# ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY APPLICATIONS

**Shanqi Pang, Yongmei Li**
**Department of Computer Science**
**Stanford University, Stanford, CA 94305, United States**

***Abstract— Considering the enhancement in technology, criminals have been using cyberspace in order to commit many crimes. Therefore, it should be noted that cybercrimes are exposed to a number of threats and intrusions if not safeguarded well. Human and physical intervention tend not to be very adequate for the protection and tracking of such infrastructure, that is why there should be the establishment of multifaceted cyber defense networks, which are flexible, robust, and adjustable in order sense a massive collection of invasion and creation of real-time choices. Nevertheless, significant number of bio-related computing techniques of AI (artificial intelligence) tend to be increasing hence a significant role is played in detecting and preventing cybercrime. The main aim of this paper is outlining the actual advancement that have been made possible due to the application of AI methods for the fight against cybercrimes, in order to reveal how the methods are efficient in sensing and preventing cyber invasions, also providing a brief overview of the future works.***

***Keywords— Computational intelligence, Artificial Intelligence, Intrusion detection and prevention systems, Cyber crime***

## I. INTRODUCTION

Due to the fact that the networked-centric fight tends to be rigidly entrenched following US military rules and operations, state and loyalty of networks and other computerized processes and resources are essential standpoint for commanders, specifically, when the network tends to be a lucrative target in cyber invasions. Nonetheless, the breadth and pace revealed in cyber-attacks need great intervention to attain an attack response and attack at a specific time. Moreover, the rate of events noted in cyberspace and workload limits are perfect for assessing a state of network assets and other infrastructure linked to the prospected network. Provided human limits and knowing that intelligent agents perform a number of cyber-attacks, it is concluded that net-centric surroundings need semi-autonomous agents for the sensing, evaluation, and reacting to cyber invasions. An essential segment of daily networked operations should be allotted to various in intelligent agent. Additionally, the CGF's (Computer generated forces) should pinpoint the attacks which are foreseen to be underway, its attack targets, effective feedback for the invasions, priority given to the feedback, presentation of suitable defense systems for any secondary attacks, direct response for primary attacks, and entirely the management of the prospected response.

Based on the late advancement on IT (information technology) cyberspace criminals have been committing vast crimes. The increasing tendency of the intricate distributed and online computing has raised concern pertaining privacy and security of various systems. The prospected cyber defense systems should be adaptable, flexible and robust in order to sense an extensive range of cyber invasions, whereas human intervention tends not to be very adequate for handling timely invasion analysis and providing effective feedback. Based on the fact that many network-centric cyber invasions are executed using intelligent agents like viruses and computer worms, fighting them using semi-autonomous agents that will sense, evaluate, and act in accordance to a specific cyber-attack will be necessitated.

The prospected computer-generated factors should be in a position of managing the whole process for the prospected attack response to be handled in a perfect manner. For instance, concluding the type of attack happening, the primary targets and the effective response, and a perfect way of preventing and prioritizing a cyber-attack.

First, it's essential noting that cyber-attacks are not localized. They are an international menace which brings about great threat to a computer network at a raging pace. On many occasions, the educated professionals were the only people who could commit an offense linked to cybercrime, though currently, due to the increment in internet, every person has gained knowledge and equipment for doing such crimes. Traditional fixed algorithms tend not to be accurate and sufficient in solving dynamically trending cyber invasions. For this reason, there is great need to presenting perfect innovative processes like the application of techniques of AI (artificial intelligence) which highly enhances learning capacities and flexibility for software that aids humans in combating cybercrimes, thanks for AI since it offer other distinct opportunities.

Massive number of nature-motivated computing techniques within the AI like (neural networks, artificial immune systems, computational intelligence, data mining, heuristics, pattern recognition, machine learning etc.) tend to be increasing hence present a crucial role in fighting of cyber-crime prevention and detection. AI equips people with the knowledge of designing automated computing solutions that are in a position of adjusting the functions, focusing on self-management techniques, self-configuration, self-tuning, and self-healing. Related to the future of internet security, Artificial intelligence methods tend to be a promising sector of research which specifically targets on enhancing security measures in cyber space. The main aim of the study is presenting improvements created so far in the sector of employing AI methods used for solving cybercrimes, for the demonstration of the way these methods are efficient equipment for sensing and preventing cyber-attacks, also providing the scope of the future works.

## II. BACKGROUND AND RELATED WORKS

Extensive work has been executed in the field of network intrusion detection system whether in HIDS (host-based intrusion detection) or rather the NIDS (network-based intrusion detection) and AI, though, there is no all-encompassing effective cyber datasets that entirely look into modern and contemporary attacks for any network intrusion within the systems. Moreover, according to researchers in [1], and subsequent co-authors claimed the research was executed far much away from the offline approach for sensing shell code series found within the data. Moreover, these networks tend to be very vulnerable daily because of modern attacks. Based on the presented systems, realistic cyber datasets that may compromise the current attacks and other zero day invasions as noted by the Canadian cyberspace via cloud computing.

### *2.1 Cybercrimes: Meaning, Underlying issues*

Until now, many people know the idea of cybercrime, though many do not fully understand the entire ramification of the cost of cybercrime. For example, hacking, specifically intended for stealing personal or financial data is a most recognized form of cybercrime, though it is far much away from being the only form of cybercrime present. Below is how cybercrime is viewed: how hard it is in prosecuting cybercrime and the necessary efforts that should be vested. Typically, cybercrime is a form of crime that occurs in a digitalized manner. Data stealing, indeed, is a common form of cybercrime, which incorporates an extensive range of dangerous activities, like cyber bullying, use of viruses or planting worms.

However, cybercrime has evolved to being a common term, since it is much difficulty explaining it in a perfect manner. Some of the fascinating definitions have been created using a number of practical methods. According to researchers in [2] and [3] they define cybercrime as a crime facilitated with the use of computers, hardware devices, network, in that the computer is the agent committing the crime. Moreover, other versions define the criminal activity which emanates from the internet, since crime that happens if computers are used or linked through a network, targets of crime etc. Additionally, cybercrimes can be segmented into two sections: ones resulting to intentional damage and ones that leads to unintentional damage. Many cases reveal that the damage is financially. For example, cyber bullying is an illegal offense that possesses a threat to any individual’s safety, related to display and coercion against several protected demographics. In such case, the danger is not witnessed financially, though it is a crime.

Unintentional damage could consider the disgruntled staff that has planted viruses or worms which always disrupts business processes. Since this may not be a similar financial damage as compared to stealing financial data of proprietary, it leads to collateral damage financially since the employee’s lost time and the funds the firm will use in solving the prospected issue. Each day great amount of digitalized data processed and stored within computers and different computing platforms augment at an exponential rate, considering people sharing, communicating, shopping, working and socializing with the aid of the internet and computers. Country and language barriers tend to have diminished and the virtual worlds have increasingly become populated unlike before. Well, the idea of crime is real when referring to people; hence cyber space is not restricted from ideas of crime and other criminals also. researchers in [4] argue that many cybercrime currently show that transfer of the actual-world crime to the cyber space that is an essential tool crime agents utilize in committing a series of old crime in diverse ways.

### *2.2 Intrusion detection and artificial intelligence*

AI also known as machine intelligence at first emanated in form of a research discipline in summer research project at Dartmouth College in 1956. Artificial intelligence is explained in two diverse ways: I) a science that is targeted at discovering intellectual essence and creation of intelligent appliances; ii) techniques for handling complex issues which may not be completed using other intelligence, for example, decisions centered on massive data scale. Within the context of applying the AI in cyber security, we have been fascinated by the second explanation. Moreover, research interest in the field of AI incorporates a number of methods for making machines that simulate human intellectual behavior like reasoning, planning, learning etc. Primarily the core issue for simulating intelligence has been pinpointed to accurate problems that comprises of a number of characteristics or capacities that the intellectual system must reveal. Here are some of the elements that tend to have more attention today, they include:

- Reasoning, deduction, problem solving
- Representation of knowledge
- Machine learning
- Natural processing of language
- Manipulation and motion
- Social intelligence
- Perception
- Creativity
- General intelligence

Ultimate AI techniques specifically focus on personal human behaviors, inference techniques, and knowledge representation. DAI (distributed artificial intelligence) highlights social behavior, like cooperation, knowledge sharing, and interaction and other distinct units. Well, the processing of looking out for some effective solutions in aligned resolutions issues is based on knowledge sharing defining an issue and agent cooperation. Typically, from these concepts the thought of intelligent multi-agent technology was created. Agent is always autonomous cognitive idea that comprehends its surrounding settings, e.g. it can be applicable solely and comprises internal choices which act entirely within agents' decisions. Based on multi-agent systems, a number of mobile autonomous agents link up in a coordinated and intellectual way for solving a number of issues of classes of problems. Somehow, they are in a position of understanding the surrounding environment, communicating and making fruitful decisions with different agents. Multi-agent technology comprises of essential technological applications, though the study only explains the applications used for defense over cyber intrusions.

Moreover, intelligent agent frameworks tend to be part of something big. An AI approach known as CI (computational intelligence) is used. The CI incorporates some essential nature inspired methods for example, neural networks, evolutionary computations, fuzzy logic, machine learning, swarm intelligence, and artificial immune systems [5]. The mentioned techniques present stiff decision making systems for creation of a dynamic environment like the cyber security applications. When referring to, "nature inspired" this implies that there is always a demand in the field of computing for mimicking biological systems and how remarkable they can learn, recognize, classify, memorize and process data in a perfect manner. AISs (Artificial immune systems) tend to be an example of this type of technology. AISs seem to be computational frameworks that have been motivated by biological immune systems that are adjustable to the ever-changing environment and in a position of dynamically and continuous learning [6]. That is why AISs are perfectly crafted in order to imitate a natural immune system within computer security applications generally and the IDSs (intrusion detection systems) specifically.

Genetic algorithms are examples of AI methods for example; machine learning approaches based on evolutionary computation theories that seemingly imitate the natural selection process. Moreover, such system presents an adaptive, optimal, and robust solution also for the complex computing issues. ANNs (artificial neural networks) comprises of artificial neurons which learns and handles various problems once they have been combined. Neural networks tend to possess that capability of learning, processing and distributing data, adjusting, and organizing, have been in a position of handling problems which needs conditionality, ambiguity, and imprecision at the same moment [7]. During the time that the neural networks comprise of massive numbers of artificial neurons, provision of functionality of extensively parallel learning and decisions using great speed that makes it suitable for learning a number of patterns, classification, and selection of feedback regarding the prospected attacks.

## III. CHARACTERISTICS FOR THE IDPS

On the other hand, evaluators are required to comprehend the components of a specific organization's framework and networking environment in order for compatible IDPS to be chosen which would effectively monitor certain activities on certain systems or networks. Moreover, evaluators must articulate various objectives and goals people ought to use within the IDPS, like bringing halt to various invasions, pinpointing improperly handled wireless networked devices and sensing the inappropriate use of a firm's network and assets. Furthermore, evaluators must effective review present security rules that act in accordance to a number of features whereby the IDPS products should be offered. Nevertheless, evaluators must be in a position of comprehending if or not a specific firm is overseeing or being reviewed by a different organization [8]. If this is true, there should be the determination if the overseeing process needs the IDPSs or rather other unique security systems resources. Resource limitation must be considered by a number of evaluators. Hence, evaluators should describe a number of unique requirements as shown below:

- Real-time detection of intrusion – during the attack process of just after the attack
- False alarms should be reduced
- Human supervision must be minimized, and consistent activities must be ascertained
- System crashes recoverability like ones emanating from accidents or attacks
- Individual monitoring capacity to sense attackers trials in diverting the entire system
- Security policy compliance for system monitoring
- Adjustability of system changes and other client behaviors over some time

### *2.3 AI use for defending Cyber Crimes*

For the past few years the present world has witnessed a steady and ever changing flow of great profile data invasions that hit the deadlines. It doesn't matter if the outcome of an identified web problem, DDOS invasion or rather the entire lax corporate data safety rules, data breaches tend to happen in everyday life. Subsequently, it is entirely assumed that there is no firm that is secure from hackers that tend to be using more complex breaching techniques, though these can be halted prior leading to any damage to the entire business. Considering the increase of inter-linked workplace environments, and the enhancement of mobile and cloud technologies, firms may not be in a position of relying wholly on network and other endpoint protection. Such attacks have immensely emerged and firms which would have bolstered its cyber defense or would have invested appropriate equipment and get themselves in vulnerable circumstances within the business. With the increased low security, internet endpoints and other cloud-based applications tend to be a dream for cyber criminals.

Conventional approached used in cyber security are utilized for the prevention of centric strategic focus that block certain attacks. Importantly, today's motivated and advanced threats tend to be circumventing perimeters designed using stealthy, creativity, targeted, and other persistent invasions which tend not to be detected for a great period of time. Based on these shortcomings used by the prospected approach, and other problems used in securing massively complex IT atmosphere, firms require to be shifting a number of resources and enactment of strategies which are specifically based on rapid threat sensing and other responses. AI (artificial intelligence) and the manner it has been applied is diversely explained, focusing on the increasingly ways that CEO are discovering in order to use technology for enhancing business activities. Data protection and cyber security protection tend to be unsurprising considering the top of mind when the prospected conversations, though scholars are not sure how extensive AI plays its part and implementation of certain strategies.

### *2.4 Intelligent agent application*

Intelligent agents tend to be autonomous and computer-developed forces that link up with one another in order transmit data and relate to one another to plan and enact effectively in an event of unexpected events. Its adaptability and mobility within various environment deployed also its collaborative nature, brings about intellectual agent technology effective for handling cyber-attacks. The researchers in [9] created a perfect counter plan that helped in preventing certain cyber-attacks with the aid of multi-agent strategically planning several novel inference techniques. The researchers in [10] designed the MWDCM, which is a multi-agent framework for computer worm detection and suppression within metropolitan networking zone that automatically comprises worm propagation which would waste massive network bandwidth and leads to router setbacks. This type of experiment revealed that the whole system can perfectly thwart the worm propagation at an increased worm infection rate. The researchers in [11] highlighted some distributed agent coalition framework which can preserve operations, enact security and operational strategies, handling of unforeseen events, also the protection of dangerous insiders, mistakes and invasions within an aligned electric power grid.

The researchers in [12] proposed a suitable theoretically based layered process used for the protection of power grids systems from cyber-attacks that would emanate from internet or other internal networking sources. A crucial component of such framework include security agents whereby others include intelligent and comprises of abilities of sensing intrusive activities and events found within the controllers. Such an outcome acquired through the evaluation of the prospected prototype for the recommended approach revealed that the entire system is in a position of managing and following common vulnerable problems of the power grid automation systems. The researchers in [13 presented the SaaS, a cloud scenario sensing system security audit that is in form of a service. Its systems is specifically centered on intelligent autonomous agents that understand various underlying business mistakes and errors that are used in cloud services, hence delivering supported, flexible and its supported over customer event monitoring for the cloud infrastructure. The researchers in [14] proposed the IDS centered on community association amid multiple agents used for sensing cyber intrusion within the SCADA (supervisory control and data acquisition) networking places. Some of the proposed architecture incorporates SCADA network connectivity and topology limitations. The researchers in [15] and [16] recommended the use of a multi intelligent agent centered on an approach for the network intrusion sensing focusing the data mined.

## IV. APPLICATION OF ANN (ARTIFICIAL NEURAL NETWORKS)

Well, ANN is just a computational system which simulates functional and structural aspects for neural networks present within biological nervous systems. Such mechanisms are effective for predicting, controlling, and classifying complex and dynamic computer environment. The researchers in [17] designed the NeuroNet, which is a neural network set system that accumulates and transmits data, coordinates activities of the networked devices, identifies various irregularities, pings alerts, presents suitable countermeasures. Various experiments revealed how the NeuroNet has been useful over the low-rate TCP specifically designed to the DoS invasions. The researchers in [18] highlighted intrusion detection system focusing on neural network designed modeling (IDS-NNM) that proved to be in a position of sensing every intrusion trials within the network communication while not providing any false updates. The researchers in [19] outlined a comprehensive architecture defining the distribution of the IDS centered on artificial neural networking system for the augmented intrusion detection within the networks.

The researchers in [20] employed neural networking techniques for evaluating DoS invasions. Its experiments revealed that the neural networking approaches senses the DoS invasions with great precision and accuracy compared to any other method. The researchers in [21] highlighted a hybrid technique policy centered on the propagation and processing of neural networks used in spam filtering. Its approach asserts it is much robust unlike other spam sensing methods which include keywords, since spamming characteristics are transitioning. The researchers in [22] focused on a more complex approach used in zombie PCs sensing focusing on the neural networking systems. A series of practical events revealed that such approaches are computationally effective, simple for deploying in actual networking circumstances and attains perfect zombie detection outcomes.

The researchers in [23] focused on a host-based and networking centered intrusion sensing system that is unique on system which uses artificial neural networks for sensing malicious traffic. The researchers in [24] created a complex neural network for the IDS which promptly sensed and grouped a number of attacks. The researchers in [25] consequently looked into the enhancement of the IDS centered on neural networking frameworks. Their entire experiments revealed that each system proposed comprises of an intrusion rate same to other IDSs, though, it is proven to be more than 20.5 times greater in sensing of the DoS invasions.

## V. AI RISKS IN CYBER SECURITY

Though the AI presents several benefits, its integration in a working environment presents underlying risks which is always difficult attaining. Rigid security precautions by users ensure that they are vulnerable to these attacks. More often, when users do not understand these security risks encountered during the process of using such technology. Regular clients may neglect essential security patches used for the devices. Hence they operate and rune the prospected applications without any patches. Due to these, unpatched applications operate in background and at times regular users might not use them. Considering the increased use of AI, data pertaining AI tends to be easily located by any user. In 2018, the department of defense advanced research project agency (DARPA) executed a hunting competition. The process incorporated CTF (capture the flag) operations. CTF issues tend to be very important within the hacking community as it permits users in understanding different methods. In the competing process, users employed automated AI equipment which identified internal problems and patched them up. To that point, MIT (Massachusetts institute of technology) scholars employed AI for sensing how cyber security is used which does not only mention criminals but also national actors. The national actors are in a position of exploiting unidentified vulnerabilities in a quick manner, fashion, and ex-filtrating crucial data which might comprise data regarding the power grids. Such data is leveraged to be used over the nation. AI is a newly established weapon that is used in cyber espionage.

## VI. CONCLUSION

With the increased development of the IT sector there has been a positive impact seen and conveniences is seen in people’s lives. But, it leads to a number of issues which are very hard to handle like emergencies that arise in cybercrime. Considering the evolution of technology, criminal events change in a corresponding manner. Daily, people encounter outrageous cases of cybercrime, due to the fact that technology offers a clear way for criminals to attain their ultimate targets. Vital infrastructures tend to be vulnerable. AI technique applications are used for human fight over cybercrimes since they are flexible and relate closely to the IDPS software. Furthermore, it is obvious that the massive knowledge use for the decision making processes needs intellectual decision support within the cyber space that is successfully attained focusing such AI techniques. Accessible academic resources reveal the way the AI methods have vast applications when it comes to combating cybercrimes. The paper briefly highlights advancement that has been made in the field of AI methods that have been set to fighting cybercrimes, its present limitations and its prospected features.

## References

[1] L. Vôhandu, "Artificial intelligence frontiers in statistics", Engineering Applications of Artificial Intelligence, vol. 7, no. 1, p. 87, 1994. Available: 10.1016/0952-1976(94)90049-3.

[2] Y. Kharin, "Artificial intelligence frontiers in statistics AI and statistics III", Knowledge-Based Systems, vol. 7, no. 1, pp. 57-58, 1994. Available: 10.1016/0950-7051(94)90017-5.

[3] M. Rao, "Frontiers and challenges of intelligent process control", Engineering Applications of Artificial Intelligence, vol. 5, no. 6, pp. 475-481, 1992. Available: 10.1016/0952-1976(92)90024-e.

[4] P. Giudici, "Fintech Risk Management: A Research Challenge for Artificial Intelligence in Finance", Frontiers in Artificial Intelligence, vol. 1, 2018. Available: 10.3389/frai.2018.00001.

[5] S. O'Halloran and N. Nowaczyk, "An Artificial Intelligence Approach to Regulating Systemic Risk", Frontiers in Artificial Intelligence, vol. 2, 2019. Available: 10.3389/frai.2019.00007.

[6] S. Bredt, "Artificial Intelligence (AI) in the Financial Sector—Potential and Public Strategies", Frontiers in Artificial Intelligence, vol. 2, 2019. Available: 10.3389/frai.2019.00016.

[7] D. Dubois and H. Prade, "Fuzzy set and possibility theory-based methods in artificial intelligence", Artificial Intelligence, vol. 148, no. 1-2, pp. 1-9, 2003. Available: 10.1016/s0004-3702(03)00118-8.

[8] D. Dubois and H. Prade, "Special Issue of the journal Artificial Intelligence on "Fuzzy Set and Possibility Theory-Based Methods in Artificial Intelligence"", Artificial Intelligence, vol. 127, no. 2, pp. 269-270, 2001. Available: 10.1016/s0004-3702(01)00080-7.

[9] "Advances in artificial intelligence natural language and knowledge-based systems", Artificial Intelligence in Engineering, vol. 6, no. 4, p. 212, 1991. Available: 10.1016/0954-1810(91)90028-m.

[10] L. Chittaro and R. Ranon, "Hierarchical model-based diagnosis based on structural abstraction", Artificial Intelligence, vol. 155, no. 1-2, pp. 147-182, 2004. Available: 10.1016/j.artint.2003.06.003.

[11] S. Panneerselvam, "SURVEY OF ARTIFICIAL INTELLIGENCE USED IN INDUSTRIES A REVIEW," Industrial Engineering Journal, vol. 12, no. 5, 2019. Available: 10.26488/iej.12.5.1188.

[12] . Kaur and S. Sood, "Cloud-Centric IoT-Based Green Framework for Smart Drought Prediction", *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1111-1121, 2020. Available: 10.1109/jiot.2019.2951610.

[13] F. Song, M. Zhu, Y. Zhou, I. You and H. Zhang, "Smart Collaborative Tracking for Ubiquitous Power IoT in Edge-Cloud Interplay Domain", *IEEE Internet of Things Journal*, pp. 1-1, 2019. Available: 10.1109/jiot.2019.2958097.

[14] C. Lin, K. Ramakrishnan, J. Liu and E. Ngai, "Guest Editorial Special Issue on Cloud Computing for IoT", *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 254-256, 2016. Available: 10.1109/jiot.2016.2554738.

[15] T. Pflanzner and A. Kertesz, "A Taxonomy and Survey of IoT Cloud Applications", *EAI Endorsed Transactions on Internet of Things*, vol. 3, no. 12, p. 154391, 2018. Available: 10.4108/eai.6-4-2018.154391.

[16] S. Guo, Y. Dai, S. Xu, X. Qiu and F. Qi, "Trusted Cloud-Edge Network Resource Management: DRL-driven Service Function Chain Orchestration for IoT", *IEEE Internet of Things Journal*, pp. 1-1, 2019. Available: 10.1109/jiot.2019.2951593.

[17] Z. Lv and W. Xiu, "Interaction of Edge-Cloud Computing Based on SDN and NFV for Next Generation IoT", *IEEE Internet of Things Journal*, pp. 1-1, 2019. Available: 10.1109/jiot.2019.2942719.

[18] P. van Oorschot and S. Smith, "The Internet of Things: Security Challenges", *IEEE Security & Privacy*, vol. 17, no. 5, pp. 7-9, 2019. Available: 10.1109/msec.2019.2925918.

[19] R. Weber, "Internet of Things – New security and privacy challenges", *Computer Law & Security Review*, vol. 26, no. 1, pp. 23-30, 2010. Available: 10.1016/j.clsr.2009.11.008.

[20] M. Losavio, K. Chow, A. Koltay and J. James, "The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security", *Security and Privacy*, vol. 1, no. 3, p. e23, 2018. Available: 10.1002/spy2.23.

[21] P. Khanale and S. Chitnis, "Handwritten Devanagari Character Recognition using Artificial Neural Network", Journal of Artificial Intelligence, vol. 4, no. 1, pp. 55-62, 2011. Available: 10.3923/jai.2011.55.62.

[22] N. Abbas, Y. Nasser and K. Ahmad, "Recent advances on artificial intelligence and learning techniques in cognitive radio networks", EURASIP Journal on Wireless Communications and Networking, vol. 2015, no. 1, 2015. Available: 10.1186/s13638-015-0381-7.

[23] Z. Shang, "Application of artificial intelligence CFD based on neural network in vapor–water two-phase flow", Engineering Applications of Artificial Intelligence, vol. 18, no. 6, pp. 663-671, 2005. Available: 10.1016/j.engappai.2005.01.007.

[24] X. Chang, X. Mi and J. Muppala, "Performance evaluation of artificial intelligence algorithms for virtual network embedding", Engineering Applications of Artificial Intelligence, vol. 26, no. 10, pp. 2540-2550, 2013. Available: 10.1016/ j.engappai.2013.07.007.

[25] V. Nastase and M. Strube, "Transforming Wikipedia into a large scale multilingual concept network", Artificial Intelligence, vol. 194, pp. 62-85, 2013. Available: 10.1016/j.artint.2012.06.008.