CYBER SECURITY: DETECTION OF MALICIOUS INSIDERS FOR THE FINANCIAL BENEFIT OF COTE D'IVOIRE

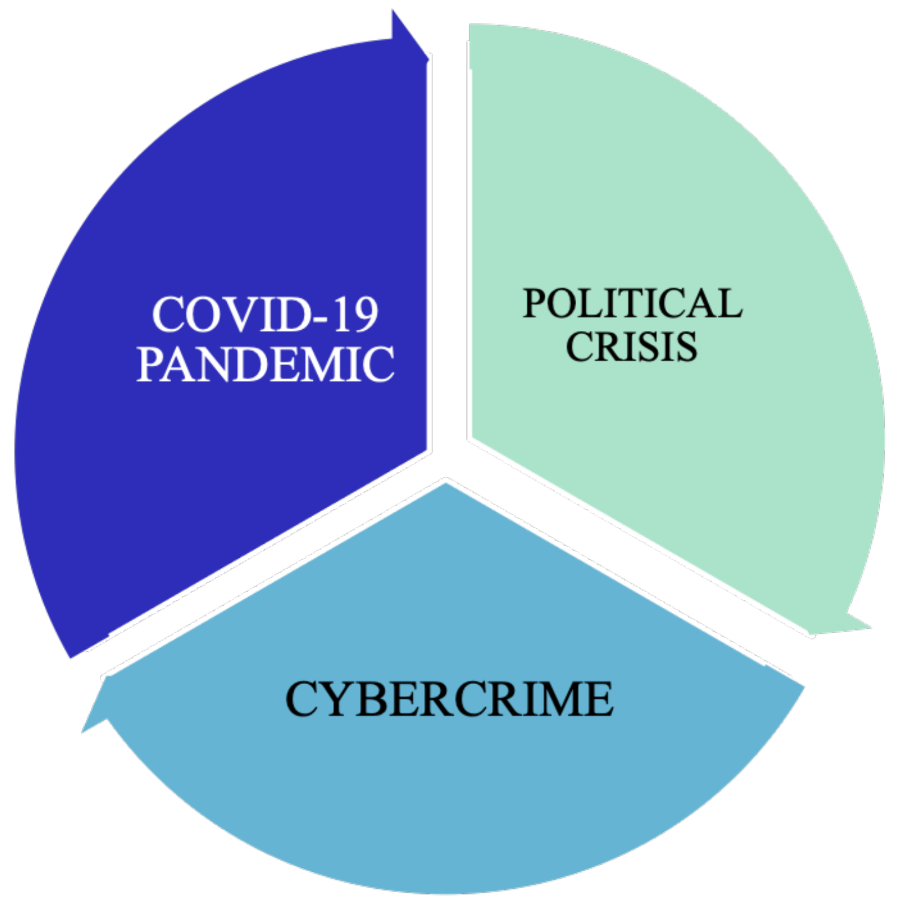
Leama Nolvenne Tah
Instructors: Carmen J. Falasco, Elisabeth Sasser |Facilitator : Yonghao Li
English Language Institute, Syracuse University

ABSTRACT

According to '*Croissance Afrique*', a local magazine, the annual economic impact of cybercrime in Cote d'Ivoire is estimated to be 10 million dollars per year (2022). Furthermore, cybercrime is a costly issue in Cote d'Ivoire and the country is included in the list of countries with poor cyber security. Cybercrime affects not only the country but also has a worldwide impact. Improving cyber security will have a positive economic impact on the country.

Figure 1. Unlocked Data. Source: Walborn (2022)

Figure 2. Three Main Causes of financial distress in Cote D'Ivoire



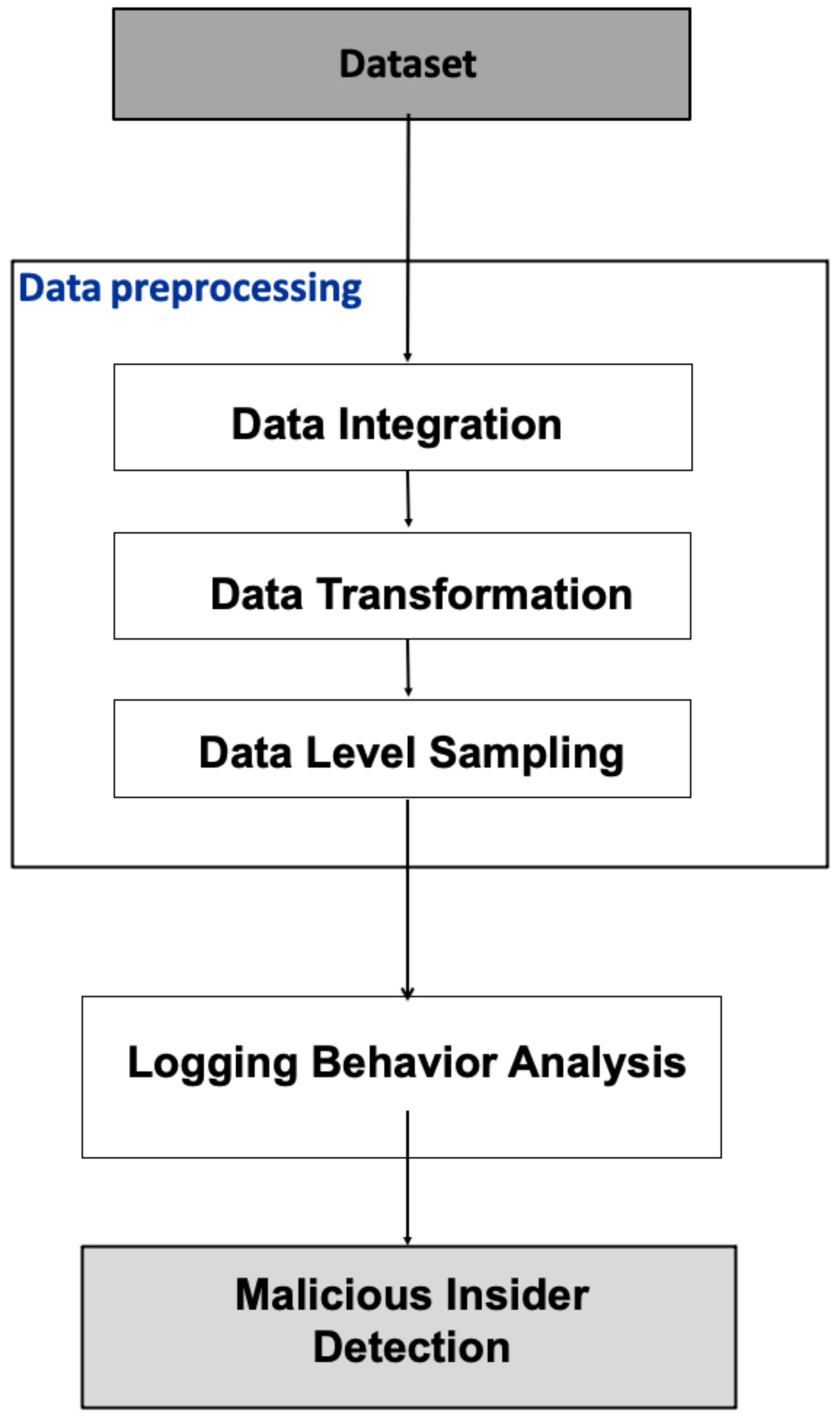
INTRODUCTION

Cybercriminals in Cote D'Ivoire are referred to as ***brouteur*** in Ivorian slang. This term is commonly used to describe a criminal who is capable of stealing people's identities online, blackmailing them, and accessing unauthorized systems. The lack of cyber security in the country has contributed to the rise of this criminal activity. The financial sector, prospective investors, e-commerce, public institutions in Africa, and individual Ivorians are among the most vulnerable for this crime. Therefore, the recommended approach to combatting cybercrime in the country is to utilize web-search analysis to identify malicious Insiders and to protect the data using RSA algorithm.

METHODS

US Computer Emergency Response Team (CERT) utilizes the Web Search Analysis method, also known as behavior analysis, to identify malicious insiders. This technique is based on the collection of data from email, Weblog, and various types of recorded users. It is composed of four phases: data collection, data preprocessing and logging behavior analysis, as well as malicious insider detection as showed in figure 3 (Padmavathi et al., 2021).

Figure 3. Methodology Overview. Source: Padmavathi et al., (2021)



ILLUSTRATION

For example, suppose two individuals (D1 and D2) are working on a computer. D1 is primarily active on social media, using external drives and visiting unauthorized websites. D2 is also active on social media and uploading several images.

Dataset: Data from the monitoring process is collected in various log files, such as emails, weblogs, data logs, firewall logs, network traffic logs and various types of users recorded.

Data integration: The collected data is pre-processed by using concatenation technique. This data is then **transformed** into a series of epochs and applied to the **data level sampling** using a Near-Miss 2 algorithm. Then, **Logging Behavior Analysis** is conducted to gain a better understanding of the activities of each individual. The websites visited by each individual are analyzed to determine the malicious user behavior.

ALGORITHM

RSA algorithm to secure data

Figure 4. Encrypted Algorithm. Source: Johnson (2023)

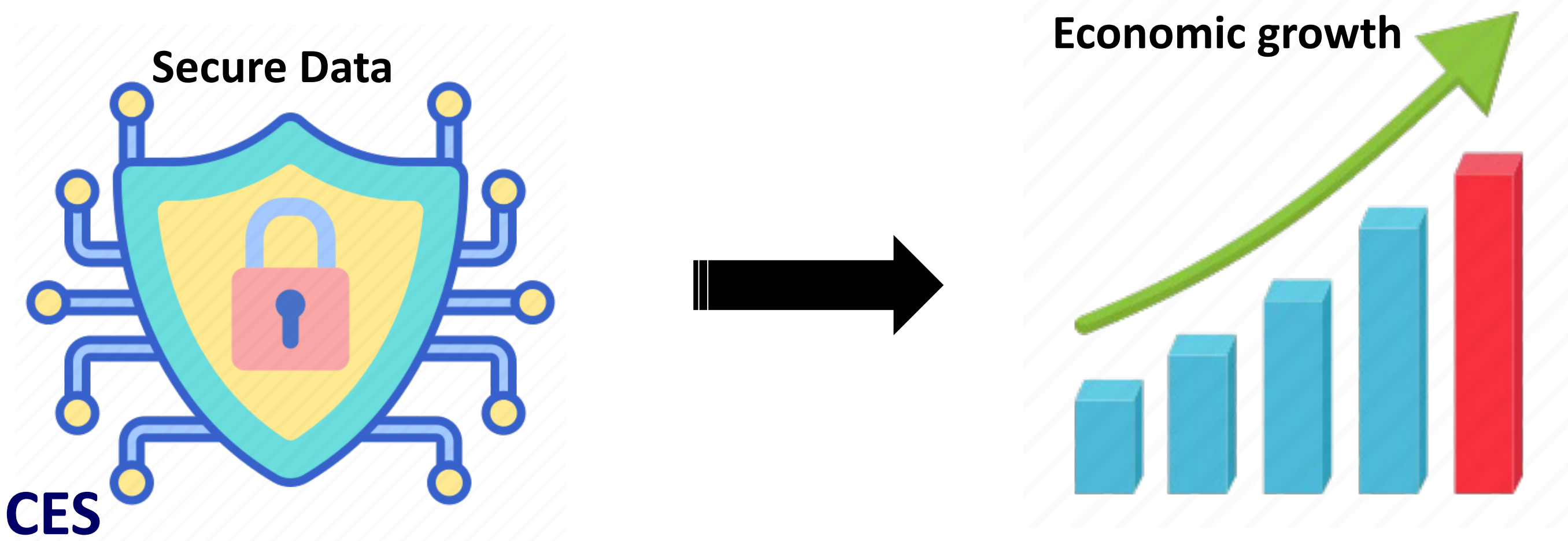
This algorithm is employed for the purpose of encrypting and decrypting messages. It outlines an effective method for safeguarding data from unauthorized intruders. The sender encrypts their message prior to transmission, and the message is encoded in the form of an integer. The recipient uses the key to decrypt the message (Handschuh 2017).

FINDINGS

The outcome of this illustration shows that the number of activities conducted by D1 is higher than those conducted by D2. Analysis of the frequency of visits to unauthorized websites by D1 leads to the conclusion that the malicious insider is D1.

This practice can be used to track down cybercriminals in Cote D'Ivoire and decrease their number annually. The financial gain of this is that the country will no longer be included in the list of countries with poor cyber security, thus attracting more investors. Furthermore, the expansion of e-commerce will generate more revenue and the security of each Ivorian online will increase.

Figure 5. Prospective for the upcoming year if Cybercrime is reduced in Cote d'Ivoire. Source: Iconfinder



REFERENCES

1. Padmavathi, G., Shanmugapriya, D., and Nethra, D. (2021). Progressions made in Cyber Security World' Seri-2021. Retrieved from https://www.taylorfrancis.com/books/edit/10.1201/9781003302384/progressions-made-cyber-security-world-nethra-pingala-suthishni-asha-Roshni.
2. Handschuh, H. (2017).Topic in Cryptology-CT-RSA. Retrieved from https://link.springer.com/book/10.1007/978-3-319-52153-4.
3. Croissanceafrik (2022). Côte d'Ivoire: l'impact de la Cybercriminalité . Retrieved from https://www.itsecurityguru.org/2021/03/19/cybercrime-has-cost-organisations-and-individuals-over-4-billion-in-2020/.
4. Walborn, D. (2022).Why don't people care about cybersecurity. *Network Tigers*. Retrieved from https://news.networktigers.com/all-articles/why-dont-people-care-about-cybersecurity/.
5. Johnson, D. (2023). Post-quantum algorithm vulnerable to side channel attacks. *Scmagazine*. Retrieved from https://www.scmagazine.com/analysis/post-quantum-algorithm-attack.