International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 01 | January - 2023 Impact Factor: 7.185 ISSN: 2582-3930

Development of Cyber Security Mechanism to Detect Cyber Attacks on Cyber Physical Systems by Using Bayesian Belief Networks

D Suma, D Roopa, Pirangi Hymavathi, M Madhavi Latha, Dr. Mahesh Kotha

Assistant Professor, Department of CSE (AI/DS), Sri Indu College of Engineering and Technology, Hyderabad.
Assistant Professor, CSE Department, Sri Indu College of Engineering and Technology, Hyderabad.
Assistant Professor, CSE Department, Sri Indu College of Engineering and Technology, Hyderabad.
Assistant Professor, Princeton Institute of Engineering and Technology for Women, Hyderabad.
Associate professor, Department of CSE (AI&ML), CMR Technical Campus, Hyderabad.

Abstract: A cyber physical systems (CPS) is a complicated device that integrates sensing, computation, manipulate and networking into bodily methods and items over Internet. It performs a key function in cutting-edge enterprise because it connects bodily and cyber worlds. In order to fulfill ever-converting commercial requirements, its systems and capabilities are continuously improved. Identifying cyberattack vectors on cyber supply chains (CSC) withinside the occasion of cyber assaults are very vital in mitigating cybercrimes successfully on Cyber Physical Systems CPS. A ubiquitous hassle is the truth that cyber assaults can purpose full-size harm to commercial systems, and as a result has received growing interest from researchers and practitioners. However, withinside the cyber protection domain, the invincibility nature of cybercrimes makes it hard and hard to are expecting the chance opportunity and effect of cyber assaults. Although cybercrime phenomenon, risks, and treats include a number of unpredictability's, uncertainties and fuzziness, cyberattack detection have to be practical, methodical and affordable to be implemented. We discover Bayesian Belief Networks (BBN) as information illustration in synthetic intelligence which will be officially carried out probabilistic inference withinside the cyber protection domain. The goal of this paper is to apply Bayesian Belief Networks to hit upon cyberattacks on CSC withinside the CPS domain. We version cyberattacks the usage of DAG approach to decide the assault propagation. Further, we use a clever grid case observe to illustrate the applicability of assault and the cascading effects. The consequences display that BBN will be tailored to decide uncertainties withinside the occasion of cyberattacks withinside the CSC domain. In this paper, we gift a Bayesian community technique for mastering the causal family members among cyber and bodily variables in

addition to their temporal correlations from unlabeled information. We describe the information variations that we finished to cope with the heterogeneous traits of the cyber and bodily information, in order that the included dataset may be used to analyze the Bayesian community shape and parameters. We then gift scalable algorithms to hit upon special anomalies and isolate their respective root-purpose the usage of a Bayesian community. We additionally gift consequences from comparing our algorithms on an unlabeled dataset which include anomalies because of cyber assaults and bodily faults in a industrial constructing device.

Keywords: Cyber Physical System, Cyber Attacks, Cyber Supply Chain Threats, Bayesian Belief Network, Cybercrime.

I.INTRODUCTION

Cyber-physical systems (CPS) combine computing and communication capabilities with monitoring and control of entities in the physical world. CPS systems are part of many safety critical infrastructures and industrial control systems, such as electric power grids and building automation systems. Traditional approaches for protecting control systems have primarily focused on gradual deterioration or abrupt faults in physical components. However, the coupling between information and communication technologies and the physical controllers in a CPS system makes the control system more vulnerable, especially since networked systems make it possible to launch remote attacks. Hence, there is a growing need for protecting control systems against malicious cyber attacks. As part of cyber-security mechanisms, several authentication and access control technologies have been developed for protecting information. These technologies can also be used to prevent attacks in cyber-physical control systems to some extent. However, in addition, a resilient CPS architecture needs to include mechanisms for detecting and reacting to anomalies.

The aim of this paper is to use Bayesian Belief Networks to detect cyberattacks on CSC in the CPS domain. The novelty contribution is to improve CSC security. To achieve that we model cyberattacks using DAG method to determine the attack propagation. Further, we use a smart grid case study to demonstrate the applicability of attacks and cascading effects. The results show that BBN could be adapted to determine uncertainties in the event of cyberattack in the CSC domain.

With the development of supporting technologies such as sensing devices, Cloud, and IoT Technology, the Age of the internet has empowered the physical universe (such as sensing devices in diagnostic instruments, agriculture, and other fields) to link with cybersecurity [1]. The state-of-the-art IoT technology had already emerged as a consequence of a tremendous amount of time and effort injected into IoT, as well as various de facto standards exist on the bundle for implementation. Industry 4.0 integrated combined Connected devices, business networks, and industrial automation architecture inside the business with the introduction of Connected devices Commonly used terms have become sentient and communicative due to the IoT. Any technology that involves interaction amongst network components has always had a network infrastructure as just an integrated element.

II.LITERATURE SURVEY

With the rapid development of modern industry, demands for CPS integration are growing to make up for shortcomings among networks, technologies, tools, and devices. The integration of systems and technologies in CPS tends to be complex and diverse, making it a compatible and open system, which unfortunately provides a platform for adversaries to exploit CPS and results in numerous security issues. One of the most ubiquitous problems is cyber attacks, which can degrade system performance, or even cause catastrophic consequences. An example of a vicious event was the attack on Ukrainian power grids. The power grid is a typical CPS that consists of a power plant, transmission and distribution stations, consumers, control centers, and communication networks. Different components are monitored and connected by sensors and networks respectively, to guarantee a healthy system status. The Ukrainian power system contained a lot of open-source information in 2015, which provided an opportunity for attackers. First, a phishing email spread across networks to introduce a Black Energy malware. It allowed attackers to gain confidential data and critical system information. Such actions enabled access to control centers and shutdown of substations remotely. Then, another piece of malware was activated to destroy critical files and

prevent the system from rebooting. Finally, a denial-of-service (DoS) attack was launched on call centers to deny consumers access to the latest information on blackout. Nearly 225 000 consumers suffered from this power outage for 1 to 6 hours. Another example is that many healthcare organizations were threatened by cyber attacks during the coronavirus disease 2019 (COVID-19), where attackers attempted to steal research data related to COVID-19 and cause chaos in the hospitals to gain revenue. For instance, a Czech hospital shut down its network due to a cyber attack in March 2020, which greatly impacted diagnosis of COVID-19 and patient

care [8]. Important attack events are given in Table I, each of which has caused significant damage to global industry. Therefore, there is a growing interest in cyber attacks on CPSs.

Security of CPSs is guaranteed by three features, i.e., availability, integrity, and confidentiality. Availability guarantees that the system is available whenever needed, i.e., every component of the system works correctly at all times. Integrity prevents data or signals in sensors, controllers and electronic devices from being altered by unauthorized parties. Confidentiality ensures security and personal privacy, i.e., key data and information can only be accessed by authorized parties [9]. Once one of these features is lost, the system is at risk of security problems. Hence, these three features are commonly used to determine if a system is secure. They form a security criterion, namely, any security deployment must ensure the availability, integrity and confidentiality of a system. On the other hand, they become targets of cyber criminals.

Attackers often work to compromise them to degrade system security, especially availability and integrity. On the basis of the intentions of attackers, cyber attacks on CPS can be divided into three classes, namely, availability, integrity and confidentiality ones. The availability attack is the most common cyber attack. Its objective is to block the communication network by making data and information unavailable. Typical availability attacks include DoS, distributed DoS and jamming ones. an integrity attack can occur on sensors, actuators, communication networks, and computing and control centers as data and control commands can be falsified under such an attack. There are many types of integrity attacks, e.g., false data injection attacks, middlemen, sparse and replay attacks. Confidentiality attacks may occur at any part of a system since any system information may be targeted by an attacker. Attack methods include eavesdropping, and the combination of DoS and integrity attacks.

Recently, many efforts have been made on dealing with cyber attacks in CPS based on system control theory, since a CPS can be considered as a physical system that is controlled by industrial control technologies. Based on system control theory, researchers study cyber attacks in two ways, i.e., attack and defense strategies. The former is to find the weaknesses of CPS and to propose possible attack strategies, while the latter is to design detection or control methods to defend attacks. Some surveys have outlined the recent work from the perspective of system control [10]. Table II shows their coverage in terms of: 1) attack types; 2) system models; 3) attack strategies; 4) defense strategies, and provides the main focus of them. It is clear that none of the existing surveys covers all the aspects indicated in the table, while they are important since they indicate attacks and

methodologies in recent work. For the purpose of identifying current concerns, technologies, bottlenecks and future research, this paper provides a survey for cyber attacks on CPS that covers all the issues in Table II. More specifically, we review recent advances on availability, integrity and confidentiality attacks. In particular, attack and defense strategies for CPS availability and integrity are discussed based on time-driven and event-driven system models. Some challenges and open issues are summarized according to the survey.

Year	Country/Institution	Details
2010	Iran	Stuxnet attack destroying core controllers of industries
2015	Ukraine	BlackEnergy attack on power grid, leading to massive power outage
2017	Russia, Ukraine, India, China	WannaCry attack aiming to encrypt data and demand ransom payments
2020	Brno University Hospital, Czech Republic	A cyber attack that shut down IT network of a Czech hospital
2020	US Dept. Health & Human Services	Unspecified attack on servers
2021	Colonial Pipeline, US	A ransomware attack on a US fuel pipeline, leading to shutdown of a critical fuel network

Table I: Typical Cyber Attack Events From Years 2010 to Present

(DT: Discrete-time system; CS: Continuous-time system)

Target	Model type	Attack type	Methodologies	Advantages	Disadvantages
Multi-area power system	CS	DoS	ET transmission,load frequency control	Improving the transaction efficiency	Limited attack duration time
CPS	CS	Asynchronous DoS	ET sampling and transmission	Handling system disturbance and measurement noise	Constraints on DoS frequency and duration
NCS	CS	Periodic DoS	Observer-based ET transmission	Preserving good control performance	A uniform lower bound for the attack sleeping period
Networked system	CS	Non-periodic DoS	ET transmission,H_∞ filtering	Achieving good filter performance and reducing unnecessary resource consumption	Known sleeping and active intervals of DoS attacks
Uncertain NCS	CS	PWM DoS	ET transmission	Handling system parameter uncertainties	Full state information
Stochastic NCS	CS	Non-periodic DoS	Observer-based ET framework	Preserving stability with a L_2-gain performance level	Constraints on DoS frequency and duration
Stochastic NCS	DT	Bernoulli distributed DoS	ET sampling	Handling active, consecutive packets dropout	Specified attack location
Nonlinear NCS	CS	Periodic DoS	ET transmission	Handling fault-prone systems	A uniform lower bound for the attack sleeping period
NCS	CS	DoS	Dynamic observer-based control	Handling general DoS attacks	Constraints on DoS frequency and duration
NCS	CS	Stochastic DoS	Markov process	Constructing stability and stabilization criterion	Sufficient knowledge on DoS attack
CPS	CS	DoS	Multi-transmission	Reducing the probability of being attacked	Full state information
NCS	CS	DoS	Sampled-data model	Handling random and periodic DoS attacks	Limited attack duration time
DT partially observed system	DT	Markov modulated DoS	Markov process	Optimal risk-sensitive control	Many assumptions
CPS	CS	Mode-switching DoS	k-connected graph, extended Laplacian matrix	A more general attack model	Negative effects on the system

Table II: Summary of Recent Defense Work on DoS Attack

The major contribution of this literature work is:

- This study gathers various research papers on cyber-physical systems security described in depth.
- Each of the collected research works has been analyzed in different aspects like application, type of attacks, datasets collected, and techniques used for attack detection.
- The performance of the research papers is identified and it is tabulated.
- The recent research gaps identified in cyber security in cyber-physical systems are addressed, and this will be a milestone for future researchers.

III.RETALTED WORK

CPS systems, notwithstanding their obvious advantages, remain vulnerable to a variety of cyberspace and/or physical security risks, assaults, as well as obstacles. Their diverse character, dependence on sensitive and private data, and large-scale implementation all contribute to something like this. As a consequence, purposeful or unintentional breaches of the technologies might have disastrous consequences, necessitating the implementation of strong security precautions. This, nevertheless, might result in unacceptably high network overhead, significantly in relation of delay [6]. Continuous software, program, and operating system upgrades also should help to reduce zero-day flaws.

CPSs have a variety of major weaknesses where cyber-physical attack vulnerability penetrates, resulting in security vulnerabilities to controlling networks' dependability and robustness [4]. In today's environment, as the number of devices targeted during information flow grows, cyber-physical security system requires extra work [5]. CPS cybersecurity faces issues like trustworthiness, authenticity, validity, and confidentiality. As a result of the potential for cyber assaults, the system's ability to supply services is jeopardized, and security constraints play a significant role.

i. ***Confidentiality:*** A condition of confidentiality is obtained in CPS under various attacks by a system that is capable of detecting prevented users or intruders [6].

ii. Integrity: Information travelling from the local record system to a data center over the network may be tampered with as a result of a cyber assault. While information goes across numerous hardware devices, the integrity of CPS may be maintained by using a robust firewall mechanism to prevent unauthorized users or intruders [7].

iii. Availability: CPSs are highly structured sophisticated power systems that provide nonstop services to their clients and have mechanisms in place to prevent power outages. The Markov mechanism [8] presents a multi-cyber architecture to improve the availability of CPS.

iv. Dependability: CPS reliability is critical for the correct operation of the CPS environment. When examining the impact of unauthorized users, the reliability of such systems is critical.

v. A Stochastic Petri nets technique to monitoring services delivered by sensors and actuators during procedure execution may be used to assess the likelihood of CPS [9].

vi. Robustness: The accessibility of CPS to a particular stage allows appropriate operation of the entire system, which determines the level of robustness. Mathis proposes a rule-based resilience mechanism in terms of CPS durability for incorrectly entered parameters [3].

vii. Reliable: The reliability of such devices is determined by system tasks that correctly react to service under environmental and operational circumstances specified by the system controller or programmer, or over a certain time frame [1].

In 2015, Vellaithurai et al. [1] developed a security-oriented probabilistic risk assessment approach referred to as CPINDEX for “cyber-physical security indices” towards assessing the underlying cyber-physical environment's security posture. On a particular host machine, CPINDEX deploys necessary cyber-side monitoring devices to proactively record and characterize low-level system operations including inter-process interactions across operational system assets. CPINDEX develops “stochastic Bayesian network models”

integrity of the entire cyber-physical architecture using the produced records as well as geometric data about the electricity supply design, and updates them continuously depending on the latest condition of the underpinning electricity system.

In 2018, Bernieri et al. [2] introduced a modular approach for industrial control systems to provide cyber-physical security. The Deep Detection Architecture (DDA) was developed to bridge the barrier between computer science and control theory. Furthermore, as a baseline for validation, they provided a new cyber-physical simulation technique.

In 2017, Haller et al. [3] presented an approach to developing intrusion detection systems (IDS) in cyber and physical systems. The method uses a three-phase design technique that includes risk assessment, cross-association, and optimum IDS architecture to cut the volume of monitored data. Phase 1 employs sensitivity analysis in order to identify sensitive parameters to intervention programs (e.g., control signals and cyber-attacks), phase 2 employs cross-association evaluation to ideally construct the processing parameters in clusters that are the most sympathetic to organizations of initiatives, and phase 3 consists of assigning the most vulnerable processing parameters to IDS while attempting to enforce the IDS inherent limitations as well as availability prerequisites.

In 2017, Bezemskij et al. [4] developed a Bayesian Networks-based technique for determining how an automatic car is now under threat, and whether the assault occurred in the cyber or materialistic worldview.

Investigations with command injection, malicious nodes, and electromagnetic resonance assaults have shown that the method is effective. In 2021, Xiao et al. [5] have developed a “software-defined network paradigm” into CPS design to simplify CPS administration and find a resolution to networking cyber security threats. The suggested method is evaluated by employing the constructed information as well as the NSL-KDD dataset's 7 features set. It has also been proven to be successful, with accuracy rates of 99.4% and 75.44%, respectively.

In 2017, Heussen et al. [6] developed a novel work based on the cyber-physical intrusion detection mechanism, and it is based on field data. This demonstrates how to identify distinctive responding patterns or how to keep the characterization up-to-date. Furthermore, as a component of a cyber-physical invasion security mechanism,

researchers suggest a way to use this behaviors patterns characterization to identify abnormal and possibly hazardous activity alterations.

In this paper, we propose an anomaly detection method that relies on a probabilistic graphical model of the underlying CPS. Specifically, we use a Bayesian network to characterize a CPS under nominal operation. This approach follows an unsupervised generative modeling concept where the model learns the individual characteristics of subcomponents (sensors/actuators) and the causal relationships among them under nominal condition, from a dataset. Then during regular operation, if a fault occurs in the system, it manifests itself as a low probability or anomalous event. Given an anomalous condition, further analysis can be performed to isolate which individual characteristics or causal relationship has changed to cause the anomaly. This provides a mechanism to perform root-cause analysis without using explicitly labeled training datasets for different faults. Thus, this approach potentially has good coverage, such that a single model can be leveraged for the detection and root cause isolation of multiple types of faults (even those that are previously unknown) in a CPS.

IV.CYBER SECURITY ANALYSIS USING BAYESIAN NETWORKS

Graphical security models are useful for visually representing and analyzing vulnerabilities in a system. Threat trees and Bayesian networks are two of the well-known graphical formalisms for security modeling [7]. Bayesian networks are versatile in that they can be constructed from attack models and domain knowledge, or learned from data. Attack graphs model how multiple vulnerabilities can be combined to result in an attack. Bayesian attack graphs combine attack graphs with computational procedures of Bayesian networks [8]. Wang et al. propose a probabilistic security metric for nodes in an attack graph and provide an algorithm for computing this metric in an attack graph [9]. Frigault et al. [10] provide a method to assign conditional probability to nodes in a Bayesian attack graph based on Common Vulnerability Scoring System scores (CVSS) and use that to calculate security metrics. They later extend their work to dynamic Bayesian networks to account for the evolving nature of vulnerabilities and availability of software patches [11]. Likewise, Houmb et al. quantify security risk level from CVSS estimates of frequency and impact using Bayesian networks [12].

A Bayesian network modeling approach for separating different sources of uncertainty, such as uncertainty in attacker actions and attack success, for real-time security analysis is described in [13]. Feng and Xie provide an algorithm for merging expert knowledge and information stored in databases into a single Bayesian network

[14]. PGMs have also been successfully used for root-cause analysis in different domains. For instance, Bayesian networks have been used for fault isolation in electrical power system [15], automotive systems [6], telecommunication networks [7] and manufacturing processes [8]. While the references cited above illustrate the use of graphical models for security analysis in different domains, we are not aware of any previous work that has developed Bayesian network models for anomaly detection and root-cause analysis in a cyber physical system based on unlabeled data. We first formulate the challenge problem in the following section and then describe our technical approach to solve the problem.

V.CYBER ATTACK MECHANISMS AND PHYSICAL FAULTS

The networked building system described above is vulnerable to different types of attacks, since the BacNet protocol currently does not provide strong authentication mechanisms. An adversary may launch data integrity attacks remotely by sending erroneous sensor measurements and estimates or by setting incorrect actuator values. Such data integrity attacks affect the operational goals of the building system and render the information untrustworthy. A confidentiality attack results in unauthorized users gaining access to information about the physical parameters. A denial-of-service (DoS) attack can be launched by flooding the communication channels of the building system.

In this work, we primarily focus on data integrity attacks that are launched from BacNet. We capture the BacNet traffic to the building sensors and actuators using Wireshark, which is a network sniffer. The network logs indicate which values were queried or written. The physical faults in a building HVAC system can occur in the form of malfunctioning actuators, e.g., leaky water valves and stuck air dampers. Such physical anomalies are induced through electronic actuator override mechanisms for this current study.

VI.METHODOLOGY

We now layout the process for anomaly detection and root cause isolation, which begins with learning a Bayesian Network from a given training set that contains data from nominal operation

of the CPS system. The resulting Bayesian network characterizes the normal operation and hence, is capable of detecting anomalies as low probability events. The same Bayesian network also enables isolation of the root-cause of the detected anomaly. In the following sections we describe the aforementioned steps in greater detail.

Learning Bayesian Networks

In addition to aligning the time of the cyber events to the physical state, as discussed in the previous section, we also discretized the continuous variables. This data transformation is needed, because our learning process is based on discrete Bayesian networks. To this end, we used the discretization policy proposed in [20], that automatically determines the optimal number of bins and their widths, given the multivariate distribution of the variables. After discretizing that data, we learned a network structure (Directed Acyclic Graph) that maximizes the likelihood of observing the training data. As mentioned earlier, finding such a DAG is an NP-hard problem, hence we used efficient

heuristics to approximate the underlying structure. It is important to penalize dense structures as they typically lead to overparameterization and hence, over-fitting (bias-variance tradeoff). To address this tradeoff, we track the Bayesian Information Criterion (BIC) to drive our search for the best DAG. Figure 1 shows the Bayesian Network structure that was learned with the help of the GeNIe tool [2], using the building dataset that was described in the previous section. The thickness of an edge between a pair of nodes reflects the degree of statistical dependency between those nodes. For example Act2 has a very strong impact on Sense2. Hence, in Figure 1, we see that the edge connecting the two nodes is very thick. It should be noted that learning the parameters (conditional probability tables) is done as part of the structure learning process and need not be carried out separately.

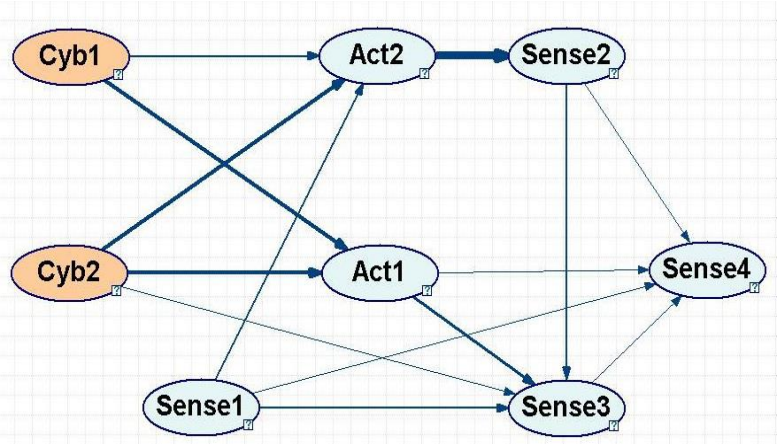

Figure 2. Bayesian Network Structure Based on The Building CPS Dataset

VII. PROPOSED APPROACH

Expert opinions provide us the mixed method approach of a positivist and interpretative research philosophy in a subjective manner. Ref [16]. The interpretive approach provides understand the human thought and actions in a social and organizational context. Ref [7] posit that interpretive approaches provide a greater scope to address issues of influence and impact. We integrate subjective expert judgments and Bayesian Belief Network (BBN) for detecting CSC attacks. This section provides an overview of Bayesian Belief Network (BBN) and subjective expert judgment.

Subjective Interpretation has the potential to produce deep insight into the cybersecurity phenomenon including the management of CSC systems development and security. The heterogeneous nature of CPS among components and its interoperability within the mechanisms itself results in a lack of understanding of cyber threats. We model the uncertainties involve in cyberattack using conditional probability distribution which maps with the expert opinion.

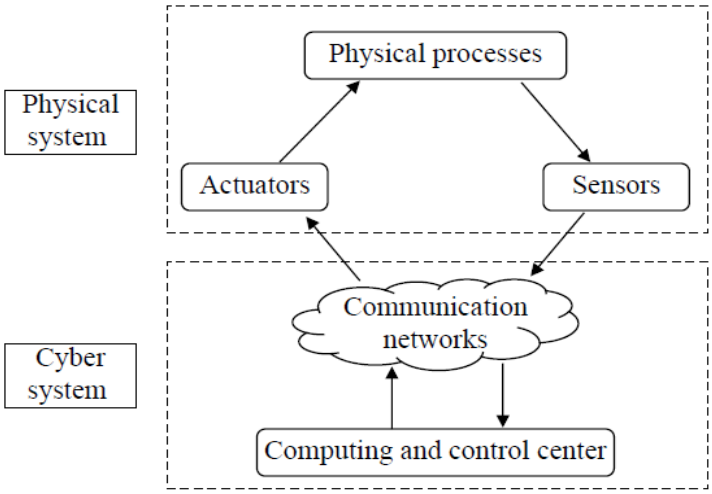

Fig. 2. An architecture of a CPS.

A CPS consists of a physical system and a cyber system. It results from an integration of physical processing, sensing, computation, communication and control [7]. Its general architecture is shown in Fig. 1. The physical system consists of physical processes, sensors and actuators. The cyber system includes communication

networks, computing and control centers. Physical processes are usually considered as a plant that is controlled by a cyber system. As for other components, they have the following functions:

1) Sensors: They are used for real-time data acquisition.

2) Actuator: Control commands are executed by corresponding actuators to realize desired physical actions.

3) Computing and control center: It is responsible for receiving data measured by sensors. By analyzing the received data, corresponding control decisions are made by the control center to ensure that physical processes are performed correctly.

4) Communication network: It provides a communication platform for the control center and physical system. To be precise, measurements obtained by sensors are transmitted over the communication network to the control center. Control signals or decisions are transmitted from the control center to actuators by the communication network.

BBN is a mathematical model that depicts the interrelationship of several events by defining the conditional probability between events. BBM is presented as a direct acyclic graph (DAG) together with an associated set of probability tables [14]. The concepts include how to describe and represent the relationship in the presences of uncertainties as well as how to manipulate such knowledge to make inferences. The DAG graphs consist of two portions: nodes representing the variables and arcs representing the causal/relevance dependencies between these variables. The nodes are of variable types, i.e. parent or observable, target and intermediate nodes are denoted as stochastic (randomly changing over time) or decision variables where multiple variables are often used to determine the state of each node. Each state of the individual node is expressed using probability density functions [15]. Probability density specifies the confidence in various outcomes of a set of variables connected to a node and depends conditionally on the status of the parent nodes at the incoming edges. For instance. The Figure below depicts concepts of cybercrime and the types of attack and causal but in between the attack and causals remains the uncertainties that exist due to lack of expert knowledge and attack modeling concepts.

VIII. CONCLUSION

The invincibility nature of cyberattacks and cybercrimes on CSC system and the heterogeneous nature of CPS systems generate a lot of uncertainties in predicting supply chain attacks, risks, and impacts. The uncertainties involve a lot of factors including lack of understanding of cyber threat intelligence and the attack life cycle such as attack pattern, attack prerequisites, attack vectors, TTP and threat modeling. Other factors include the inabilities to align organization goal, assets, requirements and business process to the cyber threat intelligence for strategic management understanding and accurate security controls. We have modeled cyberattack using BBN in the AI domain to provide a base to understand CSC threats and causalities relative to the uncertainties. Similarly, the difficulty is due to the evolving nature of cybercrimes, cyber threat landscape, and evolving organizational landscapes. Therefore, subjective judgment supports attack modeling, threat indicators, information sharing, and supply chain security controls. We have used a case
study to model threat probabilities using BBN node to determine the likelihood of an attack and its cascading impact. Further, the study will include using Machine Learning and CTI approach to model CSC attacks.

IX.REFERENCES

[1]. A. Yeboah-Ofori, and S. Islam. “Cyber Security Threat Modeling for Supply Chain Organizational Environments”. Future Internet, 2019. 11, 63, doi: 10.3390/611030063.

[2]. Controller and Audit General. “Investigation: Wanna Cry Cyberattack and the NHS.” National Audit Office. 2017. UK.

[3]. B. Woods, and A. Bochman, “Supply Chain in the Software Era” Atlantic Council, 2018, Washington, DC, USA.

[4] Ravindra Changala, “Evaluation and Analysis of Discovered Patterns Using Pattern Classification Methods in Text Mining” ,in ARPN Journal of Engineering and Applied Sciences, Volume 13, Issue 11, Pages 3706-3717 with ISSN:1819-6608 in June 2018.

[5] Y. Zhang, M. K. Qiu, C. W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data," IEEE Syst. J., vol. 11, no. 1, pp. 88–95, Mar. 2017.

[6] Y. Liu, Y. Peng, B. L. Wang, S. R. Yao, and Z. H. Liu, "Review on cyber-physical systems," IEEE/CAA J. Autom. Sinica, vol. 4, no. 1, pp. 27–40, Jan. 2017.

[7] A. Rashidinejad, B. Wetzels, M. Reniers, L. Y. Lin, Y. T. Zhu, and R. Su, "Supervisory control of discrete-event systems under attacks: An overview and outlook," in Proc. 18th European Control Conf., Naples, Italy, 2019, pp. 1732−1739.

[8]. A. Yeboah-Ofori, J. D. Abduli, F. Katsriku. "Cybercrime and Risks for Cyber Physical Systems" International Journal of Cyber Security and Digital Forensics. 2019.

[9]. W. Wang, and Z. Lu, "Cyber Security in Smart Grid: Survey and Challenges" Elsevier. Computer Networks, Vol 5, 2013. Issue 5, Pages 1344-1371, doi.org/10.1016/j.comnet.2012.12.017.

[10]. C, Sun, A. Hahn and C. Liu, "Cyber Security of a Power Grid: State of the Art." Elsevier. Electrical Power and Energy System. 2018. 99. 45-56. doi.org/10.1016/j.ijepes.2017.12.020

[11] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," Neurocomputing, vol. 338, pp. 101–115, Apr. 2019.

[12] Y. Lu, "Cyber physical system (CPS)-based industry 4.0: A survey," J.Ind. Int. Manage., vol. 2, no. 3, p. 1750014, Sep. 2017. DOI:10.1142/S2424862217500142.

[13] Ravindra Changala, "Object Tracking in Wireless Sensor networks using Data mining Techniques", in IOSR Journal of Electrical and Electronics Engineering, 2015.

[14] Ravindra Changala, "A Survey on Development of Pattern Evolving Model for Discovery of Patterns in Text Mining Using Data Mining Techniques" in Journal of Theoretical and Applied Information Technology, 31st August 2017. Vol.95. No.16, ISSN: 1817-3195, pp.3974-3987.

[15] G. Franze, G. Fortino, X. H. Cao, G. M. L. Sarne, and Z. Song, "Resilient control in large-scale networked cyber-physical systems: Guest editorial," IEEE/CAA J. Autom. Sinica, vol. 7, no. 5, pp. 1201-1203, Sept. 2020.

[16] S. Karnouskos, "Cyber-physical systems in the SmartGrid," in Proc. 9th IEEE Int. Conf. Industrial Informatics, Lisbon, Portugal, 2011, pp. 20–23.

[17] D. R. Ding, Q. L. Han, Y. Xiang, X. H. Ge, and X. M. Zhang, "A survey on security control and attack detection for industrial cyberphysical systems," Neurocomputing, vol. 275, pp. 1674–1683, 2018.

[18] Ravindra Changala, "Statistical Models in Data Mining: A Bayesian Classification" in International Journal of Recent Trends in Engineering & Research (IJRTER), volume 3, issue 1, pp.290-293. in 2017.

[19] J. Giraldo, D. Urbina, A. Cardenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physicsbased attack detection in cyber-physical systems," ACM Comput. Surv., vol. 51, no. 4, pp. 1–36, Jul. 2018.