Detecting Cyber Supply Chain Attacks on Cyber Physical Systems Using Bayesian Belief Network

Abel Yeboah-Ofori
Sch. of Arch, Computing & Eng.
University of East London
London, E16 2RD, UK
u0118547@uel.ac.uk

Shareeful Islam
Sch. of Arch, Computing & Eng.
University of East London
London, E16 2RD, UK
shareeful@uel.ac.uk

Allan Brimicombe
Sch. of Geo Information System
University of East London
London, E16 2RD, UK
a.j.brimicombe@uel.ac.uk

Abstract: **Identifying cyberattack vectors on cyber supply chains (CSC) in the event of cyberattacks are very important in mitigating cybercrimes effectively on Cyber Physical Systems CPS. However, in the cyber security domain, the invincibility nature of cybercrimes makes it difficult and challenging to predict the threat probability and impact of cyber attacks. Although cybercrime phenomenon, risks, and treats contain a lot of unpredictability's, uncertainties and fuzziness, cyberattack detection should be practical, methodical and reasonable to be implemented. We explore Bayesian Belief Networks (BBN) as knowledge representation in artificial intelligence to be able to be formally applied probabilistic inference in the cyber security domain. The aim of this paper is to use Bayesian Belief Networks to detect cyberattacks on CSC in the CPS domain. We model cyberattacks using DAG method to determine the attack propagation. Further, we use a smart grid case study to demonstrate the applicability of attack and the cascading effects. The results show that BBN could be adapted to determine uncertainties in the event of cyberattacks in the CSC domain.**

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

I. Introduction

The emergence of CPS in the supply chain domain has enhanced productivity and global demand and supply [1]. CSC has evolved over time and have improved business processes amongst organizations and third party vendors as well as the ability to incorporate electronic transactions with banking services. The autonomous nature of CPS requires real-time decision making and real-time information availability using agents. However, that has brought with it a significant upsurge in cyberattacks and threat agents. Recent CPS attacks include Wanna Cry Ransomware attack 2017, that infected several companies and energy sectors companies worldwide [2]. Ukraine Power Grid attack 2015, caused many homes and businesses to be without electricity. [3]. Saudi Aramco cyberattack 2017, an electric grid was halted from operation by cyber attackers at the Saudi Aramco power station [4]. There are several methods that have been deployed to detect cyberattacks such as integrating the threat modeling and attack vectors [1] [5] [6] and using case studies and vulnerability assessment methods to determine how threats propagate. However, in the cyber security domain, the invincibility nature of cybercrimes makes it difficult and challenging to predict the threat probability and impact of cyberattacks. Although cybercrime phenomenon, risks, and treats contain a lot of unpredictability's, uncertainties and fuzziness, we consider using BBN and subjective judgment to provide a practical, methodical and reasonable approach to implement cyberattack detection on CSC.

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.

II. Related Works

This section discusses related works in the CSC security domains, the start of the art in CPS developments and recent attacks. Ref [7] discussed attack scenarios that outline how cyberattacks and cybercrimes could jeopardize the security of supply chain systems on EU economies including socio-economic, political and ideological impacts. Ref [8] proposed a method of identifying cybercrimes and risks on the smart grid business application system by using Analytical Hierarchy Process (AHP) approach to identify cybercrime and risk on CPS that provides specific risk mitigation goals. Ref [9] proposed a design and secure network protocols to achieve efficient and secure information delivery in the smart grid architecture by reviewing security requirements, network vulnerabilities and attack countermeasures. Ref [1] proposed a discrete probability method for calculating the cyberattack and effectively analyze the threats using conditional probabilities to determine attack propagation and cascading effects on the CSC system. Ref [10] proposed an IADS and CCADS and applied a method to validate the anomaly detection capabilities on CPS using the IEEE bus 39 system by collecting attack information and analyzing the predefined relationships using a similarity index [10]. Ref [11] proposed a security mechanism that decreases the severity if cyber-attacks by employing a divers set of methods reduces repetition of a single vulnerability.

978-1-7281-7417-4/19/$31.00 ©2019 IEEE
DOI 10.1109/ICSIoT47925.2019.00014

The authors focused on the allocation of diver's security mechanisms and tried to increase the security of the cyber assets located within the electronic security perimeter of a substation by and also used a game theory to analyze the vulnerability assessment for power grid network. Ref [12] evaluated cybersecurity risk of power CPS by using modified hypergraph that determines the probability of successful cyberattacks on Substation Auto Systems (SAS) and their countermeasures.

A. The rationale for Using BBN in CSC Attack Detection

BBN is used as probabilistic inference to solve issues of uncertainty. It is used in a cybersecurity domain and Artificial Intelligence (AI) concepts where domain knowledge is not clear. Further Based on the Bayes Theorem, BBN provides an effective technique for reasoning and modeling uncertainties in safety critical system domains. [13, 14]. Similarly, Reference [15], posits that the BBN theory has been used in scientific disciplines to judge the relative validity of hypothesis in the face of noise, sparse, uncertainty, and to adjust the parameters of a specific model. We use conditional probabilities method and causality principles with cyberattack scenarios and assumptions (subjective judgment) to determine the event and cascading effects.

III. 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 [17] 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.

A. Subjective Expect 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.

IV. Bayesian Belief Network Process

This section presents the concepts for the proposed approach. Our work contributes to using BBN to model and analyzing cyberattacks for the CSC domain.

A. Bayesian Belief Network (BBN)

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.

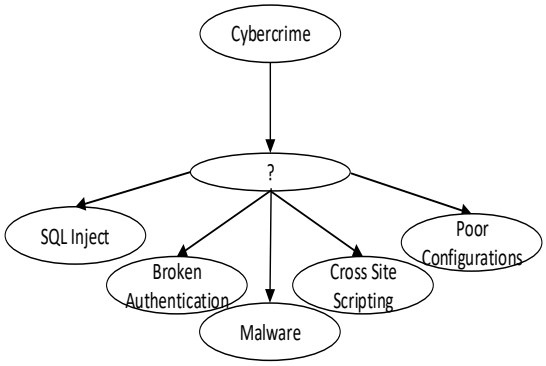


Figure 1. Relationship in the Presences of Uncertainties

The figure below depicts that lack of expert opinion and lack of attack modeling of vectors increasing the likelihood of supply chain requirements errors and consequence impact is a Cyber Physical Systems (CPS) threat landscape. To ensure secure CSC systems, BBN techniques are used to predict the lack of expert judgment and lack of attack vector modeling as the root cause of the parent nodes.

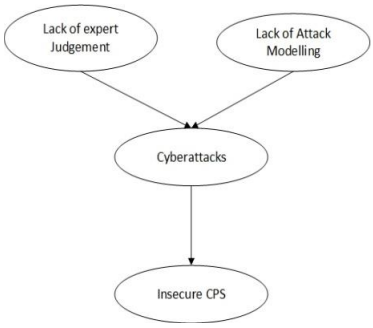


Figure 2. Bayesian Belief Network

B. Challenges of Modeling Cybercrimes

The most challenging aspect of cybercrimes is the complex nature of modeling the various threat and uncertainties. BBN allows us to model and reason about the uncertainties and forces the assessor to assume all assumptions about the impact. We factor in causes that are responsible and influence of attacks wherein serial attacks, X influences Y and Y influence Z conditionally. In Divergent attacks X influence Y and X concurrently. Then in convergent attacks X and Y includes X. We adopt the Bayes rule [19] to demonstrate how to model the uncertainties as follows.

C. Bayes Rule

In Bayes rule, joint probabilities of two events X&Y are expressed as

$$P(XY) = P(X\backslash Y)P(X) \quad 1$$

$$= P(Y\backslash X)P(Y) \quad 2$$

We assume that one of the events is the Hypothesis, H, and the other is Data D. We want to judge the relative truth of the hypothesis given the data. According to the Bayes rule, we calculate this rule using the relationship below:

$$P(H\backslash D) = \frac{P(D\backslash H)P(H)}{P(D)} \quad 3$$

The formula P(H\D) is the likelihood function and it assesses the probability of the observed data arising from the hypothesis. We will insert the value as we gather the expert data to determine the hypothesis. The P(H) represents the Prior knowledge of the subjective expect judgment before the data are considered. P(D) is obtained by integrating P(D\H)P(H) overall H. The P(H\D) is the information that reflects the probability of the hypothesis after consideration of the data.

D. The Smart Grid

The smart grid is made up of Generation, Transmission, and Distribution System. The infrastructure is made up of the backbone of the SCADA system, ITU and EIDs that connected to wireless communication network technologies that connect the physical system to the cyber physical systems. For detailed discussion refer to [9 - 11]. Out model emphasis on the cyberattacks motive and intent. We identify, three threat actor. Threat Actor 1, could attack from a remote source, threat actor 2 could attack from the vendor's system gateway, threat actor 3, could attack from the substation and threat actor for may be an internal attacker.

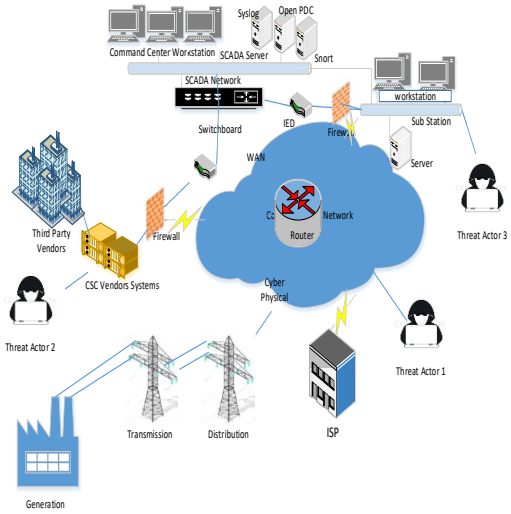


Figure 3. Smart Grid Model

E. The scenario of a Malware Attack on the CSC

An organization has purchased and installed software that is bought off the shelf on the system. The software integrates with suppliers, distributors, third party vendors and individual customers on the supply inbound and outbound chains. Unknown to the organization, malware has been inserted as a spyware program in the software that downloads itself whenever the user is prompted to update their software. Whenever, the users on the supply chain click on the download to update, steals password details that provide the threat actor access to takes advantage of user data and is able to manipulate data the CSC chain systems.

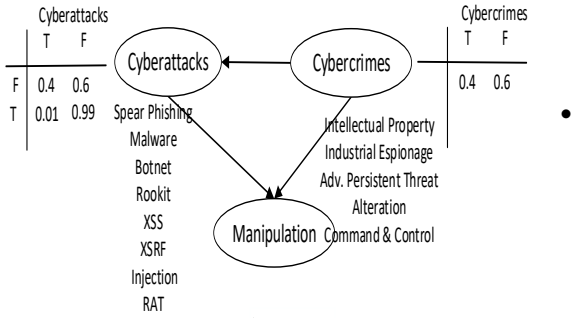
V. Modeling the Attack Using Bayesian Belief Network

In this section, we use the scenario in section IV (*E*) above to model out the attack. From the case study, two events can cause an attack on the CSC: Cyberattack and cybercrime. Cyberattacks are the physical actions malware, XSS, RAT, session high jacking against the supply chain infrastructure and system resources. Whereas, Cybercrimes are the actual crimes committed after gaining access to manipulate, delete, alter, redirect

or compromise the system and cause further exploitations including intellectual property theft, industrial espionage, and advanced persistent threats.

A. Conditional Probability Theory

Cyberattacks have a direct effect on cybercrimes, in that in an event of cybercrime, the threat actor has direct access to manipulate the CSC system. This situation can be modeled with the BBN [16] as follows. We use conditional probability theory to determine the set of discrete and mutually dependent random variables. Each variable has true (T) and false (F) values:



		Manipulation	
Cyberattacks	Cybercrimes	T	F
F	F	0.4	0.6
F	T	0.01	0.99
T	F	0.9	0.1
T	T	0.99	0.01

Figure 4. Conditional Probability Table

For our study, we, define the joint probability function as:

$$\Pr(M, A, C) = \Pr(M|A, C)\Pr(A|C)\Pr(M) \quad 4$$

Where:

- A = Cyberattack (True/False),
- C = Cybercrime (True/False)
- M = Manipulation (True/False)

We use this model to answer uncertainty questions about an event of an attack, given the event as an effect of an inverse probability. For instance we as the question:

What is the probability that there is manipulation on the CSC, given that there is a cyber attack, by using the conditional probability formula in table 1 and summing up to overall the nuisance variables?

$$\Pr(M = T|A = M) = \frac{Pr\ (M=T,\ C=T)}{\Pr(M=T)} = \frac{\sum A_{\epsilon}(T,F)}{\sum A,C_{\epsilon}(T,F)} \frac{Pr\ (M=T,\ A,C=T)}{Pr\ (M=T,\ A,T)} \quad 5$$

Using the expansion of the joint probability function Pr(M, A, C) and the conditional probabilities table in figure 4, we evaluate each term in the sums in the numerator and denominator: For example.

$$\Pr(M = T, A = T, C = T) =$$

$$\Pr(M = T|A = T, C = T)\Pr(A = T|C = T)\Pr(M,T) \quad 6$$

$$= + 0.99 \text{ x } 0.01 \text{ x } 0.2$$

The numerical results:

$$\Pr(M = T|A = M) = \frac{0.00198T\tau\tau\tau + 0.1584\tau_{\mathbf{F}}\tau}{0.00198\tau\tau\tau + 0.288\tau\tau_{\mathbf{F}} + 0.1584\tau_{\mathbf{F}}\tau + 0.0\tau_{\mathbf{FF}}} = \frac{891}{2491} = 35.77\% \quad 7$$

We ask an interventional question such as:

What is the probability that the cybercrime occurred, given that attack was initiated by an internal threat actor?

We answer to try to answer the question is directed by the previous intervention of the joint probability distribution function i.e:

$$\Pr(A, C\backslash do\ (M = T)) = \Pr(A\backslash C)P(C) \quad 8$$

To answer that: we removing the factor Pr(M\A, C) from the pre-intervention distribution obtaining by. The do operator forces the value to Manipulation (M) to be true. The probability of Cyberattack is not affected as the internal attacker does not need to attack externally.

$$\Pr(A\backslash do(M = T) = \Pr(C) \quad 9$$

To predict the impact of detecting the cyberattack, we model the probability as:

$$\Pr(C, M\backslash do(A = T)) = \Pr(C)\Pr(G\backslash C, A=T) \quad 10$$

Our result show that with the formula Pr(A = T\C) removed showing that the cyberattack affects the CSC system but not the cybercrime.

B. Malware Threat Propagation

There are so many uncertainties in the cyber attack. Therefore, for our study, we identify whether a malware attack was initiated on the CSC through manipulation during production or during distribution. The purpose of malware is to exploit vulnerable spots on the network system. We use the adversary attack, techniques and procedures (TTP) to determine the actual sources of a worm or virus and whether the cause of the attack on the CSC was initiated through malware installed or malware executed program. We equate malware installed to be from a virus, botnet, spyware or rootkit attack and malware executed to be through email phishing or spear phishing attacks.

C. Malware Installed

Malware installed are virus embedded within the host network and replicates itself within the other systems on the supply chain. When the user executes the host program infected with the virus, the virus code executes first, then the virus looks for another executable program and creates another virus, propagates to other nodes on the supply chain causing a cascading effect.

D. How Virus Replicates / Cascade

1. A computer user executes program A, which is infected with a virus.
2. The program A executes and identifies B which could be a third party vendor node.
3. After finding another executable code, program B create a new version of A infected with the virus.
4. The virus passes control to A on the supply chain to infect C and D as well.
5. The user who expects A to execute suspects nothing

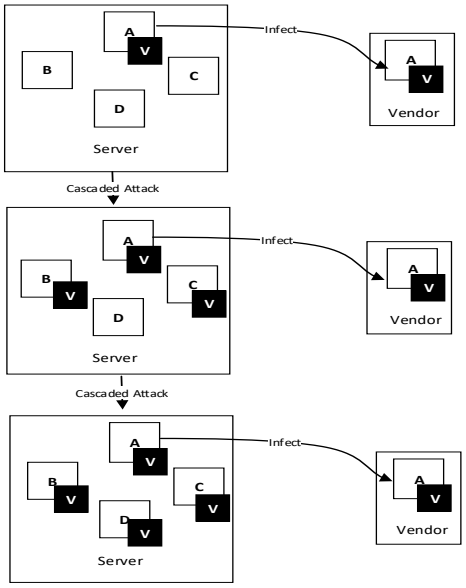


Figure 5. Malware Executable

E. Malware Executable

The malware executable is the viruses attacks sent through email phishing or spear phishing. Here, the threat actor sends an email to a targeted group (spear phishing) with a caption that may be relevant to the business process. The user unaware of the virus open and read the email with an attachment which has a virus, the virus attaches itself to the user's email address book, infect and cascade to others on the network.

1. Attacked send a spear phishing email to a targeted group on the organization supply chain
2. A user reads the email and opens the attachment which contains a virus
3. The virus executes itself and attached itself to the user's email address book
4. The virus sends emails to others containing attachments with a virus

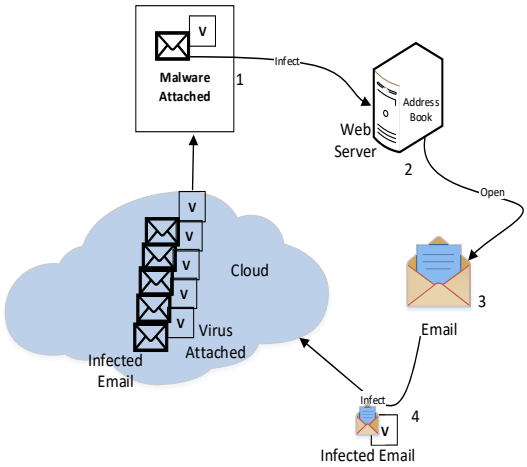


Figure 6. Malware Installed Spear Phishing Email Attack

F. Detecting Malware Propagation

In the case of a malware attack on the organization system, we follow the TTP method by analyzing and identifying the following in a CSC environment:

1. Category of malware: We analyze the CSC system to identify the course of attack whether it was Virus, Trojan, Rootkit, and Botnet as the adversary can use different methods to get to the system.
2. Sources of the malware: The source of the attack gives us an indication of the vulnerable spots that were exploited such as Spear Phishing, Redirect Script, XSS. The adversary used a spear phishing email to target his victims. Or attached malware to a website link that the customers use often so that when they visit the website it will download and provide the attacker the access.
3. The subject of the malware: The name the adversary uses in the subject to prevent the victim from suspecting them. Adversary's use catchy subjects that easily get the attention of their victims. Most victims often do not pay particular attention to the source of an email especially the managers who mostly read their emails on the go.
4. Vector: RAT attack to penetrate to the victim system. Cross-site scripting and cross (XSS) site request forgery attacks are most embedded in the victims URLs from the victims end in the case of

XSS or from the web server end in the case of (XSRF) attacks.

5. Categories of attachments and specific attachments (Malware Installed or Malware Executed): Here we analyze the attachments to determine whether the attack was a malware installed from links that were downloaded or from an email attachment that the victim opened unaware.
6. Analyze and Evaluate the Malware: We compare the extent of the malware attack to the organizational resources and that of the third party vendors in order to determine the probable risks

VI. SUMMARY

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.

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 Cyber-attack 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]. K. Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” 2016.

[5]. STIX 2.0: Assets Affected in an Incident.

[6]. C. Vellaithurai, A. Srivastava, S. Zonouz,. "CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures." *IEEE Transactions on Smart Grid*, vol. 6, no.2, 2017, pp.566-575, doi.org/10.1016/j.egypro.2017.12.405.

[7]. L. Urciuoli, T Mannosto, J Hintatsa, T Khan. “Supply Chain Cyber Security - Potential Threats” Information & Security: An International Journal. 2013. doi.org/10.11610/isjs.2940. 51-68.

[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. Touhiduzzaman, A. Hahn, and A. Srivastava. “A Diversity-based Substation Cyber Defense Strategy Utilizing the Colouring Game” IEEE Transactions ion Smart Grid. November 2018, pp 1-1, doi: 10.1109/TSG.2018.2881672.

[12]. F. Youping, L, Jingjiao, Z. Dai, P, Jei, S. Jiahan, and Z. Guo. “Supporting Sustainable maintenance of Substations under Cyber-Threats: A Power Evaluation Method of Cybersecurity Risk for Power CPS” MDPI, Sustainability 2019, 11(4), 982. doi.org/10.3390/su11040982.

[13]. D. Vose, “Risk A Analysis: A Quantitative Guide.” John Wesley & Sons Ltd. 2000.

[14]. F. V. Jensen. “Introduction to Bayesian Networks” Springer-Verlag. New York, Inc. Secaucus, NJ, USA, 1996.

[15]. S. Islam. “Software Risk Management Model – A Goal-Driven Approach. Ph.D. Thesis. 2011.

[16]. H. K. Klein and M. D. Myers. “A Set of Principles for Conducting and Evaluating Interpretative Field Studies in Information Systems.” MIS Quarterly. Vol.23 1, 1999, pp, 67-94.

[17]. W. J. Orilkowsli and J.J. Baroudi. “Studying Information Technology in Organizations: Research Approaches and Assumptions.” The Institute of Management Studies, 1991, doi: 1047-7047/91/0201/$01.25

[18]. B. A. Olshausen, Bayesian Probability Theory. 2004.

[19]. I, Ben-Gal, Bayesian Networks, in Ruggeri F, Faltin F & Kennett R, “ Encyclopedia of Statistics in Quality & Reliability. Wiley & Sons, 2007