

## Financial Crime: A Conceptual Framework Implementation for Prevention of Malicious Request from a VPN or Proxy Server

Grace Odette Boussi<sup>a</sup>, Himanshu Gupta<sup>b</sup>, Syed Akhter Hossain<sup>c</sup>

<sup>a</sup> Ph.D. Scholar at Amity Institute of Information Technology, Amity University Noida (India)

<sup>b</sup> Associate Professor at Amity Institute of Information Technology, Amity University Noida (India)

<sup>c</sup> Professor and head of Computer Science and Engineering department, University of Liberal Arts (Bangladesh)

### Abstract:

Cybercrime is no longer a crime that needs to be introduced as it has an impact all over the world in many aspects. It is a daily fight and new ideas, proposals, and suggestions are welcomed to overcome that issue. Every day, people, and organizations are a victim of cyber-attack despite the efforts that have been done. During a cyber-attack, most of the time, the hacker utilizes a VPN to hide their identities such as IP address and location details and this makes tracking difficult. Having a method for having their details will help us to track them and this will lead the concerned organization to catch them, make legitimate moves against them, and will stop their fraudulent activities. One of the main reasons behind a cyberattack is money, therefore, financial organizations are mostly targeted and are likewise confronting an immense impact. In this paper, we propose a framework that is going to prevent a request that comes from a VPN or proxy server. Our work can be implemented in many areas like banking, social media, organization, and so forth.

**Keywords:** 1.VPN, 2.Cyberattack, 3.Cybercrime, 4.Impact, 5.Complaints, 6.losses.

### Introduction:

Cybercrime is presently not a wrongdoing that should be presented as it has influenced all around the world from numerous perspectives. It is a day-to-day battle where groundbreaking thoughts, recommendations, and the facilities of computer technology usage did not come without inconvenience; it has made life so quick and fast but thrown under the eclipse of the threat of the deadliest type of crime called "cybercrime" (Das, S., & Nayak, T. 2013). Without a computer, many businesses and work would have not functioned, and some would have not been possible. There are a huge number of attacks that are happening, and the number of victims is still increasing as there is a facility of having good tools online to purchase an attack. We should not forget that attackers are people with knowledge who are often called a black hacker. The difference between black and white hackers is the purpose of their work else both have the same knowledge and the same capacity of level. This makes the task of a white hacker difficult because when they implement some security layers, black hackers are also working harder to bypass them, therefore a white hacker should always be one step ahead when it comes to security. Hackers most of the time follow a dynamic process that has four levels: Gathering Information, Identifying the targets, Selecting the attack Method, and lastly employing social engineering techniques (Naidoo, R.2020). Cyberattacks can be classified by categories and one of the best ways to handle them is to first start by proposing a solution or protection category wise then the situation will be under control; we can find a global solution. Most of the time, unawareness and carelessness can also be considered as a gateway for opening cybercrime in the organization. (Amarullah, A. H., Runturambi, A. J. S., & Widiawan, B. 2021, June) said that phishing is the hardest one to detect because it takes advantage of people's unawareness. As

cybercrime is touching everyone without any expectation, in some parts of the world, the lack of advanced technologies to prevent organizations against cybercrime and protect their data seems to be the cause of the increase in cybercrime.

Cybercrime is any fraudulent activity that happens over the internet. The growth of internet facilities and familiarity has also facilitated the expansion of cybercrimes. Nowadays, many activities are done online, we are so dependent on online services that using any offline activity will make old fashion. (Nicholls, J., Kuppa, A., & Le-Khac, N. A. 2021) said that machine learning and deep learning methods are widely used in the financial sector to support diverse activities, but we can also say that they are a great approach to fight against cyber-crimes.

They are different types of crimes that are included in cybercrimes, but in our work, we will only focus on common ones.

- Identity theft
- Personal data breach
- Phishing / Vishing / smishing / Pharming
- Confidence fraud (Romance scams)
- Ransomware
- Tech support fraud

#### ***Identity theft***

It is when a stolen identity is used to commit fraud, of course the victim does not know that their ID has been used for a fraudulent activity.

#### ***Personal data breach***

It is when confidential data are with an unauthorized person. When the unauthorized person has that information that can sell or use them against the will of the genuine user

#### ***Phishing / Vishing / smishing / Pharming***

They are the type of crimes that intend to trick victim either by clicking a link sent by mail or message or by calling them and pretend to be someone else.

#### ***Confidence fraud (Romance scams)***

This is a trending type of cyber-attacks that does not require developed technologies. This attack targets old and lonely people, here the criminal persuades the victim that they are in a relationship and once the victim convinced and falls in love, the criminal will take money from them and even steal their personal details with the aim to steal.

#### ***Ransomware***

It is a type of malware that prevents user to access their data until a ransom is paid.

#### ***Tech support fraud***

It is also one of the common type of crimes that we are facing, it does not require a lot of equipment or a skill in computer and cyber activities. In this attack you will receive a call, a message or a pop up saying that there is a problem with your computer.

Yearly the Federal Bureau of Investigation publishes reports of internet activities, the number of complaints made, the type of the attack, and the damage caused by the attackers. For our work, we have only taken the above-mentioned crime and we have taken the data given by the FBI between 2017 to 2021.

Our work is developed on MacBook Air 2019, processor intel core i5 using JavaScript and the server of (Tellus, 2020).

The first part of our paper is about the introduction, the second will talk about the literature review, the third part will be our proposal and the last part is all about our conclusion and future work.

### Complaints and losses of cybercrime from 2017-2018

We have taken the complaints and losses published by FBI reports from 2017 to 2021 and we can see the number of crimes in 5 years is considerably increasing. In 2017 we had 1.4 billion in losses caused by cybercrime and over 6.9 billion in 2021 (Internet Crime Report, 2021).

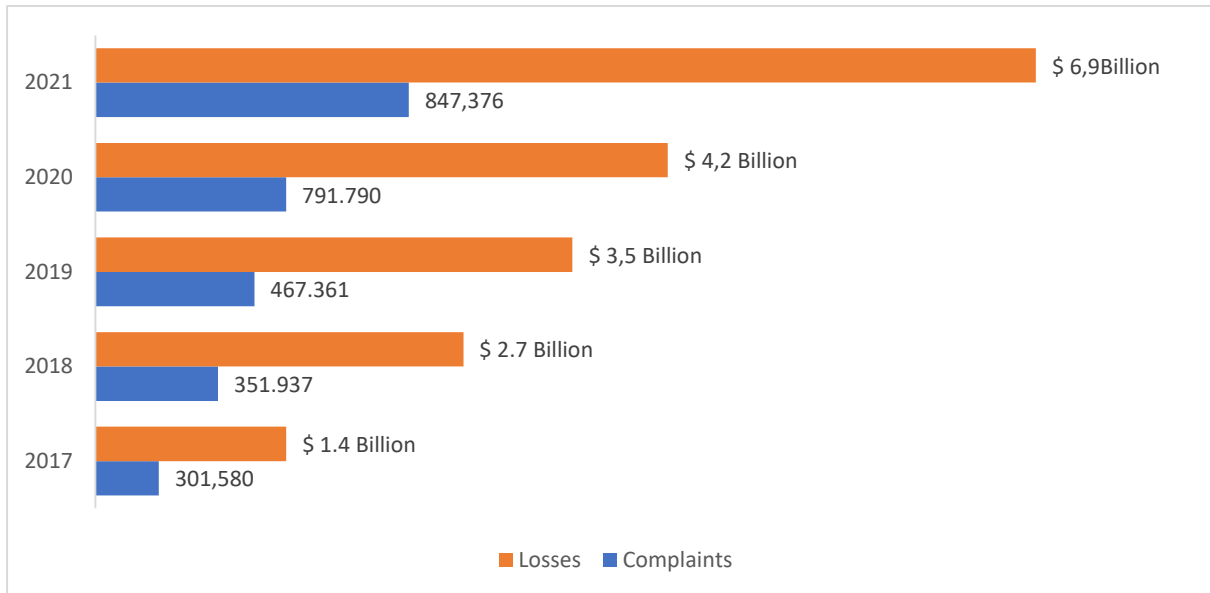


Fig.1 Complaints and losses over five years

By observing the above chart, we can see that in 2021 only a romance scam has caused a huge loss, over \$956 million was lost, 24299 complaints were registered by the FBI and those complaints came from different countries (Internet Crime Report, 2021 'a'). Phishing on the other hand has caused less loss as compared to other crimes on our list.

### Losses caused by cyber-crime from 2017 – 2021

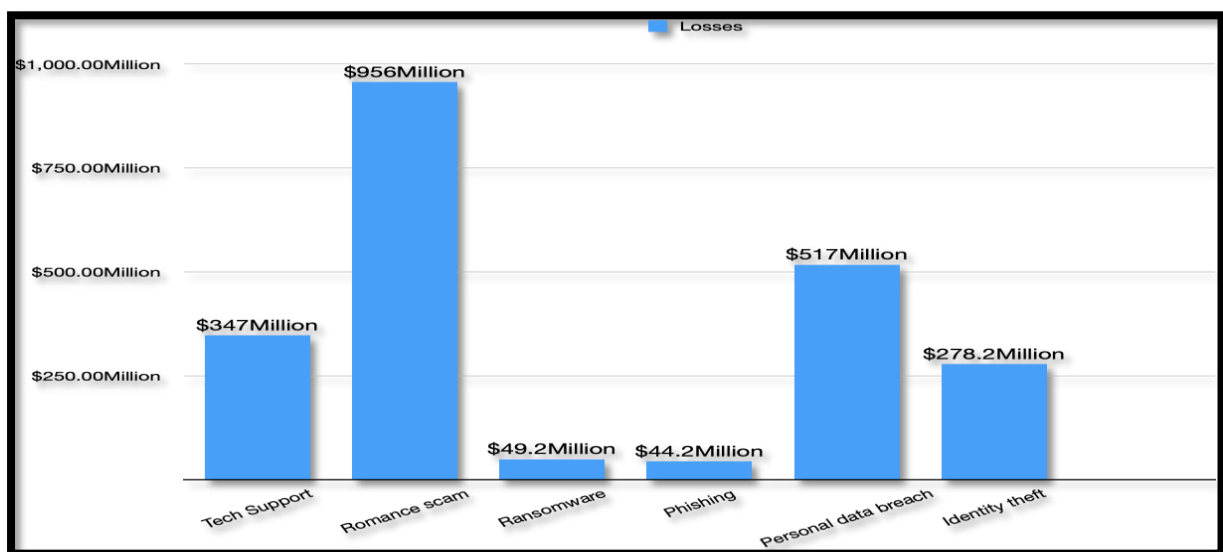


Fig.2 Losses caused by cyber-crime from 2017-2021

The above chart illustrates the loss caused by the five (5) crimes that we have selected for our work in 5 years. Please note that in phishing impact we have vishing and smishing. The data were collected from victims around the world, and we can see that romance scam has caused a huge lost as compared to others.

### Top 20 victims' countries

Attackers target certain countries to perform their activities. Most of the time developed countries are targeted, here is the list of 20 countries' victims of cyber-attack in 2021, the report was given by the FBI and the attacks came from different branches of cybercrimes. Turkey has a smaller number of attacks reported while the United States has a high number of attacks. The difference between these two countries is so high and many factors can be the reason. We can also note that not all people especially organization reports their fraud, some prefer to not report because of their reputation, therefore we believe that the number of victims is higher than the report given.

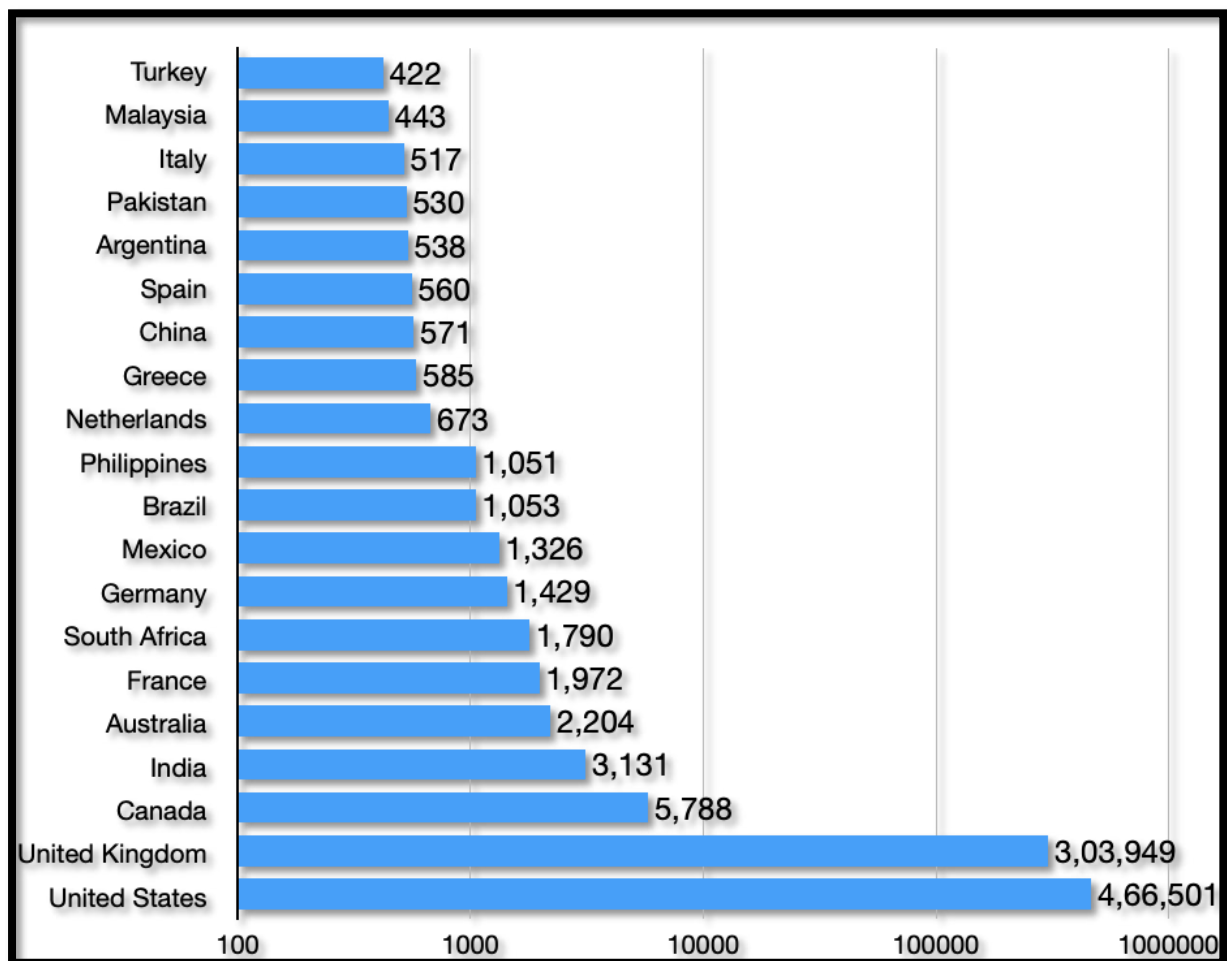


Fig.3 Record of victim's countries in 2021

Here is the list of the number of victims who reported a cybercrime in 2021, we have selected 6 crimes out of many (Internet Crime Report, 2021 'b').

Crime Type	Number of Victims
Tech Support	23903
Romance Fraud	24,299
Ransomware	3,729
Phishing and variants	323,972
Personal Data Breach	51,829
Identity Theft	51,629

**Table 1 Number of victims in 2021**

**I- Literature review:**

cybercrime is causing a lot of damage and because of the financial lost that the word is facing, many authors proposed different methods to solve that issue. We have referred to few authors in order to do our work.

Axis	Paper reference	Description	Financial Cybercrime Category or Associated Topic
1) Different fraud methods adopted by criminals	(Zakaria,2017,). (Carter,2021). (Alabdan, 2020). (Tomić, 2016). (Tamersoy, 2014).	Malware categorization and discussion. Romance fraud analysis Analysis of phishing techniques. Romance fraud analysis. Romance fraud analysis.	Ransomware Romance Fraud Phishing Attacks Money Laundering Insider Trading
2) Relevant systems, algorithms, drawbacks, constraints, and metrics used to combat each fraud type	(Al-Hashedi, 2021). (Sharma, 2013). (Ma, 2021). (Ozbayoglu, 2020). Wu, 2021). (Wu,2020). (Toth, 2018). (Saia, 2019). (Alhazmi, 2020). (Shirodkar, 2020).  (Aggarwal, 2017). (Aggarwal, 2001). (Zimek, 2012). (Chalapathy,2019). (Ahmed, 2016).  (Chandola, 2009).	Financial fraud detection survey and associated models. Analysis of detecting accounting fraud. Review of GAD and DL techniques. ML techniques to identify Windows malware. Analysis of DL applications in finance Analysis of popular cryptocurrencies. Survey on GAD Proactive Fraud Strategies. Survey on ML in credit card fraud. Survey on ML in credit card fraud including genetic algorithm. Book on AD techniques. AD techniques in high dimensional data. Survey on unsupervised AD techniques Survey on DL techniques in AD. Network AD analysis for malicious	Fraud  Fraud Applicable Algorithms Applicable Algorithms Applicable Algorithms Cryptocurrency graph pre-processing Applicable Algorithms Fraud Fraud Fraud  Applicable Algorithms Applicable Algorithms Applicable Algorithms Applicable Algorithms Applicable Algorithm Applicable Algorithms

		cyber activity. Survey on AD.	
3) Relevant personas and stakeholders involved	(Reep-van den Bergh, 2018). (Patterson, 2013).  (Sabillon, 2016).  (Hasham, 2019).	Behavioural analysis of cybercrime victims. Behavioural analysis of cybercrime victims. Behavioural analysis of cybercriminals.  McKinsey: cybersecurity analysis for financial fraud prevention	Fraud, social engineering, hacking  Fraud  Hacking, social engineering, fraud, extortion Fraud

**Table 2 Analysis table of the existing models**

The work proposed by these authors helped us to identify the similarities between them and also the gap, they all proposed nice techniques and uses good approaches and the lack of classification between good and bad requests helped us propose our reflection. Not all requests need to go through since they are all not genius. Being able to distinguish between a good and bad request is important and will help us later to focus on malicious ones and take action against them, hence our work. We believe that our work is better than the existing ones since we not only reduce the length and complexity of the task but we also show where to focus so that we can reach the real request and stop them from causing further impact.

#### **Propose work:**

Our work is done in two main parts which are:

- Front service [Service 1]
- Pipe service [Service 2]

The backend API of the application is implemented using express powered by Node.js. The entire server runs on a microservice architecture where multiple service communicates to create (simulate) a pipeline to allow secure communication (send messages) between clients. The current technology stack is composed by:

- a. Firebase Firestore database: used because it provides the real-time capability
- b. Express.js: allowing to build Rest API fast with Node.js
- c. MySQL: in this scenario used to store user information and relationship between user (will be discussed further in the section below)
- d. Google AppEngine: Google's AAS used to deploy our server app on the cloud

All the above stated feature, framework and services are used by mainly two micro-services in synergy to ensure secure and fast delivery of each message

#### **1. Front service [Service 1]**

This service is the one that receives the request from the client and starts processing the message. Once the client makes a request, "Service 1" creates a temporary message in Firestore database then returns a 201 [created] to the client and parallelly triggers a new internal request to "service 2". Doing so has the benefit of unloading the server when multiple requests are done simultaneously as well as providing seamless and fast user experience since storing messages on Firestore takes less than **200 ms**.

## 2. Pipe service [Service 2]

“Service 2” is where the main processing happens, for instance, this service will check whether the sender and the receiver have good relationship i.e., if the sender has blocked the receiver or vice-versa; most importantly this service checks whether the origin of the message is safe for the receiver, if not the service ensures its safety. In this paper, only the VPN safety assertion’s aspect of “service 2” shall be discussed. Whenever a request is received on the server (“Service 1”), the remote address value combined with the request header i.e., “X-Forwarded-For” is used to identify the address of the original requestor (client) or the last proxy. The IP address will then be used internally to check whether the client is using a VPN, in case the client uses a VPN, the message will simply no be sent otherwise further processing shall be done eventually leading to the message delivery. The goal of this work is to deny any request coming from a VPN, since we do not have access to a bank data or a server, we use Tellus us server to implement our work and show it working procedure, the same algorithm can be implemented on the bank and will produce the same result. Let's take a scenario of a bank where our algorithm will is implemented. Suppose the user wants to access their net banking for the transaction After entering their credential, they now want to send money to another account and if our algorithm is implemented on their side, it will check whether the request comes from a VPN/ proxy or not, if the request comes from the VNP or Proxy therefore the request will be interrupted, else the request will be successfully done. This work aims to stop any request coming from a VPN since most of the time when malicious activity is done, the attacker uses VPN.

The overall flowchart of the process can be visualized as follow.

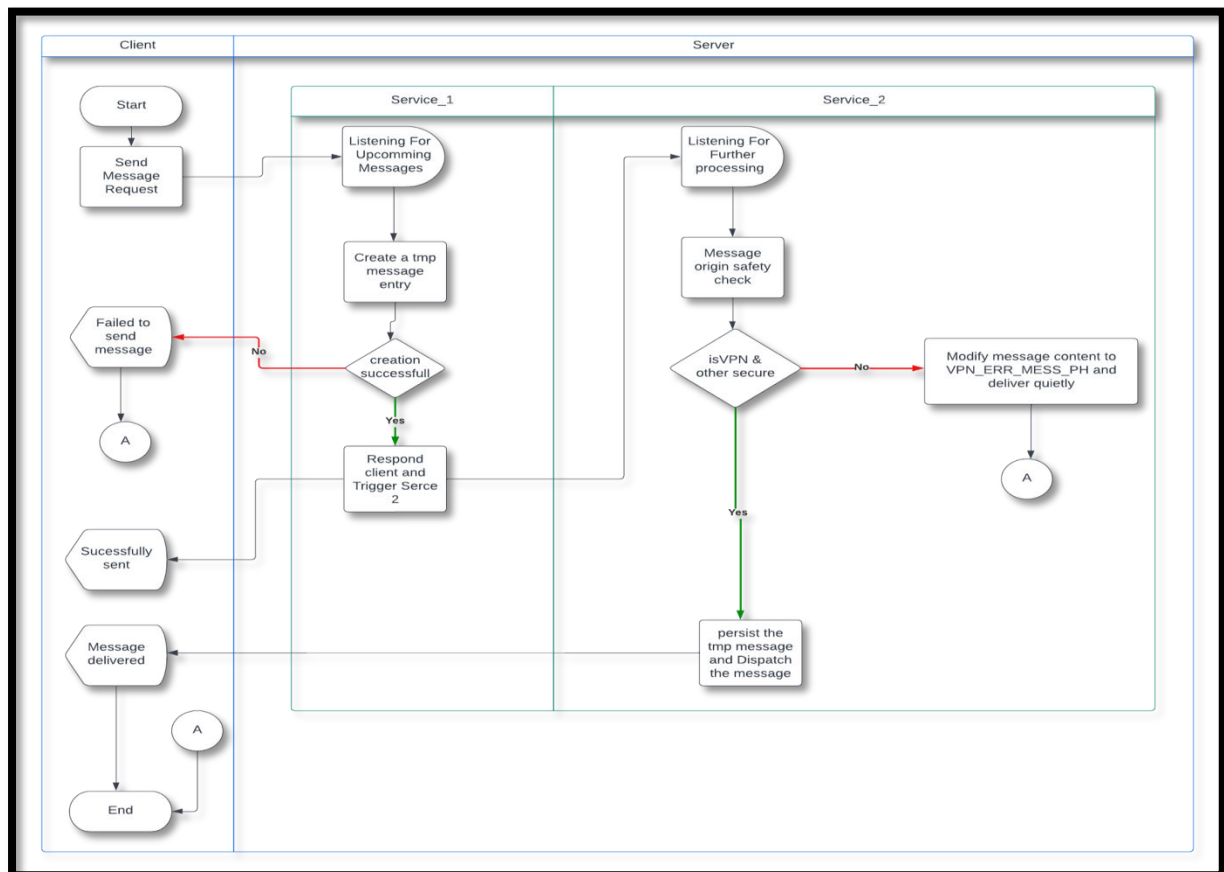
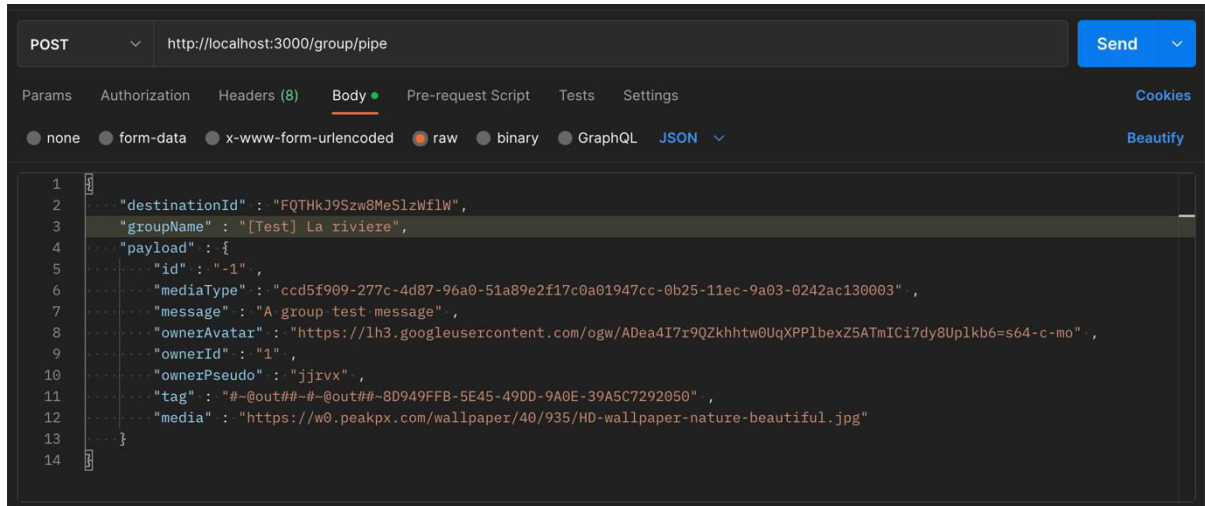


Fig.4 Flowchart of the proposed model



**Phase 1: In the use case where the client uses a VPN:**

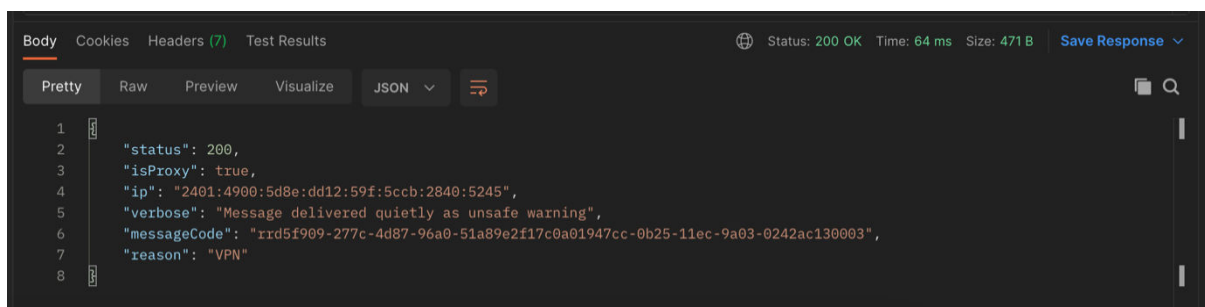
When there is an incoming request, our algorithm will examine whether it comes from a VPN or no. This is an example of how it looks like when a request come from a VPN.



**Fig.5: Case when the user uses VPN**

**Phase 2: Response on the server (“service 2”) when the request is made via a VPN**

If the request is made from a VPN, then the server will give us the details as displayed in the screenshot below so that the service 2 can be able to display the error message to the end user.



**Fig.6: Server response when the client uses VPN**

**Phase 3: The error message will be delivered to the receiver**

Indicating that the message was quietly delivered i.e. no notification and long term persistence to the DB was done, actually downgraded to a warning message (represented by “messageCode” ) that, on client device would look like the following screenshot.



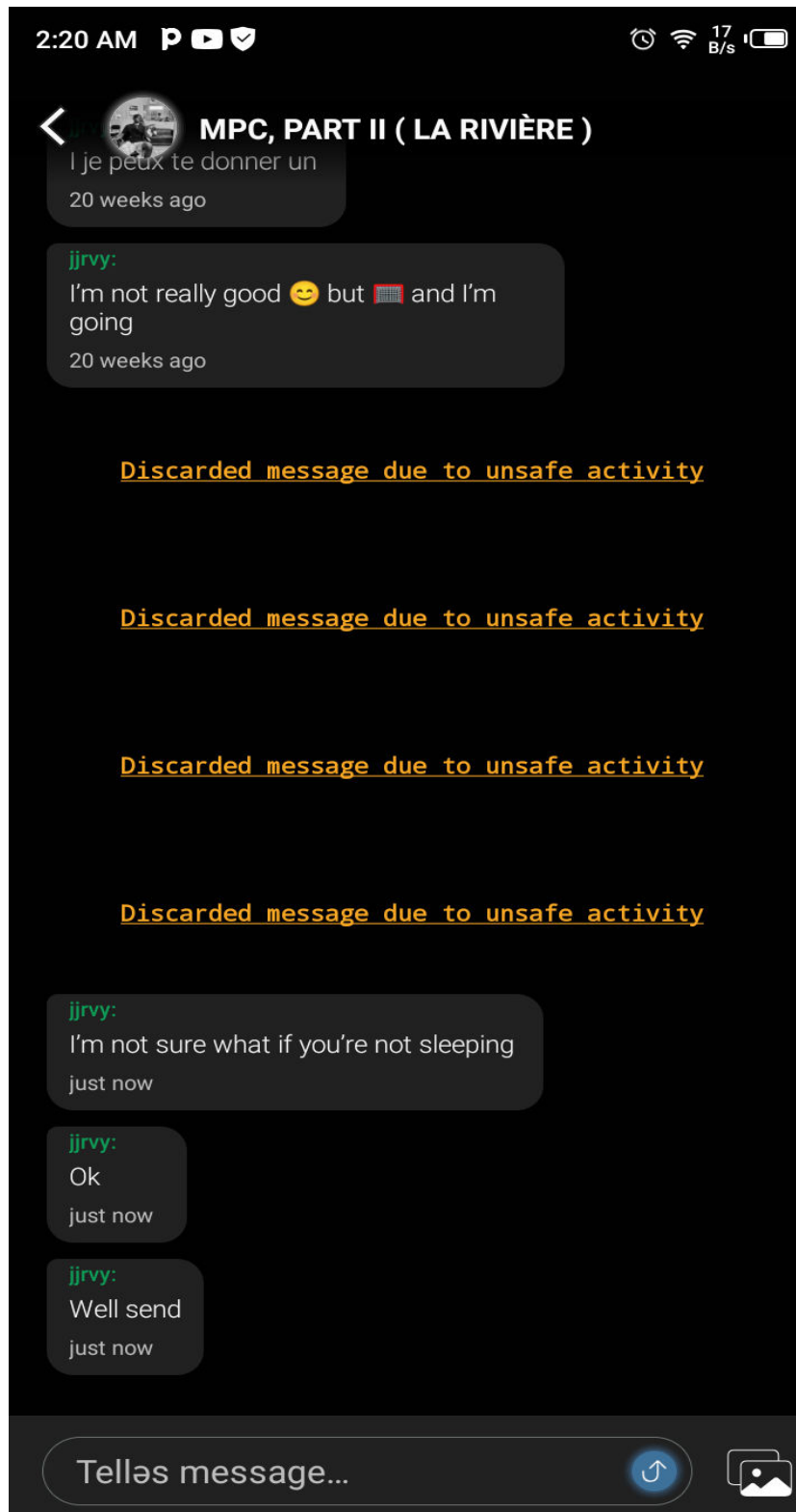


Fig.7: How the message appears on the application when the VPN is used and when it is not. In the above picture we can see if the request comes from a VPN, the error message is displayed and the message is not transferred to the reception. Once the VNP or proxy is disable, the message can now reach the receiver.

## Conclusion and Future work.

There are different types of cybercrime and the damage caused is not limited to any area. Our algorithm has been implemented on a social network which is Tellus (calendar 2.0) and shows how to detect a malicious request and stop its implementation. By doing so, it can reduce cybercrimes such as cyberbullying, debit/credit card fraud, and why not phishing, and ransomware. We have seen that if the request comes from an unidentified user, the request will be blocked, this allowed us to have the exact identification of the user such as the IP address, the city, and any other element that the application developer will deem important. Please note that these features may vary from application to application, In Tellus the important features are location and IP address, so if this algorithm is implemented in a different application where features like name, time city, and mobile device version are mandatory, so the algorithm will help in their visibility. Future work of this algorithm will be the creation of an additional algorithm that will help us to detect the hacker's IP address, it will help us not only to stop the request but also to take legal action against the perpetrator of such crimes because from the IP address we can get many details about the user.

## Reference:.

1. Aggarwal, C. C., & Yu, P. S. (2001, May). *Outlier detection for high dimensional data*. In *Proceedings of the 2001 ACM SIGMOD international conference on Management of data* (pp. 37-46).
2. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). *A survey of network anomaly detection techniques*. *Journal of Network and Computer Applications*, 60, 19-31.
3. Al-Hashedi, K. G., & Magalingam, P. (2021). *Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019*. *Computer Science Review*, 40, 100402.
4. Alabdan, R. (2020). *Phishing attacks survey: types, vectors, and technical approaches*. *Future Internet*, 12(10), 168.
5. Alhazmi, A. H., & Aljehane, N. (2020, September). *A Survey Of Credit Card Fraud Detection Use Machine Learning*. In *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1-6). IEEE.
6. Amarullah, A. H., Runturambi, A. J. S., & Widiawan, B. (2021, June). *Analyzing cyber crimes during Covid-19 time in Indonesia*. In *2021 3rd International Conference on Computer Communication and the Internet (ICCCI)* (pp. 78-83). IEEE.
7. Carter, E. (2021). *Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud*. *The British Journal of Criminology*, 61(2), 283-302.
8. Chalapathy, R., & Chawla, S. (2019). *Deep learning for anomaly detection: A survey*. *arXiv preprint arXiv:1901.03407*.
9. Chandola, V., Banerjee, A., & Kumar, V. (2009). *Anomaly detection: A survey*. *ACM computing surveys (CSUR)*, 41(3), 1-58.
10. Das, S., & Nayak, T. (2013). *Impact of cybercrime: Issues and challenges*. *International journal of engineering sciences & Emerging technologies*, 6(2), 142-153.
11. Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial crime and fraud in the age of cybersecurity*. McKinsey & Company, (October), 1-11.
12. Ma, X., Wu, J., Xue, S., Yang, J., Zhou, C., Sheng, Q. Z., ... & Akoglu, L. (2021). *A comprehensive survey on graph anomaly detection with deep learning*. *IEEE Transactions on Knowledge and Data Engineering*.
13. Naidoo, R. (2020). *A multi-level influence model of COVID-19 themed cybercrime*. *European Journal of Information Systems*, 29(3), 306-321.
14. Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). *Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape*. *IEEE Access*.

15. Ozbayoglu, A. M., Gudelek, M. U., & Sezer, O. B. (2020). Deep learning for financial applications: A survey. *Applied Soft Computing*, 93, 106384.
16. Patterson, N., Hobbs, M., & Palmer, D. (2013, July). A direct insight into victims of cybercrime. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 603-610). IEEE.
17. Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime science*, 7(1), 1-15.
18. Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, 2016, 4 (6).
19. Saia, R., & Carta, S. (2019). Evaluating the benefits of using proactive transformed-domain-based techniques in fraud detection tasks. *Future Generation Computer Systems*, 93, 18-32.
20. Sharma, A., & Panigrahi, P. K. (2013). A review of financial accounting fraud detection based on data mining techniques. *arXiv preprint arXiv:1309.3944*.
21. Shirodkar, N., Mandrekar, P., Mandrekar, R. S., Sakhalkar, R., Kumar, K. C., & Aswale, S. (2020, February). Credit card fraud detection techniques—A survey. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)* (pp. 1-7). IEEE.
22. Tamersoy, A., Khalil, E., Xie, B., Lenkey, S. L., Routledge, B. R., Chau, D. H., & Navathe, S. B. (2014). Large-scale insider trading analysis: patterns and discoveries. *Social Network Analysis and Mining*, 4(1), 1-17.
23. Tomić, N., Todorović, V., & Jakšić, M. (2016). Misuses of electronic payment systems. U: Stojanović-Aleksić, V. (ur.). In *Conference proceedings* (pp. 245-253).
24. Toth, E., & Chawla, S. (2018). Group deviation detection methods: a survey. *ACM Computing Surveys (CSUR)*, 51(4), 1-38.
25. Wu, J., Liu, J., Zhao, Y., & Zheng, Z. (2021). Analysis of cryptocurrency transactions from a network perspective: An overview. *Journal of Network and Computer Applications*, 190, 103139.
26. Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Philip, S. Y. (2020). A comprehensive survey on graph neural networks. *IEEE transactions on neural networks and learning systems*, 32(1), 4-24.
27. Zakaria, W. Z. A., Abdollah, M. F., Mohd, O., & Ariffin, A. F. M. (2017, December). The rise of ransomware. In *Proceedings of the 2017 International Conference on Software and e-Business* (pp. 66-70).
28. Zimek, A., Schubert, E., & Kriegel, H. P. (2012). A survey on unsupervised outlier detection in high-dimensional numerical data. *Statistical Analysis and Data Mining: The ASA Data Science Journal*, 5(5), 363-387.