International Journal of Advanced Research in Engineering and Applied Sciences

ISSN: 2278-6252
Impact Factor: 7.687

DEVELOPMENT OF ALGORITHMS FOR DETECTING ATTACKS ON WEBSITES USING ARTIFICIAL INTELLIGENCE

Muhammadjonov Xojiakbar Zafarjon ugli-International Islamic Academy of Uzbekistan,1st year master's degree in information security management

ABSTRACT: *in this article, by attacking in the process of information transmission, preventing negative situations such as hearing and altering data transmission channels is an important part of ensuring information security. In addition to this, the development of algorithms that identify attacks on Web sites using artificial intelligence is presented vs.*

Keywords: VPN, SI,Kee (Knowledge, Engineering Environment), FRL (FrameRepresentation Language), KRL (Knowledge Representation Language), ARTS, VEP, artificial intelligence.

The introduction of artificial intelligence technologies in our country, their wide application, expansion of the use of digital information, training of qualified personnel in this field, in a word, has been defined many tasks aimed at developing the sphere at the level of World requirements.

The intensive and extensive application of artificial intelligence technologies in the world practice, as well as the possibility of using similar digital information, ensuring the high quality of use in the life of our country, creating favorable conditions for the training of qualified personnel in this field is today's demand. The term artificial intelligence was

first proposed at the Dortmund conference in 1956 year by John McCarthy [1] and his colleagues Marvin Lee Minsky, Nathaniel Rochester, Claude Shennons. John McCarthy is accepted as the author of this term. During this time, very large scientific research has been carried out and is being carried out, as a result of which the field of application of artificial intelligence is rapidly deteriorating. Currently, artificial intelligence is being used effectively in healthcare, energy, mining, agriculture, education, machine building improvement, voice assistants, online chat and communication and software development.

Artificial intelligence (SI) is the ground for imitating the processes of human intelligence by creating and applying algorithms in a fast - paced computing environment. Simply put, artificial intelligence is a technology that focuses on thinking computers like people and finding solutions.

To achieve this goal, three main compartments are required:

* Computing systems (large capacity computers)

• Big data and their management

* SI algorithms (programming code)

The closer the result is to the human mind, the more data and computing resources (power) are required.

The application of artificial intelligence can be observed in everyday situations of our lives. For example, in the case of detection of fraud in financial services, forecasting the need for products in retail trade, making online transactions with customers or performing remote support services:[2]

*** Fraud detection.** The financial services industry uses artificial intelligence in two ways. In the initial analysis of loan applications, artificial intelligence helps in understanding the creditworthiness. And more advanced SI solutions are used to monitor the operations of plastic cards in real time and detect fraud**.**

[1] https://en.wikipedia.org/wiki/ John_McCarthy_ (computer_scientist

[2] https://www.norma.uz/qonunchilikda_yangi/uzbekistonda_suniy_intellekt_tehnologiyalari_joriy_etiladi

In the field of health care. Based on mammography analysis, SI technologies are used to diagnose breast cancer early.

• **In the field of Agriculture.** To monitor the condition of soils and crops, as well as to prevent them from falling into the stress state of plants, increase the efficiency and efficiency of irrigation using artificial intelligence technologies based on remote sensing of the Earth.

• **In the field of transport.** Control traffic light, prevent traffic jams, and route vehicles along optimal routes.

* Artificial languages.

Before these hams, LISP (Lisp) and Prolog (Prolog) [8] were the most common, numerous languages for solving artificial intelligence tasks. There are also less common languages for artificial intelligence, such as Russian-made REFALL. Their universality is less than that of traditional languages, but artificial intelligence languages are being replaced by rich possibilities for working with signicant and logical data, which are key to artificial intelligence functions. Specialized computers are created based on artificial intelligence languages, such as multihomed lisp-machines to solve artificial intelligence tasks. The disadvantage of these languages is that they are not used to create hybrid expert systems**.**In addition, the development of algorithms that identify attacks on Web sites using artificial intelligence :

It is possible to listen, change and block information in an impersonal state in the process of information transmission, in the case of information exchange carried out by telephone lines of communication, instant messaging via the internet, videoconferencing and sending of facs with the attack of hearing and change. It is possible to carry out this attack through protokols, analyzing several networks. It allows you to easily convert standard digital sound into high-quality, yet voluminous audio files (WAV) through attack-carrying software (video or audio analog signal conversion into digital signal conversion, and vice versa).

Usually the process of performing this attack is not felt by the user at all. The system will perform the specified actions without excessive strain and noise. There is absolutely no doubt about the theft of information. Only those who previously had information about

this threat and want the information being sent to retain its value will be able to share information over the protected network as a result of the use of special network frustration measures.

Due to an attack in the process of information transmission, the following incidents occur

* Swimming;

• Keep up;

* Sort;

* Falsification.

Retention-opens the way to unauthorized use of the resource. As a result, the confidentiality (confidentiality) of information is violated. Such users can be physical person, software or computer.

Turlash-not only the illegal use of the resource will open the way, but the resource will be changed by The Corrupter. As a result, the integrity of information is violated. An example of such interruptions is the modification of the contents of the data in the file, its modification with the aim of changing the functions and characteristics of the program, the modification of the contents of information transmitted over the network.

Falsification-a fake object is introduced into the system. As a result, the fragility of the original information is broken. An example of such violations is the transfer of illegal data over the network or the addition of records to a file. When the above violations are classified according to the terms passive and active attack, we can see that disconnection, stand-by, and falsification belong to the asset threat, while passive threat retention is relevant.

Ways to eliminate the main attacks on Web sites

By attacking in the process of information transmission, preventing negative situations such as hearing and altering data transmission channels is an important part of ensuring information security.

There are several effective anti-eavesdropping and anti-tampering technologies in the information sent during the exchange of information over the network:

* IPSec (Internet protocol security) protocol;

* VPN (Virtual Private Network) virtual private network;

• IDS (Intrusion Detection System) Intrusion Detection System.

Ipsec (Internet protocol security) this security provides secure data exchange over the network using protokolari as well as encryption algorithms. This ensures that programs and data as well as device tools are compatible in the interaction of computers on the network through a special standard. The Ipsec protocol ensures the confidentiality of information transmitted over the network, that is, it is understandable only to the sender and receiver, the purity of information, as well as the authentication of packets. The application of modern information technology has become a necessary tool for the development of every organization. And the Ipsec protocol provides effective protection for exactly the following:

• when connecting head offices and branches with a global network;

• in the management of the enterprise over the internet at a long distance;

* protecting the network connected with sponsors;

* to raise the level of security of electronic commerce.

VPN (Virtual Private Network) is defined as a virtual private network. This technology is aimed at providing reliable protection, the exchange of all data between users is based on the formation of an internal network within another network. The internet is used as the basis of the network for VPN.

Advantage of VPN technology. By connecting local area networks to a common VPN network, a low-cost and high-level protected tunnel can be built. To create such a network, you need to install a special VPN gateway, which serves to exchange information between branches on one computer of each network part. The exchange of information in each section is carried out in a simple way.

If you need to send data to another part of the VPN network, then in this case all the data will be sent to the gateway. In turn, the gateway performs Data Processing, encrypts it on the basis of a reliable algorithm and sends it through the Internet to another branch gateway. At the specified point, the data is deciphered again and transferred to the last computer in a simple way. All this is done at an imperceptible level for the user as a whole

and does not differ in any way from the performance on the local network. Using an Eavesdropping attack, the information listened to becomes incomprehensible.

In addition, VPN is a great way to add a separate computer to an organization's Local Area Network. Imagine that we went on a service trip with your laptop, there was a need to connect to our own network or get some information from there. With the help of a special application, we can connect with a VPN gateway and operate like every employee in the office. It is not only convenient, but also inexpensive.

Principle of operation of VPN. In order to establish a VPN network, in addition to new devices and software, it is necessary to have two main parts: the data transfer protocol and the means for its protection.

With the help of an intrusion detection system (IDS), the method or means by which a system or network is attempted to breach its security policy are identified. Intrusion detection systems have an almost quarter-century history. The first models and prototypes of intrusion detection systems were used to analyze the audit data of computer systems. This system is divided into two main classes. It is divided into network Intrusion Detection System (Network Intrusion Detection System) and Computer Intrusion Detection System (Host Intrusion Detection System).

The structure of IDS systems architecture includes:

* sensor part system that collects and analyzes cases related to the safety of protected systems;

• analysis part system designed to detect suspicious movements and attacks according to sensors data;

* facility that provides data collection about the results of the analysis and preliminary cases;

It is a conflict tracking management console that allows configuration of IDS systems, tracking IDS and protected system status, detecting analysis part systems.

This system is divided into two main classes. It is divided into network Intrusion Detection System (Network Intrusion Detection System) and Computer Intrusion Detection System (Host Intrusion Detection System). The principle of operation of the network intrusion detection system (NIDS) is as follows:

1. checks traffic that has access to the network;

2. imposes a restriction on packages that are harmful and do not have permission.

Using the listed security stages, it can be effectively protected against the threat of Eavesdropping.

Network screen is the first protective device of internal and external perimeter. The network manages incoming and outgoing data in on-screen information and Communication Technology (ICT)and provides ICT protection through data filtering, performs information verification based on established criteria, and decides whether packets will enter the system. The network screen sees all packets passing through the network and decides whether to allow them or not by checking the packets in both (input, output) directions according to the established rules. Also, the network screen performs protection between the two networks, that is, it protects the protected network from an open external network. The convenience of the protection tool listed below, especially the packet filtering function, is an effective means of protection against DOS attacks. Package filters control the following:

• physical interface, where the package comes from;

• IP address of the source;

• IP address of the recipient;

• source and receiving traffic ports.

Network screen can not provide full protection from DOS attack due to some disadvantages:

• errors or omissions in the design — various technologies of networked screens can be protected-does not cover all infect access paths to the lying network;

* implementation disadvantages-since each network screen is in view of complex software (software-hardware) it has errors. In addition, there is no general methodology for testing, which allows you to determine the quality of software implementation and make sure that all the specification on the network screen is implemented;

• shortcomings in the application (exploitation) — the management of networked screens, their configuration under the security policy is considered very complicated, and

in many cases, there are cases of incorrect configuration of networked screens. The listed shortcomings can be eliminated using the IPsec protocol. Summarizing the above, it is possible to obtain sufficient protection from a DOS attack through the proper use of network screens and IPsec protocol.

•• This group of artificial intelligence software tools includes special asloxos in general definition. According to the Koida, this library and the lisp are the ustkurma Kee (Knowledge,Engineering Environment) above the artificial intelligence language, FRL (FrameRepresentation Language), KRL (Knowledge Representation Language), ARTS, and others that allow users to work on the timelines of expert systems at a higher level than the difference from the extimal finding in the usual languages of artificial intelligence.

•* On February 17, 2021, the resolution of the president of the Republic of Uzbekistan”on measures to create conditions for the rapid introduction of artificial intelligence technologies " was adopted.

•• The purpose of this decision is to introduce the technologies of artificial intelligence in accordance with the Strategy” Digital Uzbekistan – 2030 " and to apply them widely in our country, to ensure the possibility of using digital information and their high quality, to create favorable conditions for training qualified personnel in this field.

- Conclusion

•• The document also provides for the development of the strategy for the development of artificial intelligence, which sets out the main directions and principles of the application of artificial intelligence, as well as the conditions for the formation of artificial intelligence in the near and long term, the development of unified requirements, responsibility, security and transparency in the development and use of artificial intelligence In turn, in order to improve the efficiency of state bodies in the processing of data, such objectives as the widespread use of artificial intelligence technologies, conducting fundamental and applied research on the development of useful technological solutions and the creation of a local ecosystem of innovative works in the field of artificial intelligence, which encourages their subsequent commercialization, are carried out.

•• What areas of application of artificial intelligence technologies in the decision, the tasks envisaged in this regard are also fully reflected.

•

•• For example, in the field of Agriculture: the application of artificial intelligence technologies in the process of monitoring the state of soil and agricultural crops, as well as agricultural equipment, including combiners, on the basis of data on remote sensing of the land.

• In the banking industry, the task is to increase the effectiveness of monitoring the activities of commercial banks and simplify the implementation of regulatory requirements (SubTech and RegTech) by them, as well as the application of artificial intelligence technologies for the analysis of the quality of banking services, remote biometric identification (fac-ID) of users and assessment of credit risks.

•• Analysis of budget expenditures, pension, social and insurance payments, as well as pension payments in the field of Finance

•and to increase its effectiveness, the use of artificial intelligence technologies is envisaged.

•

•• In the field of taxation, the functions of artificial intelligence technologies in the analysis of tax receipts of legal entities, in the determination of discrepancies in tax payments, in the process of managing locomotives in the field of transport, in the monitoring of their movement and warning of motorists in dangerous situations, in the analysis of the public transporti movement and determining their optimal.

• In this decision, tasks on the wide use of artificial intelligence technologies in other areas are also included.

• In accordance with the resolution, the tasks on the basis of the scientific-innovation center of Information and communication technologies under the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi and the scientific-practical center of software systems under the National University of Uzbekistan named after Mirzo Ulugbek are defined to organize the scientific-research institute of digital technologies and artificial.

• The decision also included tasks for the establishment of the Department for the introduction and development of artificial intelligence technologies, which consists of 15

state units, in the structure of the central government of the ministry for the development of Information Technologies and communications.

• At the same time, this decision also provides for the tasks of developing and approving the “road map”for the rapid and effective implementation of pilot projects within a month, the organization of training of local specialists, as well as cooperation in other areas specified in this decision.

• In this regard, it should be noted that this decision is set out in the priority directions of economic development of the state Program 2020 — the year of development of Science, Education and digital economy — The rapid development of the”digital economy", the wide introduction of digital technologies in all spheres of human activity, including automation of production and management systems in the health and education sectors, the real sector of the economy, the integrity and sustainable functioning of the information system and the implementation of tasks related to ensuring information security are also important.

Used literature:

1. Ganiev. S.K, Karimov. LocationM, Tashev K.A, Information Security.Security of Information Communication Systems. Tashkent "Contact" 2008.

2. V.F Shangin Informasionnaya bezopasnost kopyuternix sistem I setey. 2011. - 416 s

3. K.A Tashev, N.B Nasrullaev, - methodical trainings for carrying out lobaratory work on information security in computer systems and networks. Tashkent 2013

4. Fundamentals of information security: lecture course / Candidate of physical and Mathematical Sciences, senior research fellow I.LocationUnder the general edition of Karimov, Academy of Mia of the Republic of Uzbekistan, 2013.

5.http://www.ziyonet.uz

6.http://www.uzinfocom.uz