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

Grace Odette Boussi[1], Himanshu Gupta [2], Syed Akhter Hossain [3]

Scholar at Amity Institute of Information Technology, Amity University, India[1]
Associate professor at Amity Institute of Information Technology, Amity, India [2]
Professor and head of Computer Science and Engineering department, University of Liberal Arts, Bangladesh [3]

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 de efforts that have 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 thismakes tracking difficult. Having a method for having their details will help us to track them and this will lead theconcerned 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 toprevent 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: VPN, Cyberattack, Cybercrime, Impact, Complaints, losses.

I- 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 inconvenient; it has made life so quick and fast but thrown under the eclipse of the threat of the deadliest type of crime called "cybercrime"[1]. Without a computer, many businesses and work would have not functioned, and some would have not been possible. Thereare 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 [2]. 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. [3] 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 [4].

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 activitywill make old fashion. [38] said that machine learning and deep learning methods are widely used in the financial sector so 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 identify is used to commit fraud [5], of course the victim does not know thattheir ID has been used for a fraudulent activity.

Personal data breach
It is when confidential data are with an unauthorized person [6]. When the unauthorized personhas that information that can sell or use them against the will of the genius user.

Phishing / Vishing / smishing / Pharming
They are the type of crimes that intents to trick victim either by clicking a link sent by mail or message or by calling them and pretend to be someone else [7].

Confidence fraud (Romance scams)
This is a treading type of cyber-attacks that does not require develop technologies. This attack targets old and lonely people, here the criminal persuades the victim that they are in a relationship and once the victim convicted and falls in love, the criminal will take money fromthem and even steal their personal details with the aim to steal [8].

Ransomware
It is a type of malware that prevents user to access their data until a ransom is paid [9].

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 [10].

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 theserver of Tellus.
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 futurework.

Complaints and losses of cybercrime from 2017-2018

We have taken the complaints and losses published by FBI reports from 2017 to 2021 and wecan see the number of crimes in 5 years is considerably increasing. In 2017 we had 1.4 billionin losses caused by cybercrime and over 6.9 billion in 2021 [11].

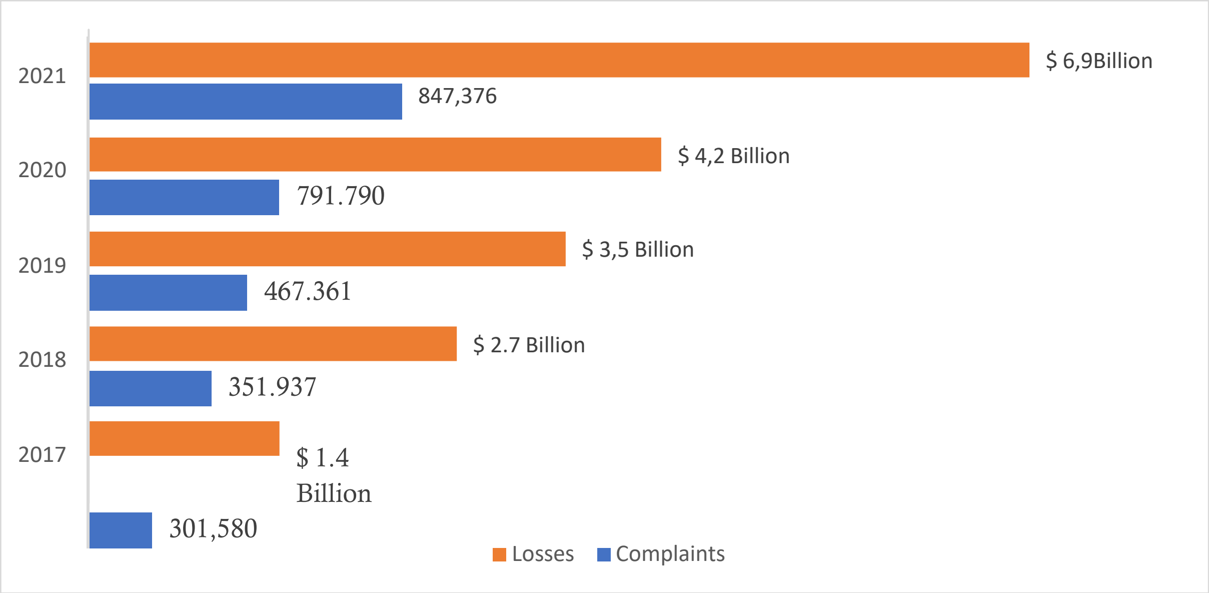


Fig.1 Complaints and losses over five years

By observing the above chart, we can see that in 2021 only a romance scam has caused a hugeloss, over $956 million was lost, 24299 complaints were registered by the FBI and those complaints came from different countries [11]. Phishing on the other hand has caused less lossas compared to other crimes on our list.

Losses caused by cyber-crime from 2017 – 2021

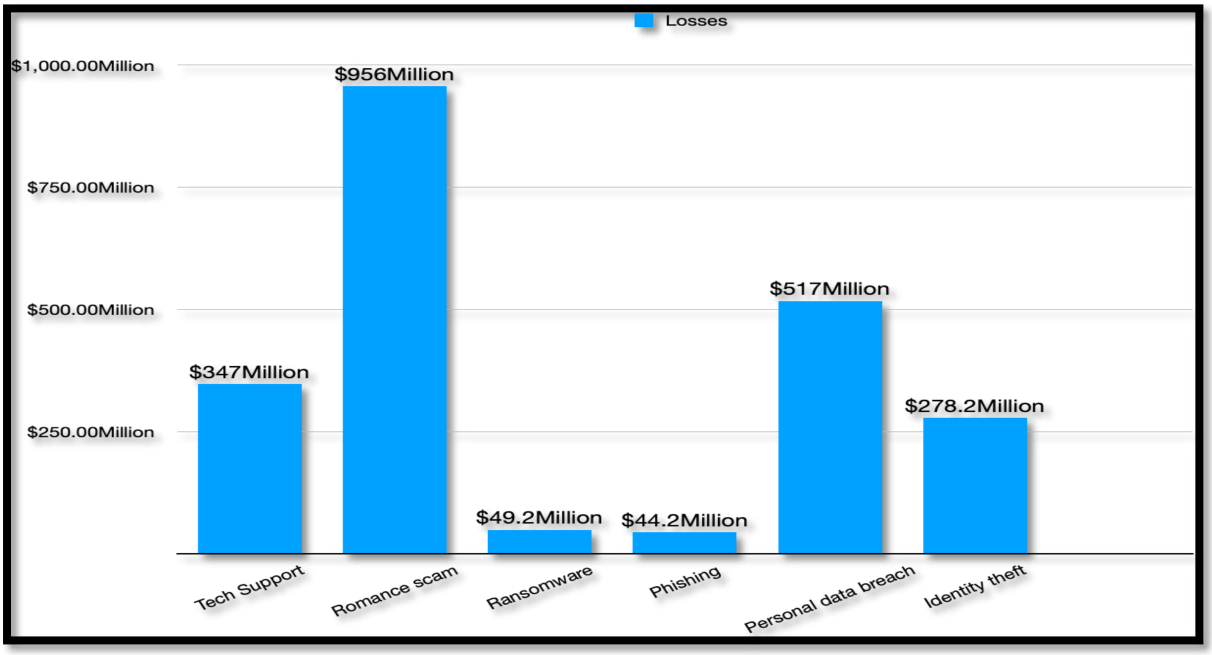


Fig.2 Losses caused by cyber-crime from 2017-2021

The above chart illustrates the loss caused by the five (5) crimes that we have selected for ourwork 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 ahuge 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 reportwas given by the FBI and the attacks came from different branches of cybercrimes. Turkey hasa 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 canalso 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.

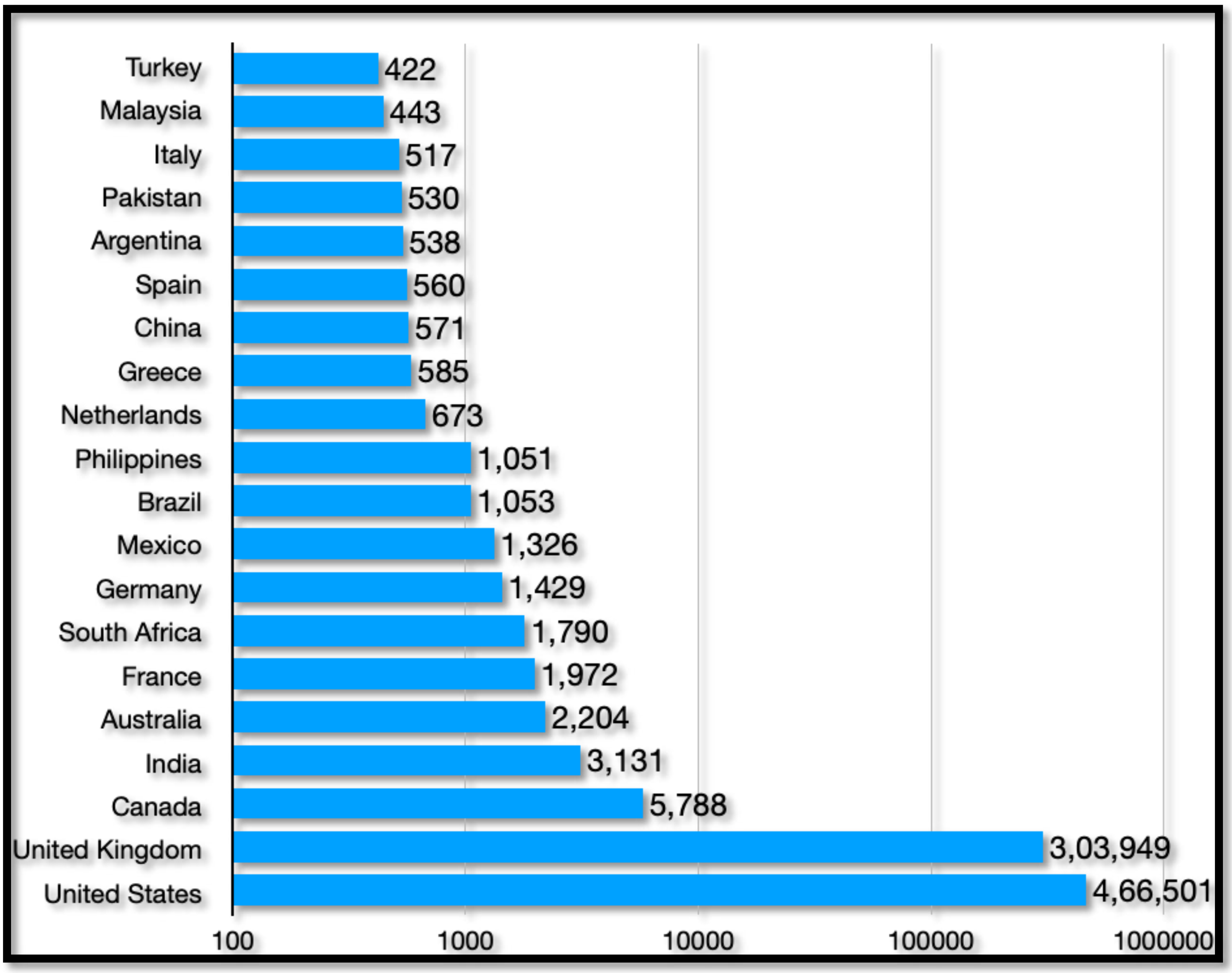


Fig.3 Record of victim's countries in 2021

Here is the list of the number of victims who reported a cybercrime in 2021, we have selected6 crimes out of many [11].

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

II- 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 authorsin order to do our work.

Axis	Paper reference	Description	Financial Cybercrime Category orAssociated Topic
1) Different fraud methods adopted by criminals	[12]	Malware categorization and discussion.	Ransomware
	[13]	Romance fraud analysis	Romance Fraud
	[14]	Analysis of phishing techniques.	Phishing Attacks
	[15]	Romance fraud analysis.	Money Laundering
	[16]	Romance fraud analysis.	Insider Trading
2) Relevant systems, algorithms, drawbacks, constraints, and metrics used to combat each fraud type	[17]	Financial fraud detection survey and associated models.	Fraud
	[18]	Analysis of detecting accounting fraud.	Fraud
	[19]	Review of GAD and DL techniques.	Applicable Algorithms
	[21]	ML techniques to identify Windows malware.	Applicable Algorithms
	[22]	Analysis of DL applications in finance	Applicable Algorithms
	[23]	Analysis of popular cryptocurrencies.	Cryptocurrency graph pre-processing
	[23]	GNN survey and taxonomy.	Applicable Algorithms
	[24]	Survey on GAD	Applicable Algorithms
	[25]	Proactive Fraud Strategies.	Fraud
	[26]	Survey on ML in credit card fraud.	Fraud
	[27]	Survey on ML in credit card fraud including genetic algorithm.	Fraud
	[28]	Book on AD techniques.	Applicable Algorithms
	[29]	AD techniques in high dimensional data.	Applicable Algorithms
	[30]	Survey on unsupervised AD techniques	Applicable Algorithms
	[31]	Survey on DL techniques in AD.	Applicable Algorithms
	[32]	Network AD analysis for malicious cyber activity.	Applicable Algorithm
	[33]	Survey on AD.	Applicable Algorithms
3) Relevant personas andstakeholders involved	[34] [351 [36] [37]	Behavioural analysis of cybercrime victims. Behavioural analysis of cybercrime victims. Behavioural analysis of cybercriminals. McKinsey: cybersecurity analysis for financialfraud prevention	Fraud, social engineering, hackingFraud 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 requestsneed to go through since they are all not genius. Being able to distinguish between a good andbad request is important and will help us later to focus on malicious ones and take action againstthem, 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 wecan reach the real request and stop them from causing further impact.

III- Propose work:

Our work is done in two main parts which are

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

- The backend API of the application is implemented using express powered byNode.js.
- The entire server runs on a microservice architecture where multiple service communicates to create (simulate) a pipeline to allow secure communication (sendmessages) 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 (willbe 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-servicesin 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 processingthe message.
- Once the client makes a request, "Service 1" creates a temporary message in Firestoredatabase then returns a 201 [created] to the client and parallelly triggers a new internalrequest 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 checkwhether the sender and the receiver have good relationship i.e., if the sender has blockedthe 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 accessto a bank data or a server, we use Tellus us server to implement our work and show it workingprocedure, 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 in this steps.

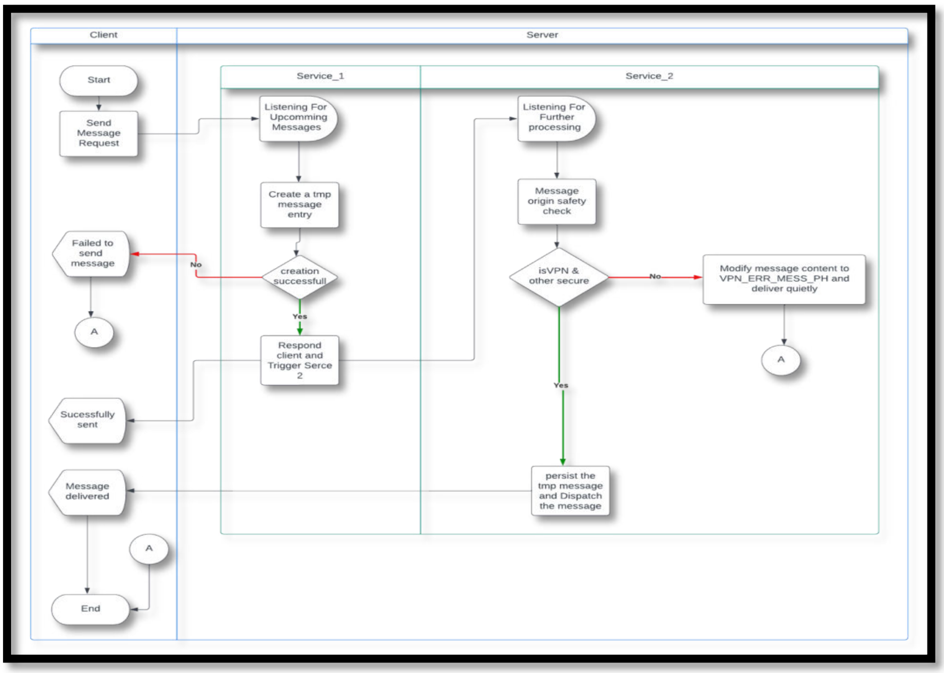
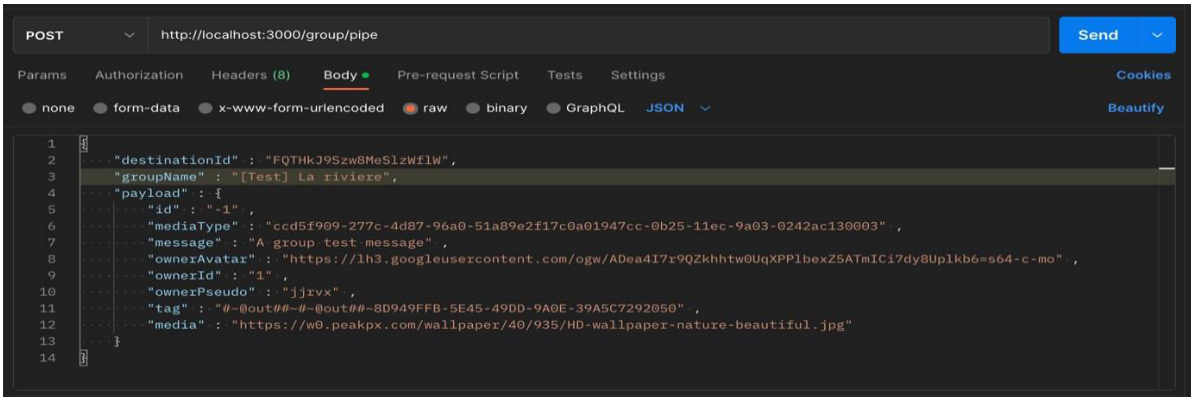

Client
Server
Service_1
Service_2
Start
Send Message Request
Listening For Upcomming Messages
Create a tmp message entry
creation successfull
No
Yes
Failed to send message
A
Respond client and Trigger Serce 2
Sucessfully sent
Listening For Further processing
Message origin safety check
isVPN & other secure
No
Modify message content to VPN_ERR_MESS_PH and deliver quietly
A
Yes
persist the tmp message and Dispatch the message
Message delivered
A
End

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 aVPN 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

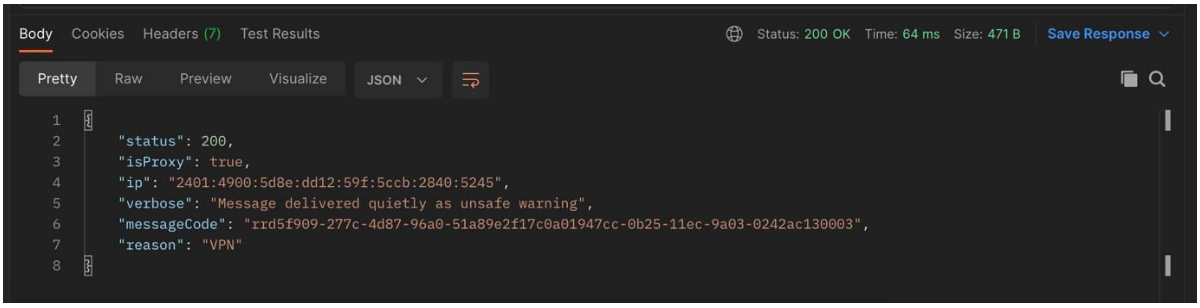


http://localhost:3000/group/pipe

```
{
    "destinationId" : "FQTHkJ9Szw8MeSlzWflW",
    "groupName" : "[Test] La riviere",
    "payload" : {
        "id" : "-1" ,
        "mediaType" : "ccd5f909-277c-4d87-96a0-51a89e2f17c0a01947cc-0b25-11ec-9a03-0242ac130003" ,
        "message" : "A group test message" ,
        "ownerAvatar" : "https://lh3.googleusercontent.com/ogw/ADea4I7r9QZkhhtw0UqXPPlbexZ5ATmICi7dy8Uplkb6=s64-c-mo" ,
        "ownerId" : "1" ,
        "ownerPseudo" : "jjrvx" ,
        "tag" : "#~@out##~#~@out##~8D949FFB-5E45-49DD-9A0E-39A5C7292050" ,
        "media" : "https://w0.peakpx.com/wallpaper/40/935/HD-wallpaper-nature-beautiful.jpg"
    }
}
```

- 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 thescreenshot below so that the service 2 can be able to display the error message to the end user.

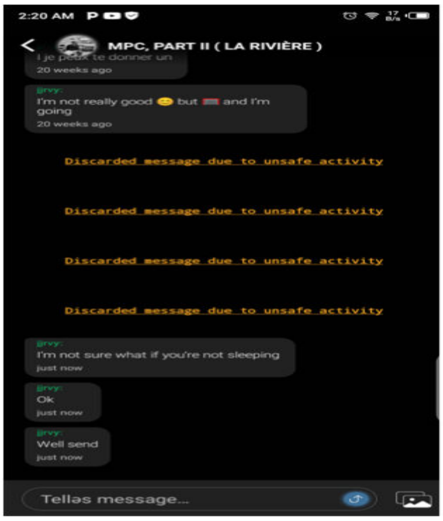


```
{
    "status": 200,
    "isProxy": true,
    "ip": "2401:4900:5d8e:dd12:59f:5ccb:2840:5245",
    "verbose": "Message delivered quietly as unsafe warning",
    "messageCode": "rrd5f909-277c-4d87-96a0-51a89e2f17c0a01947cc-0b25-11ec-9a03-0242ac130003",
    "reason": "VPN"
}
```

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 persistenceto the DB was done, actually downgraded to a warning message (represented by "messageCode") that, on client device would look like the following screenshot.



I je peux te donner un
20 weeks ago

jjrvy:
I'm not really good 😑 but and I'm going
20 weeks ago

Discarded message due to unsafe activity

Discarded message due to unsafe activity

Discarded message due to unsafe activity

Discarded message due to unsafe activity

jjrvy:
I'm not sure what if you're not sleeping
just now

jjrvy:
Ok
just now

jjrvy:
Well send
just now

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 receiption. Once the VNP or proxy is disable, the message can now reach the receiver.

IV- Conclusion and Future work.

There are different types of cybercrime and the damage caused is not limited to any particular 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 notethat 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 wherefeatures 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 therequest 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. Das, S. and Nayak, T., 2013. Impact of cybercrime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6(2), pp.142-153.
2. Naidoo, R., 2020. A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems, 29(3), pp.306-321.
3. Amarullah, A.H., Runturambi, A.J.S. and 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.
4. W. Z. A. Zakaria, M. F. Abdollah, O. Mohd, and A. F. M. Ariffin, ''The rise of ransomware,'' in Proc. ACM Int. Conf., 2017, pp. 66–70.
5. E.Carter, ''Distort,extort, deceiveandexploit: Exploringtheinnerwork- ings of a romance fraud,'' Brit. J. Criminol., vol. 61, no. 2, pp.283–302, Feb. 2021.
6. R. Alabdan, ''Phishing attacks survey: Types, vectors, and technical approaches,'' Future Internet, vol. 12, pp. 1–39, Oct. 2020.
7. A. Tamersoy, E. Khalil, B. Xie, S. L. Lenkey, B. R. Routledge, D. H. Chau, and S. B. Navathe, ''Large-scale insider trading analysis: Patterns and discoveries,'' Social Netw. Anal. Mining, vol. 4, no. 1, pp. 1–17, Dec. 2014.
8. K. G. Al-Hashedi and P. Magalingam, ''Financial fraud detection apply- ing data mining techniques: A comprehensive review from 2009 to 2019,'' Comput. Sci. Rev., vol. 40, May 2021, Art. no. 100402.
9. A. Sharma and P. K. Panigrahi, ''A review of financial accounting fraud detection based on data mining techniques,'' Int. J. Comput. Appl., vol. 39, no. 1, pp. 37–47, Feb. 2012.
10. X. Ma, J. Wu, S. Xue, J. Yang, C. Zhou, Q. Z. Sheng, H. Xiong, and L. Akoglu, ''A comprehensive survey on graph anomaly detection with deep learning,'' Aug. 2021, arXiv:2106.07178.
11. D. Ucci, L. Aniello, and R. Baldoni, ''Survey of machine learning tech- niques for malware analysis,'' Comput. Secur., vol. 81, pp.123–147, Mar. 2019
12. A. M. Ozbayoglu, M. U. Gudelek, and O. B. Sezer, ''Deep learning for financial applications : A survey,'' Appl. Soft Comput., vol. 93,Aug. 2020, Art. no. 106384
13. J. Wu, J. Liu, Y. Zhao, and Z. Zheng, ''Analysis of cryptocurrency transactions from a network perspective: An overview,'' J. NetwComput. Appl., vol. 190, Sep. 2021, Art. no. 103139.
14. Z.Wu,S.Pan,F.Chen,G.Long,C.Zhang,andP.S.Yu,''Acomprehen- sive survey on graph neural networks,'' IEEE Trans. Neural Netw. Learn. Syst., vol. 32, no. 1, pp. 4–24, Jan. 2021.
15. E. Toth and S. Chawla, ''Group deviation detection methods: A survey,'' ACM Comput. Surv., vol. 51, no. 4, pp. 1–38, Sep. 2018.
16. R. Saia and S. Carta, ''Evaluating the benefits of using proac- tive transformed-domain-based techniques in fraud detection tasks,''
Future Gener. Comput. Syst., vol. 93, pp.18–32, Apr. 2019.
17. A. H. Alhazmi and N. Aljehane, ''A survey of credit card fraud detection use machine learning,'' in Proc. Int. Conf. Comput. Inf. Technol. (ICCIT), Sep. 2020, pp. 10–15.
18. N. Shirodkar, P. Mandrekar, R. S. Mandrekar, R. Sakhalkar, K. M. C. Kumar, and S. Aswale,

''Credit card fraud detection techniques—A survey,'' in Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng. (ic-ETITE), 2020, pp. 1–7.

19. C. C. Aggarwal and P. S. Yu, ''Outlier detection for high dimensional data,'' ACM SIGMOD Rec., vol. 30, no. 2, pp. 37–46, 2001.
20. A. Zimek, E. Schubert, and H.-P. Kriegel, ''A survey on unsupervised outlier detection in high-dimensional numerical data,'' Stat.Anal. Data Mining, vol. 5, no. 5, pp. 363–387, Oct. 2012.
21. M.Ahmed,A.N.Mahmood,andJ.Hu,''Asurveyofnetworkanomaly detection techniques,'' J. Netw. Comput. Appl., vol. 60, pp. 19–31,Jan. 2016.
22. C. M. M. R. van den Bergh and M. Junger, ''Victims of cybercrime in Europe: A review of victim surveys,'' Crime Sci., vol. 7, no. 1,pp. 1–15, Dec. 2018
23. N. Patterson, M. Hobbs, and D. Palmer, ''A direct insight into victims of cybercrime,'' in Proc. 12th IEEE Int. Conf. Trust, Secur.Privacy Comput. Commun. (TrustCom), Jul. 2013, pp. 603–610.
24. R. Sabillon, J. Cano, V. Cavaller, and J. Serra, ''Cybercrime and cybercriminals: A comprehensive study,'' Int. J. Comput. Netw. Com- mun. Secur., vol. 4, no. 6, pp. 165–176, 2016.
25. S. Hasham, S. Joshi, and D. Mikkelsen, Financial Crime and Fraud in the Age of Cybersecurity. Shanghai, China: McKinsey &Company, 2019, pp. 1–11.

26. Nicholls, J., Kuppa, A. and Le-Khac, N.A., 2021. Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. IEEE Access.