Association for Information Systems

AIS Electronic Library (AISeL)

Proceedings of the 2021 Pre-ICIS SIGDSA Symposium

Special Interest Group on Decision Support and Analytics (SIGDSA)

12-2021

A text mining-based cyber-risk assessment and mitigation model for DDoS attacks

Kalpit Sharma

Arunabha Mukhopadhyay

Follow this and additional works at: https://aisel.aisnet.org/sigdsa2021

This material is brought to you by the Special Interest Group on Decision Support and Analytics (SIGDSA) at AIS Electronic Library (AISeL). It has been accepted for inclusion in Proceedings of the 2021 Pre-ICIS SIGDSA Symposium by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

A text mining-based cyber-risk assessment and mitigation model for DDoS attacks

Completed Research

Extended Abstract

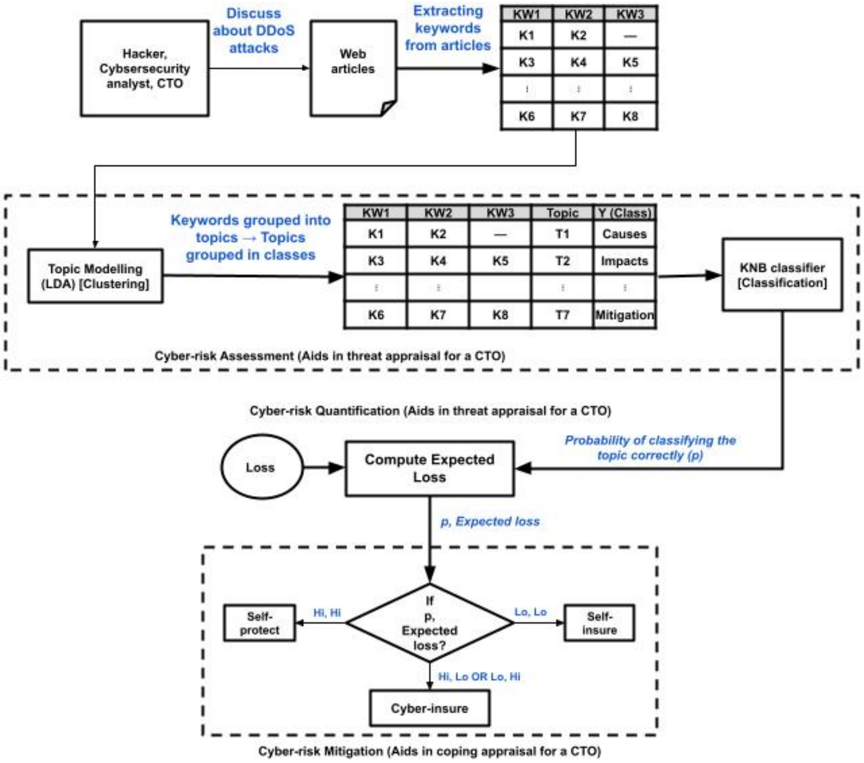
Cyber-risk is one of the pervasive risks faced by the global community in recent times. World Economic Forum (WEF) lists cybersecurity failure as one of the top 5 global risks since 2018 (McLennan, 2021). In 2020, 39 percent of the WEF survey respondents indicated cyber-risk as a highly likely and high-impact risk for industries, governments, and individuals (McLennan, 2021). During the coronavirus pandemic, most individuals shifted to work-from-home; thus, making them lucrative targets because of relatively diluted organizational cybersecurity best practices (Interpol, 2020). Cyber-attacks grew by five-fold according to WHO in 2020 (Interpol, 2020).

DDoS attacks are one of the easiest executable cyber-attacks due to the lack of social engineering expertise or technical know-how needed to launch them. In 2020, DDoS attacks increased by 12 percent in the second half. The attack intensity peaked at 2.3 Gbps on AWS and 2.5 Gbps on the Google Cloud Platform. Akamai also revealed that they blocked 809 million packets that targeted their CDN services (Hope, 2021). In Q1 2020, the number of DDoS attacks tripled compared to the same quarter in 2019. They accrued 19% of the total number of incidents in the first quarter of 2020 (Kaspersky, 2020). The attack duration increased by 25 percent as compared to the first quarter of 2019.

This study tries to devise a framework to extract critical themes related to cyber-risk management from web articles followed by appropriate mitigation strategies where top management misinterprets them. First, we propose a hybrid approach comprising Latent Dirichlet Allocation and Kernel Naïve Bayes classifier to predict the critical themes in web articles related to DDoS attacks. The final output from the CRA module computes the probability of misinterpreting critical themes and the expected loss caused due to it. Our CRM module proposes technology al interventions to reduce DDoS attacks. Additionally, we propose using financial mitigation strategies such as cyber-insurance policies (Böhme and Kataria, 2006; Böhme and Schwartz, 2006) to reduce the impact of such misinterpretations on cyber-enabled firms (Benaroch, 2002). It helps CTOs devise appropriate investment strategies to implement cyber risk mitigation strategies, including predictive and cybersecurity technological interventions (Das et al., 2017; Kesan et al., 2005; Mukhopadhyay et al., 2019; Rejda, 2007).

This study investigates (i) the web articles related to DDoS attacks to summarize their causes, (ii) quantifies subsequent losses, and (iii) proposes mitigation strategies. We propose a text mining-based Cyber-risk Assessment and Mitigation (TCRAM) model comprising three modules. Firstly, the cyber-risk assessment (CRA) module analyzes textual web articles and extracts themes using Latent Dirichlet Allocation. Subsequently, we estimate the probability of misinterpreting these themes using the kernel Naïve Bayes classifier. Next, the cyber-risk quantification (CRQ) module calculates the expected loss incurred by a firm due to DDoS attacks. Lastly, the cyber-risk mitigation (CRM) module aids the CTO in reducing, accepting, or passing the cyber-risk. Our CRA module observes that hackers use obsolete protocols to launch DDoS attacks. While, the CRQ module highlights that losses are dependent on attack size and duration based on risk theory. We also note that our model mostly misclassifies attack features and cost topics. The CRM module suggests using analytics-based mitigation strategies to reduce the cyber-risk or pass it to cyber-insurers. Based on risk theory, our framework helps CTOs invest appropriately in technology and cyber-insurance.

As shown in Figure 1, our proposed model follow from the risk theory (Kunreuther, 1997) that uncertain scenarios require resolution in three interdependent steps, our proposed model consists of three modules: cyber risk assessment (CRA), cyber risk quantification (CRQ), and cyber risk mitigation (CRM). The model takes the news articles from the Internet and outputs possible risk mitigation strategies by estimating the probability of detecting the DDoS attack traits correctly and the subsequent expected loss in intermediate steps.


Hacker, Cybsersecurity analyst, CTO
Discuss about DDoS attacks
Web articles
Extracting keywords from articles
Topic Modelling (LDA) [Clustering]
Keywords grouped into topics → Topics grouped in classes
KNB classifier [Classification]
Cyber-risk Assessment (Aids in threat appraisal for a CTO)
Cyber-risk Quantification (Aids in threat appraisal for a CTO)
Loss
Compute Expected Loss
Probability of classifying the topic correctly (p)
p, Expected loss
If p, Expected loss?
Hi, Hi
Self-protect
Lo, Lo
Self-insure
Hi, Lo OR Lo, Hi
Cyber-insure
Cyber-risk Mitigation (Aids in coping appraisal for a CTO)

KW1	KW2	KW3
K1	K2	—
K3	K4	K5
⋮	⋮	⋮
K6	K7	K8

KW1	KW2	KW3	Topic	Y (Class)
K1	K2	—	T1	Causes
K3	K4	K5	T2	Impacts
⋮	⋮		⋮	⋮
K6	K7	K8	T7	Mitigation

Figure 1: Flowchart of the proposed model

In the event of a DDOS attack, a firm tends to lose revenue as well as reputation due to the loss of productive hours. Thus, the CTO is evaluating the business environement for threats such as hackers to reduce losses for the frim.. In order to evaluate the threats they need to infer the likelihood as well as the severity of these attacks. It is in line with the threat appraisal in terms of likelihood as well as severity (Boss et al., 2015; Rogers, 1975).

According to PMT theory, to minimize the propensity of DDoS attacks, CTOs would tend to spend a substantial amount of their IT budget on perimeter security solutions to reduce the probability of DDoS attacks (D'Arcy et al., 2020; Dhillon and Backhouse, 2000), which is in concurrence with a threat appraisal. Security solutions and spending are essential points for a firm to consider proactively defending against potential DDoS attacks. It also suggests that in the event of a DDoS attack, top management plays an integral part in allaying the fears of the firm's customers and employees. We also observe that customer confidence and trust are crucial when assessing risk due to DDoS attacks. CTO can gather information about these attacks from public forums reporting attack features such as attack size, cost. Cybersecurity analysts report DDoS attack-specific information on these forums after carefully analyzing the multiple sources. In the event of an imminent attack, they can take proactive mitigation steps to counter or reduce the impact of the attacks. If the CTO misinterprets the threats or ignores them, the firms incur losses due to the delay. Thus, it becomes critical to reduce the likelihood of misinterpretation of information from these forums and reduce the severity of these attacks by either timely mitigation or cyber-insurance policies.

RQ 1(a): What are the attack traits of DDoS attacks evident determined from web articles?

RQ 1(b): What is the probability of getting attacked by a hacker if the decision-maker misinterprets the DDoS attack traits?

If the CTO misinterprets the threats or ignores them, the firms incur losses due to the delay. Thus, it becomes critical to reduce the likelihood of misinterpretation of information from these forums and reduce the severity of these attacks by either timely mitigation or cyber-insurance policies (Kunreuther, 1997). We devise these strategies (response efficacy) and decide upon them according to the CTO subjective preference structure (self-efficacy) and cost associated with each such strategy (Herath and Rao, 2009).

RQ 2: What is the distribution which best estimates the impact of the DDoS attack on customers?

Thereafter, they need to devise mitigation strategies in order to reduce both the risk and severity of DDOS attacks. It follows from the coping appraisal estimation of PMT. According to Rational choice theory (Becker, 1990; McCarthy, 2002), a decision-maker weighs the costs and benefits of diverse choices, choosing the option most closely aligned with their subjective preference structure, which concurs with a coping appraisal. Thus, it becomes critical to reduce the likelihood of misinterpretation of information from these forums and reduce the severity of these attacks by either timely mitigation or cyber-insurance policies. We devise these strategies (response efficacy) and decide upon them according to the CTO subjective preference structure (self-efficacy) and cost associated with each such strategy (Herath and Rao, 2009). They consider the firm's risk profile and decide which are the appropriate technological and financial interventions to reduce (self-protection), accept (self-insurance), or transfer (cyber-insurance) risk (Böhme, 2005; Böhme and Schwartz, 2006; Kesan et al., 2013; Majuca et al., 2006).

RQ 3: What mitigation strategies should be used for these DDoS attacks?

We contribute to the academic discussion by suggesting a framework to quantify the cyber-risk resulting from misinterpreting themes related to DDoS attacks from web articles, in line with threat and coping appraisal components of PMT. We suggest using a hybrid algorithm where a topic modeling technique such as LDA extracts themes from unstructured data such as web article text, followed by kernel Naïve Bayes classifier. THE KNB classifier aids in predicting the topic from bigrams (or trigrams). Our study contributes in the following ways. Based on risk theory, we treat cyber-risk management as a tool to reduce risk and the severity of DDoS attacks to delayed mitigation by using cyber-risk management principles. Lastly, we suggest cyber-insurance coupled with self-protection as a viable method to mitigate cyber-risk due to DDoS attacks. Firms value latency, scalability, and brand reputation as revenue drivers (D'Arcy et al., 2020). Our study has the following managerial implications. First, it helps the CTOs summarize and analyze the unstructured data such as text from web articles and highlight areas of concern and actionable insights to counter their effects. Next, it provides CTOs with a tool with easy-to-understand steps and actionable insights in the form of cyber-risk management to mitigate DDoS. The 2×2 cyber-risk mitigation heat-matrix provides exact mitigation steps along with probable investment strategies. Thus, managers could gauge whether the firm needs to invest in technology, cyber-insurance, or both. It also helps the CTO stay proactive and well-versed with the latest developments around new cyberattacks and aids them in devising robust mitigation. These mitigation strategies will discourage the hackers' purpose of causing financial loss to the firm and increase customer's confidence in the authenticity of firms' offerings.

In the event of a DDoS attack, a CTO performs threat appraisal of their firms' potential vulnerabilities and estimates the monetary impact on their business, in line with the PMT. This study analyzes the web articles related to DDoS attacks to summarize their causes, quantifies their monetary impact on business, and devises mitigation strategies. The hybrid topic clustering and classification model uses a KNB classifier and LDA-based topic modeling approach to calculate the probability of detecting a topic in the DDoS attack-related text corpus and the expected losses and suggest subsequent mitigation strategies. In 90 percent of cases, the classifier could detect the topic correctly from the text corpus. Based on risk theory, we also aid the CTO in deciding whether to accept, reduce, or transfer the cyber-risk using technological interventions and cyber-insurance.