POIS - Evaluation III

V.A. Lalitha Kameswari
2017102S

I have chosen List (linked list) as the data structure

Since python does not have pointers directly, I used a class called Linked List, which consists of several nodes (node is also a class).

I have done similarly for Hash pointers as well as hash and sign pointers.

The main advantages of hash pointer based implementation over pointer based implementation is:

(1) Simple pointer just lets us retrieve information. But, a hash pointer lets us get information and also verify that information hasn't changed.

(2) Hash pointers form the basis of cryptocurrency and blockchains.

My implementation of hash pointers shows how we can detect tampering, i.e hash pointer based implementation of a linked list can serve as TAMPER EVIDENCE LOG.

If adversary changes some value at some block, we can easily detect hash value being different from the "prev hash value" of its next cell.

If he somehow manages to change the whole chain also, the head will be modified, and we can easily detect it by ~~read~~ storing the head hash value, and initialise its prev hash to some known value.

Advantages of Hash and Sign pointer implementation

In this case, this has all the advantages which the hash pointer already has. In addition to it, we can also verify the sender, (or the person who put the value in the list) based on his public key.

This part of verifying the sender using digital signatures has applications in online transactions, digital certificates, and also cryptocurrency.