Journal of Contemporary Issues in Business and Government Vol. 27, No. 3,2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.214

ANALYSING CYBERCRIME UNDERGROUND ECONOMY USING DATA ANALYTICS

Nandini G[1], Abhishek N [2], Akash Raju M[3], Chandan K A[4], Navneeth S[5]
[1,2,3,4,5]Department of Computer Science and Engineering, RajaRajeswari College of Engineering, Bengaluru, Karnataka-560074.
[1]nanduamma@gmail.com, [2]abhisheknshetty97@gmail.com,
[3]akashrajum7@gmail.com, [4]chandanka112@gmail.com,
[5]navaneethsugandaraj16@gmail.com

ABSTRACT: Given the rapid acceleration of digital hazards, little work has been carried out into the subject's institutions or procedures that could help to guide scientists and specialists in Information Systems that handle digital security. There is also no discussion of Crime as a Service that is a criminal action program which facilitates decentralized cyber-crime. The examination whole and useful cyber-crime issue that we see has persuaded us to research underground cybercrime economy by adopting information research strategy from a scientific point of view of the structure. To accomplish this objective, we will propose 1. a structure to information investigation to break down the underground cyber-crime, 2. CaaS and product definitions for wrong-doing and 3. a model for related order. Furthermore, 4. Create a software web-app to show how the proposed system and request structure can really be actualized. At that point, we will use web applications to explore the under-ground economy of cyber-crime by breaking down a huge data-set from the web-based network. In implementing the strategy-based structure science review, this review applies objects, institutions, and strategies to the project here. It also gives professional expertise to recommend rules on how governments and associations can plan underground cybercrime assaults in all businesses.

Keywords: Digital hazard, Crime-as-a-Service, Cybercrime, Design Science, Examination, Strategy, Web Application.

1. Introduction

As the danger presented by enormous cyber attacks e.g., ransom ware and appropriated refusal of the administration assaults Distributed Denial-of-Service and cyber-crimes have developed, people, associations, and the government have battled to discover approaches to protect them. In the year 2017, the ransom ware WannaCry was liable for about 45 thousand assaults in around a hundred nations.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.214

Hazardous effects of cyber-crime had put governments compelled to build their cyber-security spending plans. US President Barack Obama spent over $19B on cyber-security as a major aspect of his financial year spending plan, an expansion of over 35% since the previous year.

Worldwide cyber attacks, for example, Petya and WannaCry are accomplished by profoundly sorted out criminal gatherings, and even national-level wrongdoing bunches have been behind numerous ongoing assaults. Normally, criminal gatherings purchase and sell the hacking apparatuses including administrations on the cyber-crime bootleg market, where aggressors share the scope of hacking-related data. The same online black market is worked by gatherings of assailants and thus bolsters the under-ground cybercrime economy. The cyber-crime under-ground has therefore developed as another sort of association that works illegal businesses and empowers cyber-crime connivances to thrive.

Since composed cyber-crime requires an online system to exist and directs its assaults, it is profoundly reliant on shut under-ground networks e.g., Cracking zilla and Hack forums. These secrecy shut gatherings imply that cyber-crime systems are organized uniquely in contrast to customary Mafia-style hierarchies[4], which are fixed, inflexible, vertical, and concentrated. Conversely, cyber-crime systems can be horizontal, diffuse, liquid, and developing. Since the internet is a system of systems [5], the danger presented by the ascent of the profoundly proficient system based cybercrime plans of action, for example, Crime-as-a-Service, remains generally undetectable to governments, associations, and people.

2. Literature review

D. Cappelli, A. Moore, D. Andrews, L. Carroll, F. Greitzer, and T. Hull proposed to manage to recognize potential perils and thereafter figuring out how to direct them, helping broaden understanding of the inside threat [6]. The drawback with this approach is that it is time-consuming to conduct workshops.

H. Abbas, A. Sajid and K. Saleem, pp.feature the security challenges that the modern SCADA frameworks face in an IOT-cloud condition [7]. It helps Increase flexibility, optimization capability, cost efficiency, scalability and availability of SCADA systems. The drawback is that It consumes huge amounts of time.

A. Sood and S. Zeadally propose structure handling among hosts and targets. Consequently [8], this system obliges the flexibility in the heterogeneous structure. This helps in reducing the risks of exploitation. The drawback is that it requires huge resources.

Caas Survey of commoditized crime-ware in the underground market by R.Venkateswaran [9]. This paper dismembers CaaS and clarifies the embodiment of the underground economy that has developed under it. Empowers remote

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.214

access to the Intranet at a fundamentally lower cost. The downside is customary private systems are not modest to design and convey.

Interaction between 5 pillars of information assurance, availability, integrity, authentication, confidentiality was highlighted by K. Wilson [10]. It helps in analyzing existing information assurance measures. The drawback is that it is time-consuming.

The consequences of effective hacking assaults against economically assaulted cyber security insurance apparatuses were shown in Some Fundamental Cyber security Concepts by K. S. Wilson and M. A. Kiyvol [11]. It shows us that trust in secure systems was misplaced though it is resource-intensive.

3. Design and Implementation

It is describing the systems in order to fulfill those specifications the components, architecture, interfaces, modules, and information. System design might see it as a product development application of system theory. The software management, process design, and device engineering fields overlap.

If "Marketing, layout and manufacturing viewpoints are merged into a common way of product development, the more general product development topic," design takes the marketing data and produces the product design to be created. The system design processes therefore designed to identify and to create systems to meet the specific needs of users.

In the data processing industry, the design of systems played a key and respected role up to the 1990s. The 1990s preserved the ability to build integrated systems due to the standardization of hardware and software. Technology on standard systems has increased the value of software engineering.

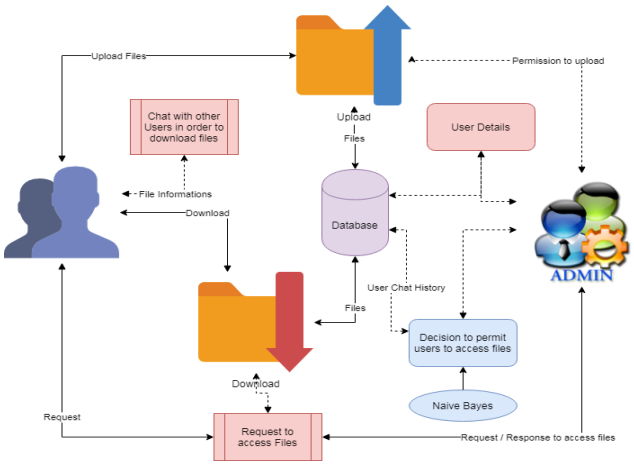

Fig. 1. Major functional blocks of the system

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.214

The standard language has been developed, quoting is necessary for object-led research and design. It is often used for application modeling and is used more often to build highly organized software systems. needed quote. Systems development is one of the most important steps in the design of technology.

4. Methodology

Modules

- **Upload Files**

Users are allowed to upload the files with the tags given. Once the file is uploaded, then it is sent to approval from admin to publish or make a view to other users. These uploaded files can be in any form document, audio or video but not allowed to upload the executable files.

- **Conversation Monitoring**

Users are allowed to communicate with other users. This could be monitored by the admin. Malicious conversation is likely to threaten the data. In order to protect the cybercrime and prevent from forming the cybercrime community. This can be achieved with the help of a classification algorithm named naïve Naive Bayes classification.

- **Download Files**

The files can be downloaded by requesting the file and once the admin approves the files then it can be downloadable. The decision to approve files can be taken from the conversation between users. Admin takes the action on download files and approvable status of users. The users are allowed further actions based on the users.

- **Graphical Representation**

The analyses of proposed systems are calculated based on the approvals and disapprovals. This can be measured with the help of graphical notations such as a pie-chart, bar-chart, and line-chart. The data can be given in dynamical data.

Naïve Bayes Equation

$$P(A \mid B) = \frac{P(A \mid B)\, P(B)}{P(B)} \quad (1)$$

5. Results and discussions

Admin can go to the user request page to see all the requests and click on the chat button to analyze chat to see if the chat is malicious or not.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.214

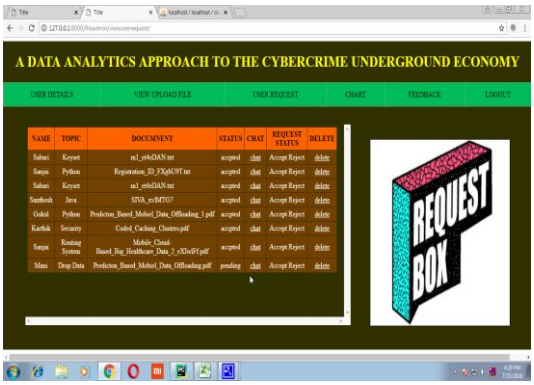

Fig. 2. User Request Page

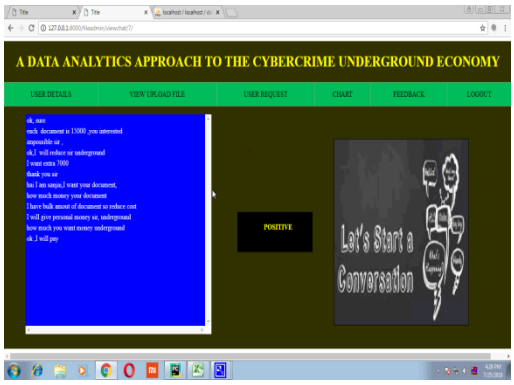

Fig. 3. Positive Chat

If the chat is malicious, the result will show up as positive.
If the chat is not malicious, the result will show up as negative.

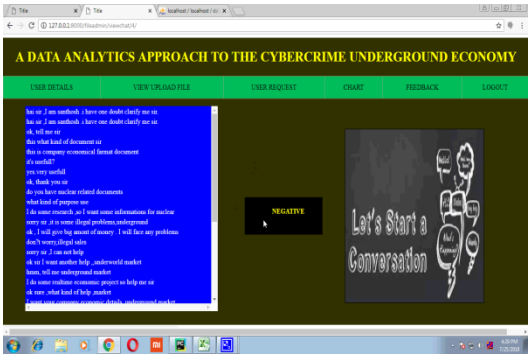

Fig. 4. Negative Chat

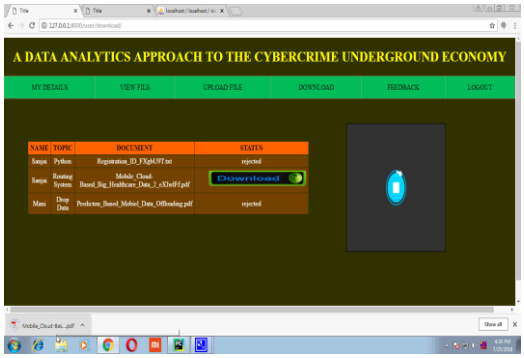

Fig. 5. Download Paget

Users can go to the download page to download accepted documents.
Admin can go to the Chart page to check all the analyzed results in the form of a bar chart or pie chart or spline chart.

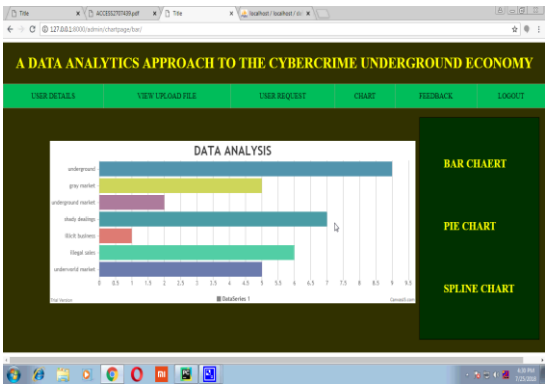

Fig. 6. Bar Chart

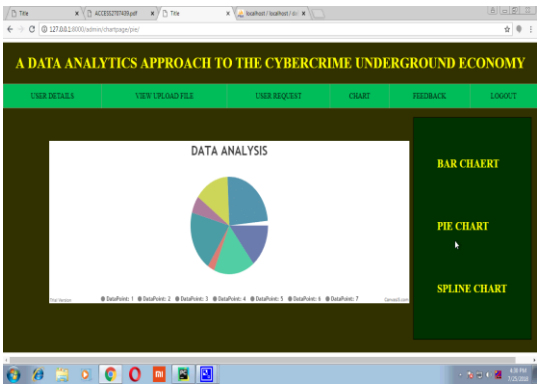

Fig. 7. Pie Chart

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.214

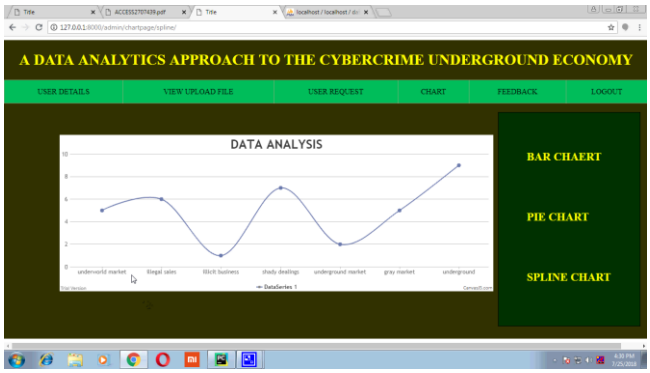

Fig. 8. Spline Graph

6. Conclusion

In this project, we have analyzed the chats; the chats were collected and divided into positive, negative by making use of the Naive Bayes algorithm. The data is then presented in the forms of charts in order to make it easy to understand. In future, we would be working towards improving our algorithm to make better predictions.

References

[1] K. Hughes, "Entering the world-wide web," ACM SIGWEB Newsl., vol. 3, no. 1, pp. 4–8, 1994.

[2] R.Venkateswaran, 2001. Crimeware as a service Survey of commoditized crimeware in the underground market.

[3] S. W. Brenner, "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships," N. C. J. Law & Technol., vol. 4, no. 1, pp. 1-50, 2002.

[4] F. Greitzer, A. Moore, D. Cappelli, D. Andrews, L. Carroll, and T. Hull, Jan./Feb. 2008. Combating the insider cyber threat.

[5] K.K R. Choo,"Orgainsed Crime Groups in Cyberspace: a Typology," Trends in Organized Crime, vol. 11, no3, pp.270-295, 2008.

[6] A. K. Sood and R. J. Enbody, "Crimeware-as-a-service—A survey of commoditized crimeware in the underground market," Int. J. Crit. Infer. Prot., vol. 6, no. 1, pp. 28–38, 2013.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.214

[7] K. S. Wilson and M. A. Kiyvol. 2, pp.116-124, 2014. Some Fundamental Cyber security concepts.

[8] D. Lin, Y. Lv, and D. Cao,(2015) ‘‘Rumour diffusion purpose analysis from social attribute to social content,” in Proc. Int. Conf. Asian Lang. Process. (IALP), Suzhou,China,Oct.2015,pp.107-110,DOI:10.1109/IALP.2015.7451543.

[9] E.Serrano, C . A. Iglesias, and M. Garijo (2015) “A novel agent-based rumour spreading model in Twitter,” in Proc. 24th Int. Conf. World Wide Web(WWW),New York,NY,USA,2015,pp. 811-814

[10] “FACT SHEET: Cyber security National Action Plan,” Ed: The White House, 2016.

[11]A. Sajid, H. Abbas, and K. Saleem, pp. 1375–1384, 2016. Cloud-Assisted IoT-Based SCADA System Security: A Review of the State of the Art and Future Challenges.

[12] A. Sood and S. Zeadally, 2016. Drive-by Download Attacks: A Comparative Study of Browser Exploit Packs Features and Attack Techniques.

[13] P. Vij and A. Kumar,(2016) “Effect of rumor propagation on stock market dynamics using cellular automata,”inProc.Int Conf. Inventive Compute Technol.(ICICT), Coimbatore, India,Aug. 2016,pp. 1-8, DOI:10.1109/INVENTIVE.2016.7830114.

[14] A.Sajid, H. Abbas, and K. Saleem pp. 1375-1384, 2016. Cloud-Assisted Iot - Based SCADA System Security: A Review of the State of the Art and Future Challenges.

[15] J. C. Wong and O. Solon. (2017, May 12). “Massive ransom ware cyber-attack hits nearly 100 countries around the world”.