A Survey: Artificial Intelligence as a Strategic Initiative for Cyber Defence

Shivani Sompura[a*], Prof. Rahul Vaghela[b], Prof. Rajan Patel[c]

[a]*PG Research Scholar, Gandhinagar Institute of Technology, Khatraj-Kalol Road, Moti Bhoyan, Kalol, Gandhinagar, Gujarat 382721*
[b]*Assistant Professor, Gandhinagar Institute of Technology, Khatraj-Kalol Road, Moti Bhoyan, Kalol, Gandhinagar, Gujarat 382721*
[c]*Professor, Gandhinagar Institute of Technology, Khatraj-Kalol Road, Moti Bhoyan, Kalol, Gandhinagar, Gujarat 382721*

Abstract

Cyber Defence plays an important role in information technology. Artificial intelligence (AI) techniques have grown rapidly in recent years, Artificial intelligence gives extensive and spreads topological in nourishing cyber defence capabilities by increasing intelligent defence system, cyber infrastructures are highly vulnerable to intrusion and other threats. Hence, there is a need for more ultra-modern cyber defence system that need to flexible, adoptable, and able to detect a wide variety of threats and make intelligent real-time decisions. The purpose of this survey is to study technical-AI based cyber defence system which can detect and support against threats and cyber attacks as well as to give the scope for future work.

*Keywords***:** Artificial Intelligence, Cyber Defence, Cyber Attacks, Cyber Threats, Intrusion Detection.

1. Introduction

The development of the technology and communication system started the new era of cyber movement, People and firms now almost fully rely on the use of the technology for their activities. It improved efficiently but this system has also led to greater risk from cyber threats, the increased use of technology means that the vital components of critical infrastructures are exposed to cyber attacks [1, 2].

The fact is that the most network-centric cyber attacks are carried out by intelligent agents such as computer worms and viruses; protecting the information of critical infrastructure and database from such disturbance and attacks is highly important, and is one of the major challenges in the future [3,4].

Cyber attack is also done by terrorists to spread propaganda and disinformation, fund raising, plan campaigns and provide information on them. They could try to launch cyber attacks on country's critical infrastructure in the future. Hence, combating them with intelligent system that can detect, evaluate and respond to cyber attacks has become a requirement [4]. Furthermore, cyber intrusion are not localized they are a global menace that poses threat to any system in the world at a growing rate. This is why we need innovative approaches such as AI-methods that provide learning capability to software which will assist humans in fighting cyber attacks [11, 15].

AI offers various possibilities; numerous nature-inspired computing methods of AI such as (computational intelligence, neural networks, intelligent agents, artificial immune system, machine learning, data mining etc.) have been increasingly playing an important role in cyber crime detection and prevention. When it comes to the future of cyber defence security, AI techniques seems very promising area of research that focuses on improving the security measures for cyber defence [4].

*Shivani Sompura

E-mail address: 210120702003@git.org.in

The purpose of this study is to present applying AI techniques for cyber defence, to demonstrate how these techniques can be effective for detection & prevention of cyber attacks, as well as to give the scope for future world.

2. Cyber Defence: Definition, Need and Issues.

Cyber defence is a computer network defence mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks. Cyber defence focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with. With the growth in volume as well as complexity of cyber attacks, cyber defence is essential for most entities in order to protect sensitive information as well as to safeguard assets [3, 4].

With the understanding of the specific environment, cyber defence analyzes the different threats possible to the given environment. It then helps in devising and driving the strategies necessary to counter the malicious attacks or threats. A wide range of different activities is involved in cyber defence for protecting the concerned entity as well as for the rapid response to a threat landscape. These could include reducing the appeal of the environment to the possible attackers, understanding the critical locations & sensitive information, enacting preventative controls to ensure attacks would be expensive, attack detection capability and reaction and response capabilities. Cyber defence also carries out technical analysis to identify the paths and areas the attackers could target [5, 6].

Cyber defence provides the much-needed assurance to run the processes and activities, free from worries about threats. It helps in enhancing the security strategy utilizations and resources in the most effective fashion. Cyber defence also helps in improving the effectiveness of the security resources and security expenses, especially in critical locations [7, 8].

Cyber defence risks pervade every organisation and aren't always under IT's direct control. Business leaders are forging ahead with their digital business initiatives, and those leaders are making technology-related risk choices every day. Increased cyber risk is real—but so are the data security solutions [12].

Cyber defence system is crucial for government and other organizations that directly affect the nation's – or world's – wellbeing and safety. Cyber attacks to government, military groups and defence suppliers are starting to supplement or replace physical attacks, putting nations in danger [13].

Today, cyber attacks are no longer stopped by antivirus software or firewalls. The risk of cyber attacks is constantly increasing and for companies and institutions it is no longer a question of "if" it will happen but rather "when". This is why cyber defence is of such great importance .Cyber security is important because it encompasses everything that relates to protecting our data from cyber attackers who want to steal this information and use it to cause harm. This can be sensitive data, governmental and industry information, personal information, personally identifiable information (PII), intellectual property [22].

Ensuring that our data remains safe is one of the biggest challenges of Cyber Security. Cyber Security challenges come in many forms, such as ransom ware, phishing attacks, malware attacks, and more. India ranks 10th globally in terms of local cyber-attacks and has witnessed 121 million incidents in 2021 already [3].

List of the top challenges of cyber defence system:

- Ransom ware attacks
- IOT attacks
- Cloud attacks
- Phishing attacks
- Block chain and Crypto currency attacks
- Software vulnerabilities
- Machine learning and AI attacks

- BYOD policies
- Insider attacks
- Outdated hardware
- Intelligence/awareness

3. The Impact of AI in Cyber Defence

Now it is essential to automate threat detection and management because extent of threats has grown beyond the point where they can be managed by people. Artificial intelligence helps to analyze web traffic and investigate suspicious automatically. Using artificial intelligence one can discover attacks before cybercriminals to access sensitive information. Also AI engine learns continuously from massive amount of data they analyze. This type of lifelong learning makes it possible to automate the defence system organization, fighting alone against potential threats. AI is regarded as a science that finds ways to solve complex problems that cannot be solved without applying some intelligence. AI application in the field of cyber defence is growing as strategic consist of those ways in which computers simulate human intelligence behaviour, such as thinking, learning, planning etc [4, 7, 8].

AI classical approach of focusing on individual human behaviour, knowledge representation and methods of inference, therefore, the intelligent agents. Was developed, on the other hand, Distributed Artificial Intelligence (DAI), which focuses on human behaviour accordingly cooperation, interaction and exchange of knowledge between different entities (agents). How the process of finding a solution to the problems is based on distributed knowledge sharing and cooperation among agents about the problem, it developed the concept of intelligent multivalent technology, technology that meets current needs. If an agent is an entity cognitive self-understanding its environment can work alone and has an internal system of decision-making that act globally, around other agents in multi-agent systems, the group of autonomous agents Mobile cooperate in a coordinated and intelligent to solve a specific problem or class of problems [7, 8].

3.1 Intrusion Detection

The general problem of simulating intelligence has been simplified to specific sub-problems:
Which have certain characteristics or capabilities that an intelligent system should exhibit? The Following characteristics have received the most attention.

- Deduction, reasoning, problem solving (embodied agents, neural networks, statistical approaches to AI);
- Knowledge representation;
- Learning (machine learning);
- Planning (multi-agent planning and cooperation);
- Social Intelligence (empathy simulation);
- Perception (speech recognition, facial, recognition, object recognition);
- Natural Language Processing (information retrieval – text mining, machine translation);
- Motion and Manipulation (navigation, localization, mapping, motion planning);
- Creativity (artificial intuition, artificial imagination); and
- General Intelligence (Strong AI).

The process of finding a solution in distributed resolution problems relies on sharing knowledge about the problem and cooperation among agents. It was from these concepts that the idea of intelligent multi-agent technology emerged. An agent is an autonomous cognitive entity which understands its environment, i.e. it can work by itself and it has an internal decision-making system that acts globally around other agents. In multi-agent systems, a group of mobile autonomous agents cooperate in a coordinated and intelligent manner in order to solve a specific problem or classes of problems [3, 4].

AISs are computational models inspired by biological immune systems which are adaptable to changing environments and capable of continuous and dynamical learning. Immune systems are responsible for detection and dealing with intruders in living organisms. AISs are designed to mimic natural immune systems in applications for computer security in general, and intrusion detection systems (IDSs) [15, 16].

Genetic algorithms are yet another example of an AI technique, i.e. machine learning approach founded on the theory of evolutionary computation, which imitate the process of natural selection. They provide robust, adaptive, and optimal solutions even for complex computing problems. They can be used for generating rules for classification of security attacks and making specific rules for different security attacks in IDSs [9, 10].

Many methods for securing data over networks and the Internet have been developed (e.g. antivirus software, firewall, encryption, secure protocols, etc.); however, adversaries can always find new ways to attack network systems. An intrusion detection and prevention system (IDPS) is software or a hardware device placed inside the network, which can detect possible intrusions and also attempt to prevent them. IDPSs provide four vital security functions: monitoring, detecting, analyzing, and responding to unauthorized activities [14, 20].

4. Application of Artificial Intelligence in Cyber Defence System

Wang et al. (2008) stated that the future of anti-virus detection technology is in application of Heuristic Technology which means "the knowledge and skills that use some methods to determine and intelligently analyze codes to detect the unknown virus by some rules while scanning". Available academic resources show that AI techniques already have numerous applications in combating cyber crimes. For instance, neural networks are being applied to intrusion detection and prevention, but there are also proposals for using neural networks in "Denial of Service (DoS) detection, computer worm detection, spam detection, zombie detection, malware classification and forensic investigations". AI techniques such as Heuristics, Data Mining, Neural Networks, and AISs, have also been applied to new-generation anti-virus technology. Some IDSs use intelligent agent technology which is sometimes even combined with mobile agent technology. Mobile intelligent agents can travel among collection points to uncover suspicious cyber activity. This section will briefly present related work and some existing [21].

- AI APPLICATION:
  - Application of Neural Networks
  - Application of Intelligent Agent
  - Application of Expert System

4.1 Application of Neural Networks(ANN)

ANN is a computational mechanism that simulates structural and functional aspects of neural networks existing in biological nervous systems. They are ideal for situations that require prediction, classification or control in dynamic and complex computer environments. The neural nets will include a wider range or variety of artificial neurons. So, neural nets offer a practicality of massively parallel learning and decision-making. Their most distinguished feature is that the speed of operation. They're well matched for learning pattern recognition, for classification, for choice of responses to attacks etc. they will be enforced either in hardware before in software system. Neural nets are well relevant in intrusion detection and intrusion bar [17, 18].

NeuroNet – a neural network system which collects and processes distributed information, coordinates the activities of core network devices, looks for irregularities, makes alerts and initiates countermeasures. Experiments showed that NeuroNet is effective against low-rate TCP-targeted distributed DoS attacks. There are proposals to use them in DoS detection, pc worm detection, spam detection, zombie detection, and malware classification and in rhetorical investigations. One of the major reasons for the recognition of neural nets in cyber security is their quickness or fast speed, if enforced in hardware or utilized in graphic processors [4, 21].

There are new developments within the neural net's technology: third generation neural nets prickling neural networks that imitate organic neurons a lot of realistically, and supply a lot of application opportunities. Neural networks in face recognition system plays an important role in AI for cyber-defence [19].

4.2 Application of Intelligent Agent

Intelligent agents are self-sufficient computer generated force that communicate with each other to share information and participate to each other so as to arrange and actualize proper reactions if there should arise an occurrence of unforeseen occasions. Their mobility and adaptability in the environments they are conveyed in, and in addition their collaborative nature, intelligent agent technology appropriate for fighting cyber assaults [18, 19].

Gou et al. (2006) designed MWDCM - a multi-agent system for computer worm detection and containment in metropolitan area networks, which automatically contains the propagation of worms that waste a lot of network bandwidth and cause router crashes. The experiments showed that their system effectively thwarts worm propagation even at the high worm infection rates. These intelligent systems are very useful in protecting against DDoS (Distributed Denial of Service) assaults. Infrastructure must be installed as for the movement and communication supports the cyber agents [13].

For efficient and operational picture of a Cyber space, we need a Multi-agent Tool, for example, neural network-based intrusion detection and hybrid multi-agent techniques. Intelligent agents are often described schematically as an abstract functional system similar to a computer program. Helano and Nogueira (2006) introduced a synthesis based mobile intelligent multi-agent system approach for combating cyber intrusions. They implemented their system in Prolog and applied it to combating DoS and distributed DoS attacks automatically and without human intervention. They tested their approach on investigating distributed DoS attacks and defence mechanisms. The results showed that cooperation and ability to adapt in intelligent agent groups considerably raises defence effectiveness [3, 13].

4.3 Application of Expert System

An expert system is a computer program that uses artificial intelligence (AI) technologies to define the judgment and behaviour of a human or an organization that has expert knowledge and experience in a particular field. Expert systems have played a large role in many industries including in financial services, telecommunications, healthcare, customer service, transportation, video games, manufacturing, aviation and written communication. An expert system incorporates a knowledge base containing accumulated experience and an inference or rules engine -- a set of rules for applying the knowledge base to each particular situation that is described to the program [21].

Current systems may include machine learning capabilities that allow them to improve their performance based on experience, just as humans do. A more recently developed expert system, ROSS, is an artificially-intelligent attorney based on IBM's Watson cognitive computing system. ROSS relies on self-learning systems that use data mining, pattern recognition, deep learning and natural language processing to mimic the way the human brain works. Expert systems and AI systems have evolved so far that they have spurred debate about the fate of humanity in the face of such intelligence, pondering if computing power has surpassed our ability to control it [20].

The Security expert system follows a set of rules to battle cyber-attacks. It checks the process with the knowledge base if it is good known processes then the security system ignores otherwise the system would terminate the process.

4.4 Other Application of AI

Machado et al. (2005) presented a novel network intrusion detection model based on mobile intelligent agent technology and AISs. They also implemented their design and showed that it is capable of differentiating between various attacks, security violations, and several other security breaches. Also there are many innovations which are done recently, here are some examples [12].

- Adding Intelligence to RPA
- Intelligent Process Automation(IPA)
- Machine Learning for Amateurs
- Advancement in Computer Vision
- AI-infused Chabots
- The Transformation of Digital Workflow etc.

5. Challenges in Cyber Defence

The main challenge is the difficulty of making a solid model of what acceptable behaviour is and what an attack is; hence, they may give a high number of false positive alarms, which may be caused by atypical behaviour that

is actually normal and authorized, since normal behaviour may easily and readily change. The active use of Artificial Intelligence is not the only challenge that the organization and cyber defence professionals need to face. There are others, caused by shortcomings in the current approach to security [12].

- Distant infrastructure. Today, systems communicate across continents, sending sensitive data AI over the world. These transfers don't undergo sufficient protection and are easier to break into.
- Manual detection. Human teams don't have 24/7 focus on security threats and suspicious patterns. Most of the time, systems go unmonitored.
- Reactivity of security teams. Most security experts focus on facing threats rather than predicting them.
- Dynamic treats. Hackers have many strategies for hiding their locations, IPs, identities, and methods. The cyber defence field, on the other hand, is a lot more transparent and open for research – data, created by businesses, is easily accessible by criminals.
- An intrusion detection system, no matter how efficient, may be disabled by attackers if they can learn how the system works.
- Another problem involves supplying intrusion detection systems that will conform to legal regulations, security requirements and/or service-level agreements in real world.

6. The Way Forward in AI

It's of little surprise that cyber security is a priority for all organizations, more so at a time when the world is moving towards digitalization. AI consultants are keenly building advanced solutions to provide a profound and strong defence mechanism. Cyber security needs much more attention. Given human limitations and the fact that agents such as computer viruses and worms are intelligent, network-centric environments require intelligent cyber sensor agents which will detect, evaluate and respond to cyber attacks in a timely manner [23].

With AI-powered tools here are few predictions on how AI will change (enhance) the cyber defence system?

- Using AI tools to monitor security incidents
- Integrating machine learning into firewalls to flag any anomaly
- Identifying the origin of cyber attacks through NLP applications
- Using RPA bots to automate rule-based tasks and processes
- Monitor and analyze mobile endpoints for cyber threats

Furthermore, a lot more research needs to be done before we are able to construct trustworthy, deployable intelligent agent systems that can manage distributed infrastructures. Future work must search for a theory of group utility function to allow groups of agents to make decisions. It is recommended to teams to not only find preventive cyber attack solutions with AI but also look to the tech to plan an aftermath [22].

7. Conclusion

AI is considered as a standout amongst the most encouraging advancement in the information age and cyber security. The fast development of information technology had a lot of positive impact and brought many conveniences into our lives. However, it also caused issues that are difficult to manage such as the emergence of cyber crimes. Therefore enhancing security execution and better protect system from an expanding number of refined cyber threats. As the technology continues to evolve, criminal cases change correspondingly. Every day we are faced with increasing number and variety of cyber crimes, since this technology presents an easy way for criminals to achieve their goals.

Organizations predict that hackers will start actively using AI in the near future, and lets' face it, typical tools can't accommodate such risks. As it is, most organizations aren't ready to face highly intelligent viruses, malware, ransom ware, and other forms of cyber threats. One thing is certain; adopting AI solutions can already help businesses spend less time and effort on their daily security tasks, while also keeping them better prepared for new risks. IT's both the weapon against current threats and investment in the future. The technology is getting more available which means; soon no business will have a reason to delay adopting AI. Instead of waiting for custom tools to implement AI on a large level, it's better to be ahead of the situation and start building powerful custom AI security too.

This paper has briefly presented advances made so far in the field of applying AI techniques for combating cyber crimes, their challenges and desired characteristics, as well as given the scope to way forward in cyber defence.

References

1. D. Dasgupta, 2006, "Computational Intelligence in Cyber Security", IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CIHSPS 2006), pp. 2–3.
2. H. Chen, F. Y. Wang, 2005, "Guest Editors' Introduction: Artificial Intelligence for Homeland Security", IEEE intelligent systems, Vol. 20, No. 5, pp. 12–16.
3. Selma Dilek, Hüseyin Çakır and Mustafa Aydın, 2015, "Applications of Articial Intelligence Techniques to Combating Cyber Crimes: A Review". International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1.
4. E. Tyugu, 2011, "Artificial intelligence in cyber defence", 3rd International Conference on Cyber Conflict (ICCC 2011), pp. 1–11.
5. KINGSLEY CHIMEZIE AMADI, 2020, Machine Learning as a Strategic Initiative for Cyber Defence Dissertation Manuscript.
6. Ishaq Azhar Mohammed, 2020, Artificial Intelligence for Cyber Security: A Systematic Mapping of Literature International Journal of Innovations in Engineering Research and Technology [IJIERT].
7. Suyash srivastav, Bijoy benny, 2021, Artificial Intelligence (A. I) and its application in Cyber Security.
8. Florentina - Loredana DRAGOMIR, ARTIFICIAL INTELLIGENCE TECHNIQUES CYBER SECURITY, International Scientific Conference "Strategies XXI", 2017.
9. Dimitar Stevo Bogatinov, Mitko Bogdanoski and Slavko Angelevski "AI based Cyber Defence for more secure Cyber Space" 2016.
10. L. Hong, 2008, "Artificial Immune System for Anomaly Detection", IEEE International Symposium on Knowledge Acquisition and Modelling Workshop, pp. 340 – 343.
11. X. B. Wang, G. Y. Yang, Y. C. Li, D. Liu, 2008, "Review on the application of Artificial Intelligence in Antivirus Detection System", IEEE Conference on Cybernetics and Intelligent Systems, pp. 506 - 509.
12. Artificial Intelligence, wikipedia.org/wiki/Artificial_intelligence, 2021.
13. L. Phillips, H. Link, R. Smith, L. Weiland, 2006, Agent-Based Control of Distributed Infrastructure Resources, U.S. Department of Energy, Sandia National Laboratories, USA.
14. M. R. Stytz, D. E. Lichtblau, S. B. Banks, 2005, "Toward using intelligent agents to detect, assess, and counter cyber attacks in a network-centric environment", Ft. Belvoir Defence Technical Information Centre, 1.Edition, Alexandria, VA.
15. J. Helano, M. Nogueira, 2006, "Mobile Intelligent Agents to Fight Cyber Intrusions", the International Journal of Forensic Computer Science (IJoFCS), Vol. 1, pp. 28-32.
16. E. Herrero, M. Corchado, A. Pellicer, A. Abraham, 2007, "Hybrid multi agent-neural network intrusion detection with mobile visualization", Innovations in Hybrid Intelligent Systems, Vol. 44, pp. 320-328.
17. C. Bitter, D.A. Elizondo, T. Watson, 2010, "Application of Artificial Neural Networks and Related
18. Techniques to Intrusion Detection", IEEE World Congress on Computational Intelligence (WCCI 2010), pp. 949 – 954.
19. E. S. Brunette, R. C. Flemmer, C. L. Flemmer, 2009, "A review of artificial intelligence", Proceedings of the 4th International Conference on Autonomous Robots and Agents, pp. 385-392.
20. J. S. Russell, P. Norvig, 2003, Artificial Intelligence: A Modern Approach, 2nd edition, Upper Saddle River, Prentice Hall, New Jersey, USA.
21. G. Luger, W. Stubblefield, 2004, Artificial Intelligence: Structures and Strategies for Complex Problem Solving, 5th edition, Addison Wesley.
22. Thanh Cong Truong, Quoc Bao Diep and Ivan Zelinka, 2020, "Artificial Intelligence in the Cyber Domain: Offense and Defence".
23. A. Patel, M. Taghavi, K. Bakhtiyari, J. Celestino Júnior, 2012, "Taxonomy and Proposed Architecture of Intrusion Detection and Prevention Systems for Cloud Computing", Y. Xiang et al. (Eds.), Springer-Verlag Berlin Heidelberg, pp. 441-458.
24. Amr Kayid, 2020, "The role of Artificial Intelligence in future Technology".

Acknowledgement

I wish to express my sincere gratitude to Professors and staff members of Department of Computer Engineering for providing me an opportunity to do my review research work and for his guidance and encouragement in carrying out this research work.

I also thank the Director of Gandhinagar Institute of Technology Dr. H N Shah for providing me the opportunity to embark on this project.