Fake News, Real Cyber Threats

Tutorial Number: 08, Group Number: 09

Group Members:

Fake news has proliferated rapidly in today's digital age, bringing about significant cybersecurity risks, particularly to businesses. This problem is especially highlighted during the COVID-19 pandemic, where fake news can attract employees working remotely to click on questionable links, hence causing data breaches. This project analyses the local case study of HealthierSG, where fake news led to compromises in cybersecurity. By understanding the strategy HealthierSG used to tackle this problem, we propose a two-pronged solution for businesses to both filter out fake news and detect cybersecurity threats. Companies can spot and filter out fake news using the Language Approach to prevent the risk of employees clicking on questionable fake news links. The Security Information and Event Management (SIEM) System then serves as a safety net to detect potential cybersecurity risks early, in the case that some fake news slips through the cracks. We acknowledge that these solutions still come with their own set of limitations and hence propose future integration of machine learning and knowledge-based approaches for improved fake news detection.

I PROBLEM STATEMENTS & AIMS

General problem statement:

Fake News results in Cybersecurity threats

Fake news attracts people to click on its links. Unsuspecting users are lured to click on these questionable links and become victims of cyber attacks such as phishing, malware, and denial of service (DoS). This leads to security breaches that can expose personal and company data. Hence, fake news is a cybersecurity threat. (Bitdefender, 2017).

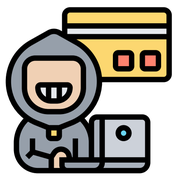
Aim:

To investigate the implications of fake news on cybersecurity, particularly concerning cybersecurity risks posed to businesses. It also explores strategies that companies can adopt to enhance their cybersecurity measures, so as to counter this problem.

II CASE STUDY: HEALTHIERSG

How scam happens from fake news:

Scammers send a **FAKE SMS** claiming to be from "Healthier SG" and download the fake HeathierSG app. Upon downloading and installing the app (which includes granting the app accessibility services), the scammers gain remote access and control over the victim's device. It enables them to steal passwords stored on the device.



Solution:

Increasing cybersecurity

- **ScamShield App**
- **Security features** (e.g., enable two-factor (2FA) or multi-factor authentication & set transaction limits on Internet banking such as PayNow).
- **Install & update anti-virus/anti-malware applications**
- **Update devices' operating systems and applications regularly** to be protected by the latest security patches.
- **Disable "Install Unknown App" or "Unknown Sources"** in your phone settings
- **Do not grant permission to persistent pop-ups** requesting access to your device's hardware or data.
- **Only download and install applications from official app stores** (i.e., Google Play Store for Android)

Noticing scam

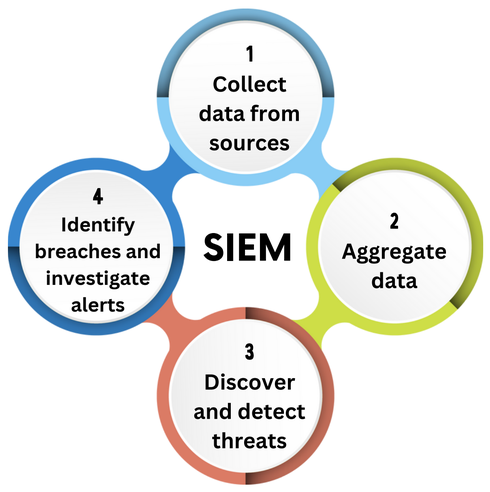
E.g. the official Healthier SG SMSes will always show the registered sender ID "MOH" in upper case and will not be sent via mobile phone numbers.)

III DETAILED DESIGN APPROACH

How to improve cybersecurity?

SIEM System

Provide a holistic view of an organization's IT security by providing real-time reporting coupled with long-term analysis of security events. It gather data, conduct analyses, and carry out security operations, all of which support quick, effective incident response. By collecting data from every nook and cranny of an area and combining it on a single, centralized platform, they offer visibility into hostile activities. This makes it possible for businesses to identify potential security issues before they affect daily operations. Additionally, SIEM saves the business' cost by automating low-level operations and accelerating the speed at which they can address events, it improves the effectiveness of the security team while decreasing the cost of running a Security Operations Center (SOC).



How to spot fake news?

Language Approach

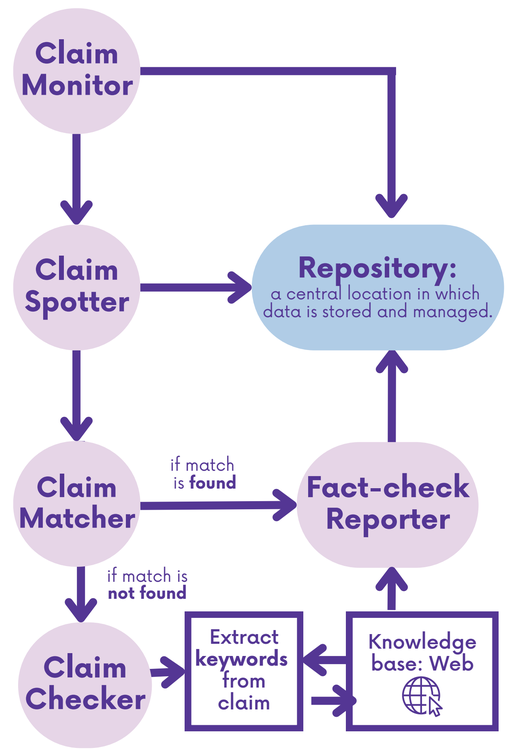
E.g. Bag of Words (BOW), Semantic Analysis, Deep Syntax.

Uses linguistics, either by human or software programs.

It emphasizes that those spreading fake news can be identified by analyzing the style of their language, particularly focusing on grammar and syntax. This approach considers the structure of words, sentences, and how they fit together in a paragraph.

Language Approach uses AI such as linguistics, to deal with well-crafted fake news that mimics the style of credible sources, so that cybersecurity could be protected against misinformation. These include fact-checking, source verification, and critical thinking. It helps to filter out the anomalies in grammar and syntax based on the inconsistent style of writing.

Example of fact-checking platform: **Claimbuster**



Comparing the novelty of our solution to HealthierSG

HealthierSG's approach only looks at how individuals can protect themselves from fake news and cybersecurity. However, companies still remain vulnerable. Employees may still click on fake news stories or associated content which can lead to security breaches that expose personal and company data.

Hence, our solution addresses the problem statement from a company's perspective:
How can a company protect itself from fake news threats to their cybersecurity?

With the Language Approach,

The company can filter out fake news more easily from real news, preventing employees from even clicking on such questionable fake news links to begin with

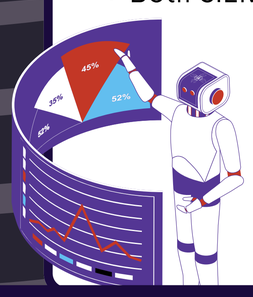
With the SIEM system,

The company can detect whether there are any potential cybersecurity risks before the risks affect the company's daily operations. This way, even if an employee were to click on a fake news link, the SIEM system can pick any threats up faster, giving the company more time to fend itself against the attack.

IV. OUTCOME AND FUTURE POSSIBILITIES

Limitations of our approach

- The language models may struggle with nuanced language.
- The language model may contain biases from training data.
- The language model may be fooled by well-crafted fake news articles, and struggle to keep up with evolving misinformation tactics.
- Both SIEM systems and language models can generate false positives.



Future possibility: Machine learning Approach

Combining machine learning with Language Approach can lead to more effective fake news detection. Machine learning can detect fake news, even well-crafted ones, by using various training datasets to refine its capabilities. Some ways it can do so are: (1) analysing text and data from news articles to find patterns and characteristics associated with misinformation, (2) supervised training with labelled datasets, (3) unsupervised grouping of articles, and (4) the assessment of news source credibility.

V. CONCLUSION

In conclusion, the intersection of fake news detection and cyber security represents a critical battleground in the increasingly digital world. The spread of fake news not only undermines the integrity of information but also poses a substantial threat to individuals, organizations, and societies as a whole. The combination of the SIEM system and the language approach helps to tackle the issue of fake news and cybersecurity from a corporate standpoint.

References:

- Hassan, N., Arslan, F. T., Li, C., & Tremayne, M. (2017). Toward Automated Fact-Checking. Toward Automated Fact-Checking: Detecting Check-worthy Factual Claims by ClaimBuster. https://doi.org/10.1145/3097983.3098131
- Juniper Networks. (n.d.). What is SIEM? | Juniper Networks US. https://www.juniper.net/us/en/research-topics/what-is-siem.html
- Police Advisory On A New Scam Variant Involving Fake SMS Leading To The Download Of A Fake Healthhub Application. (n.d.). Singapore Police Force. https://www.police.gov.sg/media-room/news/20230905_police_advisory_on_a_new_scam_variant_involving_sms_to-_fake_healthhub_application#a
- Jaiman, A. (2022, August 2). Disinformation Is a Cybersecurity Threat - The Startup - Medium. Medium. https://medium.com/swlh/disinformation-is-a-cybersecurity-threat-335681b15b48#:~:text=Cybersecurity%20experts%20have%20successfully%20understood,effective%20countermeasures%20to%20cognitive%20hacking
- De Beer, D., & Matthee, M. (2020). Approaches to Identify Fake News: A Systematic Literature review. In Lecture notes in networks and systems (pp. 13–22). https://doi.org/10.1007/978-3-030-49264-9_2