ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

An Overview on Use of Artificial Intelligence Techniques in Effective Security Management

Swapnil Ramesh Kumbhar

Assistant Professor, Department of Computer Science & Engineering, AGTI's Dr.Daulatrao Aher College of Engineering, Karad, Maharashtra, India.

ABSTRACT: The use of artificial intelligence gives new height for human being in today's world. The different artificial intelligence techniques give rise to important application areas where human processing ability weakens. Nowadays the security is important key concern for every nation. Use of different AI techniques in security management protects against the security attacks/threads by warning the user on appropriate time. This paper consists of overview of different AI techniques useful in enhancing the security infrastructure.

KEYWORDS: Artificial Intelligence; Security; Artificial Neural Networks; Data Mining; Image Processing; Fuzzy system,; Expert System; Pattern Recognition.

I. INTRODUCTION

The artificial intelligence is the process in which machine can acts like a human. This robust feature allows AI allows working in various fields easily. Some of primary application areas where the AI can massively used are Military, Antiterrorism, Automobile Industry, Internet Search Engines, Robotics etc. The working nature of AI is similar to the human brain so that AI has wide scope in research nowadays. The popular areas of artificial intelligence are Robotics, Speech Recognition, natural Language Processing, Expert system, pattern recognition, Fuzzy system etc are useful for the development of new application useful for human being. The artificial intelligence seems to play key role in security if integration of some AI technique done with the security system definitively enhances the security infrastructure of any organization or country. This paper reviews these techniques in accordance to give effective security system base on AI.

II. RELATED WORK

The Artificial Intelligence is new and emerging field in computer world. Many author presented their views on AI techniques in security management. The author [14] present the intelligent techniques are applicable for network protocol security, monitoring, measurement, and accurate prediction. The social networking issues are quite serious issue hence the author [15] presents the Artificial Intelligence techniques can help to outline basic categories of privacy concerns, including solutions to them. This paper [16] proposes a dynamic model Intelligent Intrusion Detection System, based on specific AI approach for intrusion detection. The techniques that are being investigated includes neural networks and fuzzy logic with network profiling, that uses simple data mining techniques to process the network data. The author [17] present situation of rapidly growing intelligence of malware and sophistication of cyber attacks, it is unavoidable to develop intelligent cyber defense methods. The DDoS mitigation has shown that even a defense against large-scale attacks can be successful with rather limited resources when intelligent methods are used.Many author presented their views on AI techniques for security purposes.

III. ARTIFICIAL INTELLIGENCE & SECURITY

1) Artificial Intelligence-

Use of artificial intelligence is new technology science to research and development expansion of human intelligence. Artificial intelligence is branch of Computer Science working similar to human brain. It give rise to human intelligence

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

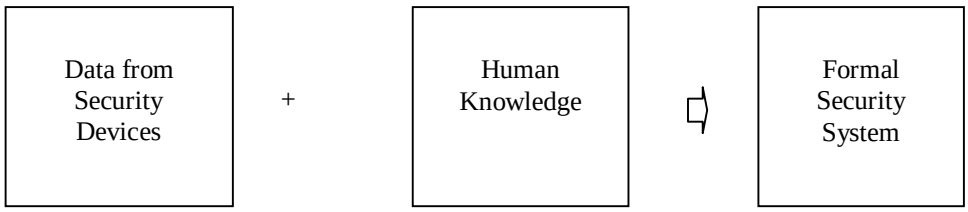
through the machine perspective. The research in Artificial intelligence started in 1956. The University of Dartmouth firstly used the Artificial Intelligence term officially. The most of research in Artificial Intelligence is related to the logical reasoning where research began from the problem solving, reasoning, learning, and expert systems, gaming etc. The mass quantity of research yet to be carried out in this field as it has wide scope. The AI has ability to solve the differential equation, playing chess, integrated circuit design analysis, speech recognition, handwriting recognition, expert system for disease diagnosis, control of aircraft submarine without operator, Bot players introduced in computer games etc. The evolution of AI takes in the generation from 1950 to till date. Today it supposed that the robotics machine can do the human task with special capability like a human. This new era can also helpful in providing AI with security integration gives machine automated security which is focused in this paper.

2) Security-

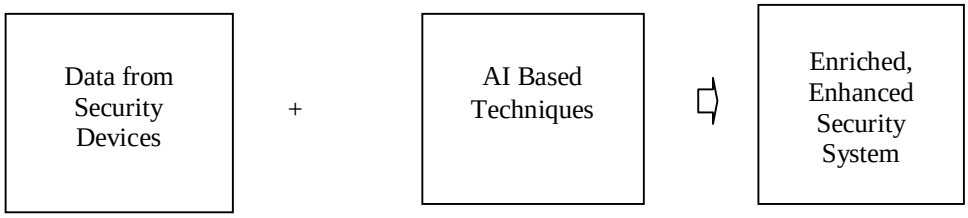
As security is important issue for any Human, Company Environment, Organization, Community and Country in accordance to maintain growth and stability. Security threat gives rise to several problem such as instability, economical setbacks, terror attacks causes loss of human lives, creates Un-safety feelings. As a human being the security is challenging task because human has several restriction on analyzing and processing several information at a time. This is big drawback identified in current security system. This drawback can overcome on more practical manner with the help of artificial intelligence techniques integration. The security system includes Homeland security, Intrusion detection system, DOS attack, Cryptography, Video vigilance System etc. Human Processing ability integrated with AI certainly raise the security at high extend.

The following diagram shows the formal security system and the security based on Artificial intelligence techniques-

- **Formal Security System-**



- **Security System based on Artificial Intelligence-**



IV. DIFFERENT AI TECHNIQUES USED IN SECURITY MANAGEMENT SYSTEM

As stated earlier the security can be increased at greater extends with the help different AI techniques. The application of some of AI techniques in security field explained below,

A. Artificial Neural Networks.
B. Data Mining Tools.
C. Pattern Recognition.
D. Image Processing/Analysis.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

E. Fuzzy Logic.
F. Expert System.

A. **Artificial Neural Networks-**

The author [1] presents Artificial Neural Networks is an effective technique which has the ability to implement security using back-propagation algorithm. Simple combinational logic and sequential machine can be well implemented using back-propagation algorithm. Artificial Neural Network can be used as a new method of encryption and decryption of data

The security threads in networks are one of the main key concerns related with the Computer security nowadays. Many Security Agency interested in the proper solution for thread, intrusion detection. The many authors provide the solution towards the ANN approach for the Intrusion detection in computer network. Currently [2] rule based method is used in identifying attacks. Output of the neural network in the form of probability helpful in provide predictive capability to find out the misuse. The disadvantage is training, for training the thousands of individual attack sequence is required since this quantity of sensitive information difficult to obtain [3].

The Back propagation algorithm, Echo state Neural Networks and Radial Basis function along with Fisher's linear discriminate function have been proposed for intrusion detection [4].

B. **Data Mining Tools-**

The automatic extraction of useful, often previously unknown information from large databases or data sets is known as data mining. This key feature of data mining made data mining as key tools towards the security management. There are several data mining tools such as Clustering, Classification, Association Rule, and Decision tree, Linear Regression, naive bayes classifier etc.The data mining tools are important because it helps to find out exact information from vast amount of data. This feature laid the data mining to find forensic evidences from collected suspicious data from crime spot. This makes task easier for security agencies for finding the criminal.

The author described project related to the finding internet crimes. The paper gives data mining technique for fraud with fake auction goods, phishing which provide preventive security [5].The internet system gives rise to several malicious activities including the spreading of viruses, network intrusion etc. This paper [6] presents malicious code detection by mining binary executable, network intrusion detection by mining network traffic, anomaly detection, data stream mining. The data mining approach also useful in 'bot' detection.

C. **Pattern Recognition-**

The Cryptography and Artificial Intelligence gives rise to the CAPTCHA.As it includes the cryptography it has wide scope for the algorithmic development with AI [7]. The pattern recognition mainly concerns with the biometric system. The Paper introduces the pattern recognition approach for the person identification using fingerprint [8].The pattern recognition approach towards security gives identification of person on the basis of face, voice, fingerprint .The paper [9] Present the MNN Modular neural network for the integration of the speech, fingerprint and face.

Pattern recognition approach gives way towards the biometric attendance system, it also useful in person identification where sensitive work carried out i.e. nuclear power plant ,military's etc where security is prime and foremost preference. The formal approach of pattern recognition is useful in security era very massively. Pattern recognition is the research area that studies the operation and design of systems that recognize patterns in data Important application areas are image analysis, character recognition, speech analysis, man and machine diagnostics, person identification and industrial inspection.

D. **Image Processing/Analysis-**

Digital Image Processing has widely used for defense and security services target detection and tracking, missile trapping, Wide area surveillance etc. The goal image processing is to find the useful information from image collected

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

from different sources. Develop the algorithm such a way that it provides way towards the autonomous system which capable for giving decision on image inputs.

Obstacle detection, radar and 3D radar image processing, sonar image processing, 3D shape retrieval and image analysis etc are key research area today in image processing towards the military security. The image Compression and Transmission for long distance in minimum bandwidth is the main research topic nowadays. The CCTV based video system using the AI is discussed by the author[10]in which he suggest nice solution towards the object identification including character, color,text,Tracking missing variable in the video stream, Incident detection based on speed of visual impression etc.

E. **Fuzzy Logic-**

The author [11] proposed anomaly based intrusion detection approach introducing fuzzy decision making module. The fuzzy rules for inference will automatically identified the by fuzzy rule making strategy which is more effective to detect the intrusion in the computer. The home security provided with the help of fuzzy system [12].

F. **Expert System-**

The Expert system allows being base on the fuzzy rule based model. The supervised learning is most important and key factor for training the expert system as compared to the unsupervised learning. The author [13] stated the fuzzy rule based expert system for cyber security.

V. DISCUSSION

The Artificial intelligence techniques in Security discussed above can be summarized based on their advantage and advantage in tabular format below

Sr No.	Artificial Intelligence Technique	Advantage	Disadvantage
1	**Artificial Neural Networks**	• Adapt to unknown situations • Robust, able to model complex functions. • Easy to use.	• Training of neural network • Not exact • Complexity of the network structure
2	**Data Mining**	• Help with decision making • find out exact information from vast amount of data	• User privacy/security is critical issue • Misuse of information • Accuracy of data
3	**Pattern Recognition**	• Quick and Accurate • Recognize & Classify unfamiliar objects • Recognise patterns quickly, with ease and automatically.	• Reliability of result depends on input
4	**Image Processing/Analysis**	• Processing of images are faster and more cost-effective. • Useful for areas where human interference is impossible.	• The initial cost can be high depending on the system used, • Input image should be

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

			optimum for recognition.
5	**Fuzzy Logic**	• Fuzzy Logic describes systems in terms of a combination of numeric's and symbolic. • The algorithms can be described with little data, so little memory is required. • Fuzzy algorithms are often robust.	• They are not very sensitive to changing environments and erroneous or forgotten rules
6	**Expert System**	• Provides consistent answers for repetitive decisions, processes and tasks • Can work round the clock	• Errors may occur in the knowledge base, and lead to wrong decisions • Cannot adapt to changing environments, unless knowledge base is changed

VI. CONCLUSION

As Security is key important issues, the integration Artificial Intelligence Techniques certainly improve the performance of the existing security system. Main thing related security is alert the user before unwanted things going to happened. The post mortem knowledge has zero value in security field. The Different Artificial Intelligence Techniques has drawback that training set which used for the training any model must be up-to-date. These different techniques certainly helpful in Home Security, Military, Surveillance, and CCTV based security system.

REFERENCES

1. Navita Agarwal & Prachi Agarwal, "Use of Artificial Neural Network in the Field of Security" MIT International Journal of Computer Science & Information Technology,Vol. 3, No. 1, pp.42–44 ,Jan. 2013.
2. James Cannady, "Artificial Neural Networks for Misuse Detection" National Information Systems Security Conference, 1998.
3. Mehdi MORADI and Mohammad ZULKERNINE,"A Neural Network Based System for Intrusion Detection and Classification of Attacks", Natural Science and Engineerign Research Council of Canada(NSERC).
4. S.Saravanakumar Umamaheshwari, "Devlopement and Implementation of artificial Neural networks for Intrusion detection in computer networks", IJCSNS International Journal Of computer Science and Network Security, VOL 10, No7, July2010.
5. Gerhard PAAß1, Wolf REINHARDT, Stefan RÜPING, and Stefan WROBEL, "Data Mining for Security and Crime Detection".
6. Bhavani Thuraisingham, Latifur Khan, Mohammad M. Masud, Kevin W. Hamlen, "Data Mining for Security Applications", IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008.
7. Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford, "CAPTCHA:Using Hard AI Problems For Security",Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques ,EUROCRYPT'03,Pages 294-311,2003.
8. Jayant V. Kulkarni, Raghunath. S. Holambe, Bhushan D. Patil, ".Network Security: Pattern Recognition Approach (Biometrics based Person Authentication), Proceedings of National Seminar on Unmanned Ground Vehicle, Vehicles Research & Development Establishment,27-28 Feb. 2006.
9. Patricia Melin, Alejandra Mancilla, Miguel Lopez, Jose Soria, Oscar Castillo, "Pattern Recognition for Industrial Monitoring and Security using the Fuzzy Sugeno Integral and Modular Neural Networks", IJCNN 2007.
10. Sizwe M.Dhlamini, Michel o kachienga,T Marwala, "Artificial intelligence as an Aide in management of security Technology", Members IEEE ,IEEE Africon 2007.
11. Thakare .S.P. and Ali M.S., "Network intrusion detection system & fuzzy logic", BIOINFO Security Informatics ISSN: 2249-9423 & EISSN: 2249-9431, Volume 2, Issue 1, 2012.
12. Muhammad Anwaar Saeed, Muhammad Saleem Khan, Khalil Ahmed, Umer Farooq, "Smart Home Security System using Fuzzy Logic International Journal of Scientific & Engineering Research", Volume 2, Issue 6, June-2011.
13. Göztepe, Kerim, "Designing a Fuzzy Rule Based Expert System for Cyber Security",International Journal of Information Security Science, Vol. 1 Issue 1, p13,March2012.
14. Emmanuel Hooper "Intelligent Techniques for Effective Network Protocol Security Monitoring, Measurement and Prediction", International Journal of Security and Its ApplicationsVol.2, No.4, October, 2008.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, September 2014

15. Sattikar, Dr. R. V. Kulkarni, "A Role of Artificial Intelligence Techniques in Security and Privacy Issues of Social Networking", IJCSET , Vol 2, Issue 1, January 2012.
16. Idris, N.B. Shanmugam.B. ," Artificial Intelligence Techniques Applied to Intrusion Detection" ,INDICON 2005 Annual IEEE Conference , pp 52 – 55,Dec. 2005
17. Enn Tyugu , "Artificial Intelligence in Cyber Defense" , 3rd International Conference on Cyber Conflict,2011

BIOGRAPHY

Swapnil Ramesh Kumbhar is working as Assistant Professor in the Computer Science & Engineering Department, AGTI's Dr.Daulatrao Aher College Of Engineering, Karad affiliated to Shivaji University,Kolhapur. He is working since July 2011. He received Bachelor of Engineering B.E. (CSE) degree in 2011 from Shivaji University, Kolhapur, MS, India. He currently pursuing M.E. (CSE) form same university. His research interests are Data Mining, Information Security, and Information Communication Technology etc.