Journal of Visual Language and Computing

journal homepage: www.ksiresearch.org/jvlc/

A Multilayer Graph Approach for Predicting Computer Network Cyber-attacks

Francesco Colace [a], Muhammad Khan [b], Marco Lombardi [a], Domenico Santaniello [a, *]

[a]DIIn University of Salerno, Italy

[a]New York University, Abu Dhabi, United Arab Emirates

ARTICLE INFO

Article History:
Submitted 8.18.2020
Revised 8.25.2020
Second Revision 10.20.2020
Accepted 11.30.2020

Keywords:
Network Security
Knowledge Management
Bayesian Network
Probabilistic Graphical Models

ABSTRACT

Today's society is heavily oriented towards digitalization, which increasingly affects the management of cities and services. This process is performed through the use of the Internet of Things (IoT) paradigm, from which arise problems related to security. In this scenario, based on the continuous exchange of information on the network, an increasingly significant role is played by systems able to guarantee data security. Protecting the modern Computer Networks could be a very complex task. In this paper, a methodology based on three graphic models (Context Dimension Tree, Ontology and Bayesian Network) is proposed. Three different models are used which use context representation and probabilistic approaches to predict cyber-attacks. The paper proposes, in fact, the use of Bayesian networks built through an ontological definition of the problem dropped on a certain context represented by a Context Dimension Tree. The proposed approach has been experimented in a real scenario providing satisfactory results.

© 2020 KSI Research

1. Introduction

Modern digitization allowed the development of increasingly smart environments capable of managing countless services designed for citizens. Nowadays, many services designed to improve users' activities are made available with the use of modern devices. This process has been made possible through the Internet of Things (IoT) paradigm [1], which represents a concept where objects and users are interconnected and exchange information through the Internet [2]. One of the particularly interesting issues of this scenario is represented by systems able to guarantee network security [3]. In particular, the security is increased through systems designed to control the network such as Intrusion Detection Systems (IDSs). IDSs are systems capable of analyzing every packet which is exchanged on the network. Those packets, containing the exchanged information, may contain possible threats that can compromise the entire network. In attempting to successfully identify cyber-attacks, these systems work through a database containing a set of rules used to identify security violations, basically comparing the content of the packets with known violation rules. However, this approach remains completely vulnerable to possible new types of attacks and cannot predict what may occur in the immediate future. Therefore, a further study of systems able to identify network attacks based not only on comparison but also on data behavior is needed.

The aim of this paper is to propose a methodology capable of recognizing and dealing with problems related to cyber-attacks, ensuring network security. The proposed methodology exploits different graphic formalisms (Ontology, Context Dimension Tree) able to represent and identify problems related to security. This approach is based not only on the comparison of known threats but also on the behavior of data on the network trying to predict potential cyber-attacks.

The paper is organized as follows: section two offers a general overview of the problem of network security with reference to related works; section three shows the proposed methodology; section four evaluates the performance of the system presented through a case study application. The article ends with the conclusions.

*Corresponding author
Email address: dsantaniello@unisa.it
Website: http://docenti.unisa.it/domenico.santaniello
ORCID: 0000-0002-5783-1847

DOI reference number: 10.18293/JVLC2020N2-006

2. Background

Internet has become a very important tool for institutions such as businesses, universities and public administration. Beyond this, the modern human being relies on the internet in many social and personal professional activities. Over the years, this type of use has given particular attention to the field of information security, in particular, the field of network security is concerned with defending networks from possible attacks, being able to recognize and classify them in order to mitigate risks that they involve. When we connect to the computer network during all our daily activities, we do it for the purpose of exchanging information. This operation, in electronic language, translates into packet exchange; however, these packets may contain malicious content that we identify with the name of malware. These malicious packets aim to establish themselves in our computer devices, extorting sensitive information and threatening the safety of the entire computer network to which the device be-longs [4]. Some of these use self-replicating technologies, therefore able to self-replicate indefinitely within a system by sending its replicas with the attempt to infect the whole system, in some cases, these malwares are designed to act without establishing any kind of explicit interaction with the user (worms). For this reason, it is important to prevent and protect not only users but also computer networks. A broad category of security threats falls into the Denial of Service (DoS) class; such attacks aim to render an IT service unusable, which, as we said earlier, can be crucial with respect to the formal fulfilment of imprints, university or public administration, which the system is called upon to perform. These types of attacks, in general, can be classified into three categories: 1) attacks on the system vulnerability, which involves sending packets to the most vulnerable system within the network; 2) Band Flooding, which involves sending a deluge of packets with the aim of obstructing the connection to the service; 3) Connection Flooding which aims to establish a large number of connections that keep the system busy, preventing connections to be established to users requesting services. Furthermore, these types of DoS attacks can be effective exploiting multiple or distributed sources, thus speaking of DDoS, increasing their danger and decreasing the possibility of detection and blocking.

In literature, several papers deal with the problem of network security in the Internet of Things or Smart City fields ([5]–[7]). A common approach is to introduce of a Framework able to analyse networks trying to manage any attacks or disruption.

Elsaeidy, in this work [8], proposes an interesting approach based on Deep Learning and user data behaviour. The aim of the approach is based on recognitions of patterns, which could predict potential cyber-attacks. In [9] is proposed an approach based on artificial intelligence techniques applied in industrial sector in order to identify any network problems or threat. The approach takes advantage of attacks trees in order to identify and design defence strategies. Moreover, in [10] the Hybrid Attack Graph (HAG) is presented, which model and combines physical and software component of attacks necessary for potential risks picture overview. Furthermore, promising results are provided in [11] where Data Mining techniques (Multilayer Perceptron, Naive Bayes and Random Forest) are used to determine the type of attack.

Starting from this general overview, and taking advantage of the literature, it seems to be possible to design an approach able to integrate semantic, probabilistic and context aware approaches in a single methodology. The approach proposed in this paper introduces a multilevel graph approach based con Ontology, Bayesian Network and Context Dimension Tree able to perform a complete and detailed analysis of the network status. Taking as reference the following articles of literature [12], [13] it was possible to create a networked ontology of security suitable for the specific problem under consideration. This tool allows us therefore to have a detailed classification of the problem with all the possible relations capable of generating the inferences useful to our approach.

Although the tree graph approach is not new in the application of this field [9], [11], the design of a specific CDT represents a novel approach to the problem. This tool is able to represent and manage all the possible contexts of the application do-main dealt with. Moreover, thanks to the combined use with ontology it is possible to apply the proposed methodology.

2.1 Intrusion Detection Systems

According to the previous paragraph, to make a computer network secure, we need to check all the packets we have exchanged. We therefore need a device that not only examines packet headers (such as a firewall, for example) but also performs a thorough and detailed check of the packet. Intrusion detection system (IDS), these systems are suspect-driven. Through them, it is possible, possibly, to prevent access to these packets [14]. These systems are used to detect a wide range of attacks, including network mapping, port scans, DoS and DDoS attacks, worms and viruses, application vulnerability attacks. Today thousands of organizations exploit this type of system in their institutional networks, acting as sensors that work together exchanging information between each other and communicating to the network administrator any suspicious activity. In general, IDS systems are classified as signature-based or anomaly-based systems. IDS based on signatures, has a database of attack signatures, which represents the set of rules concerning an intrusion activity. Operationally, this type of system checks each packet that passes through it, comparing it with the signatures in its database.

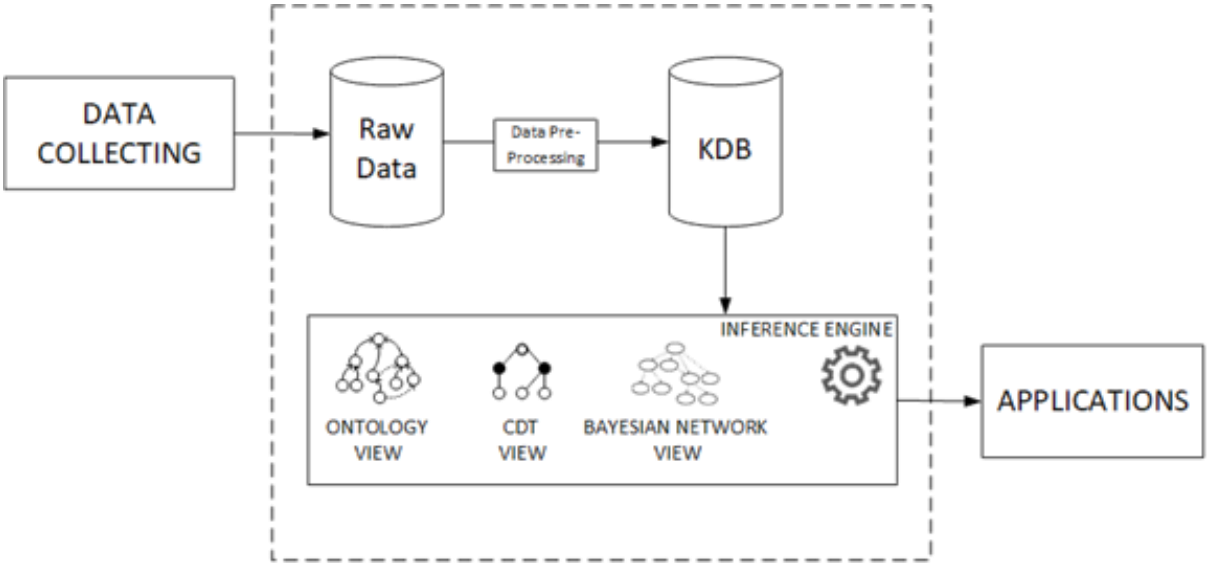

Figure 1: The System Architecture.

IDS based on anomalies, on the other hand, collects traffic information trying to find anomalous flows. In light of this, the study of a methodology that could assist these security systems, thus able to recognize possible threats, suggest possible mitigation interventions and possibly foresee such phenomena based on the context, becomes necessary to protect the computer networks and their users.

3. The Proposed Approach

In consideration of the preceding points, the proposed methodology is designed to be a predictive approach capable of adapting to the context. This approach is useful in various fields [15]–[17]. In particular, this article presents an application of the proposed methodology in the field of cyber-attacks. Three graph approaches such as Ontology, CDT and Bayesian Network are exploited to detect and predict the occurrence of events malicious to the network that would compromise the service and security for users. Bayesian Networks are particularly useful in the attempt to predict specific events [18], moreover, they are able to interface adequately with other graph approaches. The CDT is a tree able to manage and customize information present in all possible contexts [19]. Furthermore, Ontologies are used for the representation of reality, being particularly useful and interfaceable with the other two graph approaches used [20]–[22].

According to the proposed approach, the two graph approaches, responsible for the representation of the context (CDT and Ontology), can be combined in order to obtain a list of constraints useful for the design of the Bayesian Networks. In detail, a recognition of all possible context combinations can be made through the CDT. These combinations of contexts are useful for extracting relationships through the various nodes represented through the Ontology view. The relationships extracted from the Ontological view can be transformed into useful constraints for the construction of the structure of the Bayesian Network, which will be improved through knowledge of the context.

The figure 1 shows the system architecture, which, by collecting raw data, uses them to return the appropriate usage application. In the first phase there is the collection of data from the IDS and other sensors allocated in the computer network, which are stored raw. These data are harmonized and sorted in the pre-processing phase and stored in a database that powers the inference engine. Inside the inferential engine are the three graph views previously described (CDTs, Ontologies and Bayesian Networks) which provide an interpretation of the knowledge acquired and collected in Knowledge Database (KDB).

In practice, the detection of malicious attacks, given a certain context, could be done through the described architecture that exploits the right information characterized by innovative elements based on formal context representation, knowledge management organization and inferential engines.

Information management systems require particular attention to the efficiency of data organization. In this regard, Ontologies represent a particularly suitable means for the organization and reuse of shared and collaborative knowledge, bringing advantages in terms of overall system efficiency [23]. The proposed system makes use of Context Awareness, wants to be able to manage real-time contextual information that could bring improvements in the identification and predictive capacity of the system. The CDT is a tree with the ability to represents all possible contexts, composed of a root node, a set of leaf nodes interconnected each other. The CDT's nodes are divided in 1) Black Nodes,

which represents the dimension nodes of the domain; 2) White Nodes or concept nodes, which contains all dimensions values. A Context is specified as an "and" among different context elements where each element is defined as an assignment dimension_namei = value: several context elements, combined with each other, give rise to a context [24]. The proposed approach, moreover, takes advantage of probabilistic approach through Bayesian Networks, which are used to compute and update the probability of a given event taking advantage of Bayes' Theorem.

4. Experimental Results

The purpose of this section is to illustrate the experimental application of the proposed methodology to a real case. The methodology proposed, as previously mentioned, combines three approaches to graph (CDT, Ontology and BN) in order to provide answers in terms of forecasting events; in particular, in this experimental case the events refer to network attacks. The proposed approach is able to combine the CDT and Ontology views to extrapolate the conceptual relationships, these relationships are transformed into constraints and are used to service the construction of the Bayesian Network. By means of this graph, which contains all the relations and the relative weights between the available data, it is possible to predict the occurrence of an event as the boundary conditions vary.

The experimental phase was conducted through the use of a dataset containing data from Intrusion Detection Systems at the service of a university computer network. The dataset contains over twenty thousand instances and represents a reduced set of the monitoring database at service since 2008.In particular, the dataset used contains over two thousand attempts to attack, of which only about 5% succeeded in penetrate the computer network. To perform the analysis of the proposed approach it was necessary to divide the dataset into training set (90%) and testing set (10%), this subdivision was made taking into account a balance between number and type of events and periods of intense information communication technologies activities. The training set is fundamental during the learning phase of the network structure, instead, through the test set, the network is validated verifying if it is able to correctly classify the events present in the test set. For the purposes of validating the model, an automatic network learning algorithm was chosen, and a comparison was made between two cases. The first case, which involves the use of the learning algorithm only to define the network structure, and the second case that use the proposed methodology, which combines the same automatic learning algorithm with a list of constraints coming from the combination of CDT and the Ontological view as described above. The machine-learning algorithm chosen is Hill Climbing with score K2 [25], which, among the various selected algorithms, has provided greater feedback in terms of Overall Accuracy in reference to our case study. The results obtained from the experimental case are shown in terms of Overall Confusion Matrix Accuracy Precision and Recall. The confusion matrix is a useful tool for representing the accuracy of statistical classification, through this matrix it is possible to have an overall view of the classification ability of the Bayesian Network built, furthermore it is possible to calculate several coefficients that help us to understand reliability of the Bayes Network. The coefficients used are the Accuracy which represents the proportion of events correctly classified with respect to all events, the Precision which can be seen as a measure of accuracy or fidelity of the forecasts and the Recall which can be seen as a measure of completeness.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

The analysis was carried out on a dataset of data from Intrusion Detection System monitoring a university network. Among the many data available, the following types of network attacks were selected:

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- Spear Phishing (SPh)
- Web Deface (WD)
- Password Harvesting (PH)

The aim of this experimentation phase, therefore, was to foresee such attacks, first through a network trained through a selected learning algorithm, and subsequently using the proposed methodology.

As shown in Table 1, the confusion matrix of the first case refers to the matrix learned by means of the selected learning algorithm. Through this algorithm, it was possible to obtain a network, which is able to correctly classify some events, in particular many DoS attacks. The obtained matrix does not show excellent results in terms of Overall Accuracy (Table 1) and in terms of Precision and Recall (Table 3).

Table 1: Confusion Matrix Case1.

		Reference				
		DDoS	DoS	WD	SPh	PH
Prediction	DDoS	189	87	25	21	79
	DoS	77	254	14	65	78
	WD	23	94	280	46	45
	SPh	45	32	42	172	88
	PH	13	96	42	31	209

Overall Accuracy : 51,42%

The Table 2 shows the confusion matrix obtained from the Bayesian Network Structure designed by the proposed approach. In fact, compared to previous case

(Table1), there is an increasing of the number of correctly classified events and a decreasing of incorrectly classified events.

Table 2: Confusion Matrix Case2.

		Reference				
		DDoS	DoS	WD	SPh	PH
Prediction	DDoS	358	62	14	11	37
	DoS	57	419	20	18	36
	WD	18	41	348	39	24
	SPh	33	12	24	216	19
	PH	7	18	4	23	289

Overall Accuracy : 75,92%

This improvement can be seen in the increase of Overall Accuracy, which exceeds 75%, and as witnessed in Table 3 a significant increase compared to the previous case in terms of Precision and Recall.

Table 3: Precision and Recall Parameters Case1 and Case2.

		DDoS	DoS	WD	SPh	PH
Case 1	Precision	47,13%	52,05%	57,38%	45,38%	53,45%
	Recall	54,47%	45,11%	69,48%	51,34%	41,89%
Case 2	Precision	74,27%	76,18%	74,04%	71,05%	84,75%
	Recall	75,69%	75,91%	84,88%	70,36%	71,36%

The value of about 76% of Overall Accuracy may seem a reasonable result, nevertheless, compared to the performance of modern machine learning algorithms, it is not a great result in absolute terms of forecasting. However, another aspect related to the proposed methodology can be analysed, which can be fundamental in the attempt to classify the attacks that actually have been successful. This aspect was analysed by testing the Bayesian Network, which was learned through the use of the proposed methodology, through an ad hoc test dataset, which contains only the cyber-attacks that penetrated the computer network. In this case, as can be seen in Figure 2, the system was able to correctly classify over 60% of the events. The result obtained was achieved through the system's ability to understand the context by classifying events, unlike traditional control tools, according to data behaviour. This aspect suggests to us that the capacity of the adopted methodology can be fundamental in further reducing the percentage of network attacks that have been successful in the attack of the networks, intervening especially where the traditional control system does not recognize the packets as possible attacks.

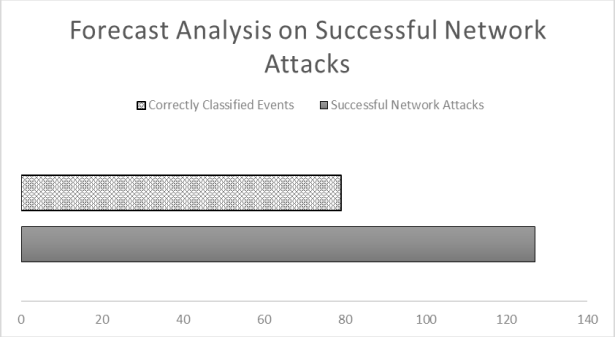

Figure 2: Forecast Analysis on Successful Network Attacks.

5. Conclusions

This paper aimed to introduce and analyse the performance of a multi-level graph methodology for cyber-attacks predictions. To perform the analysis was used a dataset of Intrusion Detection Systems, which monitor the computer network at the service of a university institution. The dataset includes over two thousand attack attempts, of which about 5% defeat the computer network security systems. The analysis was conducted using part of dataset to build the Bayesian Network structure, which was tested with the remaining part of data. Therefore, was compared the performance of the Bayesian Network structure built through a machine learning algorithm and the Bayesian Network structure built through the proposed methodology. Furthermore, is evaluated the performance of Bayesian Network structure learned through the proposed methodology in predict the cyber-attack events that defeated the security systems of the networks.

According to the confusion matrices (Table 1 and Table 2) and the results in terms of Prediction and Recall (Table 3), the proposed system, compared to a traditional structural learning algorithm, has been able to provide good performance in terms of Overall Accuracy, Prediction and Recall. The results seem not enough in absolute classification terms; however, the system strength lies in using graph approaches, which provide a better description of the problem allowing prediction and classifying of events based on data behaviour. In fact, the structure of the network learned in the second case, that is through our approach, despite having obtained only about 76% of accuracy, when it was tested with a dataset containing only the attacks on the computer network that actually penetrated the system, is was able to correctly classify over 60% of these events (Figure 2).

From the analysis of the experimental data, it is clear that the proposed system does not want to a replacement of the modern Intrusion Detection Systems but can be adequately able to support them. In particular, the capacity of the proposed system lies in intervening against unknown cyber-attacks that could compromise the security of the computer network. The main advantages that can lead the proposed system to

improve its efficiency are two: the amount of data and the use of graph formalisms. In particular, as the number of data increases, the system is able to build Bayesian Network structures more reliable and able to provide more accurate results. The use of graph formalisms of the proposed approach, such as Ontologies, enable our system to communicate with other similar systems, exchanging useful information and knowledge that could lead the system to a continuous improvement.

References

[1] K. Ashton, "That 'Internet of Things' Thing," *RFiD J.*, 2009 DOI:10.1016/j.amjcard.2013.11.014.

[2] M. Carratu, M. Ferro, A. Pietrosanto, P. Sommella, and V. Paciello, "A Smart Wireless Sensor Network for PM10 Measurement," in *2019 IEEE International Symposium on Measurements and Networking, M and N 2019 - Proceedings*, 2019 DOI:10.1109/IWMN.2019.8805015.

[3] A. Castiglione, F. Palmieri, F. Colace, M. Lombardi, D. Santaniello, and G. D'Aniello, "Securing the internet of vehicles through lightweight block ciphers," *Pattern Recognit. Lett.*, 2020 DOI:10.1016/j.patrec.2020.04.038.

[4] J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, *Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security)*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2004.

[5] A. Essa, T. Al-Shoura, A. Al Nabulsi, A. R. Al-Ali, and F. Aloul, "Cyber Physical Sensors System Security: Threats, Vulnerabilities, and Solutions," in *2018 2nd International Conference on Smart Grid and Smart Cities (ICSGSC)*, 2018, pp. 62–67 DOI:10.1109/ICSGSC.2018.8541316.

[6] S. Chakrabarty and D. W. Engels, "A secure IoT architecture for Smart Cities," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, 2016, pp. 812–813 DOI:10.1109/CCNC.2016.7444889.

[7] J. Pacheco and S. Hariri, "IoT Security Framework for Smart Cyber Infrastructures," in *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*, 2016, pp. 242–247 DOI:10.1109/FAS-W.2016.58.

[8] [A. Elsaeidy, I. Elgendi, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "A smart city cyber security platform for narrowband networks," in *2017 27th International Telecommunication Networks and Applications Conference, ITNAC 2017*, 2017, vol. 2017-Janua, pp. 1–6 DOI:10.1109/ATNAC.2017.8215388.

[9] G. Falco, A. Viswanathan, C. Caldera, and H. Shrobe, "A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities," *IEEE Access*, vol. 6, pp. 48360–48373, 2018 DOI:10.1109/ACCESS.2018.2867556.

[10] P. J. Hawrylak, M. Haney, M. Papa, and J. Hale, "Using hybrid attack graphs to model cyber-physical attacks in the Smart Grid," in *Proceedings - 2012 5th International Symposium on Resilient Control Systems, ISRCS 2012*, 2012, pp. 161–164 DOI:10.1109/ISRCS.2012.6309311.

[11] M. Alkasassbeh, G. Al-Naymat, A. B. Hassanat, and M. Almseidin, "Detecting distributed denial of service attacks using data mining techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 1, 2016.

[12] M. Iannacone, S. Bohn, G. Nakamura, J. Gerth, K. Huffer, R. Bridges, E. Ferragut, and J. Goodall, "Developing an Ontology for Cyber Security Knowledge Graphs," in *Proceedings of the 10th Annual Cyber and Information Security Research Conference on - CISR '15*, 2015, pp. 1–4 DOI:10.1145/2746266.2746278.

[13] A. Oltramari, L. F. Cranor, R. J. Walls, and P. McDaniel, "Building an ontology of cyber security," in *CEUR Workshop Proceedings*, 2014.

[14] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 16–24, Jan. 2013 DOI:10.1016/J.JNCA.2012.09.004.

[15] F. Clarizia, F. Colace, M. De Santo, M. Lombardi, F. Pascale, D. Santaniello, and A. Tuker, "A multilevel graph approach for rainfall forecasting: A preliminary study case on London area," *Concurr. Comput. Pract. Exp.*, vol. 32, no. 8, Apr. 2020 DOI:10.1002/cpe.5289.

[16] F. Colace, M. Lombardi, F. Pascale, D. Santaniello, A. Tucker, and P. Villani, "MuG : A Multilevel Graph Representation for Big Data Interpretation," in *IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems*, 2018, pp. 1410–1415 DOI:10.1109/HPCC/SmartCity/DSS.2018.00233.

[17] F. Clarizia, F. Colace, M. Lombardi, F. Pascale, and D. Santaniello, "A Multilevel Graph Approach for Road Accidents Data Interpretation," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11161 LNCS, 2018, pp. 303–316 DOI:10.1007/978-3-030-01689-0_24.

[18] P. Weber, G. Medina-Oliva, C. Simon, and B. Iung, "Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas," *Engineering Applications of Artificial Intelligence*. 2012 DOI:10.1016/j.engappai.2010.06.002.

[19] M. Casillo, F. Clarizia, G. D'Aniello, M. De Santo, M. Lombardi, and D. Santaniello, "CHAT-Bot: a Cultural Heritage Aware Teller-Bot for supporting touristic experiences," *Pattern Recognit. Lett.*, Jan. 2020 DOI:10.1016/j.patrec.2020.01.003.

[20] H. Chen, T. Finin, and A. Joshi, "An ontology for context-aware pervasive computing environments," *Knowl. Eng. Rev.*, vol. 18, no. 3, pp. 197–207, 2003.

[21] E. M. Helsper and L. C. Van Der Gaag, "Building Bayesian networks through ontologies," *ECAI2002, Proc. 15th Eur. Conf. Artif. Intell.*, pp. 680–684, 2002.

[22] F. Colace and M. De Santo, "Ontology for E-learning: A Bayesian approach," *IEEE Trans. Educ.*, vol. 53, no. 2, pp. 223–233, 2010.

[23] F. Colace, M. Lombardi, F. Pascale, and D. Santaniello, "A Multilevel Graph Representation for Big Data Interpretation in Real Scenarios," in *Proceedings - 2018 3rd International Conference on System Reliability and Safety, ICSRS 2018*, 2019 DOI:10.1109/ICSRS.2018.8688834.

[24] M. Casillo, F. Clarizia, F. Colace, M. Lombardi, F. Pascale, and D. Santaniello, "An Approach for Recommending Contextualized Services in e-Tourism," *Information*, vol. 10, no. 5, p. 180, May 2019 DOI:10.3390/info10050180.

[25] G. F. Cooper and E. Herskovits, "A Bayesian Method for the Induction of Probabilistic Networks from Data," *Mach. Learn.*, 1992 DOI:10.1023/A:1022649401552.