J Grid Computing (2020) 18:863–878
https://doi.org/10.1007/s10723-020-09528-w

Vulnerability Modelling for Hybrid Industrial Control System Networks

Attiq Ur-Rehman · Iqbal Gondal · Joarder Kamruzzaman · Alireza Jolfaei

Received: 3 February 2020 / Accepted: 19 June 2020 / Published online: 4 July 2020

Abstract With the emergence of internet-based devices, the traditional industrial control system (ICS) networks have evolved to co-exist with the conventional IT and internet enabled IoT networks, hence facing various security challenges. The IT industry around the world has widely adopted the common vulnerability scoring system (CVSS) as an industry standard to numerically evaluate the vulnerabilities in software systems. This mathematical score of vulnerabilities is combined with environmental knowledge to determine the vulnerable nodes and attack paths. IoT and ICS systems have unique dynamics and specific functionality as compared to traditional computer networks, and therefore, the legacy cyber security models would not fit these advanced networks. In this paper, we studied the CVSS v3.1 framework's application to ICS embedded networks and an improved vulnerability framework, named $CVSS_{IoT\text{-}ICS}$, is proposed. $CVSS_{IoT\text{-}ICS}$ and CVSS v3.1 are applied to a realistic supply chain hybrid network which consists of IT, IoT, and ICS nodes. This hybrid network is assigned with actual vulnerabilities listed in the national vulnerability database (NVD). The comparison results confirm the effectiveness of $CVSS_{IoT\text{-}ICS}$ framework as it is equally applicable to all nodes of a hybrid network and evaluates the vulnerabilities based on the distinct features of each node type.

Keywords Industrial control system · Internet of things (IoT) · Supply chain · Security · Vulnerability modelling

1 Introduction

Industrial control systems (ICS) are the integral part of modern industries. ICS are integrated with all types of industries like power generation systems, water supply, oil and gas, advanced manufacturing, medical equipment, aviation, smart devices, etc. Industrial control systems are evolving from thousands of years. Ctesibius's water clock is considered as one of the oldest control systems invented in Alexandria, Egypt [1]. Control systems have evolved a lot since then and have several classifications like distributed systems, supervisory control and data acquisition systems (SCADA), manufacturing execution and programmable logic systems [2]. In recent years, industries are integrating legacy control systems with enterprise information networks, especially with the internet enabled devices

A. Ur-Rehman · I. Gondal · J. Kamruzzaman
Internet Commerce Security Lab; (ICSL), Federation University Mount Helen VIC, Mount Helen, VIC, Australia

A. Ur-Rehman
e-mail: attiqur-rehman@students.federation.edu.au

I. Gondal
e-mail: Iqbal.Gondal@federation.edu.au

J. Kamruzzaman
e-mail: joarder.kamruzzaman@federation.edu.au

A. Jolfaei (✉)
Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: alireza.jolfaei@mq.edu.au

(IoT) for improved productivity, safety, real time visibility and reliable operations. But along with these benefits, it has also attracted the typical cyber security threats into the ICS space. This integration has opened the door to remotely control the ICS and exploit its vulnerabilities [3], [41–44].

Due to the typical culture of hiding the weaknesses by industrial organizations, most of ICS security challenges and attacks are not publicly reported [4]. But as per available information, in the past few years, ICS vulnerability is growing. As listed in the national vulnerability database (NVD) and other vulnerability databases, only 19 vulnerabilities were reported in 2010 while 189 were reported in 2015. CVSS has scored 92, out of these 189 vulnerabilities, as critical whereas 79 are marked as medium [5].

Common vulnerability scoring system (CVSS) is one of the most comprehensive and widely used vulnerability scoring system [6]. CVSS was first introduced in 2005 with the goal of assigning universally acceptable severity to software and computer vulnerabilities. After having the industry feedback, version 2 was released in 2007 represented as CVSS v2. Based on the further adjustments, CVSS V3 was released in 2015. The most recent version of CVSS was released in 2019 with minor adjustments and marked as CVSS V3.1 [7]. CVSS framework assigns severity ranking to vulnerabilities ranging from 0 to 10; where 0 is the least severe and 10 is the most severe score. CVSS consists of three metric groups called Base, Temporal and Environmental metrics as shown in Fig. 1. Usually, system administrators only refer to the base metric score for accessing the vulnerability impact.

Base Metrics measure attacker accessibility, attack complexity, privileges and preconditions required for an attack and its accomplishment. It also assesses the scope and gage of a given vulnerability and its impression on integrity, confidentially and availability.

Temporal Metrics assess the changes to vulnerability, patch and fix availability that grows over the passage of the time.

Environmental Metrics re-evaluate the vulnerabilities using organizational environmental factors and priorities.

Based on the CVSS score, this framework helps security administrators to drive their mitigation strategy and allocate resources according to the severity level. The Internet Security Threat Report (ISTR), published by Symantec security and endorsed by Cisco, has listed 'phishing' as the most used attack in 2017 and 2018. This is mainly the result of the ICS integration with internet faced corporate networks [8].

Though the above reports suggested the increase in vulnerability in the ICS space, their scorings are widely criticized by ICS security specialists due to the fact the vulnerability tools used to evaluate the ICS system are not appropriate for the ICS systems. These tools were designed basically for IT computer networks and do not best fit due to the unique characters of the ICS system [9]. Traditional computer networks are usually connected with multiuse devices, have decent processing power and storage facilities. These networks are equipped with security protocols and protected with sophisticated encryption and intrusion detection systems, whereas the industrial control system networks were originally

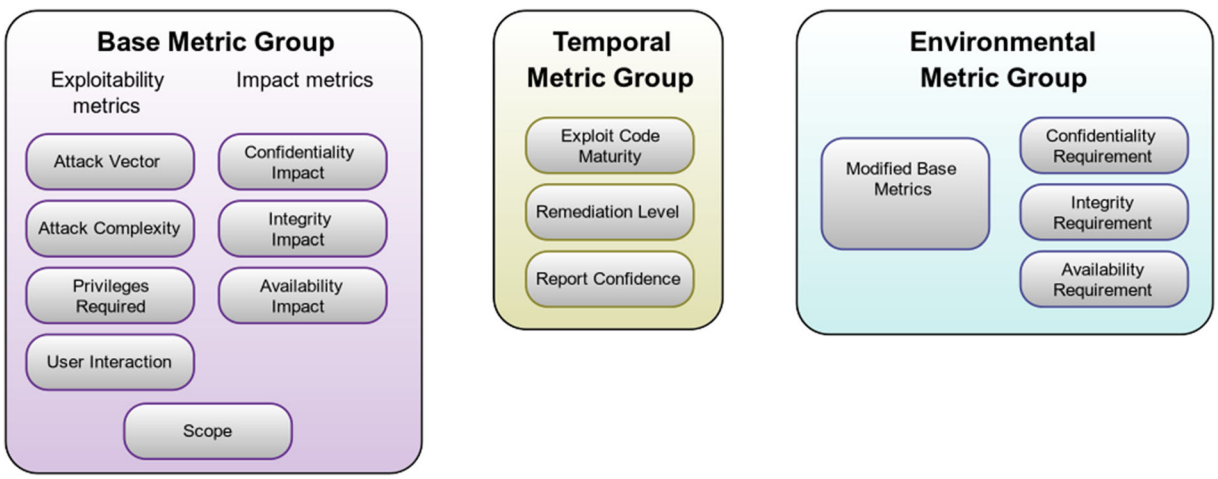

Fig. 1 CVSS V3.1 groups

designed in isolated environments. The primary purpose of these control systems is reliability, continuous and precise functionality in a time critical framework. ICS are designed around particular business logics, hence have limited computing powers and storage capacity [10].

Primarily, ICS are built for performance, compromising on security features like encryption, anti-virus software and intrusion detection systems. These systems have a specific operating system with hard-coded passwords and purpose build protocols. Network protocols are unauthenticated, and commands are in plain text with no or low level of data encryption. The patch management in a control system is kept minimum to avoid unnecessary risks to the production line [11]. As these features are not evaluated in the native CVSS framework, ICS security administrators argue the validity of its scores and raise questions on the credibility of the reports generated using CVSS and other IT related vulnerability models.

In recent years, various ICS specific vulnerability modelling systems were proposed to address the above concerns. Due to the advancement in communication technologies, the ICS networks are hardly isolated, rather integrated with the typical IT and IoT networks. In this work, these multi node networks are called "hybrid networks". With the wide adoption of IT and IoT devices in ICS networks, the ideal vulnerability modelling solution should fit the characters of each device in a hybrid network [12]. It should correctly evaluate the vulnerabilities for typical IT systems and concomitantly address the exclusive features and limitations of the IoT and ICS devices. As modern ICS networks are evolving, instead of designing a brand-new vulnerability modelling solution and then waiting for its industry wide adoption to gain maturity, it is much practical to evolve an existing industry wide accepted solution for hybrid network, by integrating the distinct ICS features into it. In our previous work [13], we have evolved CVSS framework for IoT devices by embedding the IoT exclusive characteristic in it, called $CVSS_{IoT}$.

In this work, we have further evolved $CVSS_{IoT}$ framework for hybrid networks by embedding the ICS specific features into CVSS V3.1. As ICS networks are usually tightly coupled with local industrial needs, these features are implanted in environmental metrics. This empowers the local administrators to choose the value for environmental metrics to meet their specific needs without affecting the universal base score of CVSS framework. We have used the attack graphs theory to build the relationship in selected vulnerabilities on a variety of nodes for a multistep attack on a hybrid network. Attack graphs are used to reveal the relationship between diverse vulnerabilities and detect potential threats to the most critical nodes. With the help of attack graph recommendations, mitigation strategies are prioritized, and resources are allocated to secure the critical nodes [14].

In this work, we have identified the deficiencies of the CVSS v3.1 framework for ICS nodes. These deficiencies are addressed by embedding the ICS specific features in the CVSS framework. The evolved model, named $CVSS_{IoT\text{-}ICS}$, is equally applicable for all nodes of hybrid networks including traditional IT and IoT devices, along with ICS. The proposed new framework is validated using a realistic use case of a supply chain model. This supply chain model consists of ICS nodes, IoT sensors and typical IT systems, hence forming a hybrid network. The nodes of this hybrid network are then assigned with the vulnerabilities listed in the NVD database [15]. The probabilities between the connected nodes of our hybrid network are computed using the CVSS scores of these vulnerabilities. Firstly CVSS V3.1 score is used, then the same calculations are repeated using the proposed $CVSS_{IoT\text{-}ICS}$ framework. Vulnerability security analyser (VSA) tools are used to determine the recommendations of the attack graph. Based on the results, it is established that $CVSS_{IoT\text{-}ICS}$ evaluations are more realistic, as it reflects the exclusive features of all nodes types in a hybrid network.

2 Related work

Industrial control system (ICS) security has always been a point of interest for research. Wei et al. conducted the detailed cyber security analyses of the smart grids system and proposed a cyber security framework based on securing the network traffic management, automation and power switch management [16]. It was a basic framework limited to the protection of Smart Grid.

Knowles et al. conducted a detailed survey on various security frameworks and standards in twenty-two industries including oil, gas and chemical sectors [17]. They concluded that the USA based cyber security standards and practices are dominating in these industries for securing the ICS networks.

Kim et al. proposed a novel approach to identify the vulnerabilities in ICT by scanning and analysing the network traffic [18]. In this approach fuzzing based classification were used to generate the three type of test cases after analysing the network traffic protocol (i.e., protocol length, protocol contents, and protocol data). The ambiguities in network traffic are reported based on these three basic tests to generate the alerts.

Kobara et al. reviewed the existing security issues for industrial control systems and industrial IoT devices. Based on the recent attacks, they discovered that middleware IT and IoT devices are used to launch attacks on ICS networks [19]. Hence, to secure the ICS, the linked IT and IoT devices should be monitored and secured.

Busby et al. conducted a detailed analysis of the affordability and timely adaption for cyber security solutions to industrial control system [20]. In their lab, using the attack graph theory model, they injected each node with some known risks (i.e., assigned weak password to each node) and analysed the node behaviour. In the next several iterations, they kept adding the complexity in the node password and kept analysing system for adoptability for this change along with the average time and cost associated with this. Using this information each path is ranked based on affordability and performance score. They argue that this ranking is useful for system administrators to execute their mitigation policy for testing the vulnerabilities in their systems.

Though the above are useful techniques to understand adoptability of ICS network, these are limited to specific use cases or scenarios. This ranking may be best for certain types of vulnerabilities in a specific ICS but may mislead the system administrators for vulnerabilities of varying dynamics.

Yilmaz proposed an attack detection and prevention system for ICS built on scanning network packets [21]. In this model network traffic is continuously scanned to detect the ambiguities in network traffic. These ambiguities are then matched with predefined attack patterns. If the attack is matched with a predefined pattern, then appropriate actions are executed to prevent this attack. This model is intelligent and detects known attacks in initial stages. However, it does not have the capability to detect new attacks. The proposed model suits the network traffic monitoring rather than being a complete security model.

Laszka explored the evolution in IoT based industrial control systems and rise in its privacy challenges [22]. They proposed the Privacy-preserving Energy Transactions (PETra) solution by providing a strong blockchain encryption to deal with system security, safety and privacy concerns in these modern ICS networks. Though strong encryption means strong security, it is directly proportional to processing power. IoT devices are low budget devices and usually lack strong processing power. Though PETra may suit some specialised IoT based ICS systems to address privacy issues, it may not be appropriate for industry-wide adoption. Zimba et al. explained the attack dynamics on a modern ICS system in [23]. The system is multi layered, where ICS nodes are usually integrated with supervisory networks and these supervisory networks are integrated with internet enabled corporate networking nodes. The supervisory networks and corporate networks are mostly fitted with traditional IT systems. Aaron explained that external attackers are using the internet connected nodes to launch attacks on ICS system. So, in modern ICS networks, the security of all connected nodes is vital for the overall security of the system.

On similar lines, Ge explored the unique cyber security characteristics for industrial IoT based control systems. He discovered that the ICS nodes attract various types of threats based on their functions [24]. Most of these attacks are executed on the ICS nodes from inside corporate networks. As compared to traditional IT nodes, the IoT and ICS are more in number and widely used in various industries and have collateral damage risk linked with it. The work proposed Forum Alert Traffic Security (FATS) architect to monitors network traffic and generated alerts for ambiguities in network traffic based on defined patterns.

Farris et al. conducted a very detailed survey on current security threats to industrial based IoT system [25]. They investigated the security features of various IoT topologies and highlighted the security risk associated with these setups.

The above work shows the research interest in current ICS networks. ICS networks are usually configured in a separate zone (DMZ) with almost no direct connectivity with public networks. However, with the emergence of internet base devices, the ICS networks are evolved to exist side by side with existing IT and IoT systems. Though this model has open new horizons for modernizing the traditional ICS networks, at the same time it has also opened the door for IT cyber security issues to arrive into ICS networks. Attackers are using the IT and IoT system as a stage to execute attack on ICS network. Due to this fact, a comprehensive security

model not only secures ICS network, but also considers IT, IoT and ICS networks as a whole. It should take care of the unique characteristic of ICS nodes like cascading impact, impact on the production line, monitoring and data loss issue. Though the above models proposed in the literature are reasonable, these are mainly limited to ICS networks with specialised industries. They fail to address the cyber security issues of IT and IoT nodes of hybrid network.

As CVSS is the most widely used industry standard for the traditional IT system, Johnson et al. conducted a detailed Bayesian analysis of CVSS system [26]. In this study, they compared the vulnerability database of NVD for CVSS, X-Force from IBM, open source vulnerability database (OSVDB), CERT-VN from software engineering institute (SEI). They used Bayesian analysis to investigate "how good is each vulnerability database at predicting the true values of a vulnerability". They concluded that, in general, NVD database of CVSS assigns the more reliable score to vulnerabilities as compared to other databases.

For the same reason, in the recent years, the research trend has gone towards evolving CVSS for IT, IoT, and ICS devices. Houmb et al. proposed a model to estimate vulnerability frequency and impact for IT networks from CVSS 2.0 metric using Bayesian belief network (BBN) [27]. The vulnerability impact is predicted using CVSS environmental metrics by combining it with integrity, confidentiality and availability score of base metrics. Similarly, the vulnerability frequency score is predicted using CVSS temporal metrics group, access vector, access complexity and authentication metric scores. They used BBN technique to predicts these additional values. BBN method has the potential to drive scores for newly embedded factors in CVSS framework for IT, IoT and ICS nodes.

Sing et al. proposed new factors in CVSS for estimating the "vulnerability frequency" score using the CVSS exploitability and temporal Metric for digital networks [28]. Spring conducted a detailed analysis for CVSS V3.0 and highlighted significant usability issues for CVSS V3 framework [29]. As CVSS score mirrors the severity of the vulnerability but not the risk to the overall system. It does not reflect the risk for the systems where data loss is important. CVSS designed for traditional IT systems, it does not truly reflect the severity of IoT and industrial control systems. As these modern nodes have complex dynamics and have specific safety and privacy concerns, Spring recommended improving the CVSS system to address the above challenges, but he did not suggest any improvements.

Yigit et al. proposed a cost-aware security model for IoT nodes working with industrial control network using attack graphs model [30]. They used the CVSS exploitability score of base metric as a success probability of node vulnerability. They have also assigned the cost and time weight from 0 to 5 to each link to mitigate node vulnerabilities. Based on these weight values each link in the attack graph is evaluated and assigned a new score. This way the most costly and time effective vulnerable paths are identified. These paths are preferred in applying mitigating strategies against vulnerabilities.

Although this vulnerability model represents the overall security of the entire network having IT, IoT ICS nodes, it does not factor in the unique characteristics linked with IoT and ICS devices like collateral damage, cascading impact, business continuity impact, etc. Thus, using the CVSS score for these nodes may deceive the administrators for prioritising and executing mitigation policies. For example, Yigit assumed the random weights for cost and time ranking but predicting these random weights is a challenge as it may change from human to human and industry to industry.

In summary, the traditional ICS networks are shifting and adopting the internet interactive devices. The typical ICS networks are embedded with traditional IT and IoT systems. However, IoT and ICS systems have exclusive dynamics as compared to legacy IT systems. Though traditional IT systems are around from decades, their cyber security models and standards are well established and adopted worldwide. But these IT based security models leave gaps when extended for these exclusive nodes. So instead of proposing brand-new solution for ICS embedded systems, it is much practical to evolve existing solutions for hybrid networks.

3 Proposed $CVSS_{IoT\text{-}ICS}$ Framework

3.1 Deficiencies of current CVSS framework

As CVSS is the most used industry standard for IT systems to predict vulnerability, researchers tend to evolve this for IoT and ICS systems by implanting the exclusive dynamics of these networks. But these proposals are limited for a specific industry or scenario and cannot be adopted as universal vulnerability modelling solutions. In our previous work [13], we have addressed this gap in CVSS V3.0 by

embedding the unique dynamics of IoT nodes and this was named $CVSS_{IoT}$. Meanwhile CVSS v3.1 is released by the Forum of Incident Response and Security Teams (FIRST) with minor changes. In this version, the FIRST has accepted the fact that diverse industries may have a variety of factors to consider for their specific need of vulnerability calculations and introduced the CVSS extension framework to CVSS V3.1 to accommodate additional factors [31].

As identified in our literature review, the main purpose of ICS to provide reliability and continuity to the industrial production process. So based on extensive study, we have identified following ICS specific factors to be evaluated for vulnerability calculation in the CVSS framework.

- *Process visibility* [32].
- *Process monitoring* [33].
- *Process control* [34].
- *Process cascading sequence* [34].
- *Process system safety* [35].
- *Production impact* [36].
- *Business continuity impact* [36].

3.2 Formulation of Vulnerability Scoring in CVSS framework

To answer the deficiencies in CVSS 3.1, we have implanted the ICS context into this framework. We have used CVSS 3.1 extension framework to fill the gap by embedding the above factors into our previous work of $CVSS_{IoT}$ by extending environmental metrics. Environmental metrics are selected as it provides the flexibility for industries to adjust the values according to their specific need, without pervading the universal scoring. The extended framework is called $CVSS_{IoT\text{-}ICS}$. The environmental metrics now evaluate the following.

- Process visibility impact (PV): to measure influence on the ability to accurately and completely view production processes.
- Process monitoring impact (PM): to quantify the impact on process monitoring assessments.
- Process control impact (PC): to account for the effect on process stability, and consistency.
- Process cascading sequence impact (PCS): to measure the influence on the chain of process sequences.
- Process system safety impact (PSS): to measure the effects on the overall safety of the system.
- Production impact (PI): to incorporate the influence on the manufacturing process.
- Business continuity impact (BCI): to quantify the impact on the ability to maintain essential functions.

Figure 2 shows the embedded features in the CVSS framework. The base metric group of this figure reflects our previous work related to IoT devices, where environmental metric group shows our current work of embedding ICS dynamics in hybrid networks. The differences between Fig. 1 and Fig. 2 are highlighted with a red outline reflecting the embedded changes in the CVSS framework.

To evaluate the vulnerability impact on the process visibility, a new vector Process Visibility (PV) is introduced in environmental metrics with values of "Not Defined" (X), Low (Li), Medium (Mi) and High (Hi). For $CVSS_{IoT\text{-}ICS}$, the numeric values of PV vector are [X, Li = 0.04, Mi = 0.60, Hi = 0.97]. These proposed values are calculated using Bayesian Networks Model [37]. Selecting this vector value as "X" means this factor not being considered for vulnerability scoring. On a similar note, the impact on Process Monitoring (PM), Process control (PC), Process cascading sequence (PCS), Process system safety (PSS), Production impact (PI), Business continuity impact (BCI) are calculated.

The numeric values for the newly introduced metric are predicted using the Bayesian Believe Networks (BBN). BBN is a diagram (called a directed graph) together with an associated set of probabilities. It is used to determine conditional probabilities. Figure 3 reflect the BBN model of $CVSS_{IoT\text{-}ICS}$ metrics used to predict the numeric values of ICS embedded features.

For example, the process visibility (PV) value is predicted using BBN rule as follows:

$$P(A,B) = P(A|B)P(B) = P(B|A)P(A) \tag{1}$$

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{2}$$

where $P(A, B)$ is a combined probability of both events A and B. $P(A|B)$ represents the probability of A under the assumption that B is known. For n variables,

$$P(A_1, A_2, \ldots, A_n) = P(A_1|\, A_2, \ldots, A_n)\, P(A_2|\, A_3, \ldots, A_n) \ldots \tag{3}$$

$$P(A_{n-1}|A_n)P(A_n).$$

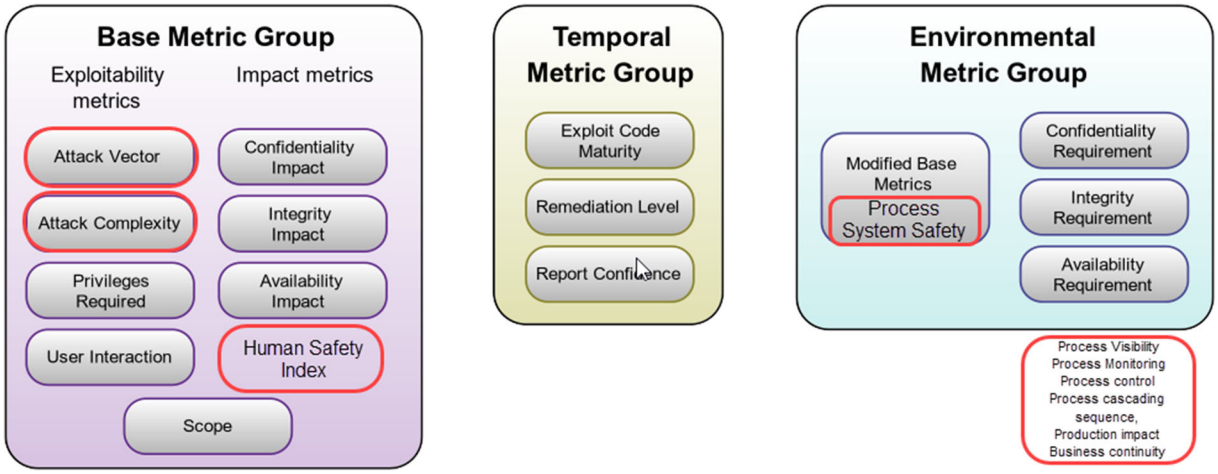

Fig. 2 Embedded features of $CVSS_{IoT\text{-}ICS}$

As shown in Fig. 3, the unknown probability of process visibility $P(PV)$ is directly impacted by probabilities of confidentiality $P(C)$, user interaction $P(Ui)$, privileged access required. Where the privileged-access-required further depends on the scope change $P(SC)$ or scope unchanged $P(SU)$. We used the base score of CVSS V3.1 as $P(C)$, $P(UI)$, $P(SC)$, $P(SU)$. First intermediate possibilities $P(V1)$, $P(V2)$ are determined and these intermediate possibilities are used to predict the probabilities for $P(PV)$. Table 1 shows the node probability for $P(PV)$.

3.3 Integration of CVSS v3.1 with $CVSS_{IoT\text{-}ICS}$

The proposed $CVSS_{IoT\text{-}ICS}$ is inegrated with the existing CVSS v3.1 with the purpose to have a single framework equally applicable to all node types in a hybrid network. In this integration, the numerical

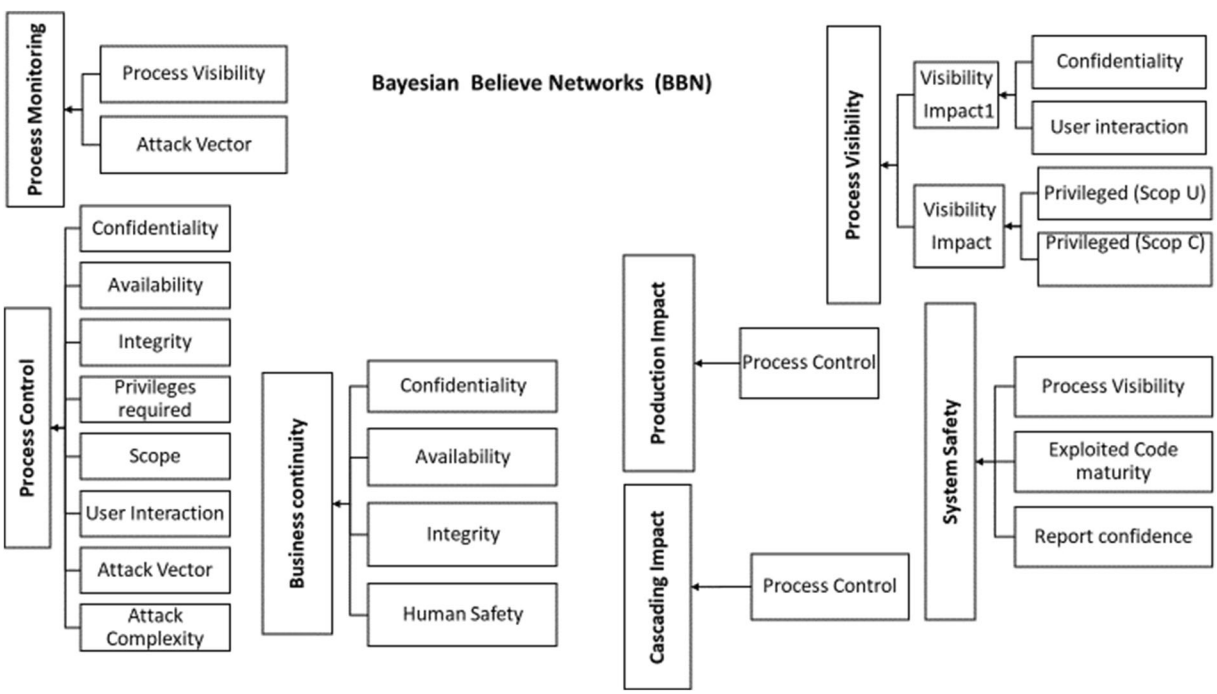

Fig. 3 BBN Topology for $CVSS_{IoT\text{-}ICS}$

Table 1 CVSS attributes for P(PV)

CVSS base values	Rating	Values	Intermediate values	P (PV)	
Confidentiality (*C*)	High (*H*)	0.56	*PV*1	High (*H*)	0.97
	Low (*L*)	0.22	0.66	Low (*L*)	0.60
	None (*N*)	0.00	0.20	None (*N*)	0
User Interaction (*UI*)	None (*N*)	0.85	0.0		
	Required (*R*)	0.62			
Privileged (Scope Changed) (*PSC*)	None (*N*)	0.85	*PV*2		
	Low (*L*)	0.66	0.96		
	High (*H*)	0.50	0.77		
Privileged (Scope UN Changed) (*PSU*)	None (*N*)	0.85	0.27		
	Low (*L*)	0.62			
	High (*H*)	0.27			

evaluation for traditional computing nodes and systems is driven like the same as of CVSS v3.1, but values to IoT and ICS nodes are accessed and assigned after evaluating the dynamic feature of these nodes. This way legacy computer nodes have the same value of CVSS v3.1, but other nodes, having additional factors, are evaluated using evolved metrics. These metric values are listed in Table 2, the IoT and ICS related values are listed with subscript i.

The differences between CVSS and $CVSS_{IoT\text{-}ICS}$ are in bold font. The numeric values for the newly introduced metric are predicted using the BBN and listed in Table 3.

The Environmental equation for $CVSS_{IoT\text{-}ICS}$ is as follow.

$$MISS = Minimum\Big(1-\Big[\ \Big(1-ConfidentialityRequirement \times ModifiedConfidentiality\Big) \times (1-IntegrityRequirement \times ModifiedIntegrity) \times (1-AvailabilityRequirement \times ModifiedAvailability) \times (1-ProcessVisibility \times ModifiedPV) \times (1-ProcessMonitoring \times ModifiedPM) \times (1-ImpactHistoricaldata \times ModifiedIHD) \times (1-ProcessControll \times ModifiedPC) \times (1-PotentialOfCascadingImpact \times ModifiedPCI) \times (1-BusinessContinutityImpact \times ModifiedBCI) \times (1-FinancialLostImpact \times ModifiedFLI)\Big], 0.915\Big).$$

$$ModifiedImpact = \begin{cases} If\ ModifiedScope\ is\ Unchanged\quad then \\ 6.42 \times MISS \\ If\ ModifiedScope\ is\ Changed\quad then \\ 7.52 \times (MISS - 0.029) - 3.25 \times (MISS \times 0.9731 - 0.02)^{13} \end{cases}$$

$$\begin{aligned} ModifiedExploitability &= 8.22 \times ModifiedAttackVector \\ &\times ModifiedAttackComplexity \\ &\times ModifiedPrivilegesRequired \\ &\times ModifiedUserInteraction \\ &\times \ ModifiedHumanSafety \\ &\times Modified\ SystemSafetyImpact \end{aligned}$$

$$EnvironmentalScore = \begin{cases} If\ ModifiedImpact \le 0\ then\ 0, \quad else \\ \begin{aligned} &If\ ModifiedScope\ is\ Unchanged \\ &= Roundup\ (\ Roundup\ [Minimum\ ([ModifiedImpact \\ &+ ModifiedExploitability], 10)\ \times ExploitCodeMaturity \\ &\times RemediationLevel \times ReportConfidence) \end{aligned} \end{cases}$$

Table 2 CVSS $_{\text{IoT-ICS}}$ possible values

CVSS $_{\text{IoT-ICS}}$ possible values			
Metric	Metric Name	Possible Values	Mandatory
Base	Attack Vector *AV*	[*N*, *A*, *L*, ***Li***, *P*, ***Pi***]	Yes
	Attack Complexity *AC*	[*L*, *Mi*, *H*, ***Hi***]	
	Privileges Required *PR*	[*N*, *L*, *H*]	
	User Interaction *UI*	[*N*, *R*]	
	Scope *S*	[*U*, *C*]	
	Confidentiality *C*	[*H*, *L*, *N*]	
	Integrity *I*	[*H*, *L*, *N*]	
	Availability *A*	[*H*, *L*, *N*]	
	Human Safety Index *HI*	**[*Ni*, *Li*, *Hi*]**	
Temporal	Exploit Code Maturity *E*	[*X*, *H*, *F*, *P*, *U*]	No
	Remediation Level *RL*	[*X*, *U*, *W*, *T*, *O*]	
	Report Confidence *RC*	[*X*, *C*, *R*, *U*]	
Environmental	Confidentiality Req *CR*	[*X*, *H*, *M*, *L*]	No
	Integrity Req *IR*	[*X*, *H*, *M*, *L*]	
	Availability Req *AR*	[*X*, *H*, *M*, *L*]	
	Modified Attack Vector *MAV*	[*X*, *N*, *A*, *L*, ***Li***, *P*, ***Pi***]	
	Modified Attack Complexity *MAC*	[*X*, *L*, ***Mi***, *H*, ***Hi***]	
	Modified Privileges Required *MPR*	[*X*, *N*, *L*, *H*]	
	Modified User Interaction *MUI*	[*X*, *N*, *R*]	
	Modified Human Safety Index *HI*	[*X*, ***Ni***, ***Li***, ***Hi***]	
	Modified Scope *MS*	[*X*, *U*, *C*]	
	Modified Confidentiality *MC*	[*X*, *N*, *L*, *H*]	
	Modified Integrity *MI*	[*X*, *N*, *L*, *H*]	
	Modified Availability *MA*	[*X*, *N*, *L*, *H*]	
	Process Visibility	[*X*, ***Hi***, ***Mi***, ***Li***]	
	Process Monitoring	[*X*, ***Hi***, ***Mi***, ***Li***]	
	Process Control	[*X*, ***Hi***, ***Li***]	
	Process Cascading Sequence	[*X*, ***Hi***, ***Li***]	
	Process System Safety	[*X*, ***Hi***, ***Mi***, ***Li***]	
	Production Impact	[*X*, ***Hi***, ***Mi***]	
	Business Continuity Impact	[*X*, ***Hi***, ***Mi***, ***Li***]	

$$
\begin{aligned}
&\textit{If ModifiedScope is Changed}\\
&\quad = \textit{Roundup}\,(\,\textit{Roundup}\,[\textit{Minimum}\,(1.08\\
&\quad \times [\textit{ModifiedImpact} + \textit{ModifiedExploitability}], 10)]\\
&\qquad \times \textit{ExploitCodeMaturity} \times \textit{RemediationLevel}\\
&\qquad \times \textit{ReportConfidence})
\end{aligned}
$$

4 Case Study

To access and analyse the CVSS$_{\text{IoT-ICS}}$, we implemented this proposed framework on a supply chain system having various types of nodes. It has traditional computer nodes like inventory management and payment systems, and internet enabled devices like temperature sensors and GPS system, and industrial control nodes like robotic arms. In a

Table 3 CVSS $_{\text{IoT-ICS}}$ updated matrix values

CVSS $_{\text{IoT-ICS}}$ possible values			
Metric	Metric Name	Possible Values	Mandatory
Environmental	Process Visibility	[*X*, 0.97, 0.60,0.0]	No
	Process Monitoring	[*X*, 0.99, 0.70, 0]	
	Process Control	[*X*, 0.97, 0.45]	
	Process Cascading Sequence	[*X*, 0.97, 0.45]	
	Process System Safety	[*X*, 0.91, 0.55, 0.06]	
	Production Impact	[*X*, 0.97, 0.45]	
	Business Continuity Impact	[*X*, 0.99, 0.4, 0.08]	

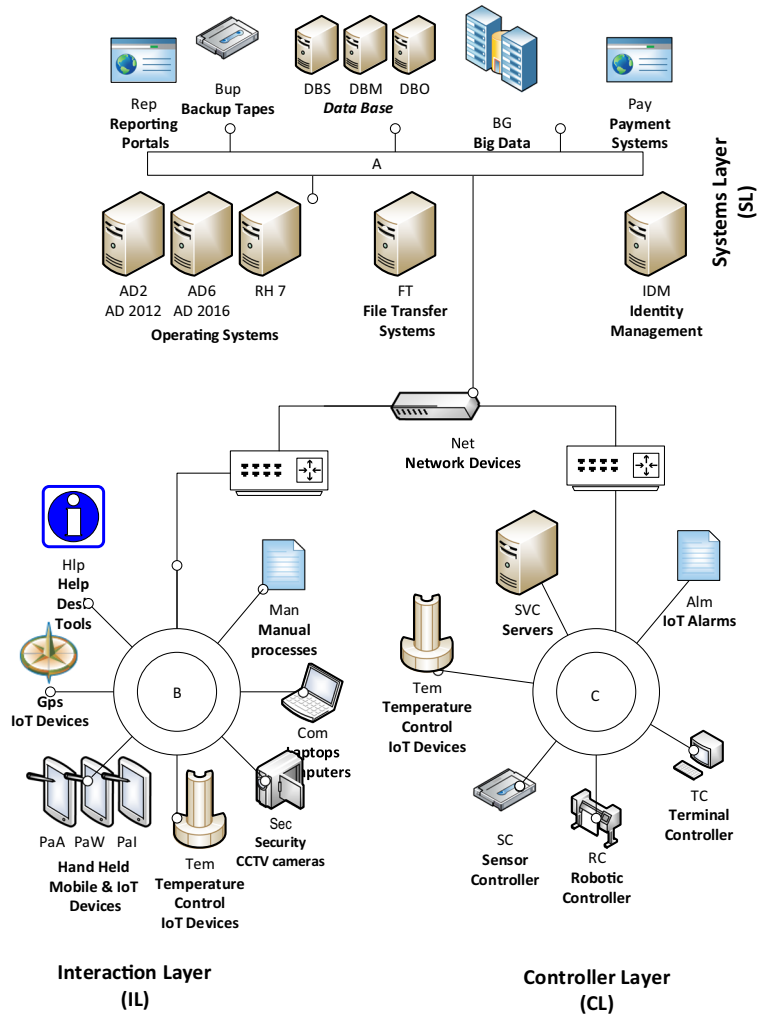

Fig. 4 Layers and nodes of selected supply chain system

supply chain system, the robotic arms are very important to meet production timelines and goals. The malfunction of these industrial controllers may result in worker's safety and damaging the business reputation. It may cause food quality concerns and hence may result in health and safety issues.

Table 4 CVSS $_{\text{IoT-ICS}}$ updated matrix values

Nodes	CVE	CVSS v3.1	$CVSS_{IoT-ICS}$
Robotic Controller (RC)	CVE-2017-5753	4.0	6.6
Temperature (Tem)	CVE-2018-11,315	3.6	3.8
Alarm (Alm)	CVE-2019-11,561	2.6	2.7
Sensor Controller (SC)	CVE-2019-11,895	1.6	6.1
Servers (SVC)	CVE-2018-1111	7.5	7.5
Terminal controller (TC)	CVE-2019-14,402	3.3	4.9
Network devices (Net)	CVE-2019-0690	2.8	2.8
Interactive layer (IL)	Combined average	4.9	5.3
Systems layer (SL)	Combined Average	9.1	9.1

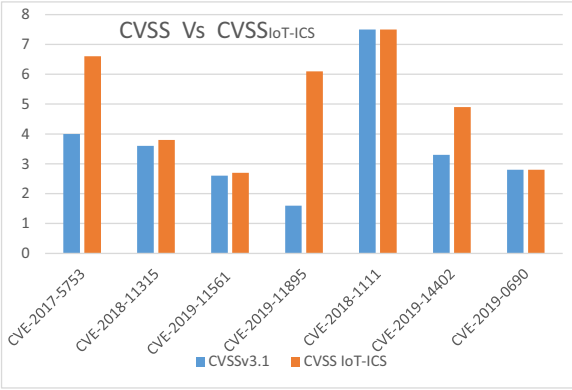

Fig. 5 Value Compression between CVSS and CVSS $_{\text{IoT-ICS}}$

Our supply chain model, as shown in Fig. 4. have three layers. Figure 4 is not a network topology diagram but the layers in this diagram are classified based on functionality and physical access to the nodes.

Systems Layer (SL) The traditional IT system like servers and backup systems are usually protected with firewall, and have no or very limited direct access to end users. These systems are managed using a variety of admin tools and rich in processing power and storage space.

Interaction Layer (IL) The interactive layer usually has direct access to the end users on the front end. The nodes in this layer communicate with systems layers using inner network devices. The devices in this layer may have physical or public access.

Controller Layer (CL) These are industrial control systems (ICS).

In this layer, the devices are mostly restricted and usually in demilitarized (DMZ) network zone. But some of the nodes in this domain like alarms, and control serves have specialised interactive interface.

For our study, the nodes in Fig. 4 are assigned the real vulnerabilities from the National Vulnerability Database (NVD) [19]. These vulnerabilities are then assigned the bases score listed in the NVD database. The robotic controller (RC) is assigned CVE-2017-5753 vulnerability from NVD. The RC node is connected to many other devices including the system layer nodes with network devices. NVD listed base score for CVE-2017-5753 is 4.0. This value is used as node probability for RC node. Similarly, the other nodes are assigned with vulnerabilities and their CVSS base score from the NVD database. The selected values are listed in Table 4. Using these scores of node probability, the link probability between these nodes is calculated. The link probabilities are then passed to the vulnerability analyser tool (VSA) to identify the critical nodes and weakest path to the target nodes. VSA is a security analyser tool, it takes the nodes and path probabilities as input and builds an attack graph of the requested network. It lists all possible paths from interactive nodes to the target node. It also identifies the easiest path and most vulnerable node to the target node.

5 Results

The 3rd column of Table 4 shows the environmental metric score of CVE vulnerabilities. This is the same as the base metric score because no adjustments are made in the environmental matric for our supply chain system in CVSS v3.1. The 4th column in the same table lists the environmental metric score under CVSS$_{\text{IoT-ICS}}$. As we have three types of nodes in controller layer, the traditional IT nodes like servers (SVC) have the same vulnerability score in both columns. The IoT nodes like Temperature sensor (Tem) have higher values under CVSS$_{\text{IoT-ICS}}$ as compared to the native CVSS.

The difference is due to IoT related characteristics, such as the human safety index linked to temperature

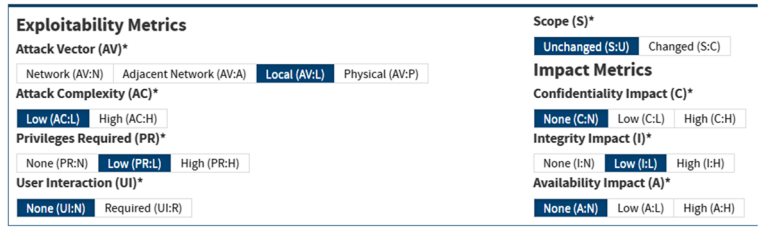

Fig. 6 CVE-2019-14,402 under CVSS

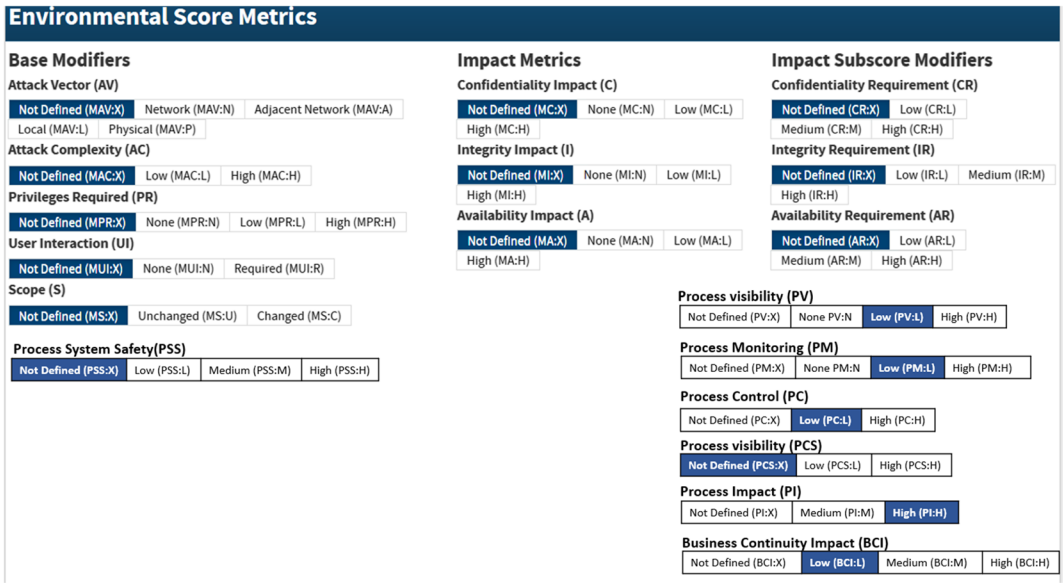

Fig. 7 CVE-2019-14,402 under $CVSS_{IoT\text{-}ICS}$

and alarms nodes (IoT devices). Similarly, ICS nodes also influence the process visibility (PV), processing monitoring (PM) and business continuity impacts (BCI) under $CVSS_{IoT\text{-}ICS}$, calculating higher values as compared to the native CVSS framework. Figure 5 shows the vulnerability related data, where CVE-2018-1111 and CVE-2019-0690 have same results of CVSS. But other IoT and ICS related CVE vulnerabilities like CVE-2018-11,315 and CVE-2017-5753 are rated high.

For example, CVSS base score of CVE-2019-14,402 vulnerability assigned to the terminal controller (TC) is 3.3, the cvss metric breakdown is shown in Fig. 6. Using this vulnerability, the network commands scripts may be injected to the nodes [38]. As we are not making any adjustment in the base score for environmental metric so environmental metric scores are calculated using value 'X' form Table 2. Hence it reveals the same score as of base for environmental metric.

In our supply chain system, the terminal controller is responsible for coordination between multiple robotic arms. Getting the wrong task dictated by remote network script may have a catastrophic impact on the supply chain, where the order of a certain task is important to maintain the chain sequences. This vulnerability has the potentials of hiding the process, manipulating the process monitoring statistics or may take control of the complete process. It may stop the robotic arm, further causing the business continuity impact [39]. As the native CVSS does not provide metrics to measure these distinct factors of ICS, to get more realistic scores we used $CVSS_{IoT\text{-}ICS}$ for evaluating our supply chain system. This calculation has rated the selected vulnerability higher compared to CVSS. The $CVSS_{IoT\text{-}ICS}$

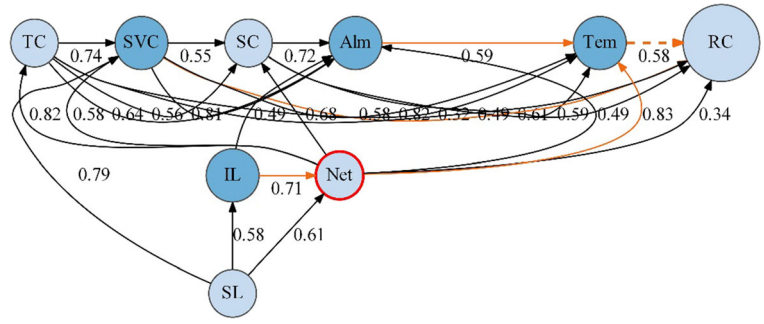

Fig. 8 VSA analysis of selected supply chain using CVSS

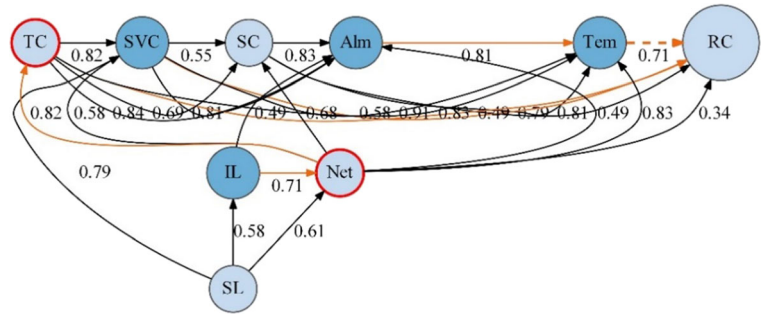

Fig. 9 VSA analysis of selected supply chain using CVSS $_{\text{IoT-ICS}}$

metric breakdown is shown in Fig. 7. The main difference is in MISS (modified Impact Sub-Score) part of Equ (1), where we have embedded IoT and ICS related factors.

In this supply chain system, the link probability between connected nodes is derived using the fitness model of graph theory [40]. This linked probability is calculated based on the CVSS vulnerability score of environmental metrics and then passed to VSA as path probability. Figure 8 and Fig. 9 are the graphical description of the results produced using the VSA tool [13]. Figure 8 results are based on CVSS values, while Fig. 9 shows the same vulnerabilities evaluated using $\text{CVSS}_{\text{IoT-ICS}}$ framework. For simplicity and better understanding, all nodes in area A of Fig. 4 are represented by a combined node called System Layer (SL).

The average score of the nodes in this area is assigned to SL and listed as a combined average in Table 4. Similarly, in Fig. 4, all nodes of area B are represented by IL (interactive layer) and assigned with average score. But area C of Fig. 4, which represents the Controller Layer (CL), is treated as individual nodes. This layer consists of IT, IoT and ICS nodes, and it is firewall protected, to separate the controller layer from corporate systems.

RC node in Fig. 8, represented by a bold light blue circle is the target node in our supply chain system. The attackers' target is to compromise this node. There are several possible paths to this target node from an interactive nodes; the middle nodes are presented with dark blue circles while the light blue circles present the interactive nodes. The possible paths to target nodes are denoted using direct arrows from the source node to the target node. The critical paths are presented using orange direct arrows and the easiest path is with dotted line arrows to the target node. In Fig. 8, the VSA tool has revealed the Network node (NET) as the critical node, presented by the red circle. The critical nodes are the most vulnerable nodes in a system and selected based on their vulnerability and accessibility to the target node. Compromising these nodes makes it easier to attack the target node.

In our supply chain system, some nodes are ICT and others are IoT devices. In our next experiment, the links probabilities are evaluated using $\text{CVSS}_{\text{IoT-ICS}}$. These results are again fed to the VSA tool. This time, Terminal controller (TC) is also revealed as a critical node along with Net node by VSA. A comparison of Fig. 8 and Fig. 9 demonstrates that $\text{CVSS}_{\text{IoT-ICS}}$ has also updated the paths to the target node of RC. The easiest path is also updated and re-ranked, due to the distinct factors considered in calculating the probability for ICS and IoT nodes. As presented in Fig. 10, the four most critical paths to the RC node are listed and compared for CVSS and $\text{CVSS}_{\text{IoT-ICS}}$ where 1 out of 4 paths is via critical

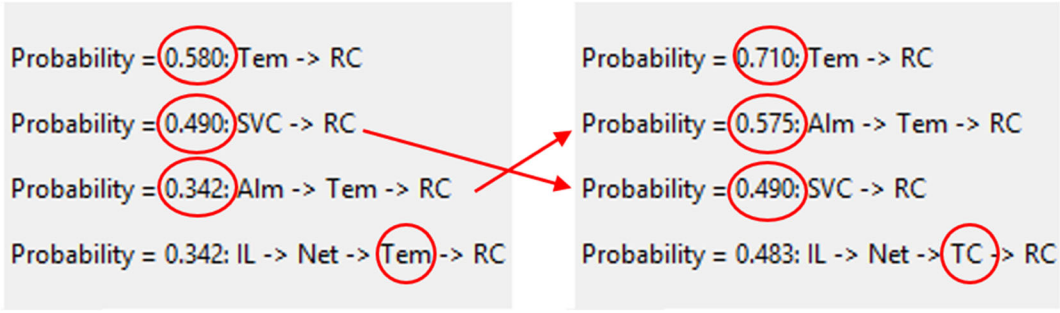

Fig. 10 CVSS vs CVSS $_{\text{IoT-ICS}}$

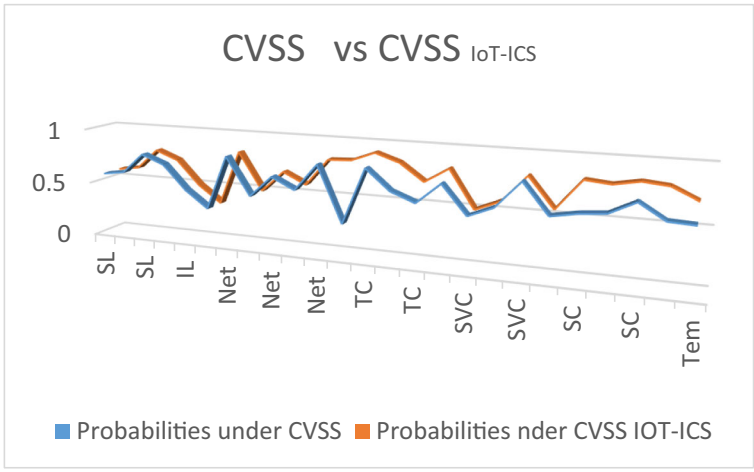

Fig. 11 Value Compression between CVSS and CVSS $_{IoT\text{-}ICS}$

nodes. On the left hand side of Fig. 10, the paths are ranked using the CVSS framework, while on the right hand side the paths are ranked using the proposed $CVSS_{IoT\text{-}ICS}$ framework. The VSA analyser has reranked the attack possibilities on the right hand side as per the probabilities are calculated including the unique factors of ICS and IoT nodes. It has included the TC nodes instead of Tem in the ranking. Under $CVSS_{IoT}$, ICS node RC is ranked up from the 3rd to the 2nd palace and IoT nodes Tem is moved out due to more realistic vector values.

Figure 11 further illustrates the differences between CVSS and CVSS $_{IoT\text{-}ICS}$. The link probability is the same for identical vulnerabilities for traditional nodes under CVSS and CVSS $_{IoT\text{-}ICS}$. However, for IoT and ICS nodes, the $CVSS_{IoT\text{-}ICS}$ assigns higher values as it evaluates ICS and IoT characters. So CVSS scores may mislead system administrators to wrongly allocate their resources and efforts. It may lead to incorrectly design their mitigation strategies. Observing Fig. 8, system engineers may direct their efforts to Network node (Net) but the attacker may get its way to the target nodes by compromising the terminal controller (TC). This gap is correctly highlighted in Fig. 9 which is revealed using $CVSS_{IoT\text{-}ICS}$ to protect the target node. The $CVSS_{IoT\text{-}ICS}$ has covered the gaps for ICS and IoT nodes as per their priorities for the same vulnerabilities.

6 Conclusion

In this paper, we proposed a $CVSS_{IoT\text{-}ICS}$ vulnerability modelling framework for the hybrid network. $CVSS_{IoT\text{-}ICS}$ is evolved from CVSS v3.1 after incorporating the distinct features of IoT and ICS nodes without changing its application to traditional IT systems. The $CVSS_{IoT\text{-}ICS}$ is compared with CVSS using real world vulnerabilities and studing developed vulnerability analysing tools for a pragmatic supply chain system. The detailed analysis endorses the $CVSS_{IoT\text{-}ICS}$ framework as it assesses and evaluates the distinct features of each type of the node in a mixture of nodes. Our future research will include analysis of $CVSS_{IoT\text{-}ICS}$ framework for complex topologies and further evolve this technique for threat modelling in hybrid networks.

Acknowledgements This was done in Internet Commerce Security Lab (ICSL), Federation University. Westpac bank, IBM and ACSC are partner in ICSL.

References

1. H. Wilsdorf and J. Landels, "Engineering in the Ancient World.", Man, vol. 13, no. 4, p. 681, 1978. Available: https://doi.org/10.2307/2801269
2. D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan and N. Meskin, "Cybersecurity for industrial control systems: a survey", computers & security, vol. 89, pp. 101677, 2020. Available: https://doi.org/10.1016/j.cose.2019.101677, 2020
3. M. Davis, "Comprehensive Modeling of Industrial Control Systems for Cyber-Security Applications." Order No. 10642514, State University of New York at Binghamton, Ann Arbor, 2017
4. U. Ani, H. He and A. Tiwari, "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective", J. Cyber Security Technol., vol. 1, no. 1, pp.

32–74, 2016. Available: https://doi.org/10.1080/23742917.2016.1252211
5. O. A Sergey, G. Gleb, G.O Kochetova," Iindustrial Controll System Vulranabilities Statictics", 2016
6. V. Murthy, "Analysis: Assessing Correlation between CVSS Scores in Vulnerability Disclosures and Patching", Biomed. Instrument. Technol., vol. 54, no. 1, pp. 44–46, 2020. Available: https://doi.org/10.2345/0899-8205-54.1.44
7. "NVD - CVSS v3.1 Official Support", Nvd.nist.gov, 2020. [Online]. Available: https://nvd.nist.gov/General/News/CVSS-v3-1-Official-Support. [Accessed: 03- Jan- 2020]
8. *Symantec Internet Security Threat Report "ISTR Healthcare*, vol. 22, April 2017
9. Stouffer, K., Falco, J., Scarfone, K.: Guide to industrial control systems (ICS) security. NIST Special Public. **800**(82), 16–16 (2011)
10. Y. Hu, A. Yang, H. Li, Y. Sun and L. Sun, "A survey of intrusion detection on industrial control systems", Int. J. Distrib. Sens. N., vol. 14, no. 8, p. 155014771879461, 2018. Available: https://doi.org/10.1177/1550147718794615 [Accessed 8 April 2020]
11. K. Knorr, "Patching our critical infrastructure," Securing Critical Infrastructures and Critical Control Systems, pp. 190–216, 2013
12. M. StJohn-Green, R. Piggin, J.A. McDermid, R. Oates, "Combined Security and Safety Risk Assessment - What Needs to be Done For ICS and The IOT". 10th IET System Safety and Cyber-Security Conference 2015
13. A. Ur-Rehman, I. Gondal, J. Kamruzzuman, and A. Jolfaei, "Vulnerability Modelling for Hybrid IT Systems," IEEE International Conference on Industrial Technology (ICIT), 2019
14. Qin, Y.: Computer network attack modeling and network attack graph study. Adv. Mater. Res. **1079-1080**, 816–819 (2014)
15. "Search and statistics," NVD. [Online]. Available: https://nvd.nist.gov/vuln/search. [Accessed: 02-Jan-2020]
16. D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting Smart Grid against cyber attacks," Innovative Smart Grid Technologies (ISGT), 2010
17. Knowles, W., Prince, D., Hutchison, D., Ferdinand, J., Disso, P., Jonesb, K.: A survey of cyber security management in industrial control systems. Int. J. Crit. Infrastruct. Prot. **9**, 52–80 (2015)
18. S. Kim, W. Jo, and T. Shon, "A Novel Vulnerability Analysis Approach to Generate Fuzzing Test Case in Industrial Control Systems," IEEE Information Technology, Networking, Electronic and Automation Control Conference, 2016
19. K. Kobara, "Cyber Physical Security for Industrial Control Systems and IoT," IEICE Transactions on Information and Systems, vol. E99.D, no. 4, pp. 787–795, 2016
20. Busby, J.S., Green, B., Hutchison, D.: Analysis of affordance, time, and adaptation in the assessment of industrial control system Cybersecurity risk. Risk Anal. **37**(7), 1298–1314 (2017)
21. Yılmaz, E.N., Gönen, S.: Attack detection/prevention system against cyber attack in industrial control systems. Comput. Secur. **77**, 94–105 (2018)
22. A. Laszka, A. Dubey,M. Walker, D. Schmidt, "Providing Privacy, Safety, and Security in IoT-Based Transactive Energy Systems Using Distributed Ledgers" 2017. https://doi.org/10.1145/3131542.3131562
23. Zimba, A., Wang, Z., Chen, H.: Multi-stage crypto ransomware attacks: a new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express. **4**(1), 14–18 (2018)
24. Ge, Y., Zhang, X., Han, B.: Complex IoT control system modeling from perspectives of environment perception and information security. Mobile N. Appl. **22**(4), 683–691 (2017)
25. Farris, I., Taleb, T., Khettab, Y., Song, J.: A survey on emerging SDN and NFV security mechanisms for IoT systems. IEEE Commun. Surv. Tutor. **21**(1), 812–837 (2019)
26. Johnson, P., Lagerstrom, R., Ekstedt, M., Franke, U.: Can the common vulnerability scoring system be trusted? A Bayesian analysis. IEEE Trans. Depend. Sec. Comput. **15**(6), 1002–1015 (2018)
27. Houmb, S.H., Franqueira, V., Engum, E.A.: Quantifying security risk level from CVSS estimates of frequency and impact. J. Syst. Softw. **83**(9), 1622–1634 (September 2010)
28. Singh, U.K., Joshi, C.: Quantitative security risk evaluation using CVSS metrics by estimation of frequency and maturity of exploit. World Congr. Eng. Comput. Sci. **1**, 170–175 (2016)
29. J.M. Spring, E. Hatleback, A. Householder, A. Manion, D. Shi, "Towards Improving CVSS" Software Engineering Indtitute CARNEGIE MELLON UNIVERSITY, 2018
30. Yigit, B., Gurb, G., Alagoz, F., Tellenbach, B.: Cost-aware securing of IoT systems using attack graphs. Ad Hoc Networks. **86**, 23–35 (2019)
31. S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.R. Sadeghi, M. Maniatakos, R. Karri, "The Cybersecurity landscape in industrial control systems," in Proceedings of the IEEE, vol. 104, no. 5, pp. 1039–1057, May 2016
32. M. R. Asghar, Q. Hu, S. Zeadally,"Cybersecurity in industrial control systems: Issues, technologies, and challenges" Computer Networks vol. 165, 24 December 2019, 106946
33. J. Slowik "Evolution of ICS Attacks and the Prospects for Future Disruptive Events" Threat Intelligence Centre Dragos Inc., 2019
34. J. Falco, A. Wavering,F. Proctor, "IT security for industrial control systems. US Department of Commerce", National Institute of Standards and Technology; 2002 Feb 28
35. G. Sabaliauskaite and A. P. Mathur, "Aligning cyber-physical system safety and security," Complex Systems Design & Management Asia, pp. 41–53, 2015
36. X. Zhou, Z. Xu, L. Wang, K. Chen, C. Chen, and W. Zhang, "Kill Chain for Industrial Control System," MATEC Web of Conferences, vol. 173, p. 01013, 2018.3
37. M. Frigault, L. Wang, S. Jajodia, and A. Singhal, "Measuring the overall network security by combining CVSS scores based on attack graphs and Bayesian networks," Network Security Metrics, pp. 1–23, 2017
38. "Vulnerability Details : CVE-2019-14402," CVE. [Online]. Available: https://www.cvedetails.com/cve/CVE-2019-14402/. [Accessed: 10-Jan-2020]

39. H. Esquivel-Vargas,M. Caselli, E. Tews, D. Bucur and A. Peter, Ranking building automation and control system components by business continuity impact. In international conference on computer safety, reliability, and security, 2019 (pp. 183-199). Springer
40. G. Bianconi and A.-L. Barabasi, "Competition and multiscaling m evolving networks," The Structure and Dynamics of Networks, pp. 54–436, 2011
41. Bernabe, J.B., Perez, G.M., Skarmeta Gomez, A.F.: Intercloud trust and security decision support system: an ontology-based approach. J. Grid Computing. **13**, 425–456 (2015)
42. Song, S., Hwang, K., Kwok, Y.: Trusted grid computing with security binding and trust integration. J Grid Computing. **3**, 53–73 (2005)
43. Aziz, B.: Modelling fine-grained access control policies in grids. J Grid Computing. **14**, 477–493 (2016)
44. da Rosa Righi, R., Lehmann, M., Gomes, M.M., Nobre, J.C., da Costa, C.A., Rigo, S.J., Lena, M., Mohr, R.F., de Oliveira, L.R.B.: A survey on global management view: toward combining system monitoring, resource management, and load prediction. J Grid Computing. **17**, 473–502 (2019)