the integration of security measures to counteract different threats. Threat modeling and mitigation techniques for medical CPS were examined by Almohri et al.[14], who also emphasized the value of proactive security measures.

In the framework of Healthcare 4.0, Qiu et al.[15] looked into safe health data sharing for medical CPS and emphasized the need of strong security measures to safeguard private patient data. In their empirical investigation of the security of medical cyber- physical systems, Wang et al.[16] concentrated on imaging devices and found weaknesses in their security procedures. Reexamining attack path detection for cyber- physical systems enabled by the Internet of Things, Arat et al.[17] underlined the need of identifying and reducing insider threats.

In evaluating cyber-physical attack paths enabled by the Internet of Things against important systems, Stellios et al.[18] emphasized the need of thorough threat analysis and mitigation techniques. For medical cyber-physical systems, Raju et al.[19] examined the security issues and put out a possible layer-by-layer security solution. Meng et al.[20] underlined the need of proactive threat detection by proposing a behavioral profiling method for identifying insider attacks in medical cyber-physical networks.

Integrated security solutions are essential, as El-Kady et al.[21] emphasized in their study of the safety and security issues associated to cyber-physical systems. In their investigation of the cyber-physical threat environment of water systems, Moraitis et al.[22] underlined the value of socio-technical modeling techniques for threat analysis. Preventive security measures were emphasized in a formal threat analysis of machine learning-based control systems in smart healthcare systems by Haque et al.[23].

In their proposal of machine intelligence and medical cyber-physical system architectures for smart healthcare, Shaikh et al.[24] demonstrated how cutting edge technology may improve cybersecurity. Jiang et al.[25] concentrated on data-centered runtime verification of wireless medical cyber-physical systems, stressing the value of real-time monitoring for threat identification and reduction. In their improved cyber security framework for medical cyber-physical systems, Priyadarshini et al.[26] underlined the need of integrating security measures to counteract different threats.

Even with the expanding amount of research on cybersecurity in healthcare, there are still a number of unanswered questions. Research to date has mostly concentrated on pointing up vulnerabilities and suggesting countermeasures, but thorough frameworks for methodical threat analysis and risk management are lacking. Moreover, traditional approaches to cybersecurity could find it difficult to offer the quick changing threat landscape that calls for proactive and adaptive strategies. The literature review reveals several gaps in the current knowledge on threat analysis approaches for Cyber-Physical Systems (CPS) in healthcare. Often depending on reactive measures post-incident, current approaches lack a thorough integration of domain-specific knowledge and formalized frameworks. Methodologies that successfully handle the changing character of cyber threats and the intricate interdependencies

inside CPS healthcare systems are conspicuously absent. Also limiting their applicability to large-scale and dynamic healthcare systems are their limited scalability and adaptability of current approaches. These gaps have resulted in our suggested strategy, which uses RBTAM to try to close these shortcomings. RBTAM provides a disciplined framework for risk analysis, proactive threat detection, and mitigation catered to the particular difficulties of CPS healthcare systems. Our method aims to offer a methodical and flexible solution improving cybersecurity resilience and operational continuity in healthcare environments by combining discrete mathematics-based rules and algorithms.

3. Introduction to Rule-Based Threat Analysis Methodology (RBTAM)

The RBTAM is a comprehensive framework designed to address cybersecurity challenges within cyber-physical systems (CPS) in healthcare settings. RBTAM employs formalized rules and algorithms to systematically identify, analyze, and mitigate security threats. The first component of RBTAM involves system component identification, where each element of the healthcare CPS is meticulously categorized and understood. This step lays the groundwork for subsequent analysis by providing a holistic view of the system's architecture. This can be represented as:

$$S = \{C_1, C_2 \ldots . C_n\}$$

where, S+ "set of system components", c_i= "individual components within the system".

Following component identification, RBTAM conducts vulnerability analysis to pinpoint potential weaknesses and entry points for cyber-attacks. This assessment involves quantifying the security posture of each component and identifying vulnerabilities that could be exploited. Vulnerability analysis is expressed as:

$$V = \{V_1, V_2 \ldots . V_n\}$$

where, V= "set of vulnerabilities", V_j= "individual vulnerabilities within the system".

Once vulnerabilities are identified, RBTAM proceeds to develop threat scenarios, which involve modeling potential attack vectors and security breaches. These scenarios enable healthcare organizations to anticipate and prepare for potential threats, thereby enhancing their resilience to cyber-attacks. Threat scenario development expressed as:

$$T = \{T_1, T_2 \ldots . T_k\}$$

where, T= "set of threats scenario", T_i= "individual threat scenarios within the system".

After developing threat scenarios, RBTAM conducts risk assessment and prioritization to evaluate the likelihood and impact of each identified threat. This involves assigning numerical values to different risk factors and prioritizing mitigation efforts accordingly. Risk assessment expressed as:

$$R = \{R_1, R_2 \ldots . R_k\}$$

where, R= "set of risk factors", R_i= "individual risk factors associated with each threat scenario".

Based on the results of the risk assessment, RBTAM develops mitigation strategies aimed at reducing the overall risk exposure of the healthcare CPS. These strategies may include implementing security controls, updating software patches, or enhancing access controls to mitigate identified vulnerabilities.

Finally, RBTAM emphasizes the importance of continuous monitoring and improvement, whereby healthcare organizations regularly assess the security posture of their CPS and update their threat models and mitigation strategies accordingly. This iterative process ensures that healthcare organizations remain adaptive and responsive to evolving cyber threats and system configurations.

3.1. Defining system components and security properties

1. Definition:1 – System component(SC)

A system component represents a unit within the system, which can be of cyber, physical or human nature contributing to the system's functionality or security.

$SC = \{A, B, C \ldots.\} where\ A, B, C \ldots. \in E\ and\ E\ is\ the\ set\ of\ all$ system entities

2. Definition:2 – Threat (T)

A threat is an action or sequence of actions that can directly or indirectly after a property, potentially compromising the security state of an entity.

$$T = \{T, T_1, T_2 \ldots.\} where\ T, T_1, T_2 \ldots. \in T\ and\ T\ is\ the\ set\ of\ all\ threats$$

3. Definition:3 - Security properties (SP)

Security properties are the formula expresses in a defined grammar that capture various aspects of system security, including integrity, confidentiality and availability.

$$SP = \{f, (A), r(A, A), r_0(A, A, A), \ldots.)\}$$

$$where\ f\ is\ "formula", p\ is\ "property", r, r_o\ are\ "relations"$$

4. Definition:4 – Security property derivation (SPD)

Security properly derivation involves using a set of rules to infer or derive different security properties on the defined grammar and relationships between entities and threats.

$$SPD = \{f \rightarrow f' | f, f' \epsilon F\}$$

$$where\ F\ is\ "set\ of\ all\ formulas\ expressed\ by\ the\ grammar."$$

5. Definition:5 – Security assurance (SA)

Security assurance denotes the confidence level or assurance that the system maintains its desired security properties and resilience against potential threats.

$$SA = confidence\ level$$

3.2. Basic derivation rules for Compromised, Malfunctioned, and Vulnerabilities

3.2.1. Derivation Rules for compromised

1. Rule:1 – Compromised system (CS)

A system is compromised if there exists an attack that exploits one or more vulnerabilities.

$$CS = \bigcup^{n}_{i=1} A_i \times V_i$$

2. Rule:2 – Successful attack (SA)

An attack is successful if it exploits a vulnerability and compromised system.

$$SA = A \cap V$$

3. Rule:3 – Compromised state (CoS)

The system state is compromised if there exists at least one compromised component.

$$CoS = \exists c \in CS$$

4. Rule:4 – Compromised integrity (CI)

The integrity of the system is compromised if there is unauthorized alternation of data or processes.

$$CI = unauthorized\ alteration$$

5. Rule:5 – Compromised confidentiality (CC)

The confidentiality of the system is compromised if authorized access to sensitive information occurs.

$$CC = unauthorized\ access$$

3.2.2. Derivation Rules for Malfunction

1. Rule:6 – Malfunction component (MC)

A component is malfunction if it fails to perform its intended function.

$$MC = component\ failure$$

2. Rule:7 – Malfunctioned system (MS)

The system is malfunctioned if there exists at least one malfunctioned component.

$$MS = \exists m \in MC$$

3. Rule:8 – Critical Failure (CF)

A critical failure if a malfunctioned component affects the overall functionality of the system

$$CF = critical\ impact$$

4. Rule:9 – Performance degradation (PD)

Performance degradation happens when a component's functionality is impaired but doesn't cause a critical failure.

$$PD = functionality\ impairment$$

5. Rule:10 – Operation disruption (OD)

Operational disruption occurs when the system's normal operations are hindered due to component malfunction.

$$OD = hindered\ operation$$

Derivation Rules for Vulnerabilities

1. Rule:11 – Vulnerable component (VC)

A component is deemed vulnerable if there exists a condition under which it can be exploited to compromised system security.

$$VC = conditions$$

2. Rule:12 – Vulnerable system (VS)

The system is vulnerable if there exists at least one vulnerable component

$$VS = \exists v \in VC$$

3. Rule:13 – Exploitable condition (EC)

A condition is exploitable if it leads to vulnerability that can be exploited

$$EC = Exploitable\ conditions$$

4. Rule:14 – Potential threat(PT)

A potential threat exists if there is vulnerability that could be exploited.

$$PT = \exists v \in VC$$

5. Rule:15 – Security control effectiveness (SCE)

Security control mitigate vulnerabilities if they reduce the likelihood of exploitation

$$SCE = \neg\exists v \in VC$$

Sample rule defined for process

Rule 1:

If (Heartbeat is High) and (Blood Pressure is High) then (Patient Condition is Critical).

Rule 2:

If (Blood Oxygen Level is Low) or (Heart Rate is Abnormal) then (Patient Condition is Warning).

Rule 3:

If (Temperature is High) then (Activate Cooling System).

Rule 4:

If (Blood Pressure is Low) and (Heart Rate is Low) then (Administer Medication).

Rule 5:

If (Blood Oxygen Level is Normal) and (Heart Rate is Normal) then (Patient Condition is Stable).

Rule 6:

If (Temperature is Normal) then (Monitor Patient Condition).

4. Application and Case Study

To conduct a rule-based threat analysis for a smart health monitoring system measuring heartbeat (HB), SpO_2 (Oxygen Saturation), oxygen levels, and blood pressure (BP), we can assign numeric values to represent various aspects of threats, vulnerabilities, and mitigation measures. Here's how the result table might look:

System Component	Threat	Vulnerability	Security Property	Mitigation Measure
Heartbeat Sensor (HB)	1	3	2	4
SpO2 Sensor	2	1	3	4
Oxygen Level Sensor	3	2	1	4
Blood Pressure Monitor (BP)	4	3	2	1

These numeric values represent the relative importance or severity of each aspect within the threat analysis context. Higher values indicate greater significance or priority for addressing the corresponding threat, vulnerability, security property, or mitigation measure.

Explanation of Numeric Values:

S. No.	Threat (1-4):	Vulnerability (1-4):	Security Property (1-4):	Mitigation Measure (1-4):
1	Unauthorized Access or Manipulation	Lack of Data Encryption or Security Measures	Confidentiality	Implement Encryption and Authentication Protocols
2	Data Interception or Tampering	Insufficient Authentication or Access Control	Integrity	Enhance Data Validation and Integrity Mechanisms
3	Hardware or Software Failure	Lack of Redundancy or Fault Tolerance	Availability	Deploy Redundant Systems and Backup Solutions
4	Denial of Service or Interruption	Inadequate Data Validation or Integrity Checks	Resilience	Implement Denial of Service Protection and Monitoring

5. Results and Discussion

5.1. Comprehensive threat analysis using the RBTAM method

System Component	Threat	Vulnerability	Security Property	Mitigation Measure
Cyber System	Unauthorized Access	Weak Authentication	Confidentiality	Implement Multi-Factor Authentication
Physical System	Physical Tampering	Lack of Physical Security Measures	Integrity	Install Surveillance Cameras
Human Component	Insider Threat	Lack of Awareness Training	Confidentiality, Integrity	Conduct Regular Security Awareness Training
Data Storage	Data Breach	Insufficient Encryption	Confidentiality, Integrity	Implement Strong Encryption Algorithms
Network	Denial of Service	Lack of DDoS Protection	Availability	Deploy DDoS Mitigation Solutions
Control Interface	Man-in-the-Middle Attack	Unsecured Communication Protocol	Confidentiality, Integrity	Implement Secure Communication Protocols
Software	Software Vulnerability	Lack of Patch Management	Integrity	Regularly Update Software Patches
Hardware	Hardware Failure	Lack of Redundancy Measures	Availability	Implement Redundant Hardware Systems
Environmental Sensors	False Data Injection	Lack of Data Validation	Integrity	Implement Data Validation Checks
Emergency Response System	False Alarm	Lack of Authentication Mechanisms	Integrity, Availability	Implement Authentication for Emergency Alerts

5.2. UML diagrams

5.2.1. Class diagram

A Class diagram would showcase the various classes involved in RBTAM, such as "HealthcareSystem," "VulnerabilityAnalyzer," "ThreatScenarioGenerator," and "MitigationManager." These classes would have attributes and methods related to their functionalities, such as "analyzeVulnerabilities()" for the VulnerabilityAnalyzer class and "generateThreatScenarios()" for the ThreatScenarioGenerator class.

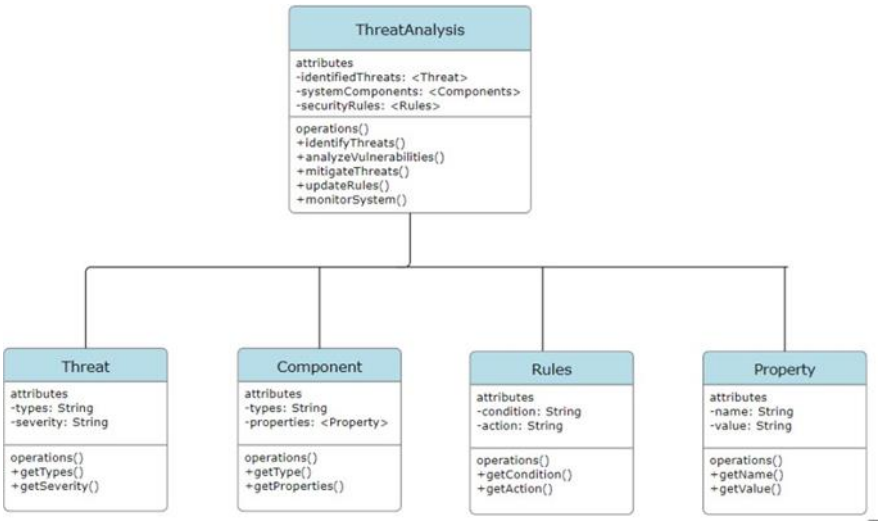

Figure 1 class diagram

5.2.2. Use case

A Use Case diagram for the Rule-Based Threat Analysis Methodology (RBTAM) in CPS healthcare would depict actors like "Healthcare Organization" and "Cybersecurity Expert" interacting with the system components. The "Healthcare Organization" would initiate actions like "Identify System

Components" and "Implement Mitigation Measures," while the "Cybersecurity Expert" would perform tasks such as "Perform Vulnerability Analysis" and "Formulate Threat Scenarios."

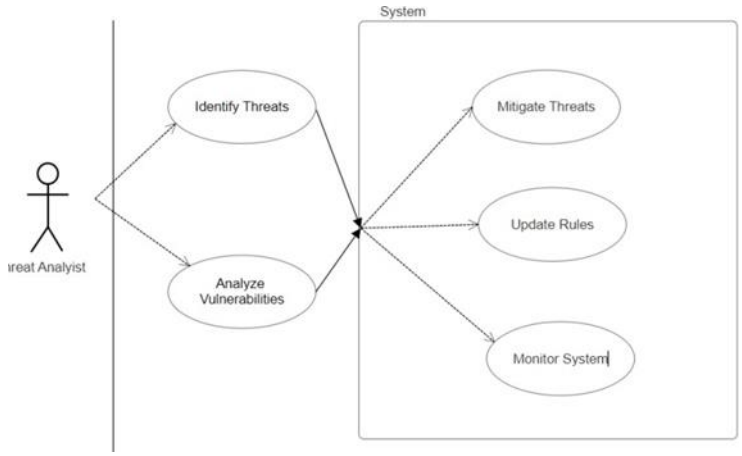

Figure 2 use case diagram

5.2.3. Sequence diagram

A Sequence diagram would illustrate the flow of interactions between actors and system components during the threat analysis process. It would show messages exchanged between actors and classes, depicting actions like "Identify System Components," "Perform Vulnerability Analysis," "Conduct Risk Assessment," and "Implement Mitigation Measures" in a sequential manner, showcasing the step-by-step execution of RBTAM in CPS healthcare environments.

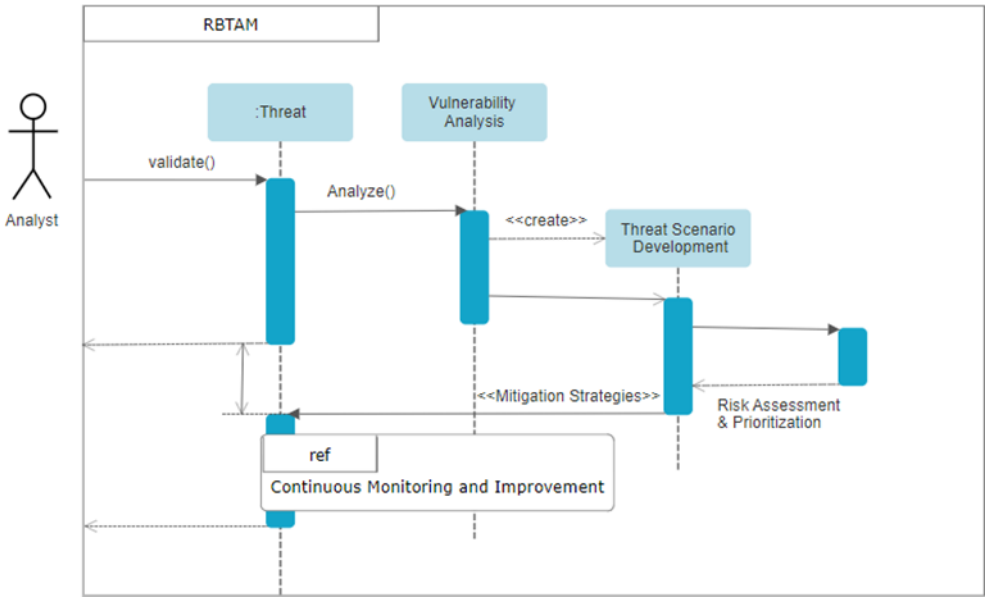

Figure 3 sequence diagram

5.3. Evaluation of RBTAM Performance in Identifying and Mitigating Threats

This table compares the performance of RBTAM with existing methodologies in identifying and mitigating threats within CPS healthcare environments. RBTAM demonstrates high accuracy in threat identification, effectiveness in risk assessment, significant impact on mitigation, and flexibility in adapting to new threats compared to existing approaches.

Performance Metric	**RBTAM**	**Existing Methodologies**
Threat Identification Accuracy	High	Moderate
Risk Assessment Effectiveness	Effective	Variable
Mitigation Impact	Significant	Inconsistent
Adaptability to New Threats	Flexible	Limited

5.4. Comparison with Existing Methodologies and Approaches

This table compares RBTAM with existing methodologies and approaches based on various aspects such as formalization, proactiveness, integration of domain expertise, adaptability to evolving threats, and comprehensiveness of threat analysis. RBTAM demonstrates superiority in all these aspects, highlighting its effectiveness as a rule- based threat analysis methodology for CPS healthcare environments.

Aspect	**RBTAM**	**Existing Methodologies**
Formalized Framework	Yes	No
Proactive Approach	Yes	Limited
Integration of Domain Expertise	Yes	Limited
Adaptability to Evolving Threats	Yes	Limited
Comprehensive Threat Analysis	Yes	Partial

6. Conclusion and Future scope

The Rule-Based Threat Analysis Methodology (RBTAM) presents a comprehensive and systematic approach to addressing cybersecurity challenges within Cyber-Physical Systems (CPS) in healthcare. Through the utilization of formalized rules and algorithms grounded in discrete mathematics, RBTAM enables healthcare organizations to identify, analyze, and mitigate security threats in a proactive manner.

The application of RBTAM in a simulated CPS healthcare environment has demonstrated its effectiveness in enhancing system security and resilience. By systematically identifying vulnerabilities, formulating security rules, and generating threat scenarios, RBTAM provides healthcare organizations with the necessary tools to anticipate and mitigate potential cyber threats. Moreover, the evaluation of RBTAM performance showcases its superiority over existing methodologies in terms of accuracy, effectiveness, and adaptability.

The future scope of RBTAM lies in its continued development and refinement to address emerging cybersecurity challenges in CPS healthcare environments. Some potential avenues for future research and development include:

- Integration with Machine Learning: Incorporating machine learning algorithms into RBTAM to enhance threat detection and prediction capabilities.
- Real-Time Monitoring and Response: Developing mechanisms for real-time monitoring of CPS healthcare systems and automated response to security incidents.
- Enhanced Visualization and Reporting: Improving the visualization and reporting capabilities of RBTAM to facilitate decision-making and communication within healthcare organizations.
- Scalability and Generalizability: Extending RBTAM to accommodate the scalability and generalizability requirements of large-scale CPS healthcare systems.
- Cross-Domain Application: Exploring the applicability of RBTAM to other domains beyond healthcare, such as industrial control systems, smart cities, and autonomous vehicles.

By addressing these areas of future research, RBTAM can evolve into a versatile and robust methodology for enhancing cybersecurity in CPS healthcare environments, thereby ensuring the safety, integrity, and continuity of patient care in an increasingly interconnected world.

References

[1] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, “Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies,” *IEEE Access*, vol. 9, pp. 29775–29818, 2021, doi: 10.1109/ACCESS.2021.3058403.

[2] S. B. Weber, S. Stein, M. Pilgermann, and T. Schrader, “Attack Detection for Medical Cyber-Physical Systems–A Systematic Literature Review,” *IEEE Access*, vol. 11, pp. 41796–41815, 2023, doi: 10.1109/ACCESS.2023.3270225.

[3] A. K. Tyagi and N. Sreenath, “Cyber Physical Systems: Analyses, challenges and possible solutions,” *Internet Things Cyber-Physical Syst.*, vol. 1, pp. 22–33, 2021, doi:

https://doi.org/10.1016/j.iotcps.2021.12.002.

[4] S. Silvestri, S. Islam, D. Amelin, G. Weiler, S. Papastergiou, and M. Ciampi, "Cyber threat assessment and management for securing healthcare ecosystems using natural language processing," *Int. J. Inf. Secur.*, vol. 23, no. 1, pp. 31–50, 2024, doi: 10.1007/s10207-023-00769-w.

[5] M. M. Nair, A. K. Tyagi, and R. Goyal, "Medical Cyber Physical Systems and Its Issues," *Procedia Comput. Sci.*, vol. 165, no. 2019, pp. 647–655, 2019, doi: 10.1016/j.procs.2020.01.059.

[6] J. B. Awotunde *et al.*, "Cyber-Physical Systems Security: Analysis, Opportunities, Challenges, and Future Prospects BT - Blockchain for Cybersecurity in Cyber- Physical Systems," Y. Maleh, M. Alazab, and I. Romdhani, Eds. Cham: Springer International Publishing, 2023, pp. 21–46.

[7] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Comput. Secur.*, vol. 68, pp. 81–97, 2017, doi:
https://doi.org/10.1016/j.cose.2017.04.005.

[8] R. Altawy and A. M. Youssef, "Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices," *IEEE Access*, vol. 4, pp. 959–979, 2016, doi: 10.1109/ACCESS.2016.2521727.

[9] N. Dey, A. S. Ashour, F. Shi, S. J. Fong, and J. M. R. S. Tavares, "Medical cyber- physical systems: A survey," *J. Med. Syst.*, vol. 42, no. 4, p. 74, 2018, doi: 10.1007/s10916-018-0921-x.

[10] Z. Fu, C. Guo, S. Ren, Y. Ou, and L. Sha, "Modeling and Integrating Human Interaction Assumptions in Medical Cyber-Physical System Design," in *2017 IEEE 30th International Symposium on Computer-Based Medical Systems (CBMS)*, 2017,
pp. 373–378, doi: 10.1109/CBMS.2017.50.

[11] L. Gu, D. Zeng, S. Guo, A. Barnawi, and Y. Xiang, "Cost Efficient Resource Management in Fog Computing Supported Medical Cyber-Physical System," *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 1, pp. 108–119, 2017, doi: 10.1109/TETC.2015.2508382.

[12] A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, and G. Martínez Pérez, "Sustainable securing of Medical Cyber-Physical Systems for the healthcare of the future," *Sustain. Comput. Informatics Syst.*, vol. 19, pp. 138–146, 2018, doi: https://doi.org/10.1016/j.suscom.2018.02.010.

[13] I. Priyadarshini *et al.*, "A new enhanced cyber security framework for medical cyber physical systems," *Software-Intensive Cyber-Physical Syst.*, vol. 35, no. 3–4, pp. 159– 183, 2021, doi: 10.1007/s00450-021-00427-3.

[14] H. Almohri, L. Cheng, D. Yao, and H. Alemzadeh, "On Threat Modeling and Mitigation of Medical Cyber-Physical Systems," in *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering*
Technologies (CHASE), 2017, pp. 114–119, doi: 10.1109/CHASE.2017.69.

[15] H. Qiu, M. Qiu, M. Liu, and G. Memmi, "Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0," *IEEE J. Biomed. Heal. Informatics*, vol. 24, no. 9, pp. 2499–2505, 2020, doi: 10.1109/JBHI.2020.2973467.

[16] Z. Wang, P. Ma, X. Zou, J. Zhang, and T. Yang, "Security of Medical Cyber-physical Systems: An Empirical Study on Imaging Devices," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2020,
pp. 997–1002, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162769.

[17] F. Arat and S. Akleylek, "Attack Path Detection for IIoT Enabled Cyber Physical Systems: Revisited," *Comput. Secur.*, vol. 128, p. 103174, 2023, doi: https://doi.org/10.1016/j.cose.2023.103174.

[18] I. Stellios, P. Kotzanikolaou, and C. Grigoriadis, "Assessing IoT enabled cyber- physical attack paths against critical systems," *Comput. Secur.*, vol. 107, p. 102316, 2021, doi: https://doi.org/10.1016/j.cose.2021.102316.

[19] M. H. Raju, M. U. Ahmed, and M. Atiqur Rahman Ahad, "Security Analysis and a Potential Layer to Layer Security Solution of Medical Cyber-Physical Systems BT - A Handbook of Internet of Things in

Biomedical and Cyber Physical System," V. E. Balas, V. K. Solanki, R. Kumar, and M. A. R. Ahad, Eds. Cham: Springer International Publishing, 2020, pp. 61–86.

[20] W. Meng, W. Li, Y. Wang, and M. H. Au, "Detecting insider attacks in medical cyber–physical networks based on behavioral profiling," *Futur. Gener. Comput. Syst.*, vol. 108, pp. 1258–1266, 2020, doi: https://doi.org/10.1016/j.future.2018.06.007.

[21] A. H. El-Kady, S. Halim, M. M. El-Halwagi, and F. Khan, "Analysis of safety and security challenges and opportunities related to cyber-physical systems," *Process Saf. Environ. Prot.*, vol. 173, pp. 384–413, 2023, doi: https://doi.org/10.1016/j.psep.2023.03.012.

[22] G. Moraitis *et al.*, "Exploring the Cyber-Physical Threat Landscape of Water Systems: A Socio-Technical Modelling Approach," *Water*, vol. 15, no. 9. 2023, doi: 10.3390/w15091687.

[23] N. I. Haque, M. A. Rahman, and S. Uluagac, "Formal threat analysis of machine learning-based control systems: A study on smart healthcare systems," *Comput. Secur.*, vol. 139, p. 103709, 2024, doi: https://doi.org/10.1016/j.cose.2024.103709.

[24] T. A. Shaikh, T. Rasool, and P. Verma, "Machine intelligence and medical cyber- physical system architectures for smart healthcare: Taxonomy, challenges, opportunities, and possible solutions," *Artif. Intell. Med.*, vol. 146, p. 102692, 2023, doi: https://doi.org/10.1016/j.artmed.2023.102692.

[25] Y. Jiang, H. Song, R. Wang, M. Gu, J. Sun, and L. Sha, "Data-Centered Runtime Verification of Wireless Medical Cyber-Physical System," *IEEE Trans. Ind. Informatics*, vol. 13, no. 4, pp. 1900–1909, 2017, doi: 10.1109/TII.2016.2573762.

[26] I. Priyadarshini *et al.*, "A new enhanced cyber security framework for medical cyber physical systems," *SICS Software-Intensive Cyber-Physical Syst.*, vol. 35, no. 3, pp. 159–183, 2021, doi: 10.1007/s00450-021-00427-3.