NATRAJ - A localized End to End encrypted internal network with Convolution Neural Network based firewall for packet monitoring and filtering to communicate with the Internet

Piyush Mishra

Department of Computer Science and Engineering, Institute of Engineering and Technology, Bundelkhand University, Jhansi

pnoop786@gmail.com

piyushmishra.professional@gmail.com

Abstract- In the modern times where the cyber - attacks are increasing at an alarming rate. The key components of the internet that is the traffic needs to be secured. The internet traffic flows in the form of packets which travel from one destination to the other. The major cyber - attacks target these packets to compromise device and network security. The paper proposes a fortified technique of internet providing to any enterprise or organization by providing a local server NATRAJ to which every device can make requests and the requests are handled by NATRAJ in such a manner that the internal security of the network stays ensured. At last these requests can communicate with the outer network and NATRAJ acts like a firewall. The proposed idea according to the paper points towards assigning a unique hash value to every device, router and their respective send and get request made to the server. This hash table can be put into use to properly deliver the packets inside the internal networks and can be ensured secured against any internal network breaches. The hash provided requests can be processed through our neural network to check for malicious packets as the other neural network can monitor the directed traffic. Both of the neural network systems can act like a two factor authentication system to cross verify the packets and the address to which they will be delivered and the entire system will act like a two factor authentication firewall for the internal network which will in last communicate with the outer network or internet.

Index Terms- End to End encryption, Encrypted traffic classification, end to end, one dimensional convolutional neural networks, IP hashing,

I. INTRODUCTION

The paper introduces a new hybrid approach to set up a local server to which every device inside a network can make request instead of individually making request to the internet which waits for major cyber threats that can be possessed to the devices. The approach is to integrate every old school technique of network security into one and making a firewall that can protect the internal as external intrusion. The approach is a setup to rest ensure the security by integration of various techniques to ensure internet traffic safety delivered to the network. The set up provides us with the use of end to end internal network that can be used to link the devices to each other with the use of the hash tables that can be feeded with unique device id for every device and router connected to the network so. The hash table can be used to deliver packets to the devices associated with their requests made to the server and the traffic can then be transferred to the internet using a convolutional based neural network. The sets of neural network will help to analyze the traffic by identifying the traffic flow and the other neural network will help to analyze the packets. The idea is to build a local server that act as a service request provider and receiver for the internet as well as act as a firewall for the complete network. The hash tables act as an extra layer of safety for the devices as the network cannot be polluted from inside the network for example the cases of unauthenticated use of the Wi-Fi router.
The major components of the NATRAJ can be classified as follows:-

1. Hash table with every device id, router id, send requests and get requests are stored in the form of hashes to provide an end to end internal encryption and distribution using key value pairs.

2. Two sets of Neural Networks one for packet filtering and another for traffic flow analyzation.

DEVICE ID (DID)	ROUTER ID (RID)	REQUEST ID (REID)	SEND ID (SEID)
X	Y	X1	Y1

```
IF(DID == REID)

{

ELSE IF(DID == REID)

{

ELSE IF (REID == SEID)

{

CONNECTION SUCCESSFUL

{

BREAK
```

So this is an overview for the hash table that can be used to generate hashed IP addresses and packets to move in the traffic inside the network. The hashes stored inside the server can then be verified at the gateway that communicate with the external network where the traffic can be decrypted. So entire set up suggests an encryption and decryption of the traffic entering and leaving the traffic which can be verified by our neural networks set up. In this manner the paper suggest a protocol for the flowing of the traffic that is entering and leaving the server maintaining the integrity of each and every device using the NATRAJ server for external communication. The storing of hash values locally at the entering point with the help of locally stored hashes of the devices inside the network will help to locate and direct the traffic in a specific direction and check the validity of the requests made and information received inside the network.

The protocol suggested according to the paper prevents the network and the devices connected inside the network from some common but major attacks attacks:-

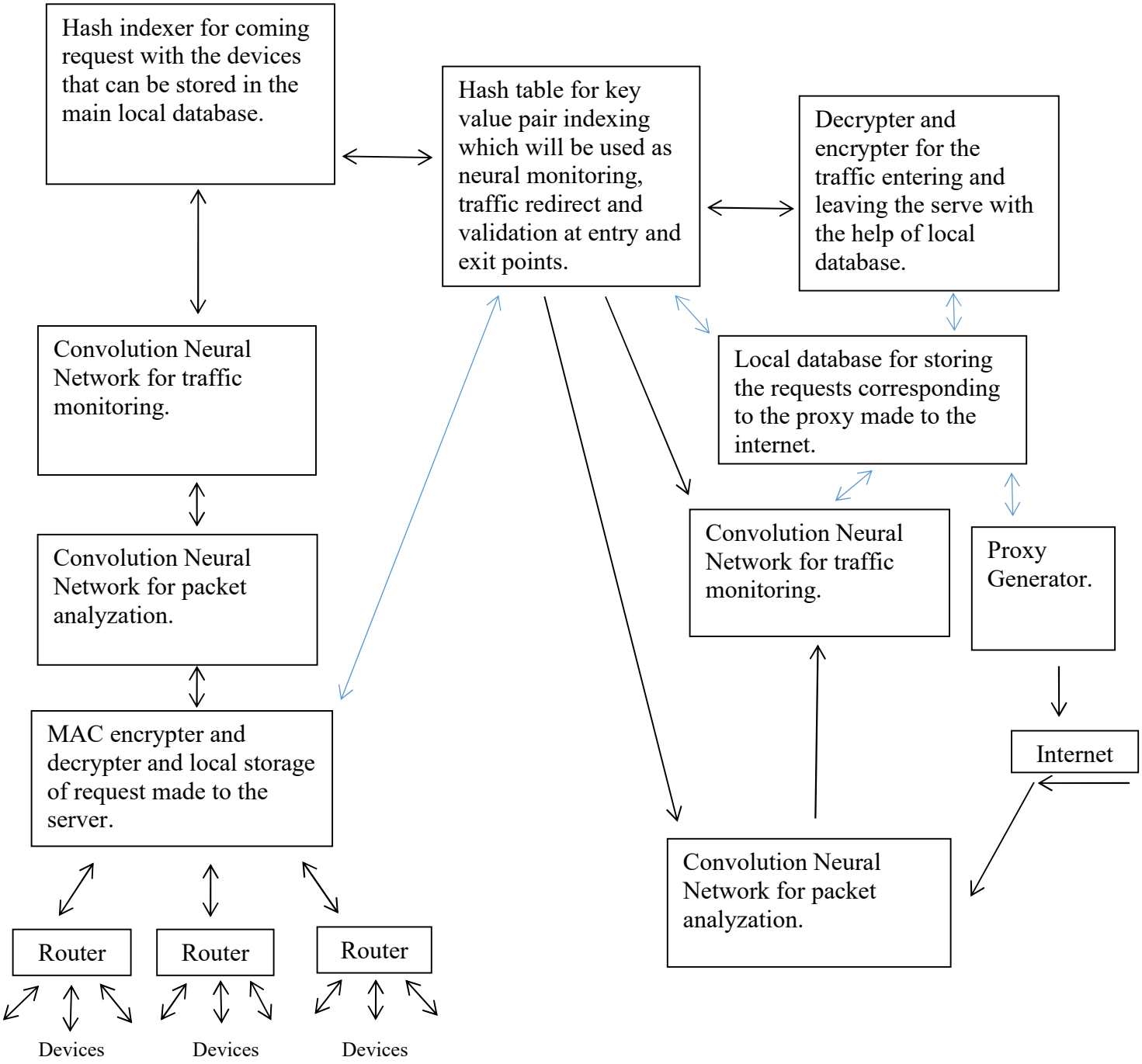
1. **Man in the middle attacks** :- The masquerading of the IP to look like the receiver of the packet, attackers use man in the middle attack. The following protocol which suggest a barricading local server like NATARAJ will prevent such attacks as the traffic entering the network and leaving the devices are encrypted and decrypted at every router and NATARAJ gateway using an asymmetric encryption technique by the hash values of the router's address and the hash values at the gateway.

2. **Phishing attacks** : - The web consists of attackers that lead or direct the traffic to false destinations in order to actively listen to the outflow or inflow of the traffic to the networks and gain sensitive information from the networks. The pair of neural networks will provide an active sight to monitor these activities and to look over to the packets delivered to the networks.

3. **DDOS attacks** : -

4. **Active listening attacks** : -

5.


Hash indexer for coming request with the devices that can be stored in the main local database.
Hash table for key value pair indexing which will be used as neural monitoring, traffic redirect and validation at entry and exit points.
Decrypter and encrypter for the traffic entering and leaving the serve with the help of local database.
Convolution Neural Network for traffic monitoring.
Local database for storing the requests corresponding to the proxy made to the internet.
Convolution Neural Network for packet analyzation.
Convolution Neural Network for traffic monitoring.
Proxy Generator.
MAC encrypter and decrypter and local storage of request made to the server.
Internet
Convolution Neural Network for packet analyzation.
Router
Router
Router
Devices
Devices
Devices

Identify the constructs of a Journal – Essentially a journal consists of five major sections. The number of pages may vary depending upon the topic of research work but generally comprises up to 5 to 7 pages. These are:

1) Abstract
2) Introduction
3) Research Elaborations
4) Results or Finding
5) Conclusions

In Introduction you can mention the introduction about your research.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

It's the foremost preliminary step for proceeding with any research work writing. While doing this go through a complete thought process of your Journal subject and research for it's viability by following means:

1) Read already published work in the same field.
2) Goggling on the topic of your research work.
3) Attend conferences, workshops and symposiums on the same fields or on related counterparts.
4) Understand the scientific terms and jargon related to your research work.

III. WRITE DOWN YOUR STUDIES AND FINDINGS

The protocol presented in the paper targets the flow of the traffic through a constraint route that is our NATRAJ server and every device connected to a network make requests to the NATRAJ server and our server will make requests to the Internet. In a way the protocol prevents the devices from directly accessing the Internet where it is wide open to several kinds of attacks. The server acts like a firewall and a proxy address for each and every device connected to the network. The storing of device's MAC address locally in our databases and encrypting and then checking the locally stored values acts like the first line of defense as it removes any unauthorized access from making requests and devices connected to the same network cannot reveal which devices are connected to the network in order to prevent any attacker from internally infecting the network using masked device address.

The pair of Neural Networks checks for the traffic and packets in parallel on the both entry and exit points of the server to cross check if the traffic and packets are redirected to meant destinations and not eavesdropped by any sort of Man-In-The-Middle-Attack.

The exit points must be ensured with proxy generator to mask the IP address by which the request is leaving the server and every IP and request must be stored in local database in the form of cache which gets replaced when the server gets a response from the internet. In this manner every request that leaves the server and every traffic received by the server can be encrypted and decrypted following the internal end to end communication protocols leaving the attackers helpless and clueless about the actual address or requests made by the devices to the internet.

The NATRAJ server basically works on the principle of packet filtering firewall with convolution neural networks to actively monitor our traffic and information send and received by our devices to the Internet to cut short malicious activities.

IV. GET PEER REVIEWED

Here comes the most crucial step for your research publication. Ensure the drafted journal is critically reviewed by your peers or any subject matter experts. Always try to get maximum review comments even if you are well confident about your paper.

For peer review send you research paper in IJSRP format to editor@ijsrp.org.

V. IMPROVEMENT AS PER REVIEWER COMMENTS

Analyze and understand all the provided review comments thoroughly. Now make the required amendments in your paper. If you are not confident about any review comment, then don't forget to get clarity about that comment. And in some cases there could be chances where your paper receives number of critical remarks. In that cases don't get disheartened and try to improvise the maximum.

After submission IJSRP will send you reviewer comment within 10-15 days of submission and you can send us the updated paper within a week for publishing.

This completes the entire process required for widespread of research work on open front. Generally all International Journals are governed by an Intellectual body and they select the most suitable paper for publishing after a thorough analysis of submitted paper. Selected paper get published (online and printed) in their periodicals and get indexed by number of sources.

After the successful review and payment, IJSRP will publish your paper for the current edition. You can find the payment details at: http://ijsrp.org/online-publication-charge.html.

VI. CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

APPENDIX

Appendixes, if needed, appear before the acknowledgment.

ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in American English is without an "e" after the "g." Use the singular heading even if you have many acknowledgments.

REFERENCES

[1] G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

[2] W.-K. Chen, *Linear Networks and Systems* (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.

[3] H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.

[4] B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.

[5] E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," *IEEE Trans. Antennas Propagat.*, to be published.

[6] J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.

AUTHORS

First Author – Author name, qualifications, associated institute (if any) and email address.
Second Author – Author name, qualifications, associated institute (if any) and email address.
Third Author – Author name, qualifications, associated institute (if any) and email address.

Correspondence Author – Author name, email address, alternate email address (if any), contact number.