Tecnológico de Monterrey

Competency Evidence

Programming of data structures

Inés Alejandro Garcia Mosqueda A00834571

Jesus Fong Ruiz A01254062

Profesores: Luis Ricardo Peña Llamas
Jorge Gonzalez

10/10/2022

Ines Alejandro

To start off with the programming structures. The most efficient type of coding tree would be the Avl BST tree since it always preserves the integrity of the tree and its worst case is complexity O(nlogn) for everything but for versatility the BST is implemented. This tree is one of the most used structures due to its simplicity, but also its complex way of analyzing data that allows the user to traverse through the data with some basic operations within the tree. The tree consists of the information and sections it by using roots. With these roots the tree uses 4 basic operations to allow the user to traverse through the information in a simple way. The 4 operations are: Searching, Deletion, Traverse and Insert. These operations are pretty basic to understand since the words are self-explanatory, searching is in charge of searching for the data through the tree in a specific order. Deletion is in charge of deleting values under some conditions. Traverse is the way the program goes through the tree and finally the user is allowed to insert values onto the tree. In conclusion these basic operations help the user create a tree with the information we input into and it's a very simple structure to follow if we wanna store information. In the case of the IP's we use this tree to analyze every single one of the values and we use one of the basic operations to find the values we need. The next topic we will be analyzing would be, how do we identify if our network is being infected? With this there are several ways we can see if our network has been compromised by cyberattacks. We will start noticing a change in the speed of the things. This means that the internet and PC speed will significantly decrease due to the attacks. Some other factors that we can analyze are the crashing of applications and programs in our devices.
In case we are evaluating the attacks of a bot net towards a server, we can make use of the registry of denials of access to the server and from the registered IPs detect which ones can be temporarily blocked to avoid the collapse of our system and follow the process of the server, without complications due to excess request. Since there will be too many IPs that can attack the server, a data structure should be implemented, which can count and filter malicious IPs, so that the functions are of little complexity and optimize the process.

Jesus Fong

The BST tree is a type of coding tree that allows the user to perform certain abilities on the information that is put in the tree. In this type of tree there are four basic operations that help us guide ourselves through the tree. These basic operations are: Insertion, Deletion, Searching and Traversals. The insertion operation is in charge of comparing the values inside the tree in order to insert the new piece of data into it. If the right and left root are correct then the process is terminated with the insertion. The searching is in charge of searching the overall tree and is aware of NULLS and values. Deletion, is in charge of deleting certain values depending on the occasions, one example can be if the node deleted has a child. Finally the last basic operation is traversal and this allows the user to revise the tree bit in different and specific orders, like post and pre-order. This tree is useful for cases similar to the evidence because it allows us to store the data in a way that we can traverse through it with the basic operations of a BST. Which gives us an advantage at saving time, and effort in revising the information in another structure. Now with this, how can we identify when a network of ours has been infected? A network can be easily infected, it can have poor protection settings or low cybersecurity. Cyber Attackers can use different hacking techniques from the Trojan method to phishing. Some symptoms that can be noticeable once a network is suffering from a cyberattack can be the following:

- Slow internet
- Slow computer
- Apps Crashing
- Fake Virus Messages