ISSN 2278-

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 332 - 336 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

Artificial Intelligence in Cyber Defense

I.Yallamanda Reddy[1], **A.Thirupathaiah**[2]
[1] II year M. Tech [SE], SACET, Chirala , A.P.,yallamanda536@gmail.com
[2]Associate Professor, Dept of IT, SACET, Chirala , A.P.,athiru73@yahoo.in

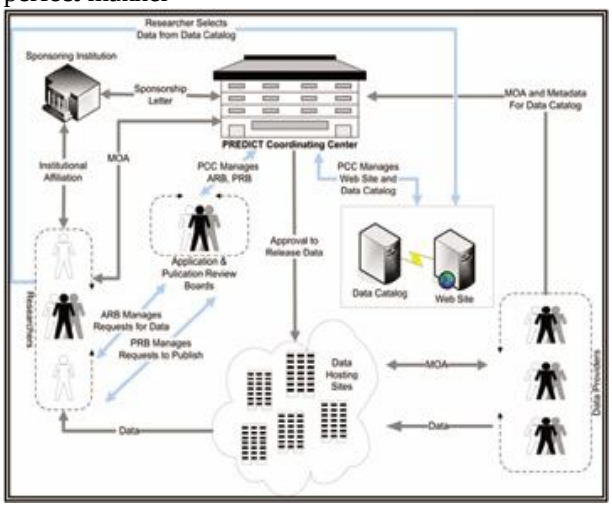
Abstract: Day by day the technology is growing and in proportion to cyber crime is also growing and it becomes very difficult to track the application and to know the loopholes in the application. In order to have a mechanism build in such a way that the application will track all such changes done against the protocols designed. This paper proposes an algorithm like to detect the cyber defense in the web based applications. The application will be designed taking the artificial intelligence in order to have a dynamic detection of cyber crime in that application with which the data will be safe and can keep track of the intruders. This paper after checking with the available artificial intelligence concepts is filtered to have an efficient and secure cyber based application. Proposed work will make sure the application blocks the intruders trying to access or modify the data present**.**

Keywords: - Artificial Intelligence, Cyber defense, security, human thinking.

I INTRODUCTION

Artificial intelligence (AI) it's a scientific method and also it old electronics system and to make it to an ideologically and to implement that in to think as humans think and it here we are using to build the software system and an implementation of application if the mistakes are came we have to do it and for that we are just using an AI for the process of an auto check algorithm and to maintain to make that problem to fix by the system an automatic option for all that things we are using artificial inelegance. In general we can see in all the game systems and like chess when we are playing system will make the next step immediate steps and it will implement things for all these we are using the AI for all these we are implementing and to increase the power sens of system should be increase and for all these we are using good implementation algorithm to search and to take an immediate action and in general we can see in Google like this as a search system and here we have the language compartmentalize what ever we search it will shows that the remaining things and which are the

In generally we consider AI as a two way process implementing and doing the process for to developing this we are using the general science help and it's implementation some of the things may not be possible without using the help of inelegance like as playing and moving the things when we playing the games and AI is providing a feature like an adviser and an advocate for doing the things in system in some cases to improve and to implement the special things we need the Cyber defense it can rectify and solve the application in a perfect manner

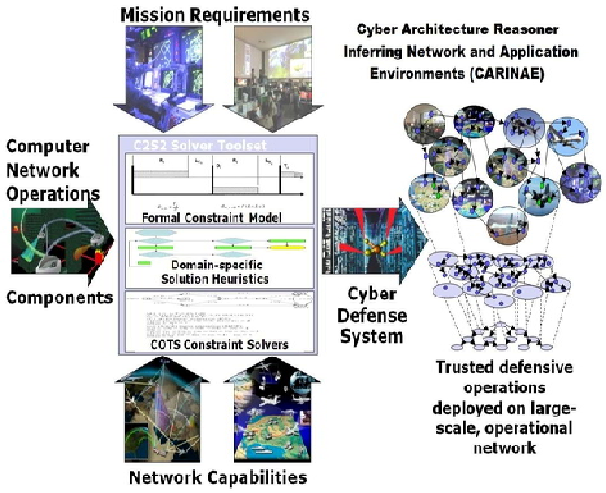


Why the role of intelligent software we need in Cyber operations are increased so rapidly? Looking very closer at the cyber space, and one can see following given answer. For that Artificial intelligence is needed, first, for rapid reactions in the Internet systems we can see. One can able to handle the large amount of data information fast in order to describe and analyze events that happen in cyber space and to make the required decisions. The speed of the introduces processes and it's amount of data has used it cannot be handled by humans without considerable the automation. However, it's difficult to develop software with conventional fixed algorithms

ISSN 2278-

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 332 - 336 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

(hard-possible for the defending against the attacks in cyber defense space, because the new threats appear in this constantly. Here there is place for artificial intelligence method. In second section of present paper of an artificial intelligence is a field of science and technology oriented. In third section we are have to look at the existing things of artificial intelligence application in cyber defenses, these all are grouped by the artificial intelligence techniques for to improve the things. In fourth section if we look into the future and suggestions the new intelligent applications is A large number of methods are developed in this artificial intelligence field application for solving the hard problem that the require intelligence of the human perspectives and human responses. Some of those methods have been reached a stage of maturity level where as we are used the sample algorithms it exist that are based on those methods. Is as follows Some methods have even become to widely known as that they are not considering belong to artificial intelligence no more, but it have become a part of the some applications for the instance and data mining algorithms that we have emerged from the learning of the sub-fields of AI. And it would be impossible to give more or less the complete survey of all are practically useful AI methods that are in a brief survey. Instead of that we have grouped it as the methods and it's architectures in several types of categories they are as fallows; neural nets, intelligent agents, machine learning, expert systems, search, data mining and constraint solving. If we are in outline these categories here and here we are giving references to the usage of the respective method in cyber defenses. Here we are not going to discuss about the natural languages understanding, robotic methods and computer vision which we considered to specify the application of AI. Robots and computer vision have definitely impressive the military application but we may not found anything that was specified in CD there.



AI is a concept which is most probable to communicate with the computer science and all of its futures and it will think like a humans how we work just we are giving a program to work the system that also has to make a response to us by the insensate time and based on our response whenever we are doing any things in our application implementation and all that of the process has be work by its own and we have to implement that to be act and work with us in an equal form and to maintain all the things has to be perfect by the side and to make it as a Challenger to us when we are working in our systems like chess and any other games when we play in two way forms that it gives the perfect support to us and by using the Cyber defense we are making it to an advance mode and to perform it as a very sensitive and more efficiently to think and work and to make it an advocate of the process to an option process

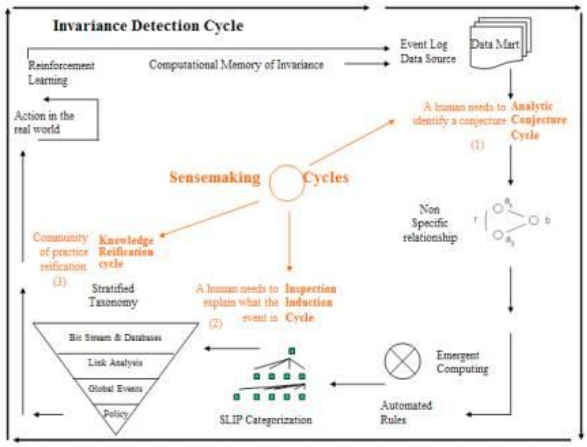
II. PROPOSED WORK

In this paper we are introduced a new way of concept and to make the previous system to work an efficient and work more user friendly for that we are used Cyber Defense (CD) through this concept we are making it's an advance and making to work in an efficiency manner for that we are implemented many ways here in this paper that is as fallows. Here in this paper we are proposed a way of providing security to the users and making to user feel safe manner and here in this when user lo-gin this application. He has to create one password it's in an existing system and in that pace we are proposed a new way to technique for the password and system will generate one password and that also system will show half password only to user for lo-gin and the remaining password should be store in server and that server can't

ISSN 2278-

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 332 - 336 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

show the remaining password and after that whenever user want to lo-gin he has to enter that half password and server will check and match it if it both will match it will accept to user log-in and after lo-gin there is no chance for user t change his password any more only one time password that was created by the system when the time of user register here there is no chance for user to put his own password and know one also guess that password by this we are providing the security to the users and here we are stopping the users credentials just here we are allowing the users to do just register and to take system given password only through this we are providing security to the user and making the things to be work more advisable and after that user lo-gin he has upload and save his files save on server for that we are providing a simple manner and making to that has to be a pubic and other people who we know that things also we can simply download. So for that here we are using a public providing thing. And after that user lo-gin for all the uploaded applications we are providing a search engine here we are providing an intelligence scientific technology for making it t be possible in all the times like as Google search when we search for one thing here autocratically the intelligence will occur and shows that the file names which is related with that of the files and all that will come in a form of page after clicking that option it will open a new page.



For this concept we are using the like command operator in this system and here we are taking a keywords for the process whenever user upload his profile files we are taking some of the keywords in that for to search that file whenever he want not by going the directory of the files uploaded by the user and not only that here we can see all the files which was related to this file name all that files will come not only the user who was lo-gin and all the users was in that site will come to the search page and to make it for the user comparable and just simply he can view that things which was designed and which was uploaded by the other user and making that as possible and to place the intelligence for the user friendly to get simply the file and reduce it search time by that of the process we are using here AI scientific concepts AI means to make user friendly and make possible things by the system making it as to think like a human and to help the users who are searching and doing anything whatever need by the user we are providing that before an user action was completed that is the main advantage of AI by implementing the Cyber Defense we making this application methods and in previous system whatever we implemented it is more problem to us to get success and the required intelligence of humans perspective it is not supporting for that we are used many matured levels of the process and a level of precise algorithms even though it became no use of it and still the problem was there and even in some of the cases we may not able to get the fields of things which is related to AI And which is not related to AI that is a big problem

For that we are used parallel algorithm even though we are getting a problem for to overcome the process of things and making it's an a implementation process and in that as we implemented the fuzzy key word logic and all the things even though some of the times it's making difficulty to get and to solve the problems. In general if we are searching a large amount of data files it be a most difficulty to load and to operate the things in to work not only the logical and basic search tectonic and to perform all the old process and to check the valid things to be work for these reason we are proposed a way of Cyber defense so by using this concept we can get the things to be possible and to work in normal manner

This is we are planned for the future planning and developed it in a manner of overcome the existing system and to reach the immediate goals of the system so we are using many number of AI methods we are using here to get an immediateness response in CD and to solve the problems that has to solve all the process of an existing system and so that till now we discussed that concepts of implementing an AI application and it advantages and of it's problems. so for these problems we are overcame using the Cyber defense and after that solving the search process and providing the immediate response of the user we are providing an option that is to find the fraud users in the online for that we are using a simplified algorithm and t detect that how many times user done mistakes and miss matched things like this we can see in Facebook and other social networks also if it was fended anything like if the user is not a valid one or he his un authenticated

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 332 - 336 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

person immoderately it will find and block that user for a pertinacity time like this we are implemented in this application and providing security to the users who ever register and using this application and for that each one we are providing three chances if he was used miss usage of that we are blocking the user.

We have grouped the methods and architectures in several categories:

They are:

Neural nets: Artificial neural networks is a computational tool, the properties belongs to biological neural systems. Neural networks excel more number of problems areas where conventional worked on computer systems have traditionally been slow and inefficient**.**

Expert systems: expert system that convers the system knowledge into different subject into a software code. The software code can be mixed with other codes it helps for answering different queries through a system.

Intelligent agents: intelligent agent works on internet, it give more information about the program or service without our permission

Search: In Artificial Intelligence (AI) search is key role to solving problems. in many issues sequence to solve required problems

Machine learning: Machine learning is really experimentally knowledge in machine learning algorithms and interdisciplinary different application in machine learning to another application

Data mining: Analyzing data is a key tools for data mining software analytical information to used cuts costs, revenue, or both.

Constraint solving: constraint solving is real time programming techniques in computer science field

When user want to download his files he need to enter the password which was generated by the system in the time of user uploading in t the server if he had not entered the valid key for that file it won't take that to download and as well as that all the miss usages of user was counted by the system so it keep store in it and it will allow the user to take that up t third option if three chances s over then that movement he is not able to download and he is not able to log-in no more also he can able to get recovery of that tings so by using these things we are

III. RESULTS

In this paper we have implemented a way of providing security and user benefit options and as well as the system has to work on its own thinking ideas and based on the performance and the response of the user it will works for that we are used cyber defense to overcome all the defects of AI problems and make it t work as an advanced one so for that we are used cyber defense here and by this we done and solved the problems in general we are facing when we working on sometimes so here for that we are used intransigence for the user friendliness and worked nice for that we are implemented fuzzy key word search for the search tectonic and as well as after that to upload and download his files and documents we are provided a security for the user data when user want to s tore and save his data at the time of uploading we are generating a key for the use data and after that also we are used one more advanced defense tectonic for the user protection that is to identify the fraud detection and identifying the user is an authenticated or not.

Def:

a) Given $f: X \rightarrow Y$ and any fuzzy set $A \in \tilde{P}(X)$, where

$$A = \mu_1/x_1 + \mu_2/x_2 + \cdots + \mu_n/x_n$$

the *extension principle* states that

$$f(A) = f(\mu_1/x_1 + \mu_2/x_2 + \cdots + \mu_n/x_n)$$
$$= \mu_1/f(x_1) + \mu_2/f(x_2) + \ldots + \mu_n/f(x_n)$$

For that of the reason we are giving three chances to the user with in that three chances he used miss mach of his data enter he should be block on certain time though this also we can simply identify that the user who is using that person is valid user or not we can save the user data and as well as in this we are proposed a new way for the user password protection and new method for the user details that is when user register into the site in normal he has to select but here we are stopped that way and we implemented a system generated password for the user when he register and even in that also we are implemented a way of sharing technique that is half password will store in system and half password will shown to user and then after when user want to log-in he should enter that half password and in this application there is no farther password changing option. Like this we are implemented and implemented the security to the user and implemented

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.5, Pages : 332 - 336 (2014)
Special Issue of ICACSSE 2014 - Held on October 10, 2014 in St.Ann's College of Engineering & Technology, Chirala, Andhra Pradesh

b) Let $X = X_1 \times X_2 \times \cdots X_r$, and $\tilde{A}_1, \tilde{A}_2, ..., \tilde{A}_r$ be r fuzzy sets in $X_1, X_2, ..., X_r$, respectively. $f: X \rightarrow Y$, $y = f(x_1, x_2, ..., x_r)$. Then a fuzzy set $\tilde{B}$ in Y is defined by

$$\tilde{B} = \{(y, \mu_{\tilde{B}}(y)) | y = f(x_1, ..., x_r), (x_1, ..., x_r) \in X\}$$

$$\mu_{\tilde{B}}(y) = \begin{cases} \sup_{(x_1,...,x_r) \in f^{-1}(y)} \min\{\mu_{\tilde{A}_1}(x_1), ..., \mu_{\tilde{A}_r}(x_r)\} & \text{if } f^{-1}(y) \neq \emptyset \\ 0 & \text{otherwise} \end{cases}$$

where f^{-1} is the inverse of f.

For $r = 1$ the *extension principle* reduces to

$$f(\tilde{A}) = f\{(x, \mu(x)) | x \in X\}$$

$$\mu_{\tilde{A}}(y) = \begin{cases} \sup_{x \in f^{-1}(y)} \mu_{\tilde{A}}(x) & \text{if } f^{-1}(y) \neq \emptyset \\ 0 & \text{otherwise} \end{cases}$$

This is the same as **a)**.

the AI in cyber defense and we make it perfect to work as a good without making problems and done this well to work and to help to user and provide security as well as thin like human and give response imminently to the user base on the situations.

IV CONCLUSION

In this project the main intension of an user is to maintain the data without containing any kind of malware (threat). Tasks to be implemented in the process are, 1)While at the time of registration user will provide his desired password but we are splitting that password into 2 half's and one half is sent to the user mail and with that required password only user is able to login into user interface. 2) The second thing is mainly related to the core part, when the user is uploading, with that file we are storing a security key and some keywords based on that particular file name. So if in that file maybe if any malware is available then our application will not allow the user to upload that file. 3) If that file is not containing any kind of malware then only the application will allow storing that file. 4) If any user knows the security key for a particular file then that user is

V REFERENCES

[1] http://en.wikipedia.org/wiki/Conficker
[2] R. A. Poell, P. C. Szklrz. R3 – Getting the Right Information to
the Right People, Right in Time. Exploiting the NATO NEC.
In: M.- Amanovicz. Concepts and Implementations for Innovative Military Communications and Information Technologies. Military University of Technology Publisher, Warsaw, 2010, 23 – 31.
[3] E. Tyugu. Algorithms and Architectures of Artificial Intelligence. IOS Press. 2007.
[4] F. Rosenblatt. The Perceptron -- a perceiving and recognizing automaton. Report 85- 460-1, Cornell Aeronautical Laboratory, 1957.
[5] G. Klein, A. Ojamaa, P. Grigorenko, M. Jahnke, E. Tyugu. Enhancing Response Selection in Impact Estimation Approaches. Military Communications and Information Systems Conference (MCC), Wroclaw, Poland, 2010.
[6] J. Bai, Y. Wu, G. Wang, S. X. Yang, and W. Qiu, "A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis," in Advances in Neural Networks - ISNN 2006, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, May 2006, pp. 255–260.
[7] F. Barika, K. Hadjar, and N. El-Kadhi, "Artificial neural network for mobile IDS solution," in Security and Management, 2009, pp. 271–277.
[8] D. A. Bitter, T. Elizondo, Watson. Application of Artificial Neural Networks and Related Techniques to Intrusion Detection. WCCI 2010 IEEE World Congress on Computational Intelligence. July, 18-23, 2010 - CCIB, Barcelona, Spain, 2010, pp. 949– 954.
[9] R.-I. Chang, L.-B. Lai, W. D. Su, J. C. Wang, and J.-S. Kouh, "Intrusion detection by back propagation neural networks with sample-query and attribute-query," International Journal of Computational Intelligence Research, vol. 3, no. 1, 2007, pp. 6–10.
[10] L. DeLooze, Attack Characterization and Intrusion Detection using an Ensemble of Self-Organizing Maps,

AUTHORS

I.YallamandaReddy received the B. Tech degree in Computer Science and Eng from JNTU Kakinada & pursuing her M. Tech in Software Engineering from JNTU Kakinada.

A.Thirupathaiah is presently working as an Associate professor, dept. Of Information Technology, in St. Ann's College of Engineering and Technology, Chirala. He has More than 12 Years of Experience in Teaching and he is a lifetime member of ISTE and CSI.