MANTECH Publications
Journal of Artificial Intelligence, Machine Learning and Soft Computing
Volume 3, Issue 1, January-June 2018

Applications of Computing Techniques to Combating Cyber Crimes: A Review

Smaranika Mohapatra[1], Dr. Kusumlata H Jain[2]
Department of Computer Science & Engineering
Maharishi Arvind Institute of Engineering & Technology, Jaipur
***Email ID**: msmaranika6@gmail.com[1], jain.kusum81@gmail.com[2]*

Abstract

With the advances in data technology (IT) criminals ar victimization Internet to commit varied cyber crimes. Cyber infrastructures ar extremely susceptible to intrusions and alternative threats. Physical devices and human intervention aren't comfortable for observation and protection of those infrastructures; therefore, there's a requirement for additional refined cyber defense systems that require to be versatile, labile and strong, and able to find a good type of threats and create intelligent time period selections. Varied bio-inspired computing strategies of AI are progressively taking part in a vital role in cyber crime detection and interference. The aim of this study is to gift advances created to date within the field of applying AI techniques for combating cyber crimes, to demonstrate however these techniques may be an efficient tool for detection and interference of cyber attacks, similarly on provide the scope for future work.

Keywords: *Cyber Crime, Artificial Intelligence, Intelligent Cyber Defense Methods, Intrusion Detection and Prevention Systems, Computational Intelligence*

INTRODUCTION

With the advances in data technology (IT) criminals square measure mistreatment internet to commit various cyber crimes. Growing trends of advanced distributed and web computing raise vital questions on data security and privacy. Cyber infrastructures square

measure extremely liable to intrusions and different threats. Physical devices like sensors and detectors don't seem to be ample for watching and protection of those infrastructures; therefore, there's a requirement for additional refined IT which will model traditional behaviors and observe abnormal ones. These cyber defense systems got to be versatile, convertible and sturdy, and ready to observe a good type of threats and create intelligent period choices [1, 2].

With the pace and quantity of cyber attacks, human intervention is solely not ample for timely attack analysis and applicable response. the actual fact is that the foremost network-centric cyber attacks square measure dispensed by intelligent agents like pc worms and viruses; therefore, combating them with intelligent semi-autonomous agents which will observe, evaluate, and answer cyber attacks has become a demand. These therefore known as computer-generated forces can ought to be ready to manage the whole method of attack response during a timely manner, i.e. to conclude what variety of attack is going on, what the targets square measure and what's the acceptable response, in addition as the way to grade and stop secondary attacks [3].

Furthermore, cyber intrusions don't seem to be localized. they're a world menace that poses threat to any system within the world at a growing rate. there have been times once solely educated specialist might commit cyber crimes, however nowadays with the growth of the net, virtually anyone has access to the information and tools for committing these crimes. standard mounted algorithms (hard-wired logic on higher cognitive process level) became ineffective against combating dynamically evolving cyber attacks. this can be why we want innovative approaches like applying ways of computing (AI) that give flexibility and learning capability to software package which can assist humans in fighting cyber crimes [4, 5]

AI offers this and varied different prospects. various nature-inspired computing ways of AI (such as procedure Intelligence, Neural Networks, Intelligent Agents, Artificial Immune Systems, Machine Learning, data processing, Pattern Recognition, formal logic, Heuristics, etc.) are more and more enjoying a crucial role in cyber crime detection and hindrance. AI allows US to style involuntary computing solutions capable of adapting to their

context of use, mistreatment the ways of self-management, self-tuning, self-configuration, self-diagnosis, and self-healing. once it involves the long run of knowledge security, AI techniques appear terribly promising space of analysis that focuses on up the safety measures for cyber area [2, 6, 7].

The purpose of this study is to gift advances created to date within the field of applying AI techniques for combating cyber crimes, to demonstrate however these techniques is an efficient tool for detection and hindrance of cyber attacks, in addition on offer the scope for future work.

CYBER CRIMES: DEFINITION, ISSUES

The fast development of computing technology and web had lots of positive impact and brought several conveniences in our lives. However, it conjointly caused problems that square measure tough to manage like emergence of latest kinds of crimes. as an example, common crimes like felony and fraud earned new kind of "Cyber Crimes" through info technology. Moreover, as this technology continues to evolve, criminal cases amendment correspondingly. daily we have a tendency to square measure featured with increasing range and style of cyber crimes, since this technology presents a simple method for criminals to realize their goals. what is more, info technology facilitates economic process of those crimes by erasing country borders and creating it a lot of tougher to watch, detect, forestall or capture cyber criminals [8, 9, 10].

Information technology is progressively being each targeted and used as a tool for committing crimes. Electronic devices and alternative sophisticated merchandise modify criminals to commit low cost and straightforward crimes. Computers, phones, web and every one alternative info systems developed for the advantage of humanity square measure vulnerable to criminal activity. Crimes that concentrate on info technology systems usually target e-mail accounts, bank accounts, computers, servers, websites, personal information, and digital records of personal and public establishments. These crimes also are called "Digital Crimes", "Computer Crimes", "Crimes of knowledge Technologies", "Network Crimes" or "Internet Crimes". Cyber crimes comprises offenses like laptop intrusions, misuse of belongings rights, economic spying, on-line extortion,

international concealing, non-delivery of products or services and a growing list of alternative offenses expedited by web [8, 10, 11].

Although "cyber crime" has become a standard phrase these days, it's tough to outline it exactly. Most of the prevailing definitions were developed by experimentation. Gordon and Ford (2006) outline cyber crime as: "any crime that's expedited or committed employing a laptop, network, or hardware device" wherever "computer or device is also the agent of the crime, the help of the crime, or the target of the crime" [12]. Dictionary.com defines cyber crime as "criminal activity or a criminal offense that involves the net, a ADP system, or laptop technology" [13]. Fisher and laboratory (2010) outlined cyber crime as "crime that happens once laptops or computer networks square measure concerned as tool, locations, or targets of crime" [14].

Every day the quantity of digital information keep and processed on computers and alternative computing systems will increase exponentially, with individuals communication, sharing, working, shopping, and socialization victimization computers and web. Language and country barriers have disappeared and virtual world has become a lot of inhabited than ever. The idea of crime is gift once managing individuals, thus cyber house has not stayed isolated from the ideas of crime and criminals either [11]. Brenner (2010) argues that "most of the cyber crime we have a tendency to see these days merely represents the migration of real-world crime to Internet that becomes the tool criminals use to commit previous crimes in new ways " [15].

ARTIFICIAL INTELLIGENCE AND INTRUSION DETECTION

AI (also referred to as machine intelligence within the beginning) emerged as a groundwork discipline at the summer research of Dartmouth in July 1956. AI is delineate in 2 ways:

i. as a science that aims to find the essence of intelligence and develop intelligent machines; or

ii. as a science of finding strategies for resolution advanced issues that can't be resolved while not applying some intelligence (e.g. creating right choices supported massive amounts of data). within the application of AI to cyber

defense, we tend to ar a lot of inquisitive about the second definition. analysis interest in AI embody ways that to create machines (computers) simulate intelligent human behavior like thinking, learning, reasoning, planning, etc. [5, 7, 16].

The general downside of simulating intelligence has been simplified to specific sub-problems that have sure characteristics or capabilities that AN intelligent system ought to exhibit. the subsequent characteristics have received the foremost attention [17, 18, 19]:

a) Deduction, reasoning, downside resolution (embodied agents, neural networks, applied mathematics approaches to AI);

b) Knowledge illustration (ontologies);

c) Planning (multi-agent coming up with and cooperation);

d) Learning (machine learning);

e) Natural Language process (information retrieval – text mining, machine translation);

f) Motion and Manipulation (navigation, localization, mapping, motion planning);

g) Perception (speech recognition, facial, recognition, object recognition);

h) Social Intelligence (empathy simulation);

i) Creativity (artificial intuition, artificial imagination); and

j) General Intelligence (Strong AI).

Classic AI approaches concentrate on individual human behavior, data illustration and reasoning strategies. Distributed computing (DAI), on the opposite hand, focuses on social behavior, i.e. cooperation, interaction and knowledge-sharing among totally different units (agents). The method of finding an answer in distributed resolution issues depends on sharing data concerning the matter and cooperation among agents. it absolutely was from these ideas that the thought of intelligent multi-agent technology emerged. AN agent is AN autonomous psychological feature entity that understands its setting, i.e. it will work by itself and it's an

indoor decision-making system that acts globally around alternative agents. In multi-agent systems, a gaggle of mobile autonomous agents join forces during a coordinated and intelligent manner so as to resolve a selected downside or categories of issues. They're somewhat capable of comprehending their setting, creating choices and communication with alternative agents [4]. Multi-agent technology has several applications; however this study can solely discuss applications to defense against cyber intrusions (See Section four.2).

Intelligent agents systems are simply a neighborhood of a far larger AI approach referred to as machine Intelligence (CI). CI includes many alternative nature-inspired techniques like neural networks, formal logic, organic process computation, swarm intelligence, machine learning and artificial immune systems.

These techniques give versatile higher cognitive process mechanisms for dynamic environments like cyber-security applications. Once we say 'nature-inspired', it means there's a growing interest within the field of computing technologies to mimic biological systems (such as biological immune system) and their exceptional skills to be told, memorize, recognize, classify and method data. Artificial immune systems (AISs) ar AN example of such technology [2].

AISs ar machine models galvanized by biological immune systems that ar all-mains to ever-changing environments and capable of continuous and driving learning. Immune systems are answerable for detection and coping with intruders in living organisms. AISs are designed to mimic natural immune systems in applications for pc security normally, and intrusion detection systems (IDSs) particularly [20].

Genetic algorithms ar {yet ANother|yet one more|one more} example of an AI technique, i.e. machine learning approach supported on the idea of organic process computation, that imitate the method of activity. they supply sturdy, adaptive, and best solutions even for advanced computing issues. they will be used for generating rules for classification of security attacks and creating specific rules for various security attacks in IDSs [21, 22].

Many strategies for securing knowledge over networks and also the net are developed (e.g. anti-virus software system, firewall, encryption, secure protocols, etc.); however, adversaries will invariably realize new ways that to attack network systems. AN intrusion detection and bar system (IDPS) (See Fig. 1) is software system or a hardware device placed within the network, which might find potential intrusions and additionally conceive to stop them. IDPSs give four very important security functions: observation, detecting, analyzing, and responding to unauthorized activities [23, 24].

Artificial Neural Networks (ANNs) comprises artificial neurons that may learn and solve issues once combined along. Neural networks that have ability to be told, method distributed info, self-organize and adapt, area unit applicable to resolution issues that need considering state, inexactitude and ambiguity at a similar time. once neural networks comprises an outsized variety of artificial neurons, they will offer a practicality of massively parallel learning and decision-making with high speed, that makes them appropriate for learning pattern recognition, classification, and choice of responses to attacks [5, 7]

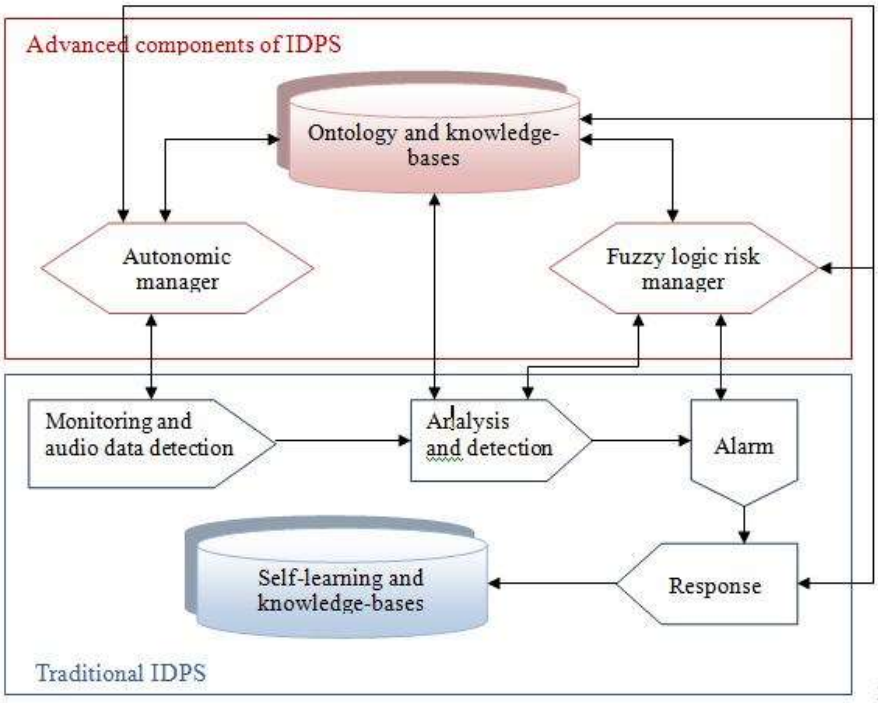

Figure 1: A typical IDPS [24].

Desired Characteristics of an IDPS

An IDPS ought to have sure characteristic so as to be ready to offer economical security against serious attacks. Those characteristics embrace the subsequent [25]:

- Real-time intrusion detection – whereas the attack is ongoing or straight off later on,
- False positive alarms should be decreased ,
- Human supervising ought to be reduced to minimum, and continuous operation ought to be ensured,
- Recoverability from system crashes, either accidental or those ensuing from attacks,
- Self-monitoring ability so as to observe attackers' makes an attempt to vary the system,
- Compliance to the safety policies of the system that's being monitored, and
- Adaptability to system changes and user behavior over time.

APPLICATIONS OF AI TO DEFENSE AGAINST CYBER CRIMES

Available educational resources show that AI techniques have already got varied applications in combating cyber crimes. for example, neural networks ar being applied to intrusion detection and hindrance, however there also are proposals for mistreatment neural networks in "Denial of Service (DoS) detection, pc worm detection, spam detection, zombie detection, malware classification and rhetorical investigations" [5]. AI techniques like Heuristics, data processing, Neural Networks, and AISs, have additionally been applied to new-generation anti-virus technology [7]. Some IDSs use intelligent agent technology that is typically even combined with mobile agent technology. Mobile intelligent agents will travel among assortment points to uncover suspicious cyber activity [2]. Wang et al. (2008) declared that the longer term of anti-virus discovering technology is in application of Heuristic Technology which suggests "the data and skills that use some strategies to work out and showing intelligence analyze codes to detect the unknown virus by some rules whereas scanning" [7]. This section can in brief gift connected work and a few existing applications of AI techniques to cyber defense

Artificial Neural Network Applications

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 [26].

Chen (2008) designed 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 [27].

Linda et al. (2009) presented the Intrusion Detection System using Neural Network based Modeling (IDS-NNM) which proved to be capable of detecting all intrusion attempts in the network communication without giving any false alerts [28].

Barika et al. (2009) presented a detailed architecture of a distributed IDS based on artificial neural network for enhanced intrusion detection in networks [29].

Itikhar et al. (2009) applied neural network approach to analyzing DoS attacks. Their experiments showed that their neural network approach detects DoS attacks with more accuracy and precision than other approaches [30].

Wu (2009) presented a hybrid method of rule-based processing and back-propagation neural networks for spam filtering. Their approach proved to be much more robust compared to other spam detection approaches that use keywords, because spamming behaviors frequently change [31].

Salvador et al. (2009) presented a novel approach for Zombie PCs detection based on neural networks. Experiments showed how their approach is computationally efficient, easy to deploy in real network scenarios and achieves good Zombie detection results [32].

Bitter et al. (2010) presented host-based and network-based intrusion detection systems with a special focus on systems that employ artificial neural networks to detect suspicious and potentially malicious traffic [26].

Al-Janabi and Saeed (2011) designed a neural network-based IDS that can

promptly detect and classify various attacks [33].

Barman and Khataniar (2012) also studied the development of IDSs based on neural network systems. Their experiments showed that the system they proposed has intrusion detection rates similar to other available IDSs, however, it proved to be at least 20.5 times faster in detection of DoS attacks [34].

Artificial Immune System Applications

AISs, a bit like the biological immune systems that they're supported, square measure utilized to uphold stability in a very dynamic atmosphere. The immune-based intrusion detection includes the evolution of immunocytes (self-tolerance, clone, variation, etc.) and antigens detection at the same time. AN system produces antibodies to resist pathogens and therefore the intrusion intensity are often calculable by variation of the protein concentration. Therefore, AISs play a vital role within the cyber security analysis [48].

Sirisanyalak ANd Sornil (2007) bestowed an AIS-based e-mail feature extraction approach for spam detection. The performance analysis results showed that the planned methodology is way additional economical in spam detection than different existing systems, with terribly low false positive and false negative rates (0.91% and 1.95% respectively) [49].

Lebbe et al. (2007) analyzed varied AIS models utilized in IDSs and introduced Danger Theory (DT) in AIS as a way for danger response in wireless mesh networks. For classification of network dangers they used Self-organizing Maps (SOMs) as classifiers. Their experiments valid their proposal of applying DT to security of wireless mesh networks [50].

Hong (2008) bestowed AN AIS-based hybrid learning formula for anomaly detection in pc systems [20].

Gianini et al. (2009) planned AN extension of AIS model for ADP system security to close intelligence domain. Their extended model will offer sensory activity functions and detection capabilities with device intelligence (e.g. transmission sensing element system interpretation) [51]. EshghiShargh (2009) additionally studied the advantages of AI generally, and AISs specially, for rising IDSs by investigation completely different IDS styles supported AISs. The results showed however AIS approach to IDS

style is often fruitful for future applications [52].

Chao and Tan (2009) planned a completely unique virus detection system supported AIS. The experimental results showed that virus detection system they planned features a "strong detection ability and smart generalization performance" [53].

Danforth (2009) investigated the chance of increasing AISs for classification of internet server attacks, which might facilitate supervisor with a warning regarding the severity of the attack and assist in mitigation of direct attacks [54].

Mohamed ANd Abdullah (2009) bestowed an AIS-based security framework for securing mobile spontanepous networks, that is scalable, robust, and has traits of disreputability, second response and self-recovery. Their design resolved some limitations found within the previous connected studies like quantifiability and information measure conservation [55].

Qiang ANd Yiqian (2010) planned an AIS-based network security scenario assessment model which may create time period and quantitative security scenario assessment of the system, and supply support needed to form time period changes of the defense measures. Theoretical analysis and experiments showed the effectiveness of the model in time period anomaly detection for network security [56].

Rui and Wanbo (2010) proposed an AIS-based self-learning intrusion response model which can recognize and classify unknown attacks. Their model has a dynamic response decision-making mechanism which can adjust the defensive tactics according to the changes in the environment and keep the system safe with the minimum cost. The experiments showed that their model has qualities such as self-adaptation, rationality, quantitative calculation, and that it provides efficient intrusion response [48].

Endy et al. (2010) used SOMs to visualize the topology of the data in order to perform cluster analysis of the textual documents related to cyber terrorism [57].

Yang et al. (2011) presented a network security evaluation model for quantitative analysis of the degree of intrusion danger level based on AIS theory, and demonstrated its advantages over

traditional models for network security evaluation [58].

Liu et al. (2011) introduced an AIS-based intrusion detection mechanism into the Internet of Things (IoT) environment, which simulates self-adaptation and self-learning mechanisms via dynamic adaptation to the environment. The analysis of their proposal showed that their model provides a new effective intrusion detection for the Internet of Things [59].

Zhang et al. (2011) proposed SGDIDS – a new hierarchical Distributed Intrusion Detection System for improving cyber security of the Smart Grid. Their system consists of an intelligent module (among other modules) which uses AIS to detect and classify malicious data and possible cyber attacks. Simulation results showed that their system is applicable to identification of malicious network traffic and improving system security [60].

Ansari and Inamullah (2011) proposed an enhancement for the anomaly detection based on AIS and showed how their model improves AIS performance in applications such as anomaly detection, ensuring security, detecting errors and performing data mining in mobile ad hoc networks [61].

Fang et al. (2012) proposed an AIS for phishing detection through memory and mature detectors. The analysis showed that their system is unique and more flexible and adaptive than other existing phishing detection systems [62].

Mavee and Ehlers (2012) proposed IISGP – a new AIS-based model for Smart Grid protection. Basically, they aimed to design a bio-inspired AIS model for intrusion detection, access control and anomaly detection in critical infrastructures which are becoming increasingly dependent on cyber technology [63].

Kumar and Reddy (2014) developed a unique agent based intrusion detection system for wireless networks that collects information from various nodes and uses this information with an evolutionary AIS to detect and prevent the intrusion via bypassing or delaying the transmission over the intrusive paths. The experimental results showed that the system is well suited for intrusion detection and prevention in wireless networks [64].

Advantages of AI Applications to IDPSs

AI techniques introduce numerous advantages into intrusion detection and prevention (see Table 1).

Table 1: Advantages that some AI techniques bring to intrusion detection and prevention

Technology	Advantages
	Parallelism in information processing;
	Learning by example;
Artificial	Nonlinearity – handling complex nonlinear functions;
Neural	Superiority over complex and perplexing differential equations;
Networks	Resilience to noise and incomplete data;
	Versatility and flexibility with learning models;
	Intuitiveness – as they are an abstraction of biological neural networks [26].
	Dynamic structure;
Artificial	Parallelism and distributed learning – using data network communications and
Immune	parallelism in detection and elimination tasks;
Systems	Self-adaptability and self-organizing – updating intrusion marks without
	human involvement; Robustness; Selective response – removing malicious activity by the best means available; Diversity – each detector node generates a statistically unique set of non-self detectors; Resource optimization; Multi-layered structure – attackers cannot succeed with their malicious activities by circumventing only one layer, since multiple layers of different structures are in charge of monitoring a single point. Disposability – not being dependent on a single component which can be easily replaced by other components [52, 56, 88].

LIMITATIONS OF CURRENT ANOMALY DETECTION/ PREVENTION SYSTEMS

Although anomaly noticeion systems provide the chance to detect antecedently unknown attacks, they need some vital limitations that require to be tackled. the most issue is that the issue of constructing a solid model of what acceptable behavior is ANd what an attack is; thence, they'll provides a high range of false positive alarms, which can be caused by atypical behavior that's truly traditional and approved, since traditional behavior could simply and without delay modification. alternative limitations embody the subsequent [25, 26, 29]:

- In order for the anomaly detection system to be able to characterize traditional patterns and make a model of the conventional behavior, wide-ranging coaching sets of the conventional system activities area unit required. Any modification within the system's traditional patterns should result in necessary update of the knowledge domain.

- If the detection and bar system inaccurately classifies a legitimate activity as a malicious one, the results are terribly unfortunate since it'll conceive to stop the activity or modification it.

- An intrusion detection system, notwithstanding however economical, could also be disabled by attackers if they'll learn the way the system works.

- In heterogeneous environments there's conjointly a difficulty of desegregation data from totally different sites.

- Another downside involves activity intrusion detection systems which will adapt to legal rules, security necessities and/or service-level agreements in world.

SCOPE FOR FUTURE WORK

Cyber security wants far more attention. Given human limitations and therefore the indisputable fact that agents like pc viruses and worms area unit intelligent, network-centric environments need intelligent cyber sensing element agents (or computer-generated forces) which can notice, assess and answer cyber attacks in a very timely manner [3].

Application of AI techniques in cyber defense can would like coming up with and future analysis. one in all the challenges is information management in

network-centric warfare, thence a promising space for analysis is introduction of standard and graded information design within the higher cognitive process code. fast scenario assessment and call superiority will solely be bonded with automatic information management. it's conjointly predictable that the grand goal of AI analysis

– Development of artificial general intelligence - is reached in not therefore distant future which might result in Singularity represented as "the technological creation of smarter-than-human intelligence". still, it's of crucial importance that we've got the flexibility to use higher AI technology in cyber defense than the one offenders possess [5].

Furthermore, lots a lot of analysis has to be done before we tend to area unit able to construct trustworthy, deployable intelligent agent systems that may manage distributed infrastructures. Future work should look for a theory of cluster utility operates to permit teams of agents to form selections [37].

For future add enhancing IDPSs, unattended learning algorithms and new techniques are thought of along to form hybrid IDPS which can improve the performance of anomaly intrusion detection [85]. Moreover, combining every kind of AI technologies can become the most development trend within the field of anti-virus technology [7].

Even though machine intelligence techniques are wide employed in the sector of pc security and forensics, there area unit bound moral and legal issues that arise because the technology quickly expands. a number of these issues area unit privacy issues or power problems on the moral facet or queries of group action on the legal facet. a good vary of each moral and legal queries return up within the light-weight of the potential autonomy of this technology. queries like "to what extent will a synthetic neural network replace human judgment", "to what degree will we wish to permit technology to require human roles" or "what legal precedent is applied to machines" can got to be answered [91].

CONCLUSION

The quick development of knowledge technology had plenty of positive impact and brought several conveniences into our lives. However, it conjointly caused problems that ar tough to manage like the emergence of cyber crimes. because the technology continues to evolve, criminal

cases modification correspondingly. daily we tend to ar sweet-faced with increasing variety and kind of cyber crimes, since this technology presents a straightforward approach for criminals to attain their goals. essential infrastructures ar particularly vulnerable.

Application of AI techniques ar already getting used to help humans in fighting cyber crimes, as they supply flexibility and learning capabilities to IDPS computer code. it's become obvious wide information usage in deciding} process needs intelligent call support in cyber defense which may be with success achieved victimisation AI strategies.

Available educational resources show that AI techniques have already got varied applications in combating cyber crimes. This paper has in short given advances created thus far within the field of applying AI techniques for combating cyber crimes, their current limitations and desired characteristics, furthermore as given the scope for future work.

REFERENCES

1. H. Chen, F. Y. Wang, (2005) "Guest Editors' Introduction: Artificial Intelligence for Homeland Security", IEEE intelligent systems, Vol. 20, No. 5, pp. 12–16.

2. 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

3. M. R. Stytz, D. E. Lichtblau, S. B. Banks, (2005) "Toward using intelligent agents to detect, assess, and counter cyberattacks in a network-centric environment", Ft. Belvoir Defense Technical Information Center, 1. Edition, Alexandria, VA.

4. 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.

5. E. Tyugu, (2011) "Artificial intelligence in cyber defense", 3rd International Conference on Cyber Conflict (ICCC 2011), pp. 1–11.

6. 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.

7. 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.

8. H. Çakir, E. Sert, (2011) “Biliðim Suçlari Ve Delillendirme Süreci”, Örgütlü Suçlar ve Yeni Trendler. O. Ö. Demir, M. Sever, (Eds.), Uluslararası Terörizm ve Sınıraðan Suçlar Sempozyumu (UTSAS 2010) Seçilmið Bildirileri, Ankara: Polis Akademisi Yayınları, Ankara, pp. 143.

9. N. Doğan, (2008) “Türkiye’de Biliðim Suçlarına Bakıð”, Popüler Bilim, Vol. 8, No. 3, pp. 14-17.

10. A. S. Poonia, A. Bhardwaj, G. S. Dangayach, (2011) “Cyber Crime: Practices and Policies for Its Prevention”, The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management, Vol. 19, No. SP1.

11. H. Dijle, N. Doğan, (2011) “Türkiye’de Biliðim Suçlarına Eğitimli nsanların Bakıði”, Biliðim Teknolojiler Dergisi, Vol. 4, No. 2.

12. S. Gordon, R. Ford, (2006) “On the definition and classification of cybercrime”, Journal in Computer Virology, Vol. 2, No. 1, pp. 13 20.

13. http://dictionary.reference.com/browse/cybercrime, (24/11/2014)

14. B. S. Fisher, S. P. Lab, (2010) Encyclopedia of Victimology and Crime Prevention, SAGE Publications, Vol. 1, pp. 251, USA.

15. S. W. Brenner, (2010) Cybercrime: Criminal Threats from Cyberspace, Greenwood publishing group, Library of Congress Cataloging-in-Publication Data, USA.

16. 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.

17. J. S. Russell, P. Norvig, (2003) Artificial Intelligence: A Modern Approach, 2nd edition, Upper Saddle River, Prentice Hall, New Jersey, USA.

18. G. Luger, W. Stubblefield, (2004) Artificial Intelligence: Structures and Strategies for Complex Problem Solving, 5th edition, Addison Wesley.

19. Artificial Intelligence, Wikipedia, http://en.wikipedia.org/wiki/Artificial_intelligence, (24/11/2014)

20. L. Hong, (2008) "Artificial Immune System for Anomaly Detection", IEEE International Symposium on Knowledge Acquisition and Modeling Workshop, pp. 340 – 343.

21. N. A. Alrajeh, J. Lloret, (2013) "Intrusion Detection Systems Based on Artificial Intelligence Techniques in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, Vol. 2013, Article ID 351047.

22. S. Shamshirband, N. B. Anuar, M. L. M. Kiah, A. Patel, (2013) "An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique," Engineering Applications of Artificial Intelligence, Vo. 26, pp. 2105–2127.

23. K. P. Kaliyamurthie, R. M. Suresh, (2012) "Artificial Intelligence Technique Applied to Intrusion Detection", International Journal of Computer Science and Telecommunications, Vol. 3, No. 4, pp. 20 25.

24. A Patel, M. Taghavi, K. Bakhtiyari, J. Celestino Junior, (2013) "An intrusion detection and prevention system in cloud computing: A systematic review", Journal of Network and Computer Applications, Elsevier, Vol. 36, pp. 25–41.

25. A. Patel, Q. Qassim, Z. Shukor, J. Nogueira, J. Júnior, C. Wills, (2010) "Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System," Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), Port Elizabeth, South Africa, May 17-18, 2010.

26. A. Bitter, D.A. Elizondo, T. Watson, (2010) "Application of Artificial Neural Networks and Related Techniques to Intrusion Detection", IEEE World Congress on Computational Intelligence (WCCI 2010), pp. 949 – 954.

27. Y. Chen, (2008) "NeuroNet: Towards an Intelligent Internet Infrastructure", 5th IEEE Consumer Communications and Networking Conference (CCNC 2008), pp. 543 547.

28. L. Ondrej, T. Vollmer, M. Manic, (2009) "Neural Network Based Intrusion Detection System for Critical Infrastructures", Proceedings of International Joint Conference on Neural Networks, pp. 1827 1834.

29. F. Barika, K. Hadjar, N. El-Kadhi, (2009) "Artificial neural network for mobile IDS solution", Security and Management, pp. 271–277.

30. Iftikhar, B.A. Azween, A. S. Alghamdi, (2009) "Application of artificial neural network in detection of dos attacks," Proceedings of the 2nd ACM international conference on Security of information and networks, pp. 229–234.

31. H. Wu, (2009) "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," Expert Systems with Applications, Vol. 36, Issue. 3, Part: 1, pp. 4321–4330.

32. P. Salvador, A. Nogueira, U. Franca, R. Valadas, (2009) "Framework for Zombie Detection using Neural Networks", Fourth International Conference on Internet Monitoring and Protection (ICIMP '09), pp.14 – 20.

33. S. T. F. Al-Janabi, H. A. Saeed, (2011) "A Neural Network Based Anomaly Intrusion Detection

System", Developments in E-systems Engineering (DeSE), pp. 221 – 226.

34. D. K. Barman, G. Khataniar, (2012) "Design Of Intrusion Detection System Based On Artificial Neural Network And Application Of Rough Set", International Journal of Computer Science and Communication Networks, Vol. 2, No. 4, pp. 548-552.

35. N. C. Rowe, "Counterplanning Deceptions To Foil Cyber-Attack Plans", Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, Information Assurance Workshop, pp. 203 210.

36. X. Gou, W. Jin, D. Zhao, (2006) "Multi-agent system for worm detection and containment in metropolitan area networks", Journal of Electronics, Vol. 23, No. 2, pp. 259-265.

37. 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.

38. Kotenko, A. Ulanov, (2007) "Multi-Agent Framework fo Simulation of Adaptive Cooperative Defense Against Internet Attacks", International Workshop on Autonomous Intelligent Systems: Agents and Data Mining (AIS-ADM 2007), Springer-Verlag, Berlin Heidelberg, vol. 4476, pp. 212–228.

39. 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.

40. H. Fu, X. Yuan, K. Zhang, X. Zhang, Q. Xie, (2007) "Investigating Novel Immune-Inspired Multi-Agent Systems for Anomaly Detection", The 2nd IEEE Asia-Pacific Service Computing Conference, pp. 466 472.

41. D. Edwards, S. Simmons, N. Wilde, (2007) “Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture”, IEEE International Conference on System of Systems Engineering (SoSE '07), pp. 1 – 6.

I. Kotenko, A. Konovalov, A.Shorov, (2010) “Agent-Based modeling and Simulation of Botnets and Botnet Defence”, Proceeding of Conference on Cyber Conflict (CCD COE).

42. X. Ye, J. Li, (2010) “A Security Architecture Based on Immune Agents for MANET”, International Conference on Wireless Communication and Sensor Computing (ICWCSC 2010), pp. 1 5.

43. D. Wei, Y. Lu, M. Jafari, P. Skare, K. Rohde, (2010) “An Integrated Security System of Protecting Smart Grid against Cyber Attacks”, Innovative Smart Grid Technologies (ISGT), pp. 1 7.

44. F. Doelitzscher, C. Reich, M. Knahl, N. Clarke, (2011) "An Autonomous Agent Based Incident Detection System for Cloud Environments," IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom), pp.197-204.

45. A. F. Shosha, P. Gladyshev, W. Shinn-Shyan, L. Chen-Ching, (2011) "Detecting cyber intrusions in SCADA networks using multi-agent collaboration," 16th International Conference on Intelligent System Application to Power Systems (ISAP), pp.1-7.

46. Ionita, L. Ionita, (2013) "An agent-based approach for building an intrusion detection system," 12th International Conference on Networking in Education and Research (RoEduNet), pp.1-6.

47. L. Rui, L. Wanbo, (2010) “Intrusion Response Model based on AIS”, International Forum on Information Technology and Applications (IFITA), Vol. 1, pp. 86 – 90.

48. B. Sirisanyalak, O. Sornil, (2007) “An artificial immunity-based spam detection system“, IEEE

Congress on Evolutionary Computation (CEC 2007), pp. 3392 3398.

49. M. A. Lebbe, J. I. Agbinya, Z. Chaczko, F. Chiang, (2007) "Self-Organized Classification of Dangers for Secure Wireless Mesh Networks", Australasian Telecommunication Networks and Applications Conference, pp. 322 – 327.

50. G. Gianini, M. Anisetti, A. Azzini, V. Bellandi, E. Damiani, S. Marrara, (2009) "An Artificial Immune System approach to Anomaly Detection in Multimedia Ambient Intelligence", 3rd IEEE International Conference on Digital Ecosystems and Technologies, pp. 502 – 506.

51. EshghiShargh, (2009) "Using Artificial Immune System on Implementation of Intrusion Detection Systems", Third UKSim European Symposium on Computer Modeling and Simulation, pp. 164 168.

52. R. Chao, Y. Tan, (2009) "A Virus Detection System Based on Artificial Immune System", International Conference on Computational Intelligence and Security, Vol. 1, pp. 6 – 10.

53. M. Danforth, (2009) "Towards a Classifying Artificial Immune System for Web Server Attacks", International Conference on Machine Learning and Applications, pp. 523 – 527.

54. Y. A. Mohamed, A. B. Abdullah, (2009) "Immune Inspired Framework for Ad Hoc Network Security", IEEE International Conference on Control and Automation, pp. 297 – 302.

55. H. Qiang, T. Yiqian, (2010) "A Network Security Evaluate Method Base on AIS", International Forum on Information Technology and Applications (IFITA), Vol. 2, pp. 42 – 45.

56. E. Endy, C. Lim, K. I. Eng, A. S. Nugroho, (2010) "Implementation of intelligent searching using self-organizing map for webmining used in document containing information in relation to cyber terrorism", Second International

Conference on Advances in Computing, Control, and Telecommunication Technologies, pp. 195 – 197.

57. Yang, T. F. Wang, C. M. Liu, B. Li, (2011) "Improved Agent Model for Network Security Evaluation Based on AIS", Fourth International Conference on Intelligent Computation Technology and Automation (ICICTA), Vol. 1, pp. 151 – 154.

58. C. Liu, J. Yang, Y. Zhang, R. Chen, J. Zeng, (2011) "Research on Immunity-based Intrusion Detection Technology for the Internet of Things", Seventh International Conference on Natural Computation (ICNC), Vol. 1, pp. 212 – 216.

59. Y. Zhang, L. Wang, W. Sun, R. C. Green II, M. Alam, (2011) "Artificial Immune System based Intrusion Detection in A Distributed Hierarchical Network Architecture of Smart Grid", IEEE Power and Energy Society General Meeting, pp. 1 – 8.

60. M. S. A. Ansari, M. Inamullah, (2011) "Misbehavior detection in mobile ad hoc networks using Artificial Immune System approach", IEEE 5th International Conference on Advanced Networks and Telecommunication Systems (ANTS), pp. 1 – 6.

61. X. Fang, N. Koceja, J. Zhan, G. Dozier, D. Dipankar, (2012) "An Artificial Immune System for Phishing Detection", IEEE World Congress on Computational Intelligence (WCCI 2012), pp.1 7.

62. S. M. A. Mavee, E. M. Ehlers, (2012) "A Multi-Agent Immunologically-Inspired Model for Critical Information Infrastructure Protection", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1089 – 1096. [64]G.V.P. Kumar, D.K. Reddy, (2014) "An Agent Based Intrusion Detection System for Wireless Network with Artificial Immune System (AIS) and Negative Clone Selection," International Conference on Electronic Systems, Signal Processing and Computing

Technologies (ICESC), pp. 429-433.

63. D. W. Kim, J. W. Yang, K. B. Sim, (2004) "Adaptive Intrusion Detection Algorithm based on Learning Algorithm", The 30th Annual Conference of the IEEE Industrial Electronics Society, Vol. 3, pp. 2229 – 2233.

64. M. A. Sekeh, M. A. Bin Maarof, (2009) "Fuzzy Intrusion Detection System via Data Mining Technique with Sequences of System Calls," Fifth International Conference on Information Assurance and Security (IAS '09.), Vol.1, pp.154-157.

65. S. Mabu, C. Chen, L. Nannan, K. Shimada, K. Hirasawa, (2011) "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol.41, No.1, pp.130-139.

66. A.A. Ojugo, A.O. Eboka, O.E. Okonta, R.E Yoro (Mrs), F.O. Aghware, (2012) "Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS)," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 8, pp. 1182 – 1194International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015

67. M. Md. M. Hassan, (2013) "Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, No. 7.

68. P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo, (2013) "Real-time intrusion detection with fuzzy genetic algorithm," 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp.1-6.

69. A. Chaudhary, V. N. Tiwari, A. Kumar, (2014) "Design an anomaly based fuzzy intrusion detection system for packet

dropping attack in mobile ad hoc networks," IEEE International Conference on Advance Computing (IACC), pp. 256-261.

70. S. E. Benaicha, L. Saoudi, S. E. Bouhouita Guermeche, O. Lounis, (2014) "Intrusion detection system using genetic algorithm," Science and Information Conference (SAI), pp. 564-568.

71. M. Padmadas, N. Krishnan, J. Kanchana, M. Karthikeyan, (2013) "Layered approach for intrusion detection systems based genetic algorithm," IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp.1-4.

72. R. B. Machado, A. Boukerche, J. B. M. Sobral , K. R. L. Juca, M. S. M.A. Notare, (2005) “A Hybrid Artificial Immune and Mobile Agent Intrusion Detection Based Model for Computer Network Operations”, Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, pp. 191a.

73. Z. Pei, J. Song, (2008) “Application of Immune Algorithm to Generate Fuzzy-detector in Intrusion detection”, Fourth International Conference on Natural Computation (ICNC), Vol. 5, pp. 183 186.

74. Y. P. Zhou, (2009) “Hybrid Model based on Artificial Immune System and PCA Neural Networks for Intrusion Detection”, Asia-Pacific Conference on Information Processing, Vol. 1, pp. 21 – 24.

75. V. Golovko, M. Komar, A. Sachenko, (2010) “Principles of Neural Network Artificial Immune System Design to Detect Attacks on Computers”, International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), pp. 237.

76. M. Elsadig, A. Abdullah, B. B. Samir, (2010) “Immune Multi Agent System for Intrusion Prevention and Self Healing System Implement a Non-Linear Classification”, International Symposium in Information

Technology (ITSim), Vol. 3, pp.1 – 6.

77. Z. S. Jing , S. W. Li, R. Hui, C. Z. Ting, Y. Yu, (2011) "Research of Intelligent Immune Intrusion Detection System about Combating Virus with "Virus"", IEEE 2nd International Conference on Software Engineering and Service Science (ICSESS), pp. 753 756.

78. C.M. Ou, Y.T. Wang, C.R. Ou, (2011) "Intrusion Detection Systems Adapted from Agent-based Artificial Immune Systems", IEEE International Conference on Fuzzy Systems, pp. 115 – 122.

79. Q. Meng, (2011) "An Immune-Neuroendocrine-Inspired Inspired Artificial Homeostatic Security-Coordination Model for E-Government System", 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), pp. 6960 6963.

80. R. Dove, (2011) "Self-Organizing Resilient Network Sensing (SornS) with Very Large Scale Anomaly Detection", IEEE International Conference on Technologies for Homeland Security (HST), pp. 487 – 493.

81. F. Jiang, M. Frater, J. Hu, (2011) "A Bio-inspired Host-based Multi-engine Detection System with Sequential Pattern Recognition", Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 145 – 150.

82. E.W.T. Ferreira, G.A. Carrijo, R. de Oliveira, N.V. de Souza Araujo, (2011) "Intrusion Detection System with Wavelet and Neural Artifical Network Approach for Networks Computers," Latin America Transactions, IEEE (Revista IEEE America Latina) , Vol. 9, No. 5, pp. 832-837.

83. N. Wattanapongsakorn, S. Srakaew, E. Wonghirunsombat, C. Sribavonmongkol, T. Junhom, P. Jongsubsook, C. Charnsripinyo, (2012) "A Practical Network-based Intrusion Detection and Prevention System", IEEE 11th International Conference on Trust, Security and

Privacy in Computing and Communications, pp. 209 – 214.

84. A. S. A. Aziz, M. A. Salama, A. Hassanien, S. E. Hanafi, (2012) "Artificial Immune System Inspired Intrusion Detection System Using Genetic Algorithm", Informatica, Vol. 36, pp. 347 358.

85. F. Barani, (2014) "A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system," Iranian Conference on Intelligent Systems (ICIS), pp.1 6.

86. P. K. Harmer, P. D. Williams, G. H. Gunsch, G. B. Lamont, (2002) "An Artificial Immune System Architecture for Computer Security Applications", IEEE transactions on evolutionary computation, Vol. 6, No. 3, pp. 252¬ 280. International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015

87. S. Sharma, S. Kumar, M. Kaur, (2014) "Recent Trend in Intrusion Detection using Fuzzy-Genetic Algorithm," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, No. 5.

88. A. Einipour, (2012) "Autonomic Agent-Based Self-Managed Intrusion Detection and Prevention System", Global Journal of Computer Science and Technology Neural & Artificial Intelligence, Vol. 12, No. 11, Version 1.0.

89. A. Stahl, D. Elizondo, M. C. Mayer, Y. Zheng, K. Wakunuma, (2010) "Ethical and Legal Issues of the Use of Computational Intelligence Techniques in Computer Security and Computer Forensics", International Joint Conference on Neural Networks (IJCNN), pp. 1 8.S