Applications and Techniques of Artificial Intelligence in Cyber Security

Dr. K. Ramasubramanian[1],Dr Lendale Venkateswarlu[2], Sneha Yerram[3]
Associate Professor in Cse Department[1] Associate Professor in Cse Department[2]Research Scholar in Cse Department [3]
KoneruLaxmaiahEducation Foundation, Hyderabad[1, 3]
Geethanjali college of engineering and technology
Cheeryal, Keesara, Hyderabad 501301[2]
ramasubramaniankrish@klh.edu.in[1]
venkatlendale.cse@gcet.edu.in[2]
yerramsneha@klh.edu.in[3]

Abstract:
Technology Growth brings up security challenges with lack of knowledge in latest development to the experts of cyber security. To prevent security breaches and cyber-attacks, experts needs a huge support, as connection between organisations leads to "Heavy traffic", "Breaches in Security", "Increase in Security attack vectors", whichbeing a challenging task for humans to handle. Traditional Algorithm fails to us sometimes with developed systems. Developing a software with auto updating logic with technology leads a tough task. Artificial Intelligence is an area to neutralize the cyber security issues to some extent."Cyber security computing applications and analyses the views of improving the cyber security abilities by suggesting AI applications and the already existing methods". This paper involves in coping up the cyber security with applications and techniques of Artificial Intelligence.

Keywords: Cyber Security, Artificial Intelligence, Expert Systems, Neural Nets, Intelligence Agent.

I. Introduction:

Security involves in many ways such as "security of information", "security of documents" and "security of property". Applications of modern techniques makes Security Stronger. From Government Infrastructure to Internet banking our world is under networked Technology. Thus Protection of Data is Essential.Globally Increasing Threads of Cyber Security leads to an Implementation of Artificial Intelligence in Security systems. As the world is running on digital data, AI and machine learning Applications are been used in every field, which gives a security challenge to Experts. A solution from "Internet threats", "Identify types of malware", "Ensure practical security standards", and "Help create better prevention and recovery strategies" is Artificial Intelligence.

AI and Machine Learning are interlinked with data science which brings down the curve of managing data from peak gradually simultaneously security for this data is mandatory. This Research comes up with contribution of AI Applications and Techniques in cybersecurity and

Involves Identifying Important areas of Artificial Intelligence that can be used in Cyber Security and role played by Expert systems, Machine Learning, Deep learning, Data mining in Improving Cyber security. An Analytical Approach based on the previous critical Theoretical literature.

II. Artificial Intelligence& Cyber Security:

AI and cyber security are two different fields, to decrease human work, AI researchers have been updating their new logical standards in form of technological update which comes up with networked data in digitalized form which need to be secured with high Expertise way. AI has been increased in modified humankind approach to solve Critical problems and perform task that a human brain can do like decision making, Analysis, Matching.

Fig 1: AI & Cybersecurity

This combination of AI and Cybersecurity can be Explained with a good example of CAPTCHAs, which is shown with combination of digits, letters in a pictorial representation by automatic pattern changing format, AI Application of sensible innovation to pattern recognition. Online platforms of reserving tickets, banking, Execution of programs, business organizations, government etc contains a crucial information includes personal details where privacy and data protection is a necessary aspect which cybersecurity play an important role. AI helps to Identify and analyse weakness and further attacks for internal part.

III. Applications of Artificial Intelligence in Cyber Security:

Internet is been a major source where the data has been generated directly or Indirectly. Data has been sent through a network in a proper transmission channel, which alerts in cybercrimes. Cyber space is been used by criminal which later leads to increase in cybersecurity [1]. AI and cybersecurity both are the terms which are used to reduce cyber-attacks. Human identifying new malware or virus is a tough job, whereas a technique from AI make it possible and facilitates malware detection as per previous cyber-attack data[2].

Expert Systems applications in cyber security: Expert systems are tools or software packages of Artificial Intelligence which help in providing knowledge required to a customer or another software package. A knowledge which required with the surrounded knowledge by an expert help are embedded in this system [3].

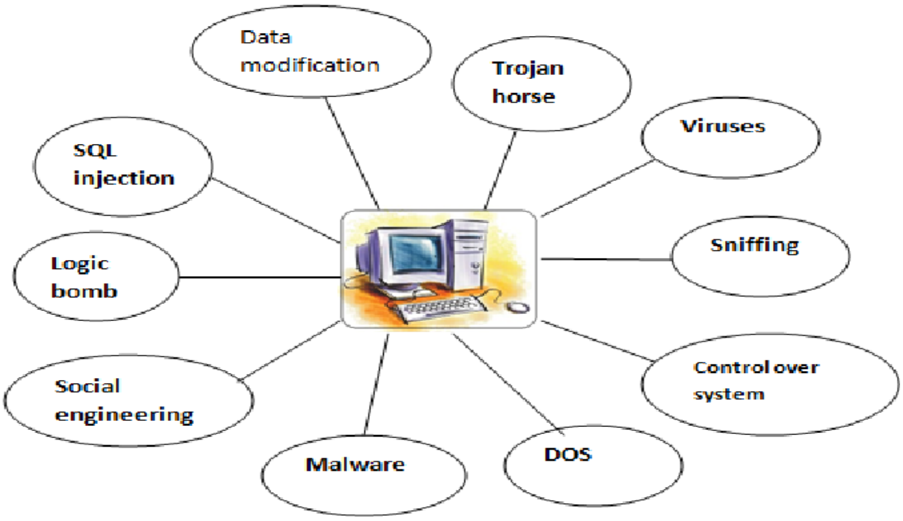


Fig 2: An Expert System for cyber security

Deep Learning Applications in Cybersecurity: A common problem in cybersecurity research is the scarcity of disaggregated data. “While this shortage is often explained by its return to secrecy factors, experience indicates even behind closed doors of large companies with significant internal expertise, security information on threats can be transformed into a categorised data set suitable for machine learning”.

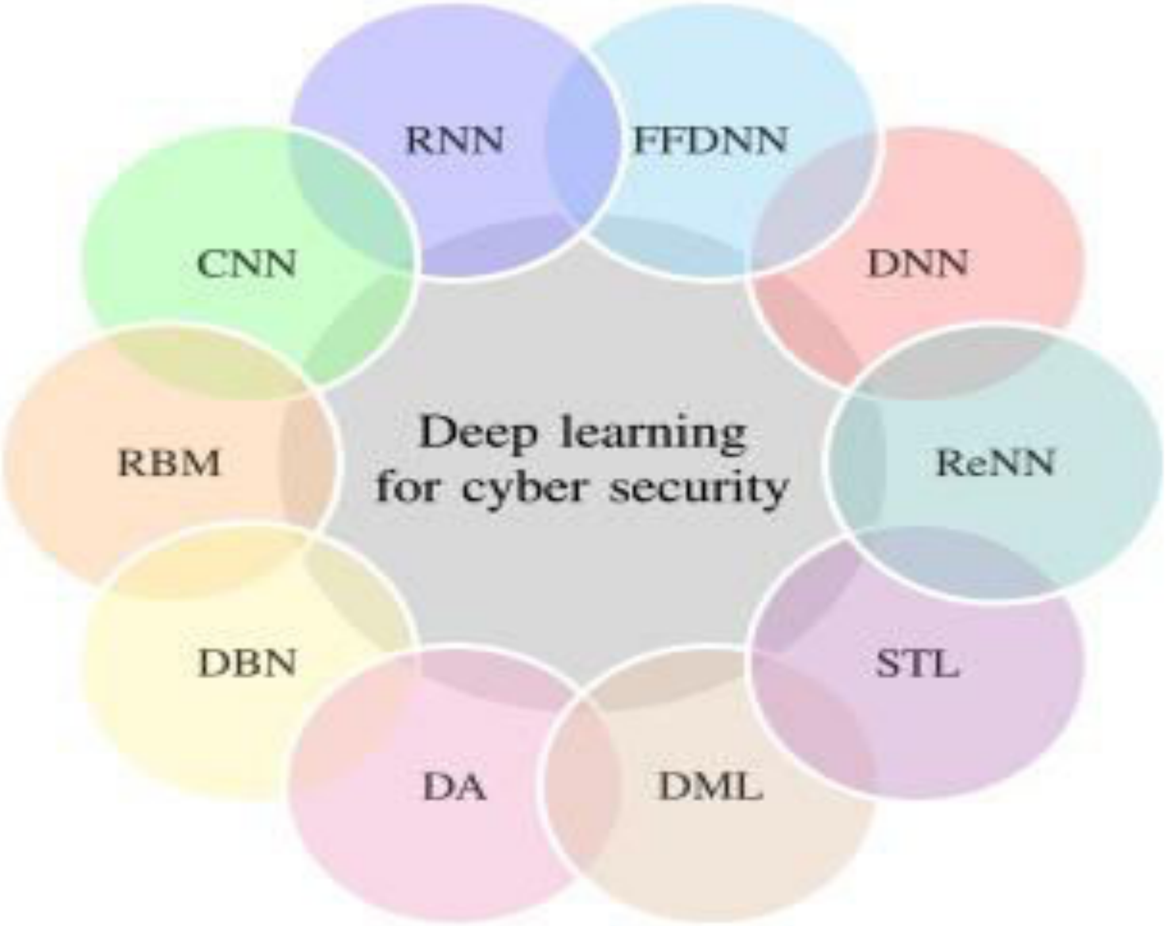


Fig 3: Deep learning for cyber security

The explanation behind this is the existence of a large number of large with unbalanced data sets, the lack of time needed to conduct manual categorization, and specific features in fields such as semantic categorization which increase the distance between technological competence and mathematical modelling [4].

Machine Learning Applications in Cyber Security: As cybersecurity threats are changing and developing constantly, immediate response is required and an automatic. Therefore, machine learning techniques, specifically deep learning that do not generally require prior experience or dependence on previous expert classifications, may be particularly important as an implementation of cybersecurity AI approaches. The study [5] analysisto the effectiveness for cybersecurity purposes of machine learning approaches. This research included the implementation of methods of machine learning to identify intrusions, spam and malware.

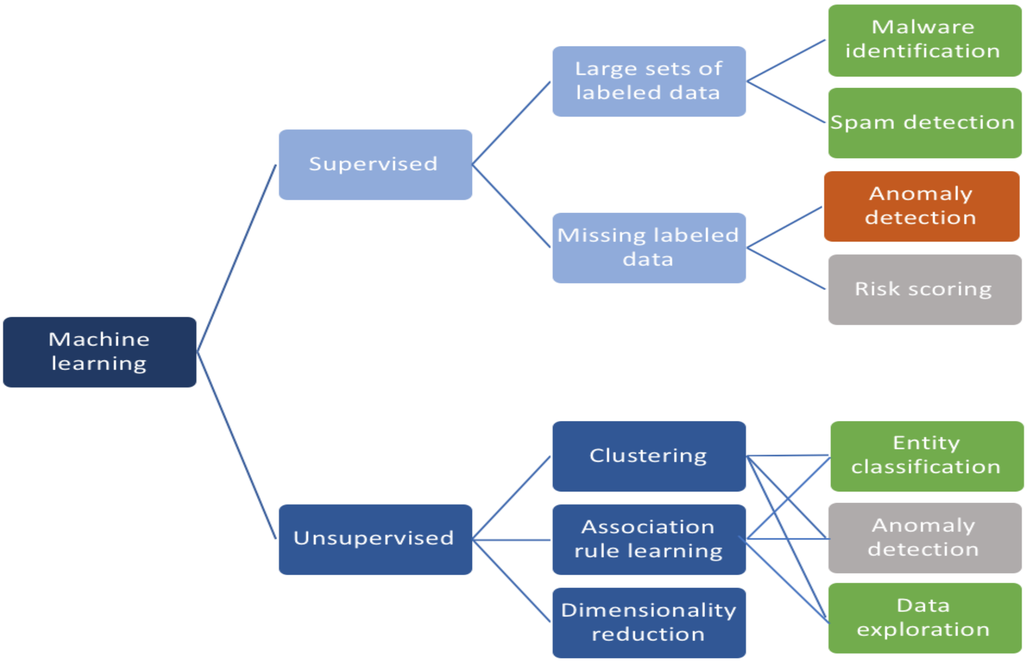


Fig 4: Machine learning in cyber security

Focus was put on the effectiveness and significant drawbacks of computer-based technologies that prevent the direct implementation of cybersecurity of machine learning approaches.

Data Mining Applications in Cybersecurity: "Data mining is the search for significant patterns and trends in large database". The technique of data mining helps to collect useful knowledge and identify hidden patterns from a large number of datasets that cannot be discovered through computational approaches. It is a large research field that involves "machine learning, databases, analytics, expert systems, visualisation, high-performance computation, rough sets, neural networks, and representation of information". A host that gathers data in different ways (e.g., “clustering, grouping, relation analysis, description, regression models, and sequence analysis”)[6] supports data mining.

IV. Artificial Intelligence Techniques for Cyber Security:

Expert Systems: Expert System is a computational system which copies a human's ability to make decisions. Which is the greatest instance of a method dependent on information. Two sub-systems constitute these knowledge-based systems: The Inference Engine and the Knowledge Base. It illustrates in the real world the assertions and illustrations.

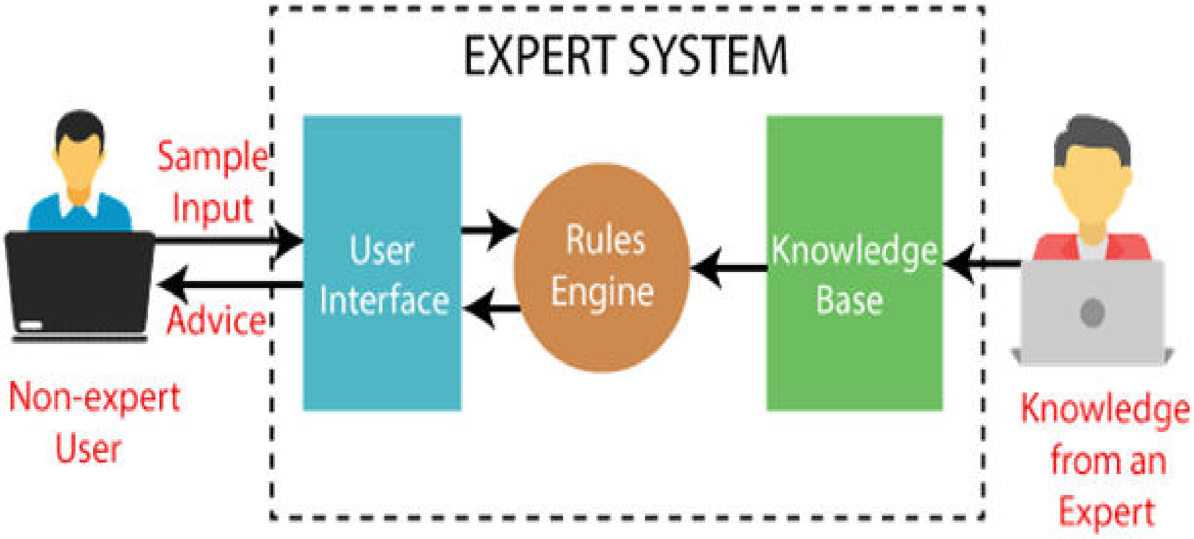


Fig 5: An Expert System for cyber security

The Inference Engine is a framework for automated reasoning. It assesses the current state of the knowledge base, applies the applicable rules to it, then claims new knowledge [7].

Neural Nets: Deep learning is known as Neural Nets. “It is an advanced AI branch. It is inspired by the human brain's functions and work. There are many neurons in our brain, which are mainly general purpose and domain independent. Any data form can be learned. In 1957, an artificial neuron (Perceptron) was developed by Frank Rosenblatt, paving the way for neural networks. By combining with other nerves, i.e., perceptron, these perceptions will learn and resolve absorbing problems. Perceptron learns to recognise the individual they are focused on by learning and analysing high-level raw data on their own, as our brain uses the signals of our sensory organ to learn on its own from the raw data”.

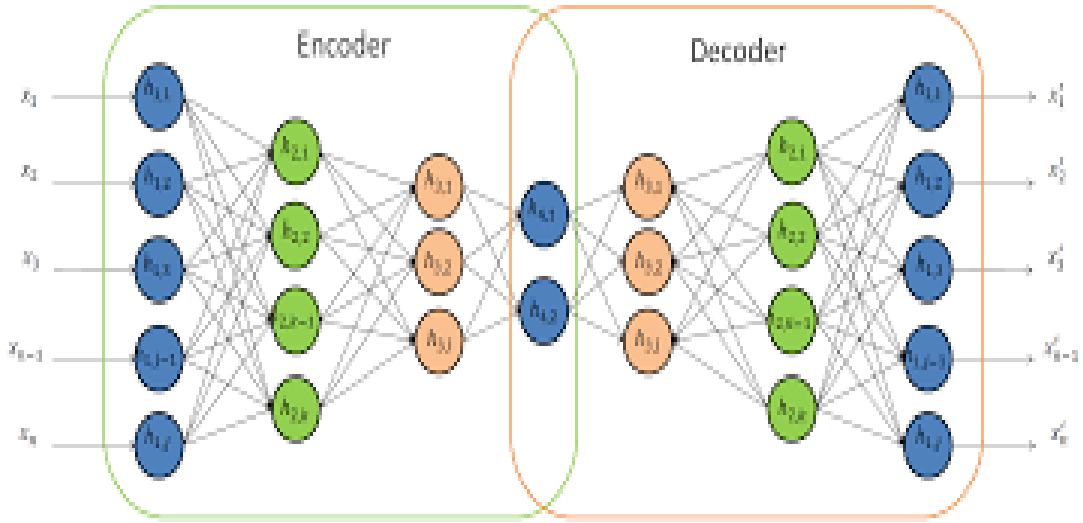


Fig 6: Neural nets for cyber security

When we extend this deep (trained) learning to computer protection, without human intervention, the machine can identify whether a file is malicious or legitimate. Compared to classical machine learning methods, this approach yields a good outcome in the identification of malicious attacks [8].

Intelligent Agents:"The Intelligent Agent (IA) is an autonomous body that detects motion by sensors and uses actuators (i.e. it is an agent) to track an environment and directs its operation towards achieving goals". Intelligent agents can also study or use a knowledge base to achieve their goals. They may be incredibly simplistic or very complex. For example, "a reflex mechanism, a thermostat, is an intelligent agent. It has behaviours like understanding the language of agent interaction, pro-activity and reactivity. They can adapt to real time, easily learn new information through contact with the world, and have standard retrieval and recovery skills focused on memory".

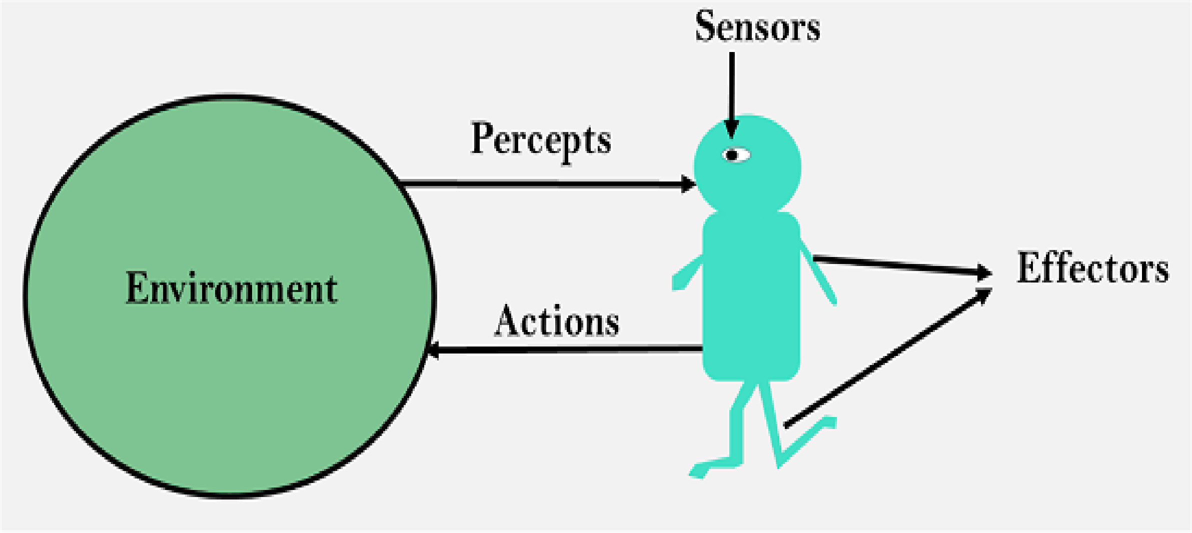
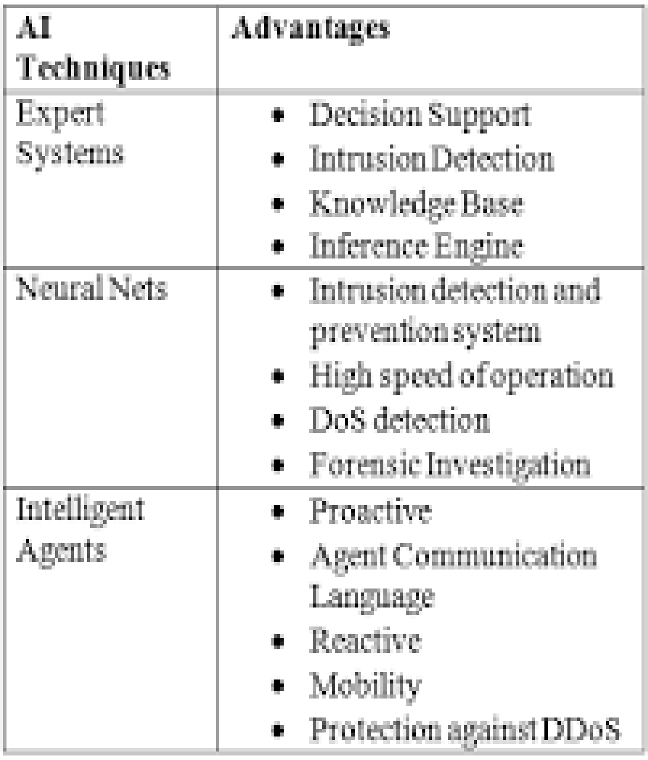


Fig 7: An Intelligent Agent

In the showdown against Distributed Denial of Service (DDoS) attacks, intelligent agents are developed. If there is some legal or business issue, creating a "Cyber Police" should be manageable. The Cyber Police should have intelligent mobile officers [9].

V. Advantages of AI Techniques:

We may use AI for cyber defence in a number of ways. In the future, we will have the cleverest systems than such processes. Indeed, attackerscan use Artificial Intelligence for attacks as well. It is clear that the recent developments in knowledge comprehension outlines and coping up with what is advanced in machine learning would enhance the digital security capability of the systems that can be used. The description of the various approaches dealt in this paper appears in the diagram below.



AI Techniques	Advantages
Expert Systems	• Decision Support • Intrusion Detection • Knowledge Base • Inference Engine
Neural Nets	• Intrusion detection and prevention system • High speed of operation • DoS detection • Forensic Investigation
Intelligent Agents	• Proactive • Agent Communication Language • Reactive • Mobility • Protection against DDoS

Fig 8: Advantages of AI Techniques

This research was applied using the methods of literature and previous reviews of empirical and descriptive research. “The findings revealed the possibility of utilising techniques of machine learning, deep learning, and data mining for cybersecurity purposes in three major areas: identification of intrusions, examination of malware, and detection of spam. Every day, malware technologies are developed and today, data mining algorithms can detect and classify malware”. To detect and classify malware, however, it is critical to develop new data mining algorithms to be fast and scalable.

Conclusion:

Current Scenario reveals increasing developments incyber-attacks and malware, an Intelligent Protection Infrastructure is required.differently in comparison to current cyber protection technologies, Artificial Intelligence approaches are resilient and agile, resulting in Improved security implementation and stronger safety against a growing range of sophisticated cyber-threats. Given the sharp shift that Artificial Intelligence has made to the field of cyber security, similar devices are not completely equipped to respond to change in their situation. While having several benefits, using AI procedures in cyber defence, Artificial Intelligence is not only protection panacea. At a moment when human enemy with an unmistakable circumvention target is targeting intelligent defence, the system would collapse. This does not mean that we can-not use Artificial Intelligence techniques, but rather that we should understand its limits and use them properly. Artificial Intelligence needs continuous training and human collaboration. Aside the threat-analysts, this Artificial Intelligence approach to cyber defence has proved to operate effectively.

Reference:

1. Kamtam, A., Kamar, A., & Patkar, U. C. (2016). Artificial Intelligence approaches in Cyber Security. International Journal on Recent and Innovation Trends in Computing and Communication, 4(4), 05-09.
2. Intelligence, S. (2019). IBM QRadar Security Intelligence. [online] Ibm.com. Available at: https://www.ibm.com/security/security-intelligence/qradar [Accessed 6 Dec. 2019].
3. Pandey, M. (2018). Artificial Intelligence in Cyber Security. On Emerging Trends In Information Technology (NCETIT'2018) with the theme-'The Changing Landscape Of Cyber Security: Challenges, 66
4. Anagnostopoulos, C. (2018). Weakly Supervised Learning: How to Engineer Labels for Machine Learning in Cyber- Security. Data Science for Cyber-security, 3, 195.
5. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cybersecurity. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 371-390). IEEE.
6. Katoua, H. S. (2013). Exploiting the Data Mining Methodology for Cyber Security. Egyptian Computer Science Journal, 37(6).
7. TF. Lunt, R. Jagannathan. A Prototype Real-Time Intrusion-Detection Expert System.Proc.
8. B. Iftikhar, A. S. Alghamdi, "Application of artificial neural network within the detection of dos attacks", 2009.
9. P. Norvig, S. Russell. "Artificial Intelligence: fashionable Approach", 2000.