Atlantis Highlights in Engineering (AHE), volume 2
International Conference on Industrial Enterprise and System Engineering (IcoIESE 2018)

Self-Adaptive Cybersecurity System

Aradea [1)], Iping Supriana [2)], Kridanto Surendro [3)]
[1, 2, 3)] School of Electrical Engineering and Informatics
Bandung Institute of Technology
Bandung, Indonesia
aradea@unsil.ac.id [1)], iping@informatika.org [2)],
endro@informatika.org [3)]

Husni Mubarok [4)]
[4)] Department of Informatics Engineering
Faculty of Engineering, Siliwangi University
Tasikmalaya, Indonesia
husni.mubarok@unsil.ac.id[4)]

Irfan Darmawan [5)]
Department of Information System
Faculty of Industrial Engineering
Telkom University Bandung, Indonesia
Irfandarmawan@telkomuniversity.ac.id [5)]

***Abstract* - Complexity of cyberspace environment nowadays, arouse security vulnerabilities for all owned assets. Appropriate way out or solution for every obstacle in a case like this is a must for ICT role. However, user trust for ICT usage raises concerns. Cyberspace environment is caused by rapid increase in cybercrime, continually, and always forming new way or kind of the offense. This paper underlining the importance of developing cybersecurity capability that not only be prepared to anticipate short-term needs but the issue of the growth of cybercrime is a significant concern that was anticipated. Key strategies used is the concept of self-adaptive formulated through the model representations goal, with control strategies that can guide us in understanding the domain and identify possible changes and growth. Modeling results showed cybersecurity system development strategy taking into account the breadth of factors so that it can anticipate future requirements.**

Keywords—Self-adaptive software; cybersecurity; goal based; control strategy

I. INTRODUCTION

Utilization of ICT system at this time faced to environment complexity. Where the environmental condition is dynamic, open and unpredictable, raising a variety of vulnerabilities to security. Even based on a research study [1], some users have been reluctant and do not believe in the benefits of ICT, although the various research community has made the number of works and efforts, government agencies, the private sector, and industry to create ICT security solutions. This is because every day we can witness the growth of a variety of information related to new cyber attacks, theft, threats and potential cybercrime, whether through print and electronic media.

According to above depiction, we saw that cybercrime activities would grow continuously day per day. So that this problem related to issues [2] that correspond to the requirement of automation, autonomy, flexibility, scalability, agility, speed, and so on. This corresponds to how the system can adapt to various possibilities of cybercrime activities, which continuously grow and thrive. This condition implying that handling of ICT system behavior is not enough prepared in anticipate cybercrime only for an operational system, but planning for control its growth [3] can become a key factor for the success of ICT system. Here we emphasize the importance of setting a perspective that can guide us in understanding the domain and identify possible changes [4] and growth. So that the ICT system developed has the knowledge services [5], and can meet the scope of the life cycle of the scheme as a whole.

This paper proposes an approach to domain model construction, that handled by control strategy to anticipate various of changing and its growth. Part II in this article depict about the cybersecurity system. Part III explains about proposed model, Part IV discussion about related works, and Part V is the conclusion.

II. CYBERSECURITY SYSTEM

Cyberspace defined [6], as a virtual environment that concentrates on various infrastructure, technology devices, and people who connected to the network, so that bring forth an evolution concept of information security of cybersecurity. This is including a small network such as home network, a big network of industry, national network, provider communication, and so on. Therefore, this condition remains risk and threat that exist for cyberspace and will be related to potential cyber-attacks, cyber-espionage, cyber-terrorism, cyber-bullying, hacktivism, etcetera.

Based on a survey and at cyberspace domain, in England [7], conducted from November 2015 to February 2016 and involve about 1008 companies, the result showed 69% says cybersecurity has very high priority (33%) or high enough (37%) for senior management. Various qualitative findings highlight the variety of factors that have helped the company to understand the importance of the cyber city. However, they do not fully understand how the company can be at risk and what action should be taken. Only half of all company (51%) that made an effort to identify risk related to cybersecurity and this just occurs among middle companies (78%) and large enterprises (94%). Many companies have a various form of rules or controls for cybersecurity, even though still under the

best-practice standard, and only 13% that determines the minimum level of cybersecurity to their supplier.

Violation of cybersecurity influencing all kind of business and spending expensive cost. One-quarter (24%) of all business detect one or more violation of cyber safety in the last 12 months. This occurs higher in middle companies (51%) and at large corporations (65%). The large corporations are also more frequently targeted, 25% of them had experienced a breach at least once a month. The most common types of violations that are suffered by a virus, spyware or malware (68%), and offenses involving imitation/impersonation of organizations (32%).

Estimated average cost of all offenses during the past 12 months is £ 3,480 and is much higher for large enterprises, namely £ 36,500. Estimated average cost of the most severe violations of the previous 12 months, is £ 2,620 in the whole business, and £ 32,300 for large companies. Breaches of the most expensive of the findings of this survey are to reach a cost of £ 3 million. Cases like this indicate that cybersecurity violation occurs on an ongoing basis and continues to grow, it has consequences for the financial companies are substantial and dangerous for survival. Therefore, in this case, essential to establish a series of measures to prevent and protect themselves from various kinds of cybercrime.

III. SELF-ADAPTIVE CYBERSECURITY

Based on the result the of a previous study [8], the self-adaptive model developed on different system needs. In response to a various change of system its self and its environment. This is related to a character like self-managing, self-configuring, self-healing, self-optimizing, self-protecting, and self-* [9]. Cybersecurity needs basically will correspond to several abilities of the character, and here we propose a model that can be implemented to anticipate not only change the needs but the handling of cybersecurity growth activities, also become our most significant attention.

A. Model Configuration

System environment configured as a model goal, where every goal and its subgoal represent the purpose of every system entity. The defined goal will have a plan, and every plan has dependency connection with a goal, resource, or another purpose component. So that if one plan has uncertainty, then all plan that corresponds to dependency with the scheme, values of every property, need to be observed.

Figure 1 shows a conceptual model is proposed. On the domain model the goal can be decomposed (AND/OR) into subgoals. It can be identified requirements (R-1, R-2, Rn) of each goal that effect on certain parameters, and have a positive or negative contribution (++ / + or - / -) to one or more soft goals (non-functional). In the control model, the property (P-1, P-2, P-n) of each of these targets are identified and transformed into system components, as well as observations on the possible amendment. Further analysis through control strategies, and determine which variation of adaptation by the determination rule is defined as a plan (Plan Sets-1, Plan Sets-2, Plan Sets-n). A more detailed description can be seen in our previous paper [10] [11] [12].

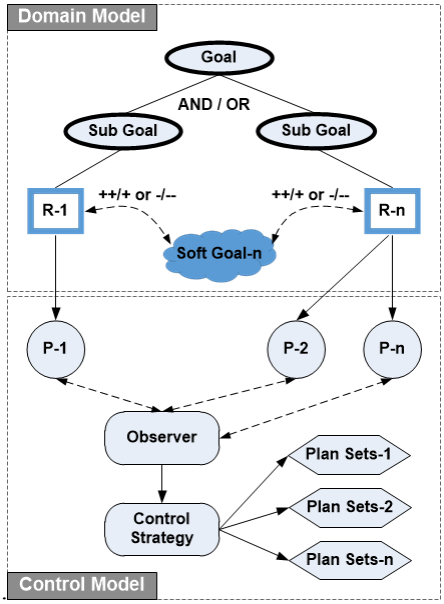


Figure 1. Conceptual model.

The control model is system behavior handling, that is the observed environment and self-adapted if needed, such as through reconfiguring when a change occurs, self-optimize when operation switch, handle the certain error, and so on. There is two principal component in this model, inference engine, and rule base. The model formulated through the rule-based system with knowledge structure base that constructed as generic and smooth, so can handle knowledge growth that represents various context and system behavior. Each additional or change of specification can be done with edit knowledge base through rule editor.

Based on the specification of model goal that becomes a system input, the system the will determine model domain that derived from the generic structure and configures the system that executed by the actuator. If necessary, a new feature on the system to be developed, but the system does not provide the feature, developers can make use of the rules and adjust module. Details of the mechanism of this model can be seen in our previous paper [13] [14] [15].

B. System Modeling

Cybersecurity system modeling, begin with identifying each entity of system and its goal, so resource and processes can be determined, including relation each other. As illustration case, we use cybersecurity entity that proposed [6], consist of the public sector, the private sector, critical infrastructure, citizen, and attacker. Then each process from the entity connected to an interface that will be system executor. Next step is each system component that has been defining, mapped into a tree structure of knowledge, as can be seen in Figure 2. The interface element is represented as an actor of the tree; here

knowledge structure prepared to anticipate requirement growth of actor, both internal actor or external actor. While entity element of the system represented as entity tree, where knowledge structure that constructed aim to anticipate change and growth of activity process of cybersecurity.

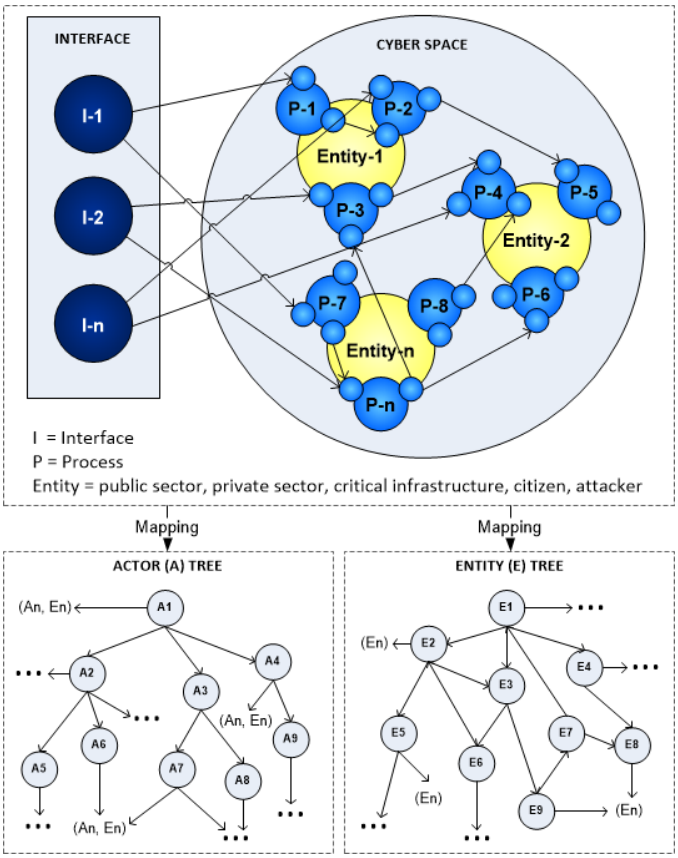


Figure 2. Modeling of actor and entity of cybersecurity

The tree structure of actor and entity tree, automatically will add, delete, update and confirm each its node, as a response from condition change, both from the internal system or external system or from the environment. As illustration, actor tree will be related to change and growth of citizen actor or attacker, such as personal, government, the private sector, industry, etcetera. While entity tree will be related to change and growth of each process activity of system entity, both private or public sector. So that, based on knowledge tree structure formula, can be defined change and growth of each process activity of cybersecurity.

Based on the model at Figure 2, it can be determined by a model goal for cybersecurity need, such as shown in Figure 3. The main aim of the system with a soft goal is to increase safety; The goal can be reached through decomposition into three subgoals, namely; a user interface, asset protection, and threat detection. Detect context-1 is a plan to detect citizen, consist of group actor that can access cyberspace system. Developed strategy in here is to detect each suitability of its properties value, such as device and role. Detect context-2 is a plan to fulfill the goal of asset protection, consist of security target for public sector (public entity and government institution) and private sector (small business group, middle, and large) that related to resources of critical infrastructure. Detect context-3 is a plan to threat detection that coming from each attacker (person or system that is trying to access, attack and demolition cyberspace system).

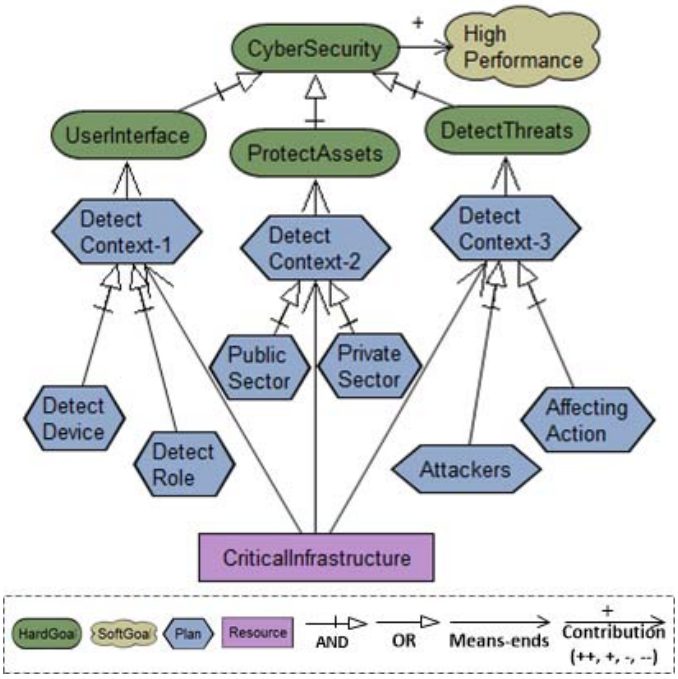
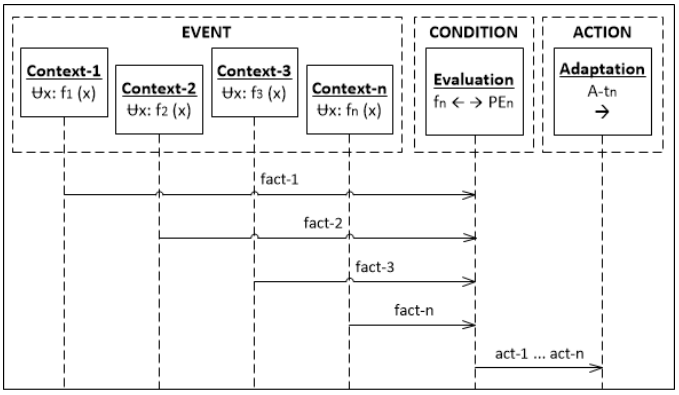


Figure 3. Goal model of cybersecurity system

Figure 4 shows the mechanism of self-adaptive systems cybersecurity, starting with event capturing system performance stemming from the fact ($\Sigma = f_1, f_2 \ldots f_n$) context information environment. Each context is associated with the specification of new facts from context-1 detect, detect context-2, and detect context-3. Condition evaluate the state refers to a particular event that occurred, including the capture characteristics of the attacks that took place in every context ($Q = fn \leftarrow \rightarrow Pen$). Evaluation is done reconfigure based policy engine (PE) to select the most appropriate action behavior. Policy This engine provides high-level goals that control the operation and functions of related systems. The general form is event-condition-action (ECA) rules to determine the action when the event is raised, and there is some certain condition is met.



Gambar 4. Dynamic adaptation behavior of cybersecurity system

The policy engine is represented as a knowledge base, that provides an interface for a system an administrator to determine and change system policy. In our version, this model enlarged with rule model editor, where addition or change specification can be done with editing knowledge base directly or re-input to the system. According to that evaluation, adaptation action (δ = A-ta$_n$) is committed, namely asset protection at a certain time (t) with consideration of assessment toward occurring of each event. The adaptation action is dealing with authorization of cyberspace service, where the authorization evaluated based on control to the growth the of knowledge tree because knowledge tree will always continue to grow and drive based on new facts that captured from every information context.

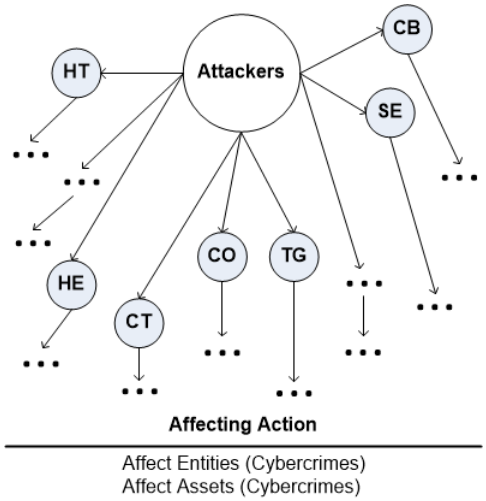


Figure 5. Attacker growth.

Figure 5. shows an example of growth specification of knowledge tree for the attacker. Achievement of detection threat goal will be accomplished by plan detect context-3, on an ongoing basis will have a growing knowledge. For example, an entity attacker will affect the other entity or its assets. Any form of attack can be detected by category, for instance [6] hacktivist (HT), hackers (HE), contractor (CT), Criminal organization (CO), a terrorist group (TG), competing businesses (CB), sabotaging employee (SE), and can continue to grow depends on the facts captured context information. In this case, the tree of knowledge actor Attackers will continue to grow and will be stored in the policy engine as input material for evaluation in determining the choice of adaptation actions cybersecurity.

If viewed from the point of view of the system reliability, so the proposed model has the principle of maintainability. The system may change when necessary and continue to improve its availability because system entity has the ability to update its knowledge as an intelligent system. This shows the level of the system reliability that continues to increase based on dynamic environmental conditions. As a future agenda, we will conduct quality testing in more detail and technically related to the ability of the system to maintain its performance level when used in various conditions, whether viewed from the characteristics of maturity, fault tolerance, and recoverability

IV. RELATED WORK

Various efforts have been made by researchers to provide a solution to the problem of the safety of a system, including Giorgini et al. [16] proposed a model of security goals that extend the model goal Tropos [17] through the concept of trusts model of relations among social actors. Mouratidis et al. [18] also propose the integration of security in cycle models and UML diagrams goal, with a view of socio-technical systems (STS), the same thing is done by Ali et al. [19] with the addition of security models to analyze the requirements of a variety of contexts. Tong Li et al. [20] introduce a holistic approach to security, new patterns, and models as a contextual model of goal attack. Atom et al. [21] proposed a framework for implementing cybersecurity through performance measurement.

The researchers adopted a similar approach to the proposed model, namely through a model approach goal to represent the domain model, but here we extend it through the concept of control strategies are formulated more flexible, so that changes and growth in cybersecurity systems can be accommodated more easily.

Additionally, Florez et al. [6] proposes a model for the analysis of the complexity of the dynamic ecosystem of cybersecurity, and produce models for a strategy of software components. While Mlakic et al., [22] introduced the method of expert systems are formulated through a fuzzy logic approach and serve to determine the appropriate response time in the event of cyber-attacks. Both researchers are proposing a computational model to determine the decision in the selection of candidate solutions to meet the characteristics of the cybersecurity, but related domain model that represents the problem domain as a system requirements have not been

covered. On this occasion, the model we will propose is to integrate the computational model into the modeling requirements so that we have the advantages of both.

Based on the description, the proposed model has coverage from two points of view, namely modeling angle for model domain represented by goal-oriented requirements engineering (GORE) approach, and computational point of view for control model represented by knowledge-based systems approach (KBS) through a specially designed control strategy. So as a step forward to meet the needs of comparison in more detail, we plan to establish one of the previous works that can be considered to meet both points of view.

V. CONCLUSION

The advantage of ICT in cybercrime very depends on its capability to understand and anticipate growth of form and kind of offenses, which constantly appears. It can foster the confidence of user to the benefits of ICT. In this paper, the self-adaptive model proposed with emphasizing of importance to understand and capture variability context and system behavior through domain goal modeling, and need of strategy control that handle solution scope more broad and smooth. We believe the proposed model can give contribution for cybersecurity domain, where the view of cybercrime must see based on life cycle of a system that continuously grows and thrives.

REFERENCES

[1] F. G. Marmol, M.G. Perez, and G. M. Perez, "I do not trust ICT: Research challenges in cybersecurity," Conference: The 10th IFIP WG 11.11 International Conference on Trust Management, At Darmstadt, Germany, Volume: 473, July 2016.

[2] I. Supriana, and Aradea, “Automatically relation modeling on the spatial relationship as self-adaptation ability,” Proceeding of International Conference on Advanced Informatics: Concept, Theory, Application (ICAICTA), IEEE, Thailand, 2015.

[3] Aradea, I. Supriana, K. Surendro, “An overview of multi agent system approach in knowledge management model,” International Conference on Information Technology Systems and Innovation, IEEE, ITB, 2014.

[4] Aradea, I. Supriana, dan K. Surendro, “Prinsip paradigma agen Dalam menjamin keberlangsungan hidup sistem,” Prosiding Konferensi Nasional Sistem Informasi (KNSI), ITB-Universitas Klabat, 2015.

[5] Aradea, I. Supriana, dan K. Surendro, “Konsepsi data dan informasi sebagai penyedia layanan pengetahuan,” Prosiding Konferensi Nasional Sistem Informasi (KNSI), ITB-Universitas Klabat, 2015.

[6] A. Florez, L. Serrano, U. Gómez, L. Suarez, A. Villarraga, and H. Rodríguez, "Analysis of dynamic complexity of the cybersecurity ecosystem of Colombia," Journal of Future Internet 8(3):33, July 2016.

[7] R. Klahr, S. Amili, J.N. Shah, M. Button, and V. Wang, "Cybersecurity Breaches Survey 2016” Main Report, Ipsos MORI Social Research Institute, Institute for Criminal Justice Studies, University of Portsmouth, © Department for Culture, Media & Sport, 2016.

[8] Aradea, I. Supriana, K. Surendro, "Roadmap dan Area Penelitian Self-Adaptive Systems," Prosiding Seminar Nasional Teknik Informatika dan Sistem Informasi (SeTISI), ISBN: 978-602-72127-1-8, FTI Universitas Maranatha Bandung, 9 April 2015.

[9] N. A. Qureshi and A. Perini, “Engineering adaptive requirements,” ICSE Workshop on Software Engineering for Adaptive and Self-Managing Systems, Vancouver, BC, Canada, May 18-19, 2009.

[10] Aradea, I. Supriana, K. Surendro, and I. Darmawan, "Variety of approaches in self-adaptation requirements: a case study," International Conference on Soft Computing and Data Mining (SCDM), Springer, Tel-U, Bandung, August 18-20, 2016.

[11] Aradea, I. Supriana, K. Surendro, and I. Darmawan, "Integration of self-adaptation approach on requirements modeling," International Conference on Soft Computing and Data Mining (SCDM), Springer, Tel-U, Bandung, August 18-20, 2016.

[12] Aradea, I. Supriana, dan K. Surendro, "Pemodelan requirements dalam mengkonstruksi perangkat lunak self-adaptive," Jurnal Ilmiah Teknologi Informasi Terapan (JITTER), Volume II, No.2, ISSN: 2407-3911, Universitas Widyatama, Bandung, April 2016.

[13] Aradea, I. Supriana, dan K. Surendro, "Struktur knowledge base sebagai komponen pembentuk perangkat lunak self-adaptive," Jurnal Siliwangi Seri Sains dan Teknologi, Vol.2 No.1, ISSN: 2477-3891, LPPM, Universitas Siliwangi, 2016.

[14] I. Supriana, Aradea, "Model self-adaptive sebagai landasan sistem untuk menunjang penumbuhan komunitas," Keynote Paper SENTIKA 2016, Seminar Nasional Teknologi Informasi dan Komunikasi, Volume: 6, Universitas Atma, 2016.

[15] I. Supriana, K. Surendro, Aradea, and E. Ramadhan, "Self-adaptive cyber city system," International Conference on Advanced Informatics: Concepts, Theory, and Applications (ICAICTA), IEEE, Penang, Malaysia, August 16 – 19, 2016.

[16] P. Giorgini, F. Massacci, N. Zannone, "Security and trust requirements engineering," In A. Aldini, R. Gorrieri, F. Martinelli, (eds.) Foundations of Security Analysis and Design III, LNCS, vol. 3655, pp. 237–272, Springer Berlin Heidelberg, 2005.

[17] P. Bresciani, A. Perini, P. Giorgini, F. Giunchiglia, and J. Mylopoulos, “Tropos: An agent-oriented software development methodology,” Autonomous Agents and Multi-Agent Systems, vol. 8, no. 3, pp. 203–236, 2004.

[18] H. Mouratidis, J. Jurjens, "From goal-driven security requirements engineering to secure design," International Journal of Intelligent System 25(8), 813–840, 2010.
[19] R. Ali, F. Dalpiaz, P. Giorgini, "A goal-based framework for contextual requirements modeling and analysis," International Journal of Requirements Engineering, 15(4), 439–458, 2010.
[20] T. Li, J. Horkoff, K. Beckers, E. Paja, and J. Mylopoulos, "A holistic approach to security attack modeling and analysis," Conference: 8th iStar workshop, 2015.
[21] I. Atoum, and A. Otoom, "Holistic performance model for cybersecurity implementation frameworks," International Journal of Security and Its Applications, Vol. 10, No. 3, pp.111-120, 2016.
[22] D. Mlakić, and L. Majdandžić, "Fuzzy rule based expert system for SCADA cybersecurity," Conference: CIGRE 47, At Paris, Volume: SC D2 Information Systems and Telecommunication, 2016.