Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27696-cd

Dynamic Vulnerability Assessment for Connected Healthcare Systems via Continuous-Time Bayesian Networks

Stefano Perone, Luca Dori, Arianna Giorgi, Simone Guarino

Unit of Automatic Control, Department of Engineering, Università Campus Bio-Medico, Rome, Italy.
E-mail: {s.perone, s.guarino}@unicampus.it, {luca.dori, arianna.giorgi}@alcampus.it

Connected healthcare environments increasingly rely on Internet of Medical Things (IoMT) devices and integrated medical networks to support clinical operations. However, this high level of connectivity expands the attack surface and introduces significant cybersecurity risks that can endanger patient safety and compromise data confidentiality. In this context, effective vulnerability assessment and prioritization are essential; nevertheless, current approaches are predominantly static and fail to capture the temporal dynamics associated with real-world vulnerability exploitation processes. For this reason, the paper introduces a vulnerability assessment approach based on Continuous-Time Bayesian Networks (CTBNs), which enable explicit modeling of vulnerability state transitions as continuous-time stochastic processes. Unlike discrete-time formulations, CTBNs incorporate time-dependent factors such as the evolving time to exploit, the likelihood of exploitation over time, and changes in adversarial capabilities. This enables the computation of exploitation probabilities as continuous functions, providing an adaptive vulnerability prioritization mechanism aligned with the operational requirements of clinical environments. The proposed approach is evaluated within a simulated hospital network. By modeling vulnerability dependencies through CTBNs, the framework enables the computation of posterior exploitation probabilities along potential attack paths targeting critical clinical assets. Preliminary results indicate that the CTBN-based approach improves the timeliness and responsiveness of vulnerability assessment compared with static methods. This dynamic perspective supports better-informed and proactive risk mitigation strategies in safety-critical healthcare settings, further improving cybersecurity management in these environments.

Keywords: Vulnerability Prioritization, Bayesian Networks, Temporal Analysis, Cybersecurity, Healthcare.

1. Introduction

The rapid digitalization of modern healthcare has led to the pervasive adoption of Internet of Medical Things (IoMT) devices – defined as the interconnection of communication-enabled medical-grade devices and their integration into wider-scale healthcare networks to improve patient outcomes Gatouillat et al. (2018) – transforming clinical infrastructures into highly interconnected cyber-physical ecosystems. While this integration enhances operational efficiency and patient monitoring, it simultaneously expands the attack surface, introducing complex interdependencies that traditional security measures struggle to address. In these environments, cybersecurity is no longer a static property but a dynamic process; vulnerabilities evolve, attacker capabilities mature, and system states fluctuate continuously over time. Consequently, the ability to assess and prioritize vulnerabilities in real-time is critical to ensuring not only data confidentiality but, more importantly, patient safety. Despite the critical nature of these systems, current vulnerability assessment methodologies predominantly rely on static scoring systems, such as the Common Vulnerability Scoring System (CVSS). While effective at providing a standardized snapshot of system security, these methods suffer from significant limitations when applied to the stochastic nature of real-world cyber-attacks. The primary drawback is their inability to capture the temporal evolution of risk: static metrics treat vulnerability exploitation as an isolated, time-invariant event. Consequently, a system deemed secure at time t_0 may become critically exposed at t_1 without any configuration change, simply due to the aging of the vulnerability information. To overcome the rigidity of deterministic scoring, the research community has increasingly turned towards probabilistic modeling as a more robust alternative. A probabilistic

approach is essential in cybersecurity because it allows for the explicit quantification of uncertainty. In complex healthcare networks, complete information about an attacker's location, capability, or intent is rarely available. Probabilistic frameworks enable the modeling of causal dependencies between network assets, allowing defenders to estimate the likelihood of compromise propagation across the infrastructure. This perspective shifts the focus from merely cataloging flaws to understanding the conditional likelihood of attack paths, providing a more realistic basis for risk prioritization Almaiah et al. (2023). Within this probabilistic domain, Bayesian Networks (BNs) have emerged as a leading tool for modeling cause-effect relationships. However, the majority of existing literature applies BNs in a discrete-time setting. As highlighted by Vairo et al. (2025), discrete approaches come with inherent drawbacks. They typically rely on static Conditional Probability Tables (CPTs) defined over fixed time intervals. This discretization imposes arbitrary time-steps that often fail to align with the actual speed of cyber-physical cascades. The use of static CPTs limits the model's ability to support true temporal inference, effectively masking rapid attack vectors that occur between time steps and simplifying the complex stochastic nature of vulnerability exploitation into rigid probability slots Cerotti et al. (2025). To address these structural limitations, this paper introduces a dynamic vulnerability assessment approach based on Continuous-Time Bayesian Networks (CTBNs), representing a fundamental shift from discrete models by treating system state transitions as continuous-time stochastic processes. This method utilizes Beta probability density functions to explicitly model the uncertainty in "time-to-exploit," capturing both epistemic and aleatory factors, while employing intensity matrices to dynamically update parameters as the threat landscape evolves. By calculating exploitation probabilities as continuous functions, the framework enables time-informed decision-making and prioritization that is highly responsive to the operational urgency of clinical environments, significantly surpassing the capabilities of static or discrete-time models.

To validate the effectiveness of the proposed framework, we apply it to a realistic case study modeling a hospital network infrastructure composed of both IT and IoMT assets. The results demonstrate that the CTBN-based approach provides a more granular and timely assessment of risk compared to traditional static or discrete methods, effectively bridging the gap between theoretical risk scoring and the dynamic reality of cyber threats in healthcare. The rest of the paper is structured in five sections. Section 2 provides an overview of the state of the art regarding vulnerability assessment in healthcare and probabilistic modeling. Section 3 details the theoretical foundations of Continuous-Time Bayesian Networks, while Section 4 describes the proposed framework for dynamic vulnerability analysis. Section 5 presents the experimental setup, the case study definition, and discusses the results obtained by our approach. Finally, Section 6 draws the conclusions and outlines future research directions.

2. Related Works

The security challenges associated with the proliferation of IoT and IoMT devices in healthcare environments have been extensively discussed in recent literature. Safavi et al. (2018) has provided a comprehensive review of cyber vulnerabilities in smart healthcare, highlighting the critical need for privacy and security in connected ecosystems. Similarly, Bracciale et al. (2023) analyzed of medical device datasets has revealed a concerning landscape where vulnerabilities often remain exposed for years even after patches are available, thus emphasizing the persistence of risk over time. To address these complexities, the research community has largely adopted probabilistic graphical models. Hunte et al. (2024) proposed a hybrid Bayesian Network (BN) method for medical device risk management, aiming to resolve the limitations of traditional Fault Tree Analysis by incorporating diverse risk factors compliant with ISO standards. In a broader industrial context, Guarino et al. (2024) introduced a holistic risk assessment framework that combine BNs with Multi-Criteria Decision Making. These approaches integrate heterogeneous risk values into a single

comprehensive metric, enhancing the granularity of the assessment. Furthermore, the need to capture system dynamics has led to the integration of data-driven techniques; for instance, Vitale et al. (2024) proposed a framework based on process mining for the development of Digital Twins connect data-driven monitoring with process-based analysis to capture the normal and faulty dynamics of Cyber-Physical Systems. Regarding the specific inclusion of the temporal dimension in risk analysis, Perone et al. (2025) presented an approach that integrates CVSS Temporal Metrics with BNs. By accounting for exploit availability and remediation levels, these methods attempt to make the assessment more adaptive compared to static baselines. From a mathematical modeling perspective, Cristiani et al. (2023) explored the dynamics of agents with predictive abilities, modeling how entities move and make decisions based on the current and future state of the system, a concept that parallels the behavior of attackers moving laterally within a network. However, despite these advancements, existing methodologies predominantly rely on Discrete-Time Bayesian Networks (DTBNs) or static scoring integrations. As highlighted by Vairo et al. (2025), discrete approaches suffer from inherent structural limitations, primarily due to the definition of static Conditional Probability Tables (CPTs) over fixed intervals. This discretization fails to support true temporal inference, often masking rapid transition events that characterize real-world cyber-attacks. In contrast, our approach introduces a vulnerability assessment framework based on Continuous-Time Bayesian Networks (CTBNs). Unlike previous works that treat time as a sequence of fixed steps or a static metric, we model vulnerability exploitation as a continuous stochastic process, utilizing Beta probability density functions to capture the evolving likelihood of compromise in real-time.

3. Background

This section introduces the theoretical foundations and the metrics adopted in the proposed framework, describing the formal definitions of Bayesian Networks and their continuous-time extension.

3.1. *Bayesian Networks (BNs)*

A Bayesian Network is a probabilistic graphical model that represents a set of random variables and their conditional dependencies via a Directed Acyclic Graph (DAG). Formally, a BN is defined as a pair $B = (G, \Theta)$, where:

- $G = (V, E)$ is a DAG where V represents the set of random variables $\{X_1, \ldots, X_n\}$ and E represents the directed edges encoding causal dependencies.
- Θ represents the set of Conditional Probability Tables (CPTs). For each variable X_i, the CPT quantifies the probability $P(X_i|Pa(X_i))$, where $Pa(X_i)$ denotes the set of parents of X_i in the graph.

The joint probability distribution of the variables is given by the chain rule:

$$P(X_1, \ldots, X_n) = \prod_{i=1}^{n} P(X_i \mid Pa(X_i)) \quad (1)$$

While BNs are powerful for modeling static uncertainties, they lack the ability to explicitly represent the temporal duration of states, which is crucial for modeling attack dynamics.

3.2. *Continuous-Time Bayesian Networks (CTBNs)*

To overcome the limitations of discrete-time models, Continuous-Time Bayesian Networks (CTBNs) extend BNs to model stochastic processes evolving over continuous time. Formally, a CTBN is defined as a tuple $\mathcal{N} = (V, G, \mathbf{Q})$, where V is the set of variables, G is the dependency graph, and $\mathbf{Q}$ is the set of Conditional Intensity Matrices (CIMs). Unlike discrete BNs where dependencies are modeled via probabilities, in CTBNs, the evolution of a variable X_i depends on the state of its parents $Pa(X_i)$ through a transition intensity matrix $Q_{X_i|Pa(X_i)}$.

For a variable X with state space S, given a specific instantiation of its parents u, the dynamics

are governed by the intensity matrix:

$$Q_{X|u} = \begin{pmatrix} -q_{x_1} & q_{x_1x_2} & \cdots \\ q_{x_2x_1} & -q_{x_2} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \tag{2}$$

where q_{xy} represents the instantaneous probability rate of transitioning from state x to state y, and $q_x = \sum_{y \neq x} q_{xy}$ is the total exit rate from state x. Crucially, the time spent in a state x before a transition occurs follows an exponential distribution with parameter q_x:

$$P(Time > t \mid X(0) = x) = e^{-q_x t} \tag{3}$$

This formulation allows the model to capture the exploitation time as a continuous variable, enabling the calculation of state probabilities $P(X(t) = x)$ at any arbitrary time t.

4. Methodology

The methodological approach proposed in this study is grounded in the probabilistic risk assessment framework developed by Vairo et al. (2025). Specifically, we adapt the principles of their *Cyber Vulnerability Assessment* module to the healthcare domain. Crucially, while original frameworks were often designed for industrial control systems, we restrict the scope of our analysis to biomedical devices and clinical support systems. This boundary definition intentionally excludes general-purpose IT infrastructure, thereby isolating the specific cyber-physical threats that jeopardize patient safety within the hospital environment. The proposed methodology unfolds through a structured pipeline comprising three main phases. First, vulnerability identification is performed to detect specific CVEs affecting the defined clinical assets. Second, attack path characterization is employed to map the logical sequences an attacker could exploit to escalate privileges or compromise critical nodes. These paths are formalized into a Bayesian Attack Graph (BAG), where nodes represent security states and edges represent the conditional dependencies between vulnerabilities. Finally, the probabilistic analysis is executed using CTBNs. Unlike discrete-time models that rely on static CPTs, our approach leverages CTBNs to model the exploitation probability as a function of time using Conditional Probability Distributions (CPDs), thereby capturing the dynamic and stochastic nature of cyber threats. To support this analysis, the model is parameterized using standard vulnerability metrics from the National Vulnerability Database (NVD) and Exploit-DB. To mathematically integrate these metrics into the CTBN, we define the operational mapping as follows: the transition intensity $q_{xy}(t)$ within the Conditional Intensity Matrix (CIM) is modeled as the time-dependent Weibull hazard rate function, capturing the evolving pressure of the exploit. Simultaneously, the Beta distribution is introduced to quantify the epistemic uncertainty associated with the expected exploitation probability. In our inference framework, this acts as a prior over the intensity parameters, allowing us to propagate uncertainty via MCMC sampling. Specifically, given a vulnerability v_i disclosed at time t_0, the probability of exploitation by assessment time T is modeled via the Weibull survival function:

$$P(v_i \text{ exploited by } T) = 1 - \exp\left(-\left(\frac{T - t_0}{\eta}\right)^m\right) \tag{4}$$

where η and m are Weibull parameters estimated from CVE-Exploit-DB historical data. In this setting, the corresponding (time-varying) hazard rate is

$$\lambda_i(t) = \frac{m}{\eta}\left(\frac{t - t_0}{\eta}\right)^{m-1}, \qquad t \geq t_0 \tag{5}$$

which we use as the CTBN transition intensity for the binary state change *not exploited→exploited* (with no backward transition). In practice, inference is performed by evaluating the model at the assessment time T, i.e., by using the local intensity $\lambda_i(T)$ (or a piecewise-constant approximation over a short window around T). The uncertainty in the Weibull estimate induces a standard deviation $\sigma_i(T)$, computed via error propagation from the Weibull fit's covariance matrix. We then use a Beta distribution to represent uncertainty on the exploitation probability at time T and to propagate it through the CTBN. The Beta parameters (α_i, β_i) are obtained by solving the moment-

matching system:

$$\begin{cases} \frac{\alpha_i}{\alpha_i+\beta_i} = \mu_i(T) \\ \sqrt{\frac{\alpha_i\beta_i}{(\alpha_i+\beta_i)^2(\alpha_i+\beta_i+1)}} = \sigma_i(T) \end{cases} \tag{6}$$

This parameter estimation procedure enables the framework to translate empirical time-to-exploit data into probabilistic distributions that capture both the temporal evolution of threats and the epistemic uncertainty inherent in predicting attacker behavior.

5. Case Study

In this section, we describe a case study in which we apply the proposed approach to analyze vulnerabilities within a simulated hospital network infrastructure. The goal is to demonstrate how integrating CVSS Metrics with Continuous-Time Bayesian Networks can enhance vulnerability assessment and prioritization.

5.1. *Setup*

We structure the hospital network infrastructure following the Purdue Model Williams (1993), adapted to hospital environments with distinct levels from physical processes (Level 0) to cloud services (Level 5). The architecture (Fig. 1) features patient care devices in a Biomedical Device VLAN, a Patient Monitor (PM) Gateway Server bridging monitors to Electronic Health Record (EHR) systems, internal VLANs regulated by an internal firewall, and a DMZ with Proxy/VPN servers behind an external firewall.

In our analysis, we identify vulnerabilities within selected systems at each network level to construct an attack graph focusing on key devices across the network. This graph visualizes the potential attack paths an adversary could leverage to reach the biomedical devices at Layer 1. Then, the exploitation probabilities along these paths are dynamically computed through Bayesian inference using CTBNs.

5.2. *Analysis and Evaluation*

In this section, we present a comprehensive analysis of the attack scenario targeting critical biomedical infrastructure within the hospital network. The evaluation is conducted using the CTBN-based framework described in Section 4, incorporating real vulnerability data and employing Bayesian inference to quantify time-dependent exploitation probabilities. We first describe the attack graph topology and the vulnerability chain, then present the probabilistic results obtained through MCMC sampling, and finally discuss the implications for cybersecurity risk management in healthcare environments. The analysis starts with the realization of the attack graph depicted in Figure 2, which illustrates a multi-stage attack path targeting the Alaris Syringe Module (ASM), a critical biomedical device directly involved in patient care. The graph originates from a Remote Attacker and progresses through several intermediate nodes, each corresponding to a specific vulnerability exploitation step. The topology reveals two initial parallel attack vectors: one targeting the VPN Server, and another targeting an internal Workstation. Both paths serve as initial footholds within the hospital network infrastructure.

The Workstation compromise enables exploitation of the Internal Firewall via CVE-2024-55591 (FortiOS Authentication Bypass). Therefore, the attack graph presents two independent paths converging at the Pump Server through an OR-gate logic: the attacker can compromise the Pump Server either directly from the VPN Server or through the Internal Firewall, both exploiting CVE-2019-0708 (BlueKeep). This OR-gate structure reflects the realistic scenario where multiple entry points exist to the same target asset. Subsequently, the attacker escalates to the Alaris Gateway (AGW) via CVE-2019-10959, a BD Alaris-specific vulnerability involving unrestricted file upload. Finally, compromise of the AGW directly leads to the impairment of the ASM, representing the ultimate objective where patient safety is directly threatened. To quantify the temporal risk dynamics along this attack graph, we parameterized the CTBN model using vulnerability metrics from NVD and Exploit-DB. Following the methodology described in Section 4, each vulnerability was modeled as a Beta-distributed random variable with parameters computed from CVSS scores and temporal factors like the date of CVE

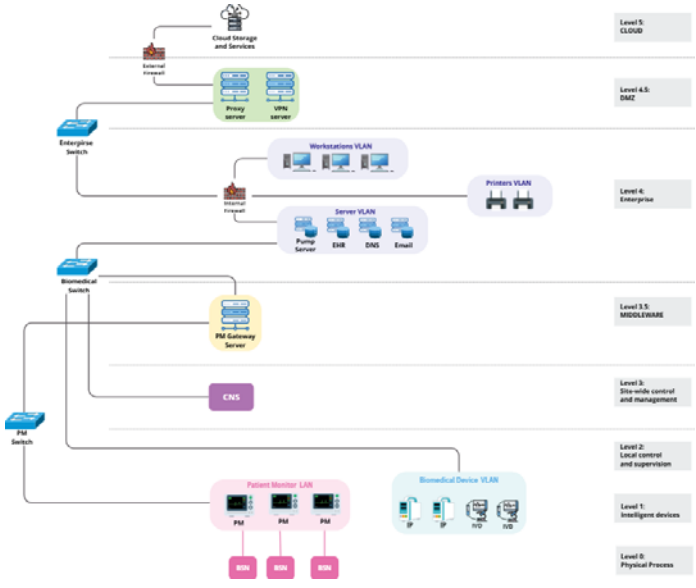

Fig. 1. Hospital network under examination

disclosure and the date of exploit publication. The resulting model was subjected to Bayesian inference using Markov Chain Monte Carlo (MCMC) sampling with the No-U-Turn Sampler (NUTS) algorithm, running 2 chains with 500 tuning iterations and 1,000 sampling iterations per chain. The posterior distributions reveal the subsequent compromise probabilities for the nodes in the network:

- VPN Server: 0.642 ($HDI_{95\%}$[a]: [0.630, 0.653])
- Workstation: 0.689 ($HDI_{95\%}$: [0.678, 0.700])
- Internal Firewall: 0.260 ($HDI_{95\%}$: [0.249, 0.271])
- Pump Server: 0.547 ($HDI_{95\%}$: [0.537, 0.558])
- AGW: 0.381 ($HDI_{95\%}$: [0.371, 0.392]).

Figure 3 provides a comparative visualization of the compromise probabilities across all nodes in the attack graph. The color gradient from red (high risk) to green (low risk) clearly illustrates how the attack probability is distributed over the network.

The final objective distribution (Figure 4) is characterized by a Beta distribution with parameters $\alpha = 22976.23$ and $\beta = 37274.43$, resulting in a highly concentrated distribution around the mean value of 0.381. This narrow distribution reflects the cumulative propagation of uncertainty through the attack chain and provides a robust statistical characterization of the overall risk to the ASM.

The CTBN-based analysis provides substantial advantages over static CVSS-based assessments. While traditional scoring would flag CVE-2024-24919 and CVE-2019-0708 as equally critical based on their Base Scores, the temporal probabilistic model reveals that the likelihood of reaching the final objective is governed by the structural dependencies of the attack chain. From a practical perspective, these results serve as a dynamic decision-support tool for hospital security administrators. For instance, although the Workstation presents a high compromise probability (0.689), the analysis identifies the Internal Firewall as a significant bottleneck with a much lower probability (0.260), suggesting that immediate remediation efforts should instead prioritize the Pump Server (0.547). As a critical junction where two paths converge, patching the Pump Server pro-

[a]Highest Density Interval (HDI) represents the narrowest credible interval containing, in the case under exam, 95% of the posterior probability mass.

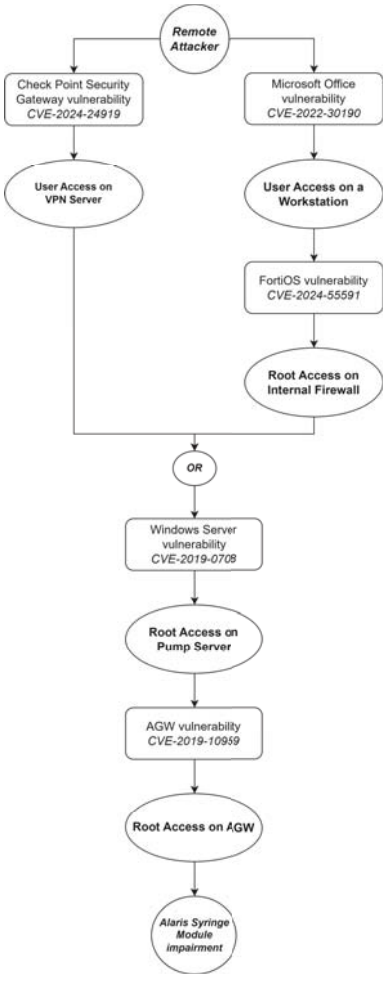

Fig. 2. Attack Graph targeting the Alaris Syringe Module

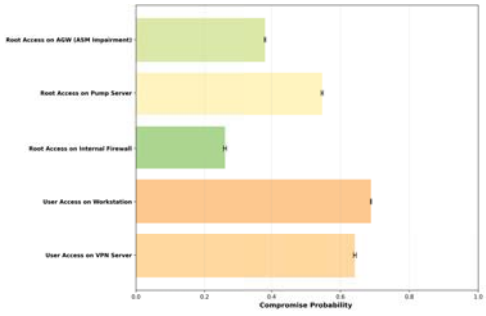

Fig. 3. Compromise probabilities for each network node

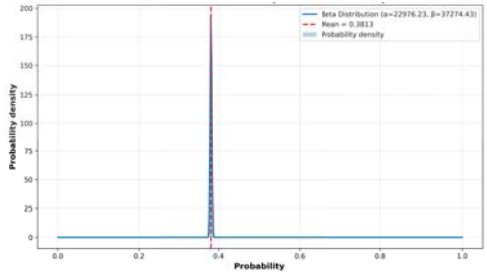

Fig. 4. Beta distribution of ASM Impairment probability

vides a more significant reduction in the overall risk to the Alaris Syringe Module than focusing on perimeter assets. This granularity allows IT staff to optimize maintenance windows, balancing security urgency with clinical continuity.

6. Conclusion

This paper has introduced a dynamic vulnerability assessment framework for connected healthcare systems based on Continuous-Time Bayesian Networks (CTBNs). Unlike traditional static scoring methods, the proposed approach explicitly models the temporal evolution of cyber threats as continuous stochastic processes, enabling the computation of time-dependent exploitation probabilities. The CTBN formulation provides true temporal dynamics by modeling vulnerability exploitation as a continuous-time Markov process, enabling precise quantification of time-to-compromise distributions rather than arbitrary discrete snapshots. At the same time, the probabilistic framework rigorously propagates epistemic and aleatory uncertainties through complex attack chains via Bayesian inference, yielding credible intervals ($\mathrm{HDI}_{95\%}$) that quantify confidence in risk estimates. The methodology was validated through a case study analyzing a hospital network infrastructure. The CTBN framework successfully captured the cascading nature of attack paths, enabling a dynamic and temporal assessment of vulnerabilities in the healthcare network. Beyond its mathematical rigor, the practical contribution of this approach lies in its ability to mitigate “alert fatigue” for clinical IT departments. By filtering

vulnerabilities through the lens of time-dependent impact and path probability, it enables a transition from reactive, checklist-based security to a proactive strategy centered on patient safety and optimized resource allocation. Limitations include dependency on vulnerability data quality, computational complexity for very large networks, and focus on known CVEs. For this reason, future research should explore integration with real-time threat intelligence, incorporation of human factors, and validation in operational healthcare environments. In conclusion, the CTBN-based framework represents a rigorous and applicable solution for addressing dynamic cybersecurity challenges in modern healthcare systems. By unifying temporal dynamics, probabilistic reasoning, and Bayesian inference within a mathematically rigorous yet computationally tractable formulation, it delivers the adaptive, time-aware, and uncertainty-quantified risk intelligence that modern connected healthcare environments urgently require.

Acknowledgement

This work was supported by Agenzia per la Cybersicurezza Nazionale under the programme for promotion of XL cycle PhD research in cybersecurity – C83C24000790001. The views expressed are those of the authors and do not represent the funding institution.

References

Almaiah, M. A., S. Yelisetti, L. Arya, N. K. Babu Christopher, K. Kaliappan, P. Vellaisamy, F. Hajjej, and T. Alkdour (2023). A novel approach for improving the security of iot–medical data systems using an enhanced dynamic bayesian network. *Electronics 12*(20), 4316.

Bracciale, L., P. Loreti, and G. Bianchi (2023). Cybersecurity vulnerability analysis of medical devices purchased by national health services. *Scientific reports 13*(1), 19509.

Cerotti, D., D. Savarro, D. C. Raiteri, G. Dondossola, L. Egidi, G. Franceschinis, L. Portinale, and R. Terruggia (2025). Dynamic bayesian networks for the detection and analysis of cyber attacks to power systems. *IEEE Access*.

Cristiani, E., A. De Santo, and M. Menci (2023). A generalized mean-field game model for the dynamics of pedestrians with limited predictive abilities. *Commun. Math. Sci. 21*(1), 65–82.

Gatouillat, A., Y. Badr, B. Massot, and E. Sejdić (2018). Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine. *IEEE internet of things journal 5*(5), 3810–3822.

Guarino, S., L. Faramondi, G. Oliva, E. Del Prete, and R. Setola (2024). Holistic risk assessment in industrial control systems: Combining multiple bayesian networks with multi-criteria decision making. In *2024 32nd Mediterranean Conference on Control and Automation (MED)*, pp. 37–42. IEEE.

Hunte, J. L., M. Neil, and N. E. Fenton (2024). A hybrid bayesian network for medical device risk assessment and management. *Reliability Engineering & System Safety 241*, 109630.

Perone, S., S. Guarino, L. Faramondi, and R. Setola (2025). Vulnerability assessment combining cvss temporal metrics and bayesian networks. In *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 606–611.

Safavi, S., A. M. Meer, E. K. J. Melanie, and Z. Shukur (2018). Cyber vulnerabilities on smart healthcare, review and solutions. In *2018 Cyber Resilience Conference (CRC)*, pp. 1–5. IEEE.

Vairo, T., S. Guarino, A. Benvenuto, B. Fabiano, and R. Setola (2025). Emergent risks in complex systems: A bayesian perspective on uncertainty and prediction. *Reliability Engineering & System Safety*, 112129.

Vitale, F., S. Guarino, F. Flammini, L. Faramondi, N. Mazzocca, and R. Setola (2024). Process mining for digital twin development of industrial cyber-physical systems. *IEEE Transactions on Industrial Informatics*.

Williams, T. (1993). The purdue enterprise reference architecture. *IFAC Proceedings Volumes 26*(2, Part 4), 559–564. 12th Triennal World Congress of the International Federation of Automatic control. Volume 4 Applications II, Sydney, Australia, 18-23 July.