Week 01 : Read 1-2 Papers

Topic 1 : Blockchain Technology : What is it good for ?

1. What is blockchain technology ?

    - Transaction and Blocks : Transactions between network members are announced to everyone and collected into a “block”

    - Proof-of-Work (PoW) : To add a block to the chain, network members (miners/verifiers) compete to solve a complex mathematical problem. This process is difficult and requires significant computing power

    - Verification and Consensus : The first miner to solve the problem broadcasts their solution and the block. Others can quickly and easily verify its correctness. The block officially add to the chain when a majority (51%) of the network’s computing power agrees on its validity.

    - Incentive and Security : The winner miner is rewarded with a set amount of currency. The high cost of solving the PoW compared to the low cost of the verification makes honestly the most profitable strategy, thus securing the network from fraudulent transaction without a central authority.

2. Potential application of blockchain technology

    a. Digital Payment : Unlike bank which is in the middle, Blockchain transmitted to every other computer which is in the network upon transaction which is why it doesn’t need third party involved although it can be slower than visa transaction which can clear transaction 2000 while blockchain only 7.

b. Contract : Smart contracts are promoted as unbreakable, self-executing code, but the historic DAO hack proved they are flawed. A bug in the code allowed an attacker to steal millions, forcing developers to reverse the supposedly unchangeable blockchain. This showed that smart contracts are not a perfect replacement for law, as they are vulnerable and ultimately arbitrated by developers rather than infallible code.

c. Database And Record Management : It is secured but only for notary for something that will be there permanently but not something that needed to trust third party.

3. The economic drawbacks of blockchain technology

   a. Redundancy : The only reason why it needed to store all the big data and each computer is to provide safety for verification and no need for third party involve. So it makes no sense for bank to do it like that by provide all the info to all its competitor.

   b. Scaling : When ever a user came in and join the network, the scale and ledge will become bigger and bigger which not good in term storing those data. So to answer to this, they have two strategies

      - **Improve the main blockchain itself (Layer 1).** This is like trying to widen a highway, but it's difficult and can make the system less decentralized
      - **Move transactions to a faster, separate layer (Layer 2).** This is like building an express toll road on top of the highway. It handles most of the traffic quickly and cheaply

   c. Regulation and Compliance : Blockchain cannot be interfered by law enforcement nor authority, if the transaction block us valid then it is and nothing can do anything about it. There’s no owner to it exactly.

    d. Blockchains are designed to be irreversible, but this is only truly the case for a massive network like Bitcoin. Other, smaller blockchains *could* theoretically be reversed by developers in an extreme crisis. **Separately**, these other blockchains are also where scams like rug pulls happen, which are devastating precisely because the scammer's final transaction is **irreversible** for the victim.

    e. Security : Blockchain is a decentralized technology whose promises of security and irreversibility are challenged by fundamental limitations in scaling and governance, with many of its core principles only truly applying to a massive network like Bitcoin.

4. Blockchain technology as a mechanism for producing digital cash : The author argues that blockchain's only proven and practical use is for creating **digital cash**, like Bitcoin.

Topic 2 : Preventing Cloud Network From Spamming Attacks Using Cloudflare and KNN

Introduction

- Various of organization use cloud server as data storage and some use it as some models which meet the requirements such as
    - Software as a Service (SaaS)
    - Infrastructure as a Service (IaaS)
    - Platform as a Service (PaaS)
- Approximately about 81% world wide relies on cloud service to defend their data.
- Majority of he attackers are considered to be inside attack which lead to researcher investigate and study about it

- While under attack, blue team uses tools like Snort, Suricata, Open source HIDs Security (OSSEC) and Zeek
- Cloud service can easily clear off attacks from outside but having a hard to time to defend when the attacks are internal. Attack such as Spamming, DDoS and Phishing
- Wherever there is an attack internal in Cloud can lead to 2 scenarios
    - A person gains unauthorized access do malicious things like spamming and misuses cloud data
    - An authorized person attacks inside the cloud server
- When attacked detected
    - Cloudflare will block the attacker’s PC’s static and dynamic IP address
    - KNN will locate attacker location

Literature

▼ Attack Methods :

- Ratio of botnet attacks and slow down the network performance of of the IoT and bypass Intrusion Detection system (IDS) and later on turning every device within the range in to zombie called “baptized BotID” which mostly built from deep learning
- Spams are mostly junks message which sometime include script of viruses
- DDoS were sent and injected on and on internal and external so defensive policy must be implemented

- Finding Solution
    - **Goal:** To build an effective system to detect complex security threats on cloud servers.
    - **Method:** An AdaBoost-based approach was created using features from the UNSW-NB cybersecurity dataset.

  - **Test:** The system was tested on its ability to detect nine different types of cyberattacks (like DoS, Worms, etc.).
  - **Result:** The proposed method successfully detected network intrusions with a high accuracy of 99.3%.

- ▼ Example with Telemedicine
  - ▼ 3D Medical Scans (like MRIs)
    - **Goal:** To prove the 3D scanned hasn’t been tampered with
    - **Method:** They created a system that embeds an invisible watermark directly into the 3D scan data itself.
    - **Result: Watermarks which can change the whole size and hard to fake with.**
  - ▼ Medical Audio Files
    - **Goal**: To protect patient information in audio recordings (like a doctor's notes) when sent online.
    - **Method**: They developed a clever two-part system:
      - **Part 1:** They add a **tough, permanent watermark** to prove who the file belongs to.
      - **Part 2:** They add a second, **removable watermark** that can be erased completely to restore the audio to its original perfect quality.
    - **Result:** The watermarks are hidden (you can't hear them) and the permanent one is strong enough to survive common changes like being turned into an MP3 file or having static added.
- ▼ Problem Formulation
  - In paper, researcher tried to use machine learning to adapt and solve the problem with spamming

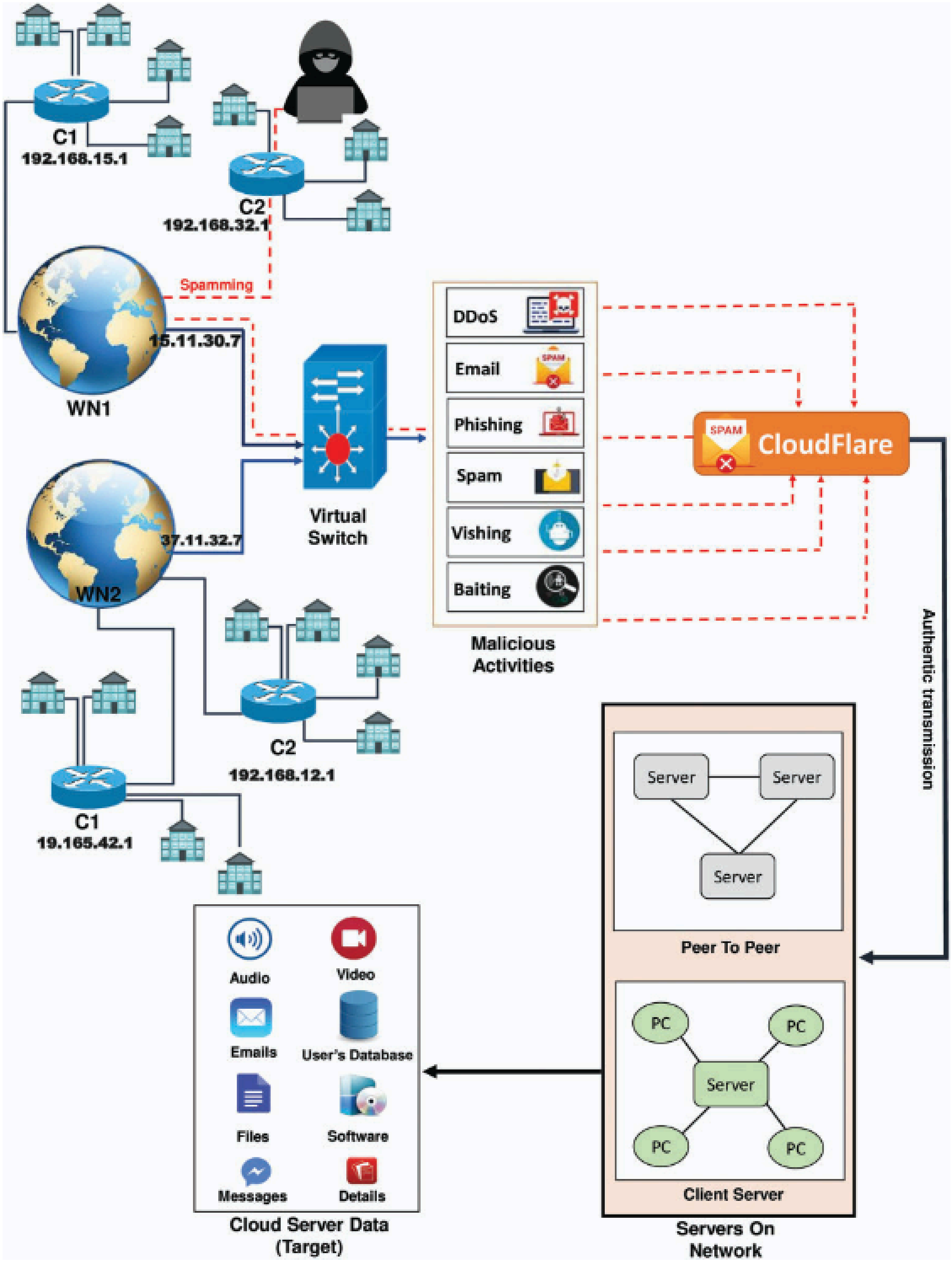
  - Later on, They develop a tool which can block the spamming by their IP address using Cloudflare and then KNN will track down the nearest neighbour’s attacker

Experiments

- ▼ Spamming attacks on cloud server
  - When the spamming enters, it’ll affect the whole network
  - Later on they will send a phishing message which give user offer to defend the system
  - If it is approved, the peer to peer connect will give access to the attacker to the network
  - If it’s not accepted, the attacker will send another boot to the network
  - And there’s more varieties of phishing like you won big money
- ▼ Prevention from spamming attacks through Cloudflare
  - Static IP can be blocked easily
  - Dynamic IP can be challenging to block
  - Even so, user can only use the limited access due to security reason
  - And this argues that Cloudflare done a wonderful job defending internal and external
  - There’s still flaw to it
  - KNN will get the access point and for the K, it will be compared to to a familiar K with almost the same value nearby both strength and timing.
  - This way they can know where the location is coming from but not the exact place or address

Propose Methodology

- ▼ Network Architecture
  - Architecture of internet are designed into WN, CN, W1 and more
  - The main goal spams attack aims to gain full access peer-to-peer network
  - Upon getting the access, they will attack on the client-server to manipulate the server data
- ▼ WN1 and WN2
  - WNx represents countries
- ▼ Virtual Switch
  - Acts as an interface for user both in country or city to connect peer-to-peer with the virtual switch, client-Sever will connect to virtual switch later on
- ▼ Server on Network
  - Data will me transmitted between 2 networks (peer-to-peer network & client-server network) . They will be in the same status no matter the label.
- ▼ Prevention from spamming attack through Cloudflare
  - It is easy to block a few spams but now a when they're repeatedly spamming
  - Cloud flare will treat the first time enter server as dynamic IP, if the actor spam, they will block for 2 hours. Upon cooldown, if they do the same, the block will be permanently.


C1
192.168.15.1
C2
192.168.32.1
Spamming
15.11.30.7
WN1
37.11.32.7
WN2
Virtual
Switch
DDoS
Email
Phishing
Spam
Vishing
Baiting
Malicious
Activities
SPAM
CloudFlare
Authentic transmission
C2
192.168.12.1
C1
19.165.42.1
Server
Server
Server
Peer To Peer
PC
PC
Server
PC
PC
Client Server
Servers On
Network
Audio
Video
Emails
User's Database
Files
Software
Messages
Details
Cloud Server Data
(Target)