International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 05 - 09

# Artificial Intelligence approaches in Cyber Security

Abhilash Kamtam
Bharati Vidyapeeth's College of Engineering,
Lavale, Pune, India.
*kamtamabhi@gmail.com*

Anshuman Kamar
Bharati Vidyapeeth's College of Engineering,
Lavale, Pune, India.
*anshumankr02@gmail.com*

Prof. U. C. Patkar
HOD Computer Department
Bharati Vidyapeeth's College of Engineering,
Lavale, Pune, India.
*patkarudayc@gmail.com*

***Abstract*—** As we all know that, the data that is been generated every second is increasing exponentially, as this information stored or received in any form is directly or indirectly is through Internet that means the data has to be travelled over a network for its completion of task, due to this the security for proper transmission of data plays a vital role in Cyber Security. The speed of processes and the amount of data to be used in defending the cyber space is cannot be handled by humans without considerable automations. However, it is difficult to develop software with conventional fixed algorithms for effectively defending against the dynamically evolving malicious attacks over the network. This situation can be handled by applying method of Artificial Intelligence that provides flexibility and learning capabilities of a network which later helps us in defending the attacks and as well as tracing down the culprits residing behind the terminology. This topic mainly emphasis on how well a packet is transferred from source to destination with proper security so that the end-user acquires the correct data as per his requirements.

***Keywords*-***Artificial Intelligence, Cyber Security, Geographic Coordinate System, TCP/IP Header Packet.*

*****

## I. INTRODUCTION

As we all know that, the data that is been generated in today's world is increasing exponentially day by day, as this information stored or received in any form is directly or indirectly is through *Internet* that means the data has to be travelled over a network for its completion of task, due to this the security of proper transmission of data plays a vital role in combating cyber-crimes which is achieved through principles of Cyber Security (CS). With the growing advancements in Information Technology (IT) criminals are using cyberspace to commit various cyber-crimes which later creating a huge disruption in the cyber society.

With the growing trends of complex distributed and Internet computing raise important questions about data security and privacy. Today's Cyber Infrastructure are highly vulnerable for intrusion detection and other threats. Even the physical devices that are available in the market such as sensors and detectors are not sufficient for monitoring and protection of these infrastructure; hence there is an essential need for more sophisticated IT that can model the normal behaviors and detect the abnormal ones. These defense systems need to be flexible, robust, reliable and should detect various kind of threats and must be able to make real-time intelligent decisions thereafter. [1][4]

As we all know the fact that most network-centric cyber-attacks are carried out through intelligently generated computer worms and viruses; hence, combating them with intelligent semi-autonomous agent that can detect, analyze, evaluate and respond to cyber-attacks has become a requirement. All these can be achieved by creating an intelligent system so called computer-generated forces which will be able to manage the entire process of attack response in a timely manner, i.e. which will be able to detect what type of attack is occurring, who all are the targets and what should be the appropriate response, as well as how intelligently the system will prioritize and prevent from secondary attacks. [1]

In order, to combat with these type of attacks we need innovative and technically strong approaches such as applying methods of Artificial Intelligence (AI) that provides flexibility and learning capability to the software which later helps in assisting humans in fighting cyber-crimes. AI offers numerous algorithmic computation methods (such as Computation Intelligence, Neural Networks, Intelligent Agents, Fuzzy Logic Systems, Artificial Immune Systems, Data Mining, Machine Learning, Pattern and Voice Recognition, etc.) which are increasingly playing an important role in cyber-crime detection and prevention. AI enables us to design an autonomic computing solutions which will be capable of adapting to their context of use, these will be using the methods of self-healing, self-diagnosis, self-management, self-tuning and self-configuration. AI provides intelligent techniques which seems promising area of research that focuses on improving the security of data/information under cyber space. [1], [2], [5].

The main purpose of study is to present advances that can be made in developing reliable and flexible cyber security elements which further leads to a high-end data security over a wide range of network.

## II. ARTIFICIAL INTELLIGENCE AND INTRUSION DETECTION

AI (which was also known as Machine Intelligence in the beginning) which emerged as a research project of Dartmouth College in 1956. This term was first coined in 1950 which later emerged as most intellect and innovative field which lead to an undefinable revolution since past decades. AI can be defined as two ways: (I) the field of science that studies the synthesis and analysis of computational agents that act

intelligently. [5] (ii) Creating a system in such a way that there will be less or no human intervention in solving any type of problems or tasks put forward toward to that system irrespective of its complexity. In the applications of AI in Cyber Security we are more interested in second definition.

The general approach to stimulate intelligent machines have been simplified to specific sub-sections which an intelligent system should exhibit for accurate result. The following sub-sections have received most responses [6], [7]:

- Deduction, Reasoning, Problem Solving (Neural Networks).
- Learning (Machine Learning).
- Knowledge Representation (Ontologies).
- Planning (Multi-agent planning and cooperation).
- Perception (Facial Recognition, Object Recognition, Speech Recognition).
- Natural Language Processing (Text Mining, Machine Translation).

AISs are the computational models that are inspired by the biological immune systems which are capable of adapting the changing environment and dynamically learning on its own. Immune systems are responsible to detect intruders i.e. various bacteria's, viruses, etc. and accordingly dealing with them. AISs are designed to mimic natural immune systems in the application of Cyber Security in general, and Intrusion Detection System (IDS) in particular.

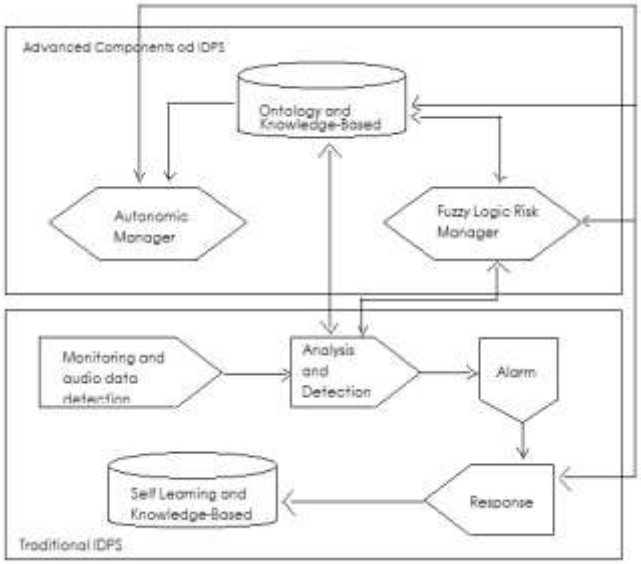


**Figure 1:** A Typical IDPS.

Many methods have been developed for securing the data over the networks and the Internet (e.g. secure protocols binding, firewalls, etc.); however, intruders create their own new path to grant the access to vital data residing over the network. An Intrusion Detection and Prevention System (IDPS) (see fig.1) is a software or hardware device which is placed inside the network which can possibly detect intruders and also attempts to prevent them. Generally, IDPS provides four basic and important security functions: monitoring, detecting, analyzing and responding to unauthorized activities or users. [1], [8], [9]

Artificial Neural Networks (ANNs) which basically works same as the human brain in which all the logic related work and instantaneous simulation is controlled by so called neurons. Here, the same terminology is used which consist of artificial neurons which and learn and solve problems accordingly when combined together. Neural Networks have ability to learn, process distributed information, self-organize and adapt, are applicable to solve problems that require considerable precision, conditionality and ambiguity at the same time. As, neural networks consist of a large number of artificial neurons which can provide a functionality of parallel learning and decision-making with high-speed, which later helps them in learning pattern recognition and selection of responses to attacks.

### A. *Characteristics of IDPS*

An IDPS should have certain desired characteristics for securing the network against serious attacks. Those characteristics are as follows [10]:

- Real-time intrusion detection – while attack is in progress (active mechanism) or immediately afterwards (passive mechanism).
- False alarms should be minimized.
- Less or no human interventions, and must be active throughout the life of the network.
- Must be in a state to recover from system crashes, either accidental or due to some attacks on the network.
- Self-monitoring ability to detect intruders, those attempting to change the system's data.
- Compliance to the security policies provided by the Cyber Security principles.

Should be able to adapt to the environment and system change by the administrator over time.

## III. Geographic Coordinate System

A geographic coordinate system is the system that enables to get every location on the Earth in order to be specified by a set of numbers or letters or symbols. The coordinates are always chosen such that one of the numbers represent vertical position, and two or three lines represent horizontal position. Here, vertical positions represent Longitudes and horizontal positions represent Latitudes, and one more parameter is taking into consideration for locating any object on this planet Earth is Elevation.

### A. *Geographic Coordinate System*

Latitudes and Longitudes are the units of Geographic Coordinate System which are used to represent the measurements in Degrees, Minutes and Seconds where 1 Degree = 60 nautical miles (69.09 miles); 1 Minute = 1 nautical mile; and 1 Second = 100.8 feet. Most of the organizations usually tells you which units they use, if not, then you can easily predict the format in which the coordinates are written. If the coordinates are given in Decimal Degrees, the coordinate is a whole number that will have 2 numbers after decimal point, or 5 numbers after the decimal point

followed by the degree symbol (e.g. 78.69541$^{o}$). In other formats, the numbers are split and the decimal and degree symbol appears inside the number. For example, Degree Decimal-Minutes which has a degree symbol first and then followed by the decimal number which indicates Degree and Minutes respectively (e.g. 107$^{o}$ 75.32175 latitude, 63$^{o}$ 29.78432 longitude). Degree, Minutes and Seconds, has a number with degree symbol, a second number followed by an accent symbol (') and then another number followed with decimal in it (e.g. 44° 40' 16.75 latitude, 93° 37' 10.05 longitude). Common practice reports the latitude value first, then the longitude value, separated by a comma. For latitude coordinate, some organizations also use the symbol "-" or S (degrees South) for location from equator; and for longitude, the direction from the prime meridian is measured using the minus symbol or W (degrees West).

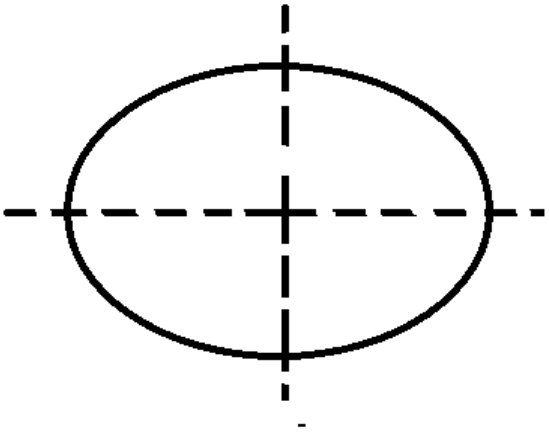

**Figure 2:** Approximate shape of the Earth.

Another important variable that should be taken into consideration while measuring the coordinate of Earth is the **Datum**. [11] As we all know that the shape of the Earth is neither spherical nor oval, the shape of Earth irregular or approximate to a biaxial ellipsoid (See fig.2). This irregular shape makes the mapping of Earth more complicated as the Earth does not fit completely into our mapping grid (which was developed for perfect sphere). Datum's are the known geographic shape of the Earth, which can be applied to maps, so that coordinate systems can work perfectly. Datum's can be classified into two broad categories: local referencing datum and global referencing datum. Local referencing datum that has been developed to set a local area on a national level. A global referencing datum approximates the shape of the Earth as a whole (on an international level) perfectly, but is not good for measuring the coordinates at national level.

## IV. TRANSMISSION CONTROL PROTOCOL: HEADER PACKET

Transmission Control Protocol (TCP) is a core protocol of the internet protocol suite. It was initially originated in the network implementation in which it complimented Internet Protocol (IP). Hence, the entire suit is referred to as TCP/IP. TCP provide reliable, ordered, connection-oriented and error-checked delivery of stream of octets between applications running on the hosts that are communicating with other hosts over an IP network. All the major internet applications such as World Wide Web (WWW), email, remote administration, file transfer protocol (FTP), etc. mainly relies on TCP. Applications which does not require reliable data stream service may use User Datagram Protocol (UDP) which is connection-less and less reliable.

The Transmission Control Protocol provide a communication service at an intermediate level between an application program and Internet Protocol. All these communication services provide host to host connectivity at Transport Layer of an OSI Model. At transport layer, the protocol handles all the handshaking activities, transmission details and also presents an abstraction of the connection established between the application and the network. At the lower levels of the protocol stack, due to some network congestion, traffic load balancing or any other unpredicted network activities, IP packets may be lost or duplicated or may be delivered out of order to the other end. TCP detects this and request retransmission of lost packets, rearranges out-of-order data, and even reduces or minimizes the network congestion and to reduce the occurrence of this type of failures. After diagnosis, even the packets remain undelivered, then it's source is notified with negative acknowledgement. Once the TCP receiver has reassembled the sequence of octets originally transmitted, are redirected to its source this is done in order to initiate the same process of transmission again. Thus, TCP abstracts the applications communication from the underlying networking details.

TCP is a reliable and connection-oriented stream delivery protocol which guarantees that all the bytes received will be identical to the bytes sent and that to in correct order. As the packet is transmitted over various networks there arises reliability issue, to resolve this issue a new concept was introduced known as Positive Acknowledgment with retransmission which is used to guarantee reliability of packets transferred. This fundamental technique requires acknowledgment to be received by the receiver as it receives the correct data. The sender keeps a record of each packet that it sends. The sender also maintains a timer from when the packet was sent, and retransmits a packet if the timer expires before the acknowledgment of the packets. The concept of timer was introduced in order have a glimpse of successful packet transmitted at specified time interval, it is also needed in case of packets are lost or corrupted.

### *A. TCP Header Format*

All the TCP segments are transmitted on a network through internet datagrams. The size of TCP Header is of 32 bits. The Internet Protocol header contains various information fields in it such as source address, destination address, etc. which are essential for successful transmission of data packet over a network. A TCP header follows the internet header, which allows supplying specific information that of TCP protocol. This division allows the existence of host level protocols other than that of TCP. Let us describe in brief the following fields that are contained in this 32 bits TCP Header (See Figure 3):

- Source Port: It is 16-bit slot which contains source address of the host.
- Destination Port: It is a 16-bit slot which contains destination address of the host.

- Sequence Number: It is a 32-bit slot this contains the sequence number of first data octets (except when SYN flag is present). If SYN flag is HIGH, then the sequence number is initial sequence number (ISN) and the first octet is given by (ISN+1).
- Acknowledgment Number: It is a 32-bit slot which contains acknowledgment number. If ACK control bit is set, then this field contains the value of the segment the sender is expecting to receive of next sequence number. This is always sent once the connection is established between the hosts.

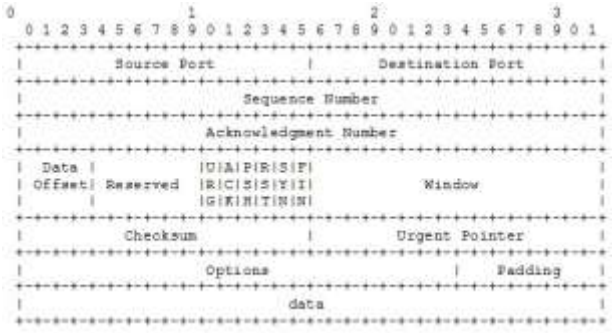


**Figure 3:** TCP Header Format

- Data Offset: It is a 4-bit slot which indicates where the data begins. The TCP Header (even one including options) is an integral number of 32 bits long.
- Reserved: It is 6-bit long slot which is reserved for future use and must be zero.
- Control Bits: It is a 6-bit slot which consist of various flags namely (from left to right),
  URG: Urgent pointer field significant.
  ACK: Acknowledgment field significant.
  PSH: Push function.
  RST: Reset the connection.
  SYN: Synchronize sequence numbers.
  FIN: No more data from sender.
- Window: It is a 16-bit slot. It contains the number of data octets beginning with the one indicated in the acknowledgment field in which the sender of this segment is willing to accept from the sender.
- Checksum: It is a 16-bit slot. It contains 2's complement of all 16 bit words in the header and data/text. If the segment contains odd number of header and text/data octets, then during checksum at source end the last octets are padded with zero on the right to form a complete 16 bits' word for checksum purposes. The pad is not transmitted as part of the segment. While computing the checksum, the checksum field itself is replaced with zeros.
- Urgent Pointer: It is a 16-bit slot. This field is used when the URG flag is set HIGH. This field communicates the current value of the urgent pointer as a positive offset from the sequence number in this segment. This points to the sequence number of the octet following the urgent data.
- Option: The size of this slot is Variable. This field may occupy space at the end of the TCP header and are a multiple of 8 bits in length. All options are included in the checksum. This field may begin on any octet boundary.
- Padding: The size of this slot is Variable. This field is used to correct the length of TCP header segment values so that they start and end at 32-bit boundary. Padding is done using zeros.

## V. PROPOSED MODEL

### *A. Artificial Intelligence approach in Cyber Security*

The main terminology and the ideology behind this approach is to provide the internet society a good, reliable, faster and the most secure connectivity to the network which will later leads to the betterment of the society. As the name suggest, there will be system or it may be a hardware dependent software which will be intelligently sensing the network throughout the lifetime of the respective network. The system that will be developed should be capable of monitoring the network continuously and must sense all the activities that is taking place onto the network. The system developed should abide all the rules and laws of artificial intelligence and the functioning done by that system over network must fulfill all the principles of cyber security and should fall under the guidelines of Cyber Security properties.

The system should be capable of self-defending itself, that is it must self-diagnose in case of any module failure so that the performance of that system should be retained even after observing some internal failures. Various concepts of AI can be used such as Artificial Neural Networks (ANNs), Machine Learning, Fuzzy Logic Control Systems, etc. for developing an intelligent system.

The system proposed should self-defend itself from any type of hazardous intrusions which may be of various kind such as viruses, malwares, Trojans, spoofing, etc. The system must first detect the type of data it contains, analyze it and then it must grant access to the required field with proper access permissions and guidelines. The Self-defending of network can be achieved by using the existing concepts of AI which will help in building a strong and intelligent system which will provide a high-level security to the data as well as the network. As the system uses AI concepts, this means the system should be active and simulate itself in such a way that it should not affect the neighboring network. The system should be strong to handle ample amount traffic load occurring on the network, network congestion and all other abnormal activities that may occur in a network. All this problems and failures should be identified by system at runtime so that it can be resolved at finest moment and will lead to sanitization of the network.

This runtime detection, analyzing and resolving of network can be achieved using adaptive mechanism. As we know that, basically there exist two type of mechanism which can be embedded in a system in order to take required actions on the network. They are:

- Adaptive Mechanism.
- Proactive Mechanism.

In Adaptive Mechanism, all the procedures such as detection, analyzing and resolving are carried out runtime that means the system must remain active throughout the lifetime of the network whereas, in Proactive Mechanism, the system performs the same task (detection, analyzing and resolving) after the attack has taken place by the intruder.

The concepts of AI actually get executed at runtime that is according to situation the system reacts and provides the required results. Hence, a system can be proposed that uses the thinking and decision making ability and react accordingly so that a good, strong, reliable and secure system can be developed. This will be incorporated with concepts of AI and the basic principles and guidelines of Cyber Security.

As we know that, every coin has two faces similarly, in this networking world everyday n number of challenges are raised up which leads to insecurity of connectivity to the network and an alternative for the existing model has to be developed. Here come the roles of Cyber Security, where various Intrusion Detection algorithms are executed in order to trace down the main culprit residing behind this terminology. As tracing down the culprits is not an easy task and if caught, then it would have taken couple of months or may be years to trace down the actual culprit. As all these activities are performed after the attack has been taken place, hence Proactive Mechanism are used for performing the required task over a network.

Similarly, here comes the proposed model that gets executed in the worst case scenario, that is if the Adaptive Mechanism based system fails due to unrecognized intrusion into the network then the system acts proactively in such a strong way that it creates an illusion of working automatically. Here, in this situation the system will place the geographic coordinate location in the packet which will be encapsulated and abstracted in the TCP Header packet. Every packet which will be routed through this device will embed geographic coordinate into the header of TCP packet which will be changed as soon as the same packet gets routed through the proposed system which may be placed at XYZ location. This process of embedding coordinates will continue until the packet reaches to destination successfully and with proper security.

In case of failure in packet transmission or a packet gets lost due to congestion in network or due to traffic load balancing the pre-existing protocol of TCP will be used which will retransmit the same packet with proper destination port, checksum, offset, acknowledge and sequence number along with geographic coordinates embedded into it. By this, a secure and reliable connection will be established which will assure safe and successful packet transmission over a wide network. If the proposed model is an intelligent system, then it can be placed at servers, routers, switches, etc. which will ease the control of flow of packets. If any intrusion takes place in a system, then it will become easy for cyber security officials to trace down the culprits behind this terminology. Hence, there will be less or no human intervention in controlling the traffic and thus reducing the human efforts in Cyber Security offices. The mechanism of the intelligent system or software will be complied under basic Cyber Security principles.

## VI. CONCLUSIONS AND FUTURE SCOPE

The proposed intelligent system will lead to a good, reliable, faster and most secure connectivity to the network. This will reduce the human efforts for tracing down the culprits who had caused an adverse effect on the network. As we know that, out of the total bandwidth provided by the service provider only 8.8-9% is used by the end-user, this % may varies accordingly for various countries. Due to the embedding of geographic coordinates into the TCP Header packet the weight of the packet correspondingly rises which later helps in using an optimum bandwidth and thus increasing the speed of data transmission from one host to another host connected over a secure network. On implementation of this proposed intelligent system, there will be less or eventually no human intervention in controlling the traffic over a network which is usually done by Cyber Security officials, they continuously monitor various types of network in order to provide better security to the user and thus providing them with proper security guidelines to the system. Hence, the conclusion for the above discussed model is that, a system which will detect, analyze and resolve the issues in the network automatically using artificial intelligent approaches under the guidelines and principles of Cyber Security must be taken in practice in order to provide security a level ahead of the existing one.

## REFERENCES

[1] Selma Dilek, Hüseyin Çakır and Mustafa Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review," International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, No. 1, January 2015, pp. 21-39.

[2] Enn Tyugu, (2011) "Artificial Intelligence in Cyber Defense," 2011 3rd International Conference on Cyber Conflict,(ICCC 2011),pp. 1-11.

[3] J. Polk, J. Schnizlein, M. Linsner, "Dynamic Host Control Protocol Option for Coordinate-based Location Configuration Information," network Working Group, Cisco Systems, July 2004 Copyright (C) The Internet Society (2004).

[4] D. Dasgupta (2006), "Computational Intelligence in Cyber Security," IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety (CHISPS 2006), pp. 2-3.

[5] 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

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

[7] Artificial Intelligence, Wikipedia, https://en.wikipedia.org/wiki/Artificial_intelligence, (30/03/2016).

[8] 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.

[9] 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. 5–41

[10] 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.

[11] A guide to coordinate system in Great Britain *D00659 v2.3, Ordnance Survey, Mar 2015*, retrieved 2015-06-22