[7] Bai, B., Li, G., Wang, S., Wu, Z., and Yan, W. (2021). Time series classification based on multi-feature dictionary representation and ensemble learning. *Expert Systems with Applications*, 169:114162.

[8] Balta, E. C., Tilbury, D. M., and Barton, K. (2018). A centralized framework for system-level control and management of additive manufacturing fleets. In *2018 IEEE 14th International Conference on Automation Science and Engineering (CASE)*, pages 1071–1078. IEEE.

[9] Bause, F. and Kritzinger, P. S. (1998). Stochastic petri nets: An introduction to the theory. *ACM SIGMETRICS Performance Evaluation Review*, 26(2):2–3.

[10] Bencsáth, B., Pék, G., Buttyán, L., and Félegyházi, M. (2012). Duqu: Analysis, detection, and lessons learned. In *ACM European Workshop on System Security (EuroSec)*, volume 2012. Citeseer.

[11] Biswas, A. and Dutta, A. (2016). A timer based leader election algorithm. In *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*, pages 432–439. IEEE.

[12] Biswas, A., Maurya, A. K., Tripathi, A. K., and Aknine, S. (2021a). Frlle: a failure rate and load-based leader election algorithm for a bidirectional ring in distributed systems. *The Journal of Supercomputing*, 77(1):751–779.

[13] Biswas, A. and Tripathi, A. K. (2021). Preselection based leader election in distributed systems. In *Proceedings. 14th International Symposium on Intelligent Distributed Computing*. Springer.

[14] Biswas, A., Tripathi, A. K., and Aknine, S. (2021b). Lea-tn: leader election algorithm considering node and link failures in a torus network. *The Journal of Supercomputing*, pages 1–38.

[15] Blank, R. (2019). *The Basics of Reliability*. CRC Press.

[16] Bonet, P., Lladó, C. M., Puijaner, R., and Knottenbelt, W. J. (2007). Pipe v2. 5: A petri net tool for performance modelling. In *Proc. 23rd Latin American Conference on Informatics (CLEI 2007)*.

[17] Bordel, B., Alcarria, R., de Rivera, D. S., and Robles, T. (2018). Process execution in cyber-physical systems using cloud and cyber-physical internet services. *The Journal of Supercomputing*, 74(8):4127–4169.

[18] Bounceur, A., Bezoui, M., Euler, R., Kadjouh, N., and Lalem, F. (2017a). Brogo: a new low energy consumption algorithm for leader election in wsns. In *2017 10Th international conference on developments in esystems engineering (deSE)*, pages 218–223. IEEE.

[19] Bounceur, A., Bezoui, M., Euler, R., and Lalem, F. (2017b). A wait-before-starting algorithm for fast, fault-tolerant and low energy leader election in wsns dedicated to smart-cities and iot. In *2017 IEEE SENSORS*, pages 1–3. IEEE.

[20] Camacho, C. R., Marczak, S., and Cruzes, D. S. (2016). Agile team members perceptions on non-functional testing: influencing factors from an empirical study. In *2016 11th international conference on availability, reliability and security (ARES)*, pages 582–589. IEEE.

[21] Castiglione, J. and Pavlovic, D. (2019). Dynamic distributed secure storage against ransomware. *IEEE Transactions on Computational Social Systems*.

[22] Cavusoglu, H., Raghunathan, S., and Cavusoglu, H. (2009). Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems. *Information Systems Research*, 20(2):198–217.

[23] Chen, D., Johansson, R., Lönn, H., Blom, H., Walker, M., Papadopoulos, Y., Torchiaro, S., Tagliabo, F., and Sandberg, A. (2011a). Integrated safety and architecture modeling for automotive embedded systems. *e & i Elektrotechnik und Informationstechnik*, 128(6):196–202.

[24] Chen, H. (2017). Applications of cyber-physical system: a literature review. *Journal of Industrial Integration and Management*, 2(03):1750012.

[25] Chen, T. M., Sanchez-Aarnoutse, J. C., and Buford, J. (2011b). Petri net modeling of cyber-physical attacks on smart grid. *IEEE Transactions on smart grid*, 2(4):741–749.

[26] Cheng, L., Tian, K., Yao, D., Sha, L., and Beyah, R. A. (2019). Checking is believing: event-aware program anomaly detection in cyber-physical systems. *IEEE Transactions on Dependable and Secure Computing.*

[27] Chiola, G., Marsan, M. A., Balbo, G., and Conte, G. (1993). Generalized stochastic petri nets: A definition at the net level and its implications. *IEEE Transactions on software engineering*, 19(2):89–107.

[28] Cho, C.-S., Chung, W.-H., and Kuo, S.-Y. (2015). Cyberphysical security and dependability analysis of digital control systems in nuclear power plants. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 46(3):356–369.

[Christoph Steitz] Christoph Steitz, E. A. German nuclear plant infected with computer viruses, operator says. `https://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS`. Accessed: 2020-12-09.

[30] Ciotti, M., Ciccozzi, M., Terrinoni, A., Jiang, W.-C., Wang, C.-B., and Bernardini, S. (2020). The covid-19 pandemic. *Critical reviews in clinical laboratory sciences*, 57(6):365–388.

[31] Cuer, R., Piétrac, L., Niel, E., Diallo, S., Minoiu-Enache, N., and Dang-Van-Nhan, C. (2018). A formal framework for the safe design of the autonomous driving supervision. *Reliability Engineering & System Safety*, 174:29–40.

[32] Dewri, R., Ray, I., Poolsappasit, N., and Whitley, D. (2012). Optimal security hardening on attack tree models of networks: a cost-benefit analysis. *International Journal of Information Security*, 11(3):167–188.

[33] Dingle, N. J., Knottenbelt, W. J., and Suto, T. (2009). Pipe2: a tool for the performance evaluation of generalised stochastic petri nets. *ACM SIGMETRICS Performance Evaluation Review*, 36(4):34–39.

[34] Dolev, S., Israeli, A., and Moran, S. (1997). Uniform dynamic self-stabilizing leader election. *IEEE Transactions on Parallel and Distributed Systems*, 8(4):424–440.

[35] Fabro, M., Gorski, E., and Spiers, N. (2016). Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies. *DHS Industrial Control Systems Cyber Emergency Response Team.*

[36] Feng, Y., Hu, B., Hao, H., Gao, Y., Li, Z., and Tan, J. (2018). Design of distributed cyber–physical systems for connected and automated vehicles with implementing methodologies. *IEEE Transactions on Industrial Informatics*, 14(9):4200–4211.

[37] Freris, N. M. et al. (2019). A software-defined architecture for control of iot cyberphysical systems. *Cluster Computing*, 22(4):1107–1122.

[38] Fu, G., Dawson, R., Khoury, M., and Bullock, S. (2014). Interdependent networks: vulnerability analysis and strategies to limit cascading failure. *The European Physical Journal B*, 87(7):1–10.

[39] Fu, R., Huang, X., Xue, Y., Wu, Y., Tang, Y., and Yue, D. (2018). Security assessment for cyber physical distribution power system under intrusion attacks. *IEEE Access*, 7:75615–75628.

[40] Gabriel, E., Fagg, G. E., Bosilca, G., Angskun, T., Dongarra, J. J., Squyres, J. M., Sahay, V., Kambadur, P., Barrett, B., Lumsdaine, A., et al. (2004). Open mpi: Goals, concept, and design of a next generation mpi implementation. In *European Parallel Virtual Machine/Message Passing Interface Users' Group Meeting*, pages 97–104. Springer.

[41] Gagniuc, P. A. (2017). *Markov chains: from theory to implementation and experimentation.* John Wiley & Sons.

[42] Ganesan, R., Raajini, X. M., Nayyar, A., Sanjeevikumar, P., Hossain, E., and Ertas, A. H. (2020). Bold: bio-inspired optimized leader election for multiple drones. *Sensors*, 20(11):3134.

[43] Garofalo, G., Giordano, A., Piro, P., Spezzano, G., and Vinci, A. (2017). A distributed real-time approach for mitigating cso and flooding in urban drainage systems. *Journal of Network and Computer Applications*, 78:30–42.

[44] Gaur, A., Scotney, B., Parr, G., and McClean, S. (2015). Smart city architecture and its applications based on iot. *Procedia computer science*, 52:1089–1094.

[45] Ghafoorian, M., Abbasinezhad-Mood, D., and Shakeri, H. (2018). A thorough trust and reputation based rbac model for secure data storage in the cloud. *IEEE Transactions on Parallel and Distributed Systems*, 30(4):778–788.

[46] Gharehchopogh, F. S. and Arjang, H. (2014). A survey and taxonomy of leader election algorithms in distributed systems. *Indian Journal of Science and Technology*, 7(6):815.

[47] Ghomi, E. J., Rahmani, A. M., and Qader, N. N. (2017). Load-balancing algorithms in cloud computing: A survey. *Journal of Network and Computer Applications*, 88:50–71.

[48] Gibbs, S. (2018). Triton: hackers take out safety systems in'watershed'attack on energy plant. *The Guardian*.

[49] Gokhale, S. S. and Trivedi, K. S. (2006). Analytical models for architecture-based software reliability prediction: A unification framework. *IEEE Transactions on reliability*, 55(4):578–590.

[50] Gómez, S., Arenas, A., Borge-Holthoefer, J., Meloni, S., and Moreno, Y. (2010). Discrete-time markov chain approach to contact-based disease spreading in complex networks. *EPL (Europhysics Letters)*, 89(3):38009.

[51] Goodloe, A. E. and Pike, L. (2010). *Monitoring distributed real-time systems: A survey and future directions*. National Aeronautics and Space Administration, Langley Research Center.

[52] Gouda, M. G. and McGuire, T. M. (1998). Accelerated heartbeat protocols. In *Proceedings. 18th International Conference on Distributed Computing Systems (Cat. No. 98CB36183)*, pages 202–209. IEEE.

[53] Gunes, V., Peter, S., Givargis, T., and Vahid, F. (2014). A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Transactions on Internet and Information Systems (TIIS)*, 8(12):4242–4268.

[54] Hanusz, Z. and Tarasińska, J. (2015). Normalization of the kolmogorov–smirnov and shapiro–wilk tests of normality. *Biometrical Letters*, 52(2):85–93.

[55] Harel, D. (1987). Statecharts: A visual formalism for complex systems. *Science of computer programming*, 8(3):231–274.

[56] Hasan, M., Islam, M. M., Zarif, M. I. I., and Hashem, M. (2019). Attack and anomaly detection in iot sensors in iot sites using machine learning approaches. *Internet of Things*, 7:100059.

[57] Hu, H., Ahn, G.-J., and Kulkarni, K. (2012). Detecting and resolving firewall policy anomalies. *IEEE Transactions on dependable and secure computing*, 9(3):318–331.

[58] Huang, L. and Zhu, Q. (2020). A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. *Computers & Security*, 89:101660.

[59] Islam, M. J., Mahin, M., Roy, S., Debnath, B. C., and Khatun, A. (2019). Distblacknet: A distributed secure black sdn-iot architecture with nfv implementation for smart cities. In *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, pages 1–6. IEEE.

[60] Ivanisenko, I. N. and Radivilova, T. A. (2015). Survey of major load balancing algorithms in distributed system. In *2015 information technologies in innovation business conference (ITIB)*, pages 89–92. IEEE.

[61] Jalali, R., El-Khatib, K., and McGregor, C. (2015). Smart city architecture for community level services through the internet of things. In *2015 18th International Conference on Intelligence in Next Generation Networks*, pages 108–113. IEEE.

[62] Jenkins, L. and Khincha, H. (1992). Deterministic and stochastic petri net models of protection schemes. *IEEE transactions on Power Delivery*, 7(1):84–90.

[63] Jiang, J.-R. (2018). An improved cyber-physical systems architecture for industry 4.0 smart factories. *Advances in Mechanical Engineering*, 10(6):1687814018784192.

[64] Johnstone, M. N. (2010). Threat modelling with stride and uml.

[65] Kanwal, S., Iqbal, Z., Irtaza, A., Ali, R., and Siddique, K. (2021). A genetic based leader election algorithm for iot cloud data processing. *CMC-COMPUTERS MATERIALS & CONTINUA*, 68(2):2469–2486.

[66] Kargl, F., Klenk, A., Schlott, S., and Weber, M. (2004). Advanced detection of selfish or malicious nodes in ad hoc networks. In *European workshop on security in Ad-hoc and sensor networks*, pages 152–165. Springer.

[67] Kathiravelu, P., Van Roy, P., and Veiga, L. (2019). Sd-cps: software-defined cyber-physical systems. taming the challenges of cps with workflows at the edge. *Cluster Computing*, 22(3):661–677.

[68] Keshtkarjahromi, Y. (2021). Method and system that determine malicious nodes in a distributed computation network. US Patent App. 17/069,077.

[69] Kiczales, G., Lamping, J., Mendhekar, A., Maeda, C., Lopes, C., Loingtier, J.-M., and Irwin, J. (1997). Aspect-oriented programming. In *European conference on object-oriented programming*, pages 220–242. Springer.

[70] Kleinmann, A. and Wool, A. (2017). Automatic construction of statechart-based anomaly detection models for multi-threaded industrial control systems. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 8(4):1–21.

[71] Kordy, B., Mauw, S., Radomirović, S., and Schweitzer, P. (2010). Foundations of attack–defense trees. In *International Workshop on Formal Aspects in Security and Trust*, pages 80–95. Springer.

[72] Kumar, V., Singh, L. K., and Tripathi, A. K. (2017). Transformation of deterministic models into state space models for safety analysis of safety critical systems: a case study of npp. *Annals of Nuclear Energy*, 105:133–143.

[73] Lamb, C. (2019). Advanced malware and nuclear power: Past present and future. Technical report, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

[74] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51.

[75] Lawal, B. H. and Nuray, A. (2018). Real-time detection and mitigation of distributed denial of service (ddos) attacks in software defined networking (sdn). In *2018 26th Signal Processing and Communications Applications Conference (SIU)*, pages 1–4. IEEE.

[76] Lawrence, J. D. (1993). Software reliability and safety in nuclear reactor protection systems. Technical report, Nuclear Regulatory Commission, Washington, DC (United States). Div. of . . . .

[77] Lee, J., Azamfar, M., and Singh, J. (2019). A blockchain enabled cyber-physical system architecture for industry 4.0 manufacturing systems. *Manufacturing letters*, 20:34–39.

[78] Lee, J., Bagheri, B., and Kao, H.-A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters*, 3:18–23.

[79] Lee, J.-Y., Woo, J.-S., and Rhee, S.-W. (1998). A transformed quantile-quantile plot for normal and bimodal distributions. *Journal of Information and Optimization Sciences*, 19(3):305–318.

[80] Leitão, P., Colombo, A. W., and Karnouskos, S. (2016). Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges. *Computers in industry*, 81:11–25.

[81] Levy, E. (2003). Crossover: online pests plaguing the off line world. *IEEE Security & Privacy*, 1(6):71–73.

[82] Liang, G., Weller, S. R., Zhao, J., Luo, F., and Dong, Z. Y. (2016). The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32(4):3317–3318.

[83] Lin, C.-L., Chen, J. K., and Ho, H.-H. (2021). Bim for smart hospital management during covid-19 using mcdm. *Sustainability*, 13(11):6181.

[84] Liu, A. X. and Gouda, M. G. (2008). Diverse firewall design. *IEEE Transactions on Parallel and Distributed Systems*, 19(9):1237–1251.

[85] Liu, J., Li, Y., Chen, M., Dong, W., and Jin, D. (2015). Software-defined internet of things for smart urban sensing. *IEEE communications magazine*, 53(9):55–63.

[86] Liu, J., Zhang, W., Ma, T., Tang, Z., Xie, Y., Gui, W., and Niyoyita, J. P. (2020). Toward security monitoring of industrial cyber-physical systems via hierarchically distributed intrusion detection. *Expert Systems with Applications*, 158:113578.

[87] Liu, X., Zhang, J., and Zhu, P. (2017a). Modeling cyber-physical attacks based on probabilistic colored petri nets and mixed-strategy game theory. *International Journal of Critical Infrastructure Protection*, 16:13–25.

[88] Liu, Y., Kuang, Y., Xiao, Y., and Xu, G. (2017b). Sdn-based data transfer security for internet of things. *IEEE Internet of Things Journal*, 5(1):257–268.

[89] Lodderstedt, T., Basin, D., and Doser, J. (2002). Secureuml: A uml-based modeling language for model-driven security. In *International Conference on the Unified Modeling Language*, pages 426–441. Springer.

[90] Madan, B. B., Goševa-Popstojanova, K., Vaidyanathan, K., and Trivedi, K. S. (2004). A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Performance Evaluation*, 56(1-4):167–186.

[91] Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, 2(2):109–134.

[92] Marashi, K., Sarvestani, S. S., and Hurson, A. R. (2017). Consideration of cyber-physical interdependencies in reliability modeling of smart grids. *IEEE Transactions on Sustainable Computing*, 3(2):73–83.

[93] Marrone, S., Nardone, R., Tedesco, A., D'Amore, P., Vittorini, V., Setola, R., De Cillis, F., and Mazzocca, N. (2013). Vulnerability modeling and analysis for critical infrastructure protection applications. *International Journal of Critical Infrastructure Protection*, 6(3-4):217–227.

[94] Maurya, A. K., Tripathi, D., Biswas, A., and Tripathi, A. K. (2018). Design issues in distributed software. In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pages 563–567. IEEE.

[95] Miller, B. and Rowe, D. (2012). A survey scada of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology*, pages 51–56.

[96] Mitchell, R. and Chen, R. (2015). Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems. *IEEE Transactions on Reliability*, 65(1):350–358.

[97] Mohan, P. (2020). Ensuring cyber security in india's nuclear systems.

[98] Molloy, M. K. (1982). Performance analysis using stochastic petri nets. *IEEE Transactions on computers*, (9):913–917.

[99] Moraitis, G., Nikolopoulos, D., Bouziotas, D., Lykou, A., Karavokiros, G., and Makropoulos, C. (2020). Quantifying failure for critical water infrastructures under cyber-physical threats. *Journal of Environmental Engineering*, 146(9):04020108.

[100] Moreno, J., Rosado, D. G., Sanchez, L. E., Serrano, M. A., and Fernandez-Medina, E. (2021). Security reference architecture for cyber-physical systems (cps). *Journal of Universal Computer Science*, 27(6):609–634.

[101] Mozafari, S. H. and Meyer, B. H. (2016). Efficient performance evaluation of multi-core simt processors with hot redundancy. *IEEE Transactions on Emerging Topics in Computing*, 6(4):498–510.

[102] Muñoz-González, L., Sgandurra, D., Barrère, M., and Lupu, E. C. (2017). Exact inference techniques for the analysis of bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 16(2):231–244.

[103] Murata, T. (1989). Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580.

[104] Murshed, M., Allen, A. R., et al. (2012). Enhanced bully algorithm for leader node election in synchronous distributed systems. *Computers*, 1(1):3–23.

[105] Nandi, A. K., Medal, H. R., and Vadlamani, S. (2016). Interdicting attack graphs to protect organizations from cyber attacks: A bi-level defender–attacker model. *Computers & Operations Research*, 75:118–131.

[106] Nicol, D. M., Sanders, W. H., and Trivedi, K. S. (2004). Model-based evaluation: from dependability to security. *IEEE Transactions on dependable and secure computing*, 1(1):48–65.

[107] Nourian, A. and Madnick, S. (2015). A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet. *IEEE Transactions on Dependable and Secure Computing*, 15(1):2–13.

[108] Orojloo, H. and Azgomi, M. A. (2017a). A game-theoretic approach to model and quantify the security of cyber-physical systems. *Computers in Industry*, 88:44–57.

[109] Orojloo, H. and Azgomi, M. A. (2017b). A method for evaluating the consequence propagation of security attacks in cyber–physical systems. *Future Generation Computer Systems*, 67:57–71.

[110] Pari, S. M. A., Noormohammadpour, M., Salehi, M. J., Khalaj, B. H., Bagheri, H., and Katz, M. (2013). A self-organizing approach to malicious detection in

leader-based mobile ad-hoc networks. In *2013 IFIP Wireless Days (WD)*, pages 1–3. IEEE.

[111] Parsamehr, R., Esfahani, A., Mantas, G., Radwan, A., Mumtaz, S., Rodriguez, J., and Martínez-Ortega, J.-F. (2019). A novel intrusion detection and prevention scheme for network coding-enabled mobile small cells. *IEEE Transactions on Computational Social Systems*, 6(6):1467–1477.

[112] Qin, L. and Xie, Y. (2021). Real-time monitoring system of exercise status based on internet of health things using safety architecture model. *IEEE Access*, 9:27333–27345.

[113] Rahman, M. U. (2019). Leader election in the internet of things: Challenges and opportunities. *arXiv preprint arXiv:1911.00759*.

[114] Ramos, G., Sanchez, J. L., Torres, A., and Rios, M. (2009). Power systems security evaluation using petri nets. *IEEE Transactions on Power Delivery*, 25(1):316–322.

[115] Rrushi, J., Farhangi, H., Howey, C., Carmichael, K., and Dabell, J. (2015). A quantitative evaluation of the target selection of havex ics malware plugin. In *Industrial Control System Security (ICSS) Workshop*.

[116] Şahin, S. and Gedik, B. (2018). C-stream: A co-routine-based elastic stream processing engine. *ACM Transactions on Parallel Computing (TOPC)*, 4(3):1–27.

[117] Saitta, P., Larcom, B., and Eddington, M. (2005). Trike v. 1 methodology document [draft]. *URL: http://dymaxion. org/trike/Trike v1 Methodology Documentdraft. pdf*.

[118] Santos, L., Gonçalves, R., Rabadao, C., and Martins, J. (2021). A flow-based intrusion detection framework for internet of things networks. *Cluster Computing*, pages 1–21.

[119] Satam, S., Satam, P., Pacheco, J., and Hariri, S. (2021). Security framework for smart cyber infrastructure. *Cluster Computing*, pages 1–12.

[120] Sengan, S., Subramaniyaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., and Ravi, L. (2020). Enhancing cyber-physical systems with hybrid smart city cyber security architecture for secure public data-smart network. *Future generation computer systems*, 112:724–737.

[121] Shang, W., Gong, T., Chen, C., Hou, J., and Zeng, P. (2019). Information security risk assessment method for ship control system based on fuzzy sets and attack trees. *Security and Communication Networks*, 2019.

[122] Sharma, B., Bhatia, R. S., and Singh, A. K. (2017). A logical structure based fault tolerant approach to handle leader election in mobile ad hoc networks. *Journal of King Saud University-Computer and Information Sciences*, 29(3):378–398.

[123] Sharma, S. and Singh, A. K. (2018). An election algorithm to ensure the high availability of leader in large mobile ad hoc networks. *International Journal of Parallel, Emergent and Distributed Systems*, 33(2):172–196.

[124] Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., and Woody, C. (2018). Threat modeling: a summary of available methods. Technical report, Carnegie Mellon University Software Engineering Institute Pittsburgh United . . . .

[125] Shin, J., Son, H., and Heo, G. (2017). Cyber security risk evaluation of a nuclear i&c using bn and et. *Nuclear Engineering and Technology*, 49(3):517–524.

[126] Singh, L., Rajput, H., Vinod, G., and Tripathi, A. K. (2016). Computing transition probability in markov chain for early prediction of software reliability. *Quality and Reliability Engineering International*, 32(3):1253–1263.

[127] Singh, L. K. and Rajput, H. (2017). Dependability analysis of safety critical real-time systems by using petri nets. *IEEE Transactions on Control Systems Technology*, 26(2):415–426.

[128] Singh, P. and Tripathi, A. K. (2012). Exploring problems and solutions in estimating testing effort for non functional requirement. *International Journal of Computers & Technology*, 3(2b):284–290.

[129] Souag, A., Salinesi, C., Mazo, R., and Comyn-Wattiau, I. (2015). A security ontology for security requirements elicitation. In *International symposium on engineering secure software and systems*, pages 157–177. Springer.

[130] Stroustrup, B. and Shopiro, J. E. (1984). *A set of C++ classes for co-routine style programming.* AT & T Bell Laboratories.

[131] Suleiman, H. and Svetinovic, D. (2013). Evaluating the effectiveness of the security quality requirements engineering (square) method: a case study using smart grid advanced metering infrastructure. *Requirements Engineering*, 18(3):251–279.

[132] Tao, M., Zuo, J., Liu, Z., Castiglione, A., and Palmieri, F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes. *Future Generation Computer Systems*, 78:1040–1051.

[133] Ten, C.-W., Liu, C.-C., and Manimaran, G. (2008). Vulnerability assessment of cybersecurity for scada systems. *IEEE Transactions on Power Systems*, 23(4):1836–1846.

[134] Tjoa, S., Jakoubi, S., Goluch, G., Kitzler, G., Goluch, S., and Quirchmayr, G. (2010). A formal approach enabling risk-aware business process modeling and simulation. *IEEE Transactions on Services Computing*, 4(2):153–166.

[135] Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., and Bilal, M. (2021). Smart home security: challenges, issues and solutions at different iot layers. *The Journal of Supercomputing*, 77(12):14053–14089.

[136] Tripathi, D., Biswas, A., Tripathi, A. K., Singh, L. K., and Chaturvedi, A. (2022). An integrated approach of designing functionality with security for distributed cyber-physical systems. *The Journal of Supercomputing*, pages 1–33.

[137] Tripathi, D., Maurya, A. K., Chaturvedi, A., and Tripathi, A. K. (2019). A study of security modeling techniques for smart systems. In *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, pages 87–92. IEEE.

[138] Tripathi, D., Singh, L. K., Tripathi, A. K., and Chaturvedi, A. (2021a). Model based security verification of cyber-physical system based on petrinet: A case study of nuclear power plant. *Annals of Nuclear Energy*, 159:108306.

[139] Tripathi, D., Tripathi, A. K., Singh, L. K., and Chaturvedi, A. (2021b). Towards analyzing the impact of intrusion prevention and response on cyber-physical system availability: A case study of npp. *Annals of Nuclear Energy*, page 108863.

[140] Trivedi, K. S. (2008). *Probability & statistics with reliability, queuing and computer science applications*. John Wiley & Sons.

[141] UcedaVelez, T. and Morana, M. M. (2015). *Risk Centric Threat Modeling: process for attack simulation and threat analysis*. John Wiley & Sons.

[142] Vandana, C. (2016). Security improvement in iot based on software defined networking (sdn). *International Journal of Science, Engineering and Technology Research (IJSETR)*, 5(1):2327–4662.

[143] Viega, J. and McGraw, G. (2011). *Building Secure Software: How to Avoid Security Problems the Right Way (paperback)(Addison-Wesley Professional Computing Series)*. Addison-Wesley Professional.

[144] Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., and Dehghantanha, A. (2020). Threats on the horizon: Understanding security threats in the era of cyber-physical systems. *The Journal of Supercomputing*, 76(4):2643–2664.

[145] Wang, J., Neil, M., and Fenton, N. (2020). A bayesian network approach for cybersecurity risk assessment implementing and extending the fair model. *Computers & Security*, 89:101659.

[146] Wu, Z., Li, G., Shen, S., Lian, X., Chen, E., and Xu, G. (2021). Constructing dummy query sequences to protect location privacy and query privacy in location-based services. *World Wide Web*, 24(1):25–49.

[147] Wu, Z., Li, R., Zhou, Z., Guo, J., Jiang, J., and Su, X. (2020a). A user sensitive subject protection approach for book search service. *Journal of the Association for Information Science and Technology*, 71(2):183–195.

[148] Wu, Z., Shen, S., Lian, X., Su, X., and Chen, E. (2020b). A dummy-based user privacy protection approach for text information retrieval. *Knowledge-Based Systems*, 195:105679.

[149] Xu, D. and Nygard, K. E. (2006). Threat-driven modeling and verification of secure software using aspect-oriented petri nets. *IEEE Transactions on Software Engineering*, 32(4):265–278.

[150] Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., and Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, 77:103201.

[151] Yang, Y., Xu, H.-Q., Gao, L., Yuan, Y.-B., McLaughlin, K., and Sezer, S. (2016). Multidimensional intrusion detection system for iec 61850-based scada networks. *IEEE Transactions on Power Delivery*, 32(2):1068–1078.

[152] Yuan, X., Nuakoh, E. B., Williams, I., and Yu, H. (2015). Developing abuse cases based on threat modeling and attack patterns. *JSw*, 10(4):491–498.

[153] Zetter, K. (2012). Meet 'flame,'the massive spy malware infiltrating iranian computers. *Wired Magazine*.

[154] Zhang, Y., Wang, L., Sun, W., Green II, R. C., and Alam, M. (2011). Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Transactions on Smart Grid*, 2(4):796–808.

[155] Zhioua, S. (2013). The middle east under malware attack dissecting cyber weapons. In *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops*, pages 11–16. IEEE.

[156] Zhou, C., Feng, Y., and Yin, Z. (2019). An algebraic complex event processing method for cyber-physical system. *Cluster Computing*, 22(6):15169–15177.

[157] Zhu, Q., Rieger, C., and Başar, T. (2011). A hierarchical security architecture for cyber-physical systems. In *2011 4th international symposium on resilient control systems*, pages 15–20. IEEE.

[158] Zurawski, R. and Zhou, M. (1994). Petri nets and industrial applications: A tutorial. *IEEE Transactions on industrial electronics*, 41(6):567–583.