The upgrade security base is organized using in-depth learning to prevent transportation

1. Mohammad Javad Shahsavari
Student of Master in electrical engineering-nanoware and micro-electronics, Iran, Kermanshah, Razi University

2. Sima Houshmand
Student of Computer Sciences, Department of Mathematics, Iran, Kermanshah, Razi University

Abstract

One of the main challenges in using databases has long been to secure these databases, as many databases contain important data or if disrupted can have adverse effects on If they have co-centered systems, we need to examine the challenges of these databases and how to address and institutionalize these challenges. In our world today, all database systems are affected by a variety of security challenges and cyber attacks. In this study, we intend to examine a specific type of attack called denial of service attack and then to review the deep learning method, which is based on how the human neural network works, then We will discuss the in-depth learning method in order to provide security against denial of service attacks. The results of the hypotheses of this study are examined using a simulator.

Keywords: deep learning, machine learning,

Introduction

The need to integrate and aggregate the data stored in the computer in a systematic and codified manner led to a sense of necessity to build databases. According to the definition of the World Institute of Standards and Technology, a database is a collection of structured and organized data stored on a computer system and can be shared with other users. This definition is necessary for sharing data stored on databases, using this definition, access levels should be introduced for users who use the database. On the other hand, using shared databases on the network carries risks and challenges. It is obvious that a database that contains data, although not important, is a good prey for hackers and hackers. Some beginners in the field of influence sometimes even try to penetrate or disable databases in order to show their abilities to others. However, all of the risks that most network-based computer systems pose to online databases are also present. Challenges and risks such as eavesdropping, intentional manipulation of data, denial of access to data, hacking for theft, etc. are among the most common issues that affect the security of databases. Most of these challenges can be prevented by using firewalls or actions such as backing up databases or access level settings, but here is a basic security challenge called a denial of access attack. In this study, we intend to review the databases, introduce and review the access denial attack. Topics to be explored in this study are:

An overview of databases, an overview of access denial attacks, an overview of in-depth learning methods and how to use it to repel denial of access attacks, conclusions and suggestions for the future.

• An overview of basic definitions and concepts of databases

Database refers to a collection of related data and structures or organizations that access this information usually through a database management system consisting of an integrated set of computer software that allows users to interact with one or more databases. And access to all information in the database, although there may be a limit to the limited access to certain information. How the various functions that import, store and retrieve large amounts of information as well as present for management show that this information is organized. Because of the

close connection between them, the term "database" is often used to refer to both a database and a DBMS. Outside of the professional IT world, databases have long been used to refer to any set of related data, such as a spreadsheet or a card index. In this article, we are only dealing with databases in which the size and essential conditions of using the database management system are important. January. The existing S allows different functions to manage a database and its data, which can be classified into three main groups.

1) Data Definition - Create, modify, and delete definitions by which we define data organization.

2) Update - insert, modify and delete real data.

3) Provide information in a form that can be used directly or for further processing by other applications. The retrieved data may be in one form essentially the same as that created in the database or in a new form obtained by modifying or combining existing data from the available stored databases.

Both the database and the DBMS conform to the principles of the specific database model. "Database system" refers collectively to the database model, database management system, and database. Physically, computer database servers are dedicated to holding real databases and running only DBMS and related software. Database servers are usually multi-computers, with memory and RAID disks used for stable storage. RAID is used for data recovery if any of the disks or. Database accelerator hardware, connected to one or more servers through a high-speed channel, is used in large volume transaction processing environments. ABM.

It is found at the heart of most database applications. January.BM It may be built around a custom multitasking core to support the network, but Di. BMS. Modern S typically exists in a standard operating system. January. BMS. S includes a significant economic marketplace for PC vendors and storage of DBMS requirements in developed applications. Databases and di. BMS. S can be categorized according to the visitor database model that supports them.

- **Database model**

  Specifies the work pattern of database users at a logical level. There are several techniques for data models. Different physical performances can

be implemented for each of the logical models and provide different levels of control in physical adaptation for users. These models include the flat model, the hierarchical model, the network model, and the relational model. The relational model is the basis of today's database management system.

- **Denial of Service (DOS) attack**

In the field of computer science, a denial-of-service attack or a distributed denial-of-service attack is an attempt to remove machine and network resources from the reach of authorized users; In fact, any attack on accessibility is considered a denial of service attack. Although the purpose of a DOS attack and the motive for doing so may vary, it generally involves trying to temporarily or permanently interrupt or suspend the services of an Internet-connected host. DOS targets usually target sites or web server hosting services with appropriate features such as banks, credit cards, and even root servers. One common method of attack involves saturating the target machine with external communication requests so that the target machine cannot respond to legitimate traffic, or responses are given at low speeds or are not available. Such attacks lead to high server overhead. A DOS attack forces the target computer to reset or consume its resources, so it can not serve the services in question and also violates the policies accepted by Internet service providers. Below is a simple image of a denial of service attack.

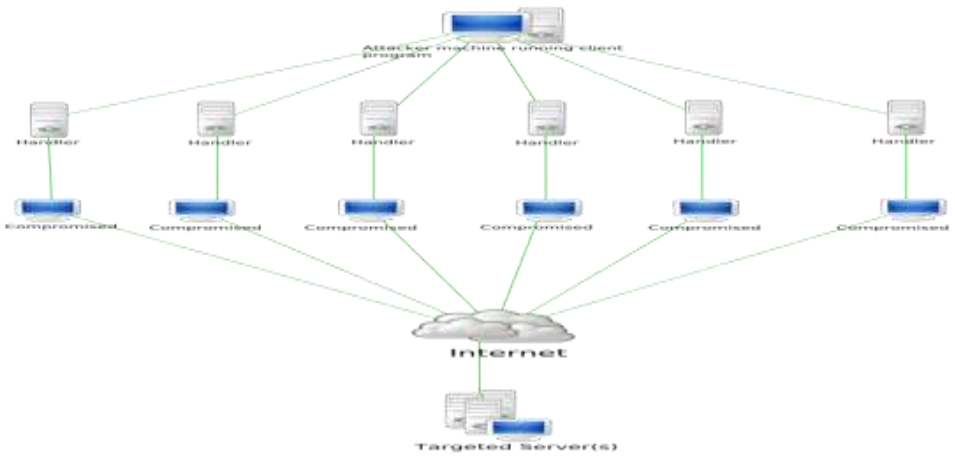

Figure 1- A simple image of a denial of service attack

A denial of service attack on a database will have the following effects:

- ✓ Slow and unusual network performance
- ✓ Significant increase in the number of received spam
- ✓ Unavailability of a specific website
- ✓ Inability to access a website
- ✓ Disconnect wireless or wired internet connection

A denial of service attack is of several types, all of which are of the same nature and are carried out with the aim of sabotaging and disabling the network, here we will only introduce the types of this type of attack.

1) Flood attack with icmp protocol
2) IP eddy current attack
3) Volumetric disturbance attack
4) Disable attack with random access
5) Attack banning remote telephony services
6) Peer-to-peer attack

Since these types of attacks lead to database crashes, inability to access the database, and general disruption of online access to the database, it is necessary to consider ways to prevent such attacks on databases. . In the continuation of this research, we intend to introduce the deep learning method and how to use this method in order to prevent and improve the security of databases.

- **Deep learning and its use in improving security**

In-depth learning is a sub-branch of machine learning based on a set of algorithms that attempt to model high-level abstract concepts in data that use a deep graph with multiple processing layers consisting of multiple conversion layers. They are linear and non-linear, they model. In other words, it is based on learning to display knowledge and features in model layers. An instructional instance can be modeled in various ways as a mathematical vector filled with values per pixel, and more generally as a set of smaller subtypes. Some of these modeling methods simplify the

machine learning process. In deep learning, there is hope to replace the extraction of these image features by human hands with fully automated, unsupervised and semi-supervised methods. The first motivation for this learning structure was inspired by examining the neural structure in the human brain, in which nerve cells make sense by sending messages to each other.

Depending on the various hypotheses about how these neurons connect, different models and structures have been proposed and studied in this area, although these models do not naturally exist in the human brain and the human brain is more complex. . These models such as deep neural network, complex neural network, deep belief network have made good progress in the fields of natural language processing, image processing. In fact, the term deep learning is the study of new methods for artificial neural networks. Deep learning is a subset of machine learning that uses multiple layers of linear transformations to process sensory signals such as audio and video. In this way, the machine divides each complex concept into simpler concepts, and as this process continues, it reaches the basic concepts that it is able to decide on, thus requiring full human supervision to determine the necessary information of the machine at any given time. is not. An important issue in deep learning is how information is presented. The information provided to the machine should be such that the machine receives the key information that it can make a decision based on in the shortest possible time. When designing deep learning algorithms, we must pay attention to the transformational factors that explain the observed information. These factors are usually not observable factors, but factors that affect the observable category or are born of human mental structures to simplify problems. are. For example, when processing speech, the transformational factors can be the speaker's accent, age, or gender. When processing a car image, the amount of sunlight is a transformative factor. One of the problems of artificial intelligence is the high impact of transformational factors on the information received. For example, many pixels received from a red car at night may look black. To solve these problems, we sometimes need a high level of understanding of information, and in fact, sometimes

finding the right way to display information is as difficult and time consuming as it is.

Use in-depth learning in deploying denial-of-service attacks

Since denial-of-service attacks follow the same basic patterns, it seems that using a neural network with in-depth learning, such attacks can be identified

and possible preventive measures considered. According to the descriptions provided for in-depth learning, a particular paradigm can be developed

Introduced for in-depth learning so that it can then be clearly identified for possible attacks. Here it is enough to examine some possible events for this type of attack.

Attack with the intention of disabling access to the database: In such a type of attack, it is enough to design an artificial neural network to protect the database from unsuccessful accesses or attempts to access the database in short periods of time. Be able to identify. This neural network can emphasize the request of IP applicants and the failure to enter the database during authentication as a key for identification. Obviously, once this type of attack is detected, the requesting IP can be blocked or the dynamic address of the database can be changed.

Attack to block access to the database: This type of attack is intended to block the bandwidth of the database, after which it will be very difficult for users to access the database. In order to detect this type of attack, the artificial neural network must be trained in such a way that in case of limitation in the bandwidth of the database, it informs the senior user of the network or uses another medium for data exchange.

Attack with the intention of disrupting the database and the data transfer medium of the database: Repelling this type of attack requires repeated training of the artificial neural network, but the general idea is similar to the previous two types of attack. In addition, an easier way to control this

type of neural network training attack is to use preventative measures such as capture codes.

Figure 2 - An example of Captcha code often used by deep learning systems to prevent denial of service attacks or the entry of robots.

Apply in-depth learning to repel denial of service attacks

Here we are going to run an experiment to test the algorithm introduced in this paper. The test was performed on a PC with an Intel core I3 6005 processor with 4 GB of RAM and Windows 11 operating system and MATLAB r2013b software. We first train a neuron with 111 characteristics as examples of an attack pattern. The training diagram of this neuron is listed below. (Output diagram received from MATLAB software)

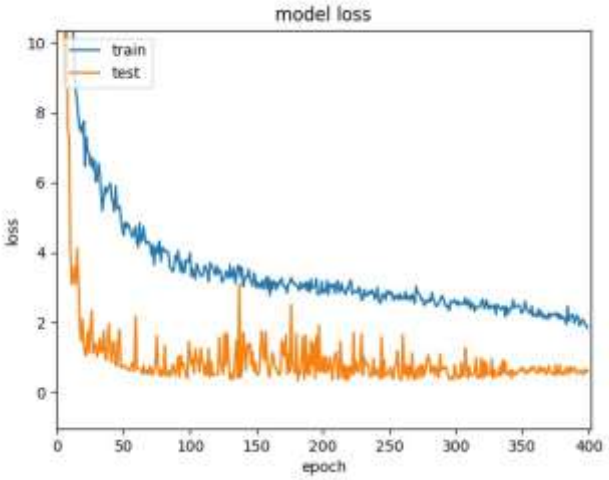

Figure 3 - Neuron learning chart and comparison of neuron behavior

After training these neurons, we considered a random number as the characteristic identifier of the neuron. This feature is waiting for a number to be received by the user, if the number matches or converges with the neural network teachings, the neuron gives a message that it is possible to approach the answer to the attack.

• Conclusions and future suggestions

Because denial-of-service attacks often have the same pattern and function as the same base, their detection requires a simple pattern recognition operation, which can be performed simply by deep learning-based artificial neural networks. However, it is necessary to provide appropriate data to introduce the pattern of this type of attack to the neural network so that if necessary, the neural network with its self-learning capability can detect this type of attack. Similar to all algorithms implemented by artificial neural networks, especially deep machine learning, there is the possibility of over-learning and its problems in this method, so it is necessary after training the neuron with pre-determined attacks. The security of the method should be validated and evaluated.

It is also suggested that in future research, this method be evaluated more widely with more neurons to measure its efficiency on a larger scale. However, this field of artificial intelligence knowledge and databases is expanding rapidly and we expect to see progress in this field in the future.

References

1) Mir Abedini, Shirin, 1397, Review of Deep Learning, Third National Conference on Technology in Electrical and Computer Engineering, Semnan, Payame Noor University

2) Abbasi, Omid and Mahdieh Soleimani, 2016, Deep Learning in Recommending Systems, 22nd Annual National Conference of Iranian Computer Association, Tehran, Sharif University of Technology - Iranian Computer Association

3) Hassan Pourmati Kalaei, Seyed Hossein and Reza Saadati, 2016, A Review of Some Popular Methods of Deep Learning, 3rd National Conference on Electrical and Computer Engineering of Distributed Systems and Intelligent Networks, Kashan, Islamic Azad University, Kashan Branch