e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 4, April 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521

6381 907 438 6381 907 438 ijmrset@gmail.com www.ijmrset.com

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704010 |

Role of Cyber Security in AI

Dr.V.Suganthi[1], Nithya Shree M[2]

[1]Associate Professor, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, India
[2]UG Student, PG & Research Department of Computer Science, Sri Ramakrishna College of Arts & Science, Coimbatore, India

ABSTRACT: Artificial Intelligence is a branch of Computer Science which aims at building machines that can think, feel and take decisions just like humans. The speed of processes and also the quantity of knowledge to be utilized in defensive the cyber area cannot be handled by humans while not sizeable automation. However, it is troublesome to develop software system with standard mounted algorithms (hard-wired logic on deciding level) for effectively defensive against the dynamically evolving attacks in networks. This example may be handled by applying strategies of computing that offer flexibility and learning capability to software system. This paper presents a quick survey of computing applications in cyber security, and analyzes the prospects of enhancing the cyber security capabilities by suggests that of accelerating the intelligence of the security systems. Once measuring the papers obtainable regarding AI applications in cyber security, we will conclude that helpful applications exist already. They belong; initial of all, to applications of artificial neural nets in perimeter security and a few alternative cyber security areas. From the opposite facet – it has become obvious that several cyber security issues may be resolved with success only strategies of AI are getting used. For instance, wide information usage is critical in deciding, and intelligent call support is one in all however unresolved issues in cyber security.

KEYWORDS: Threats, Cyber Security, expert systems, Cyber crime,

I. Introduction

Artificial intelligence (AI) as a field of research project (also known as machine intelligence within the beginning) is sort of as previous as electronic computers are a prospect of building devices/software/systems additional intelligent than persons has been from the first days of AI “on the horizon”. The matter is that the time horizon moves away once time passes. We have witnessed the determination of variety of showing intelligence exhausting issues by computers like enjoying sensible chess, as an example. Throughout the first days of computing the chess enjoying was thought of a benchmark showing a true intelligence. Even in seventies of the last century, once the pc chess was on the master’s level, it appeared nearly not possible to form a program that might beat the planet champion. it's typically accepted that AI will be thought of in 2 ways: as a science aimed toward making an attempt to get the essence of intelligence and developing typically intelligent machines, or as a science providing ways for determination complicated issues that can't be solved while not applying some intelligence like, as an example, enjoying sensible chess or creating right choices supported giant amounts of knowledge. Within the gift paper we are going to take the second approach, advocate for applying specific AI ways to cyber security issues. A large range of ways is developed within the AI field for finding laborious issues that need intelligence from the human perspective. Some of these ways have reached a stage of maturity wherever precise algorithms exist that is supported these ways. Some ways have even become thus wide known that they are not thought of happiness to AI any further, but became a section of some application area, as an example, data processing algorithms that have emerged from the training subfield of AI. It might be impossible to do to offer a lot of or less complete survey of all much helpful AI methods in a very transient survey. Instead, we have sorted the ways and architectures in many categories: neural nets, knowledgeable systems, intelligent agents, search, machine learning, data processing and constraint finding. We define these classes here, and that we provide references to the usage of individual ways in cyber security. We are not aiming to discuss tongue understanding, artificial intelligence and pc vision that we contemplate specific applications of AI. Robots and pc vision have positively spectacular military applications, however we have not found something specific to cyber security there.

1.1. **Visual nets**: visual nets have an extended history that begins with the invention of perceptron by Frank Rosenblatt in 1958 – a man-made nerve cell that has remained one among the foremost well-liked components of neural nets. Already a little variety of perceptrons combined along will learn and solve fascinating issues. However neural nets will include an oversized variety of artificial neurons.

1.2 **Expert systems:** These are unquestionably the foremost wide used AI tools. Associate skilled system is software system for locating answers to queries in some application domain bestowed either by a user or by another software system. It will be directly used for 98 call support, e.g. in diagnosing, in finances or in computer network. There's a good sort of skilled systems from little technical diagnostic systems to terribly massive and hybrid systems for finding complex issues. Conceptually, associate skilled system includes a mental object, wherever skilled information a few specific application domains are hold on. Besides the mental object, it includes associate illation engine for account answers supported this information and, possibly, further information a few state of affairs. Empty mental object and illation engine are along referred to as skilled system shell - it should be stuffed with information, before it will be used. This system shell should be supported by software system for adding information

1.3. **Intelligent agents**: Intelligent agents are software system elements that possess some options of intelligent behavior that produces them special: pro-activeness, understanding of an agent communication language, reactivity (ability to form some selections and to act). They will have a designing ability, quality and reflection ability. Within the software system engineering community, there is a thought of software system agents wherever they are thought of to be objects that are a minimum of proactive and have the flexibility to use the agent communication language. comparison agents and objects, one will say that objects is also passive, and that they do not need to perceive any language victimization intelligent agents in security against DDoS has been represented, wherever simulation shows that cooperating agents will effectively defend against DDoS attacks. Once determination some legal and conjointly industrial several issues, it should be attainable in premise to develop a "cyber police" subsisting of mobile intelligent agents. This may need implementation of infrastructure for supporting the cyber agents' quality and communication, however should be inaccessible for adversaries. This may need cooperation with ISP-s. Multi-agent tools will give a lot of complete operational image of the cyber house, as an example, a hybrid multi-agent and neural network-based intrusion detection method has been projected. Agent-based distributed intrusion detection is represented.

1.4. **Search**: Search may be a universal technique of downside finding which will be applied altogether cases once no different ways of downside finding are applicable. Individuals apply search in their daily life perpetually, while not listening to it. Little should be known so as to use some general search formula within the formal setting of the search problem: one should be able to generate candidates of solutions, and a procedure should be out there for deciding whether or not a planned candidate satisfies the wants for an answer. The αβ-search formula, originally developed for pc chess, is an implementation of a typically helpful preparation of "divide and conquer" in problem finding, and mostly in deciding once 2 adversaries are selecting their absolute best actions. It uses the estimates of minimally secured win and maximally doable loss. This allows one typically to ignore great amount of choices and significantly to hurry up the search.

1.5. **Learning**: Learning is raising a data system by extending or rearranging its cognitive content or by raising the illation engine. This is often one in all the foremost fascinating issues of AI that is beneath intensive investigation. Machine learning includes procedure strategies for getting new data, new skills and new ways that to prepare existing data. Issues of learning vary greatly by their complexness from easy constant learning which suggests learning values of some parameters, to difficult kinds of symbolic learning, for instance, learning of ideas, grammars, functions, even learning of behavior. AI provides strategies for each -- supervised learning further as unattended learning. The latter is very helpful within the case of presence of enormous quantity of knowledge, and this is often common in cyber security wherever giant logs will be collected. Data processing has originally adult out of unattended learning in AI. Unattended learning will be a practicality of neural nets, especially, of self-organizing maps. A distinguished category of learning strategies is implanted by parallel learning algorithms that are appropriate for execution on parallel hardware. These learning strategies are diagrammatical by genetic algorithms and neural nets. Genetic algorithms and symbolic logic has been, as an example, utilized in threat detection systems represented.

1.6. **Constraint finding**: Constraint finding or constraint satisfaction may be a technique developed in AI for locating solutions for issues that area unit conferred by giving a group of constraints on the answer, e.g. logical statements, tables, equations, inequalities. An answer of a drag may be a assortment of values that satisfy all constraints. Actually, there are many various constraint determination techniques, betting on the character of constraints. On a really abstract level, nearly any downside will be conferred as a constraint satisfaction downside. Particularly, several designing issues will be conferred as constraint satisfaction issues. These issues are troublesome to resolve as a result of great amount of search required normally. All constraint determination strategies are aimed toward limiting the search by taking into consideration specific info regarding the actual category of issues. Constraint determination will be used in scenario analysis and call support together with logic programming.

II. INTELLIGENT CYBER SECURITY

When coming up with the long run analysis, development and application of AI ways in Cyber Security, one needs to distinguish between the immediate goals and long views. There are varied AI ways directly applicable in Cyber Security, and present are immediate Cyber Security issues that must a lot of intelligent solutions than are enforced nowadays. As yet we have mentioned these existing immediate applications. Within the future, one will see promising views of the appliance of fully new principles of data handling in state of affairs management and deciding. These principles embrace introduction of a standard and hierarchal data design within the deciding software system. This sort of design has been planned. A difficult application space is that the data management for internet central warfare. Only automatic data management will guarantee fast state of affairs assessment that provides a choice superiority to leaders and decision manufacturers on any C2 level. Knowledgeable systems are already getting used in several applications, typically hidden within an application, like within the security measures coming up with software system. However, knowledgeable systems will get wider application, if massive data bases are going to be developed.

III. CONCLUSION

In the present scenario of quickly growing intelligence of malware and class of cyber-attacks, it is inescapable to develop intelligent cyber security ways. The expertise in DDoS mitigation has shown that even a security against large-scale attacks will be undefeated with rather restricted resources once intelligent ways are used. An analysis of publications shows that the AI results most generally applicable in cyber security are provided by the analysis in artificial visual nets. Applications of visual nets can keep on in cyber security. There is additionally an imperative would like for application of intelligent cyber security ways in many areas wherever neural nets are not the foremost appropriate technology.

REFERENCES

[1] Y. Ren, R. Werner, N. Pazzi, A. Boukerche, "Monitoring patients via a secure and mobile health-care system", IEEE Wirel. Commun. 17, pp. 59–65, 2010.

[2] J. R. Gallego, A. Hernandez-Solana, M. Canales, J. Lafuente, A. Valdovinos, J. Fernandez-Navajas, "Performance analysis of multiplexed medical data transmission for mobile emergency care over the UMTS channel", IEEE Trans. Inf Technol. Biomed. 9, pp. 13–22 2005.

[3] B. Arunachalan, J. Light, I. Watson, "Mobile agent-based messaging mechanism for emergency medical data transmission over cellular networks", 2nd International Conference on Communication Systems Software and Middleware, pp. 1–6, 2007.

[4] B.M. Prakoso,A.R.N. Pristy, M. Arsyad, A.B. Noegroho, A. Sudarsono, A. Zainudin, " Performance analysis of OLSR routing for secure medical data transmission for rural areas with Delay tolerant network", In: 2016 International Symposium on Electronics and Smart Devices (ISESD), pp. 51–56, 2016.

[5] O.H. Salman, M.F.A. Rasid, M.I. Saripan, S.K. Subramaniam, "Multi-sources data fusion framework for remote triage prioritization in telehealth", J. Med. Syst.38, 103, 2014.

[6] M. Werner, C. Pietsch, C. Joetten, C. Sgraja, G. Frank, W. Granzow, et al., 2009. Cellular in-band modem solution for ecall emergency data transmission. In: VTC Spring 2009 – IEEE 69th Vehicular Technology Conference, pp. 1–6, 2009.

[7] M. Aal-Nouman, H. Takruri-Rizka, M. Hope, "Transmission of medical messages of patient using control signal of cellular network", Telematics and Informatics, https://doi.org/10.1016/j.tele.2017.11.008, 2017.

[8] S. A. Hussain et al, "An Efficient Channel Access Scheme for Vehicular Ad Hoc Networks", Mobile Information Systems, Vol.2017, 2017.

[9] B. Yuanguo, "Neighboring vehicle-assisted fast handoff for vehicular fog communications", Special Issue on Fog Computing on Wheel. Springer, 2017.

[10] S. Midya, "An Efficient Handoff Using RFID Tags. Proc. of Intl. Conf. on Intelligent Communication, Control and Devices", Advances in Intelligent Systems and Computing 47, pp. 779, 2016.

[11] Radio Link Control (RLC) protocol specification, 3GPP Tech. Specification 25.322 v5.4.0 (2003–03), 2002.

[12] S. Misbahuddin, R. Olson, J. A. Zubairi, M. Irfan, S. M. Arif, S. Mansoor, S. Saeed, Z. Irfan, "Client-Server Based Transmission Scheme over GSM Network for MEDTOC with Patient Classification", In: International Conference on Collaboration Technologies and Systems (CTS), pp. 176–179, 2012

[13] H. Huang, T. Gong, N. Ye, R. Wang, Y. Dou, "Private and Secured Medical Data Transmission and Analysis of Wireless Sensing health-care System", IEEE Trans. on Ind. Inf. 13, pp. 1227–1237, 2017.

INNO SPACE
SJIF Scientific Journal Impact Factor

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com