Analyzing Cyber Attacks and Breaches: A Comprehensive Monitoring Approach

Kondragunta Rama Krishnaiah, Professor, Department of Computer Science and Engineering, R K College of Engineering, Vijayawada - 521456, Andhra Pradesh, India, email: kondraguntark@gmail.com

Alahari Hanumant Prasad, Professor, Department of Computer Science and Engineering, R K College of Engineering, Vijayawada - 521456, Andhra Pradesh, India, email: hanuma.alahari@gmail.com

Abstract

Analyzing cyber incident data sets is a crucial strategy to enhance our understanding of the evolving threat landscape. Although this area of research is relatively new, there is still much ground to cover. In this report, we present a statistical analysis of a data set comprising 12 years of cyber hacking activities, including malware attacks. Contrary to what has been reported in existing literature, we find that both the inter-arrival times of hacking breach incidents and the breach sizes should be modeled using stochastic processes rather than distributions due to their autocorrelations. To address this, we propose specific stochastic process models to appropriately fit the inter-arrival times and breach sizes. Moreover, these models effectively predict both the inter-arrival times and the breach sizes. To gain deeper insights into the patterns of hacking breach incidents, we conduct both qualitative and quantitative trend analyses on the data set. Through this comprehensive approach, we extract valuable cyber security insights. Notably, we observe that the frequency of cyber hacks is indeed increasing over time, indicating a worsening threat scenario. However, interestingly, the extent of the damage caused by these hacks has not shown a corresponding increase. By carefully studying these trends, we aim to contribute to the overall understanding of cyber security threats, helping organizations and researchers develop more effective strategies to protect against evolving cyber-attacks. Our findings highlight the importance of employing stochastic processes for modeling such incidents, and this work paves the way for further research and exploration in this dynamic field.

Keywords: Hacking breach, data breach cyber threats, breach prediction, trend analysis and time series.

I. Introduction

An information burst is a security event wherein sensitive, guaranteed or mystery information is copied, transmitted, saw, taken or used by an individual unapproved to do all things considered." An information break is the intentional or coincidental arrival of secure or private/classified data to an untrusted domain. Various articulations for this wonder incorporate incidental data revelation, information spill and furthermore information [1] spill. This may incorporate events, for instance, theft or loss of cutting edge media, for instance, PC tapes, hard drives, or smart phones such media whereupon such data is taken care of decoded, posting such data on the internet or on a PC by and large accessible from the Internet without authentic data security [2], [3] shields, trade of such data to a framework which isn't thoroughly open yet isn't fittingly or formally authorize for security at the confirmed measurement, for instance, decoded email or trade of such data to the data frameworks of a possibly threatening office, for instance, a fighting organization or a remote nation, where it may be introduced to progressively genuine unscrambling methodologies. While mechanical game plans can set computerized frameworks against attacks, information breaks continue being a major issue. This pushes us to depict the advancement of information [4] break events. This not solely will significant our understanding of information breaks, yet what's more revealed insight into various philosophies

for easing the mischief, for instance, security. Many trust that insurance will be significant; anyway the headway of precise cyber danger estimations to control the undertaking of assurance rates is past the compass of the current appreciation of information breaks.

Right now, make the going with responsibilities. We shoe that instead of by coursing the bursts we ought to show by stochastic methodology both the hacking break event bury section times and crack sizes. We show that these stochastic strategy models [5] can foresee the between landing times and the crack sizes. Apparently, this is the essential paper seeming stochastic strategies, rather than flows, should be used to show these computerized threat factors. We show that the dependence between the scene's entrance time and the break sizes can be satisfactorily delineated by a particular copula. This the essential works showing the nearness of this dependence and the aftereffects of dismissing it.

We furthermore show that it is important to think about the dependence while foreseeing bury passage times and break sizes commonly the results are not precise. We trust the current examination will rouse more examinations, which can offer profound experiences into substitute risk alleviation draws near. Such bits of knowledge are valuable to insurance agencies, government agencies, and regulators since they have to profoundly understand the idea of data breach risks. We trust the current examination will move more examinations, which can offer profound bits of knowledge into exchange risk moderation draws near. Such experiences are valuable to insurance agencies, government agencies, and regulators since they have to profoundly understand the idea of data breach risks. While innovative arrangements can harden cyber frameworks against attacks, data breaches keep on being a major issue. This rouses us to portray the development of data breach incidents. This not exclusively will profound our understanding of data breaches, yet in addition shed light on different methodologies for relieving the harm, for example, protection. Many accept that protection will be valuable, yet the improvement of precise cyber risk measurements to direct the task of protection rates is past the compass of the present understanding of data breaches (e.g., the absence of demonstrating approaches) [6].

II. Related Work

Prior Works Closely Related to the Present Study: Maillart and Sornette [7] investigated a dataset [8] of 956 individual character misfortune incidents that happened in the United States between year 2000 and 2008. They found that the individual personality misfortunes per incident, indicated by X, can be displayed by an overwhelming tail circulation $\Pr(X > n) - n^{-\alpha}$ where $\alpha = 0.7 \pm 0.1$. This outcome stays substantial while partitioning the dataset per kind of organizations: business, instruction, government, and clinical establishment. Since the likelihood thickness capacity of the personality misfortunes per incident is static, the situation of character misfortune is steady from the perspective of the breach size.

Edwards et al. [9] broke down an alternate breach dataset [1] of 2,253 breach incidents that length longer than 10 years (2005 to 2015). These breach incidents incorporate two categories: careless breaches (i.e., incidents brought about by lost, disposed of, taken gadgets, or different reasons) and pernicious breaching (i.e., incidents brought about by hacking, insider and different reasons). They indicated that the breach size can be displayed by the log-normal or log-skewnormal appropriation and the breach frequency can be demonstrated by the negative binomial conveyance, inferring that neither the breach size nor the breach frequency has expanded throughout the years.

Wheatley et al. [10] investigated organizational breach incidents dataset that is consolidated from [8] and [1] and ranges longer than 10 years (year 2000 to 2015). They utilized the Extreme Value Theory [11] to consider the most extreme breach size, and further demonstrated the enormous breach sizes by a doubly shortened Pareto dispersion. They additionally utilized straight relapse to contemplate the

frequency of the data breaches, and found that the frequency of enormous breaching incidents is autonomous of time for the United States organizations, yet shows an expanding pattern for non-US organizations.

Böhme and Kataria [12] considered the reliance between cyber risks of two levels: inside an organization (internal reliance) and across companies (worldwide reliance). Herath and Herath [13] utilized the Archimedean copula to display cyber risks brought about by infection incidents, and found that there exists some reliance between these risks. Mukhopadhyay et al. [14] utilized a copula-based Bayesian Belief Network to evaluate cyber weakness. Xu and Hua [15] researched utilizing copulas to demonstrate subordinate cyber risks. Xu et al. [16] utilized copulas to explore the reliance experienced when displaying the viability of cyber protection early-cautioning.

Peng et al. [17] examined multivariate cybersecurity risks with reliance. Contrasted and every one of these investigations referenced over, the current paper is one of a kind in that it utilizes another system to break down another point of view of breach incidents (i.e., cyber hacking breach incidents). This point of view is important in light of the fact that it mirrors the outcome of cyber hacking (counting malware). The new procedure found for the first time, that both the incidents inter-arrival times and the breach sizes ought to be demonstrated by stochastic procedures as opposed to appropriations, and that there exists a positive reliance between them. Other Prior Works Related to the Present Study: Eling and Loperfido [18] broke down a dataset [1] from the perspective of actuarial displaying and valuing. Bagchi and Udo [19] utilized a variation of the Gompertz model to dissect the development of PC and Internet-related violations. Condon et. al [20] utilized the ARIMA model to anticipate security incidents dependent on a dataset gave by the Office of Information Technology at the University of Maryland.

Zhan et al. [11] examined the stance of cyber threats by utilizing a dataset gathered at a network telescope. Utilizing datasets gathered at a honeypot, Zhan et al. [12], [13] abused their factual properties including long-run reliance and extraordinary qualities to portray and anticipate the quantity of attacks against the honeypot; a consistency assessment of a related dataset is depicted in [14]. Peng et al. [15] utilized a checked point procedure to anticipate extraordinary assault rates. Bakdash et al. [16] expanded these examinations into related cybersecurity situations. Liu et al. [17] examined how to utilize remotely perceptible highlights of a network (e.g., bungle side effects) to forecast the capability of data breach incidents to that network.

III. Proposed Method

The current examination is persuaded by a few inquiries that have not been explored as of recently, for example, Are data breaches brought about by cyber attacks expanding, diminishing, or settling? A principled response to this inquiry will give us an away from into the general situation of cyber threats. This inquiry was not replied by past investigations. In particular, the dataset broke down in [7] just secured the time range from 2000 to 2008 and doesn't really contain the breach incidents that are brought about by cyber attacks; the dataset investigated in [9] is more later, however contains two sorts of incidents: careless breaches (i.e., incidents brought about by lost, disposed of, taken gadgets and different reasons) and malevolent breaching. Since careless breaches speak to more human errors than cyber attacks, we don't think about them in the current examination. Since the malignant breaches concentrated in [9] contain four sub-categories: hacking (counting malware), insider, installment card misrepresentation, and obscure, this examination will concentrate on the hacking sub-category (called hacking breach dataset from that point), while taking note of that the other three sub-categories are interesting all alone and ought to be investigated independently.

Dataset Collection: The hacking breach dataset we examine right now acquired from the Privacy Rights Clearinghouse (PRC) [1], which is the biggest and most broad dataset that is likewise freely accessible. Since we center on hacking breaches, we ignore the careless breaches and the other sub-categories of pernicious breaches (i.e., insider, installment card extortion, and obscure). From the staying crude hacking breaches data, we further dismissal the deficient records with obscure/unreported/missing hacking breach sizes since breach size is one of the articles for our investigation. The subsequent dataset contains 600 hacking breach incidents in the United States between January first, 2005 and April seventh, 2017. The hacking breach casualties length more than 7 ventures: businesses-financial and insurance services (BSF); businesses-retail/merchant including online retail (BSR); businesses-other (BSO); educational institutions (EDU); government and military (GOV); healthcare, medical providers and medical insurance services (MED); and nonprofit organizations (NGO).

Preprocessing: Since we watched, as referenced over, every so often have numerous hacking breach incidents, one may propose regarding such various incidents as a solitary "joined" incident (i.e., including their number of breached records together). Notwithstanding, this technique isn't sound in light of the fact that the numerous incidents may happen to various casualties that have distinctive cyber frameworks. Given that the time goals of the dataset is a day, numerous incidents that are reported on similar data might be reported at various focuses in time of that day (e.g., 8pm versus 10pm). All things considered, we propose creating little random time intervals to isolate the incidents corresponding to that day. In particular, we randomly order the incidents corresponding to that day, and then addition a little and random time interval in the middle of two successive incidents (for the main interval, the beginning stage is 12 PM), while guaranteeing that these incidents correspond to that day (e.g., the two incidents on a two-incident day might be doled out at 8am and 1pm).

Remark: Right now, utilize various measurable systems, a thorough audit of which would be protracted. So as to consent to the space necessity, here we just quickly survey these systems at a significant level, and allude the perusers to explicit references for every method when it is utilized. We utilize the autoregressive contingent mean point process, which was presented for depicting the development of restrictive methods, to display the advancement of the inter-arrival time. We utilize the ARMA-GARCH time arrangement model to show the development of the breach size, where the ARMA part models the advancement of the mean of the breach sizes and the GARCH part models the high unpredictability of the breach sizes. We use copulas to show the nonlinear reliance between the inter-arrival times and the breach sizes.

Analysis of Breach Incidents Inter-Arrival Times: The fundamental insights of the inter-arrival times for singular casualty categories just as the total. We see that the standard deviation of the inter-arrival times in every category is likewise a lot bigger than the mean, which indicates that the procedures portraying the hacking breach incidents are not Poisson. We likewise see that the collection of the interarrival times of all categories prompts a lot littler interarrival times. For instance, the greatest inter-arrival time of NGO breach incidents is 1178 days, while the most extreme interarrival time of the total is 96 days. So as to formally respond to the inquiry whether the incidents inter-arrival times ought to be displayed by a dispersion or a stochastic procedure, we investigate the example Auto Correlation Function (ACF) and Partial Auto Correlation Function (PACF) of the inter-arrival times. Naturally, ACF measures the correlation between the perceptions at prior times and the perceptions at later times without dismissing the perceptions in the middle of them, and PACF measures the correlation between the perceptions at prior times and the perceptions at later times while ignoring the perceptions in the middle of them.

Analysis of Hacking Breach Sizes: The essential insights of the hacking breach sizes. We see that three Business categories have a lot bigger mean breach sizes than others. We further see that there exists an enormous standard deviation for the breach size in every one of the casualty categories, and that the standard deviation is in every case a lot bigger than the corresponding mean. So as to respond to the inquiry whether the breach sizes ought to be demonstrated by an appropriation or stochastic procedure, we plot the temporal correlations between the breach sizes. The example ACF and PACF for the log-transformed breach sizes, separately. We watch correlations between the breach sizes, implying that we should utilize a stochastic procedure, as opposed to a dispersion, to demonstrate the breach sizes. This is as opposed to the knowledge offered by past investigations [7] which proposes utilizing a slanted dispersion to display the breach sizes. We quality the attracting of this understanding to the way that these investigations [7], [18] didn't investigate this due point of view of temporal correlations. An important factor for deciding if to utilize dissemination or a stochastic procedure to portray something relies upon whether there is temporal autocorrelation between the individual examples. This is on the grounds that zero temporal autocorrelation implies that the examples are free of one another; otherwise, non-zero temporal autocorrelation implies that they are not autonomous of one another and ought not to be displayed by a circulation.

Dependence between Inter-Arrival Times and Breach Sizes: So as to respond to the inquiry whether there exists reliance between the inter-arrival times and the breach sizes, we propose directing the normal score transformation to the residuals that are gotten in the wake of fitting these double cross arrangement. For residuals of the LACD1 fitting, signified by e1. . . en, we utilize the fitted summed up gamma appropriation G(•|γ, k) to change over them into observational normal scores:

$$ei \rightarrow \phi -1(G(ei\ |\gamma, k)), I = 1, \ldots, n$$

Where ϕ−1 is the backwards of the standard normal dissemination. For the residuals of the ARMA (1, 1)- GARCH (1, 1) fitting, we utilize the assessed blended extraordinary worth conveyance to change over them into experimental normal scores. We see that huge transformed spans are related with huge transformed sizes, inferring a positive reliance between the inter-arrival times and the breach sizes. So as to factually test the reliance, we register the example Kendall's τ and Spearman's ρ for the incidents inter-arrival times and the breach sizes, which are 0.07578 and .11515, separately. The nonparametric position tests [13] for the two insights lead to a p-estimation of .04313 and .03956, separately, which are exceptionally little. This implies there surely exists some positive reliance between the inter-arrival times and the breach sizes.

Algorithm Used: Algorithm for Predicting the VaRα's of the Hacking Incidents Inter-Arrival Times and the Breach Sizes Separately

Input: Historical incidents inter-arrival times and breach sizes, denoted by {(dti , yti)}i=1,...,m+n, where an in-sample {(dti , yti)}i=1,...,m as mentioned above was used for fitting and an out-of-sample {(dti , yti)}i=m+1,...,n is used for evaluation prediction accuracy; α level.

1. for i = m + 1, · · · , n do
2. Estimate the LACD1 model of the incidents inter-arrival times based on {ds |s = 1, . . . , i − 1}, and predict the conditional mean
$$\Psi i = \exp\ (\omega + a1\ \log(\Psi i-1) + b1\ \log(\Psi i-1))$$
3. Estimate the ARMA-GARCH of log-transformed size, and predict the next mean ˆμi and standard error ˆσi.
4. Select a suitable Copula using the bivariate residuals from the previous models based on AIC;

5. Based on the estimated copula, simulate 10000 2-dimensional copula samples.
6. For the incidents inter-arrival times, convert the simulated dependent samples u (k) 1,i 's into the z (k) 1,i 's by using the inverse of the estimated generalized gamma distribution, k = 1, . . . , 10000.
7. For the breach sizes, convert the simulated dependent samples u (k) 2,i 's into the z (k) 2,i 's by using the inverse of the estimated mixed extreme value distribution, k = 1, . . . , 10000.
8. Compute the predicted 10000 2-dimensional breach data.
9. Compute the VaRα,d (i) for the incidents inter-arrival times and VaRα,y(i) for the log-transformed breach sizes based on the simulated breach data.
10. if d(k)i > VaRα,d (i) then
11. A violation to the incidents inter-arrival time occurs.
12. end if
13. if y(k) i > VaRα,y(i) then
14. A violation to the breach size occurs;
15. end if
16. end for

Output: Numbers of violations in inter-arrival times and breach sizes.

The situation of cyber hacking breaches mirrors the result of the cyber assault barrier interactions (e.g., regardless of whether the assault apparatuses can effectively dodge the guard devices). In spite of the fact that the specific wonder referenced above can occur under a wide range of situations and correctly nailing down of its motivation is past the extent of the current paper (basically as a result of the absence of different sorts of supporting data), one chance is the accompanying: When the assault apparatuses are never again compelling from the assailant's perspective, the aggressors may need to set aside a more drawn out time of effort to grow new assault devices for effectively breaching data.

IV. Results Analysis

Algorithm for Separate Prediction and Results: The recursive moving expectation for the inter-arrival time and the breach sizes. Since we utilize moving forecast, implying that preparation data develops as the expectation activity pushes ahead, more up to date preparing data should be re-fitted, conceivably requiring distinctive copula models. Thusly, we have to consider more reliance structure. This discloses why we have to re-select the copula structure, which can fit the recently refreshed preparing data better, through the rule of AIC. We see that the forecast models finish the entirety of the assessments at the 0.1 critical levels. Specifically, the models can foresee the future interarrival times for the entirety of the's levels. For the breach sizes, at level $\alpha = 0.90$, the model expectations have 28 infringement, while the quantity of infringement from the watched qualities is 31, which is genuinely near one another. For $\alpha = 0.95$, the quantity of infringement from the watched qualities is 20, while the model's normal number of infringement is 14. This shows the models for foreseeing the future breach sizes are to some degree preservationist.

Figure 1 plots the expectation results for the 280 out of tests. Figure 1(a) plots the expectation results for the incidents inter-arrival times. Figure 1(c) plots of the original breach sizes, however it is hard to investigate outwardly. For a superior representation impact, we plot in Figure 1(b) the log transformed breach sizes. We see from Figure 1(c) that for the breach sizes, there are a few outrageous enormous qualities, which are a long way from the anticipated VaR.95's. This implies the forecast missed a portion of the incredibly huge breaches, the expectation of which is left as an open issue. All in all, the proposed models can successfully foresee the VaR's of both the incidents interarrival time and the breach size, since the two of them finish the three factual assessments. Nonetheless, there are a few

incredibly enormous inter-arrival times and amazingly huge breach sizes that are far over the anticipated VaR.95's, implying that the proposed models will be unable to decisively foresee the specific estimations of the very huge inter-arrival times or the very huge breach sizes. In any case, as appeared in Section V-C underneath, our models can anticipate the joint probabilities that an incident of a specific greatness of breach size will happen during a future timeframe.

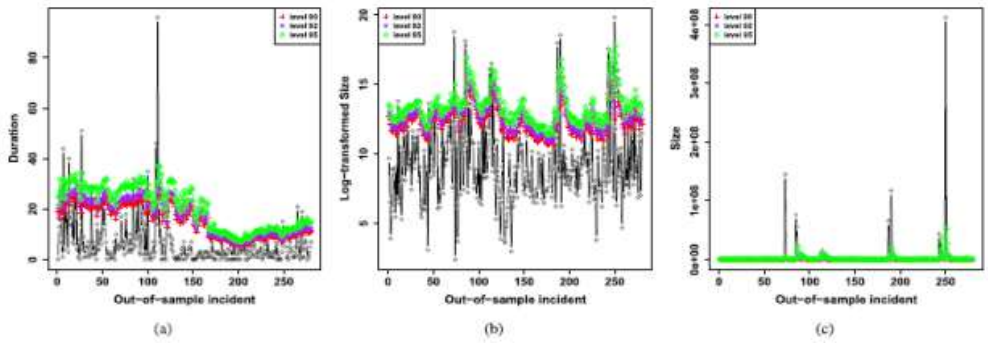

Fig1. Predicted inter-arrival times and breach sizes, where black-colored circles represent the observed values. (a) Incidents inter-arrival times. (b) Log-transformed breach sizes. (c) Breach sizes (prior to the transformation).

Performance Analysis: Practically speaking, on the off chance that one is interested in foreseeing the specific breach size at a specific future point in time, the former strategy ought to be utilized, with the "admonition" that the anticipated worth has a close to 5% possibility of being littler than the real worth that will be watched. In the event that one is interested in foreseeing the joint likelihood that a breach incident with a specific size of breach size during a specific future timeframe, the last technique ought to be utilized. This sort of expectation capacity is, similar to climate forecasting (e.g., a typhoon of a specific degree will happen inside the following 5 days), helpful in light of the fact that cyber safeguards can progressively alter their guard stance to moderate the harm, going from temporarily closing down pointless services (if relevant) to allotting extra assets in analyzing network traffic (e.g., costly however compelling profound bundle reviews or enormous scope data correlation investigations). Moreover, the expectation model may help gauge the financial limit in a barrier procedure arranging. This is important on the grounds that the effort spent to shield an endeavor against an assault (for example the measure of cost brought about by a specific guard) relies upon the probability of an assault to occur and its seriousness (i.e., quantitative risk the board). For example, when the model predicts that a gigantic data breach is probably not going to occur, the guards for that assault can be less complex (proportion cost-viability); when the model predicts that a colossal data breach is probably going to occur, the protector can set up more fragile safeguards (e.g., honeypots and more exact review frameworks). We accept that these kinds of prescient barrier (i.e., dynamic safeguard empowered by expectation capacity) are an important theme for future research, as comparably advocated by the convenience of climate forecasting in the physical world.

V. Conclusion

We examined a hacking breach dataset from the perspectives of the incidents inter-arrival time and the breach size, and demonstrated that the two of them ought to be displayed by stochastic procedures instead of conveyances. The measurable models created right now satisfactory fitting and expectation correctnesses. Specifically, we propose utilizing a copula-based way to deal with anticipate the joint likelihood that an incident with a specific greatness of breach size will happen during a future timeframe. Factual tests show that the systems proposed right now better than those which are introduced in the writing, in light of the fact that the last ignored both the temporal correlations and

the reliance between the incidents inter-arrival times and the breach sizes. We led subjective and quantitative investigations to draw further experiences. We drew a lot of cybersecurity bits of knowledge, including that the threat of cyber hacking breach incidents is to be sure deteriorating regarding their frequency, however not the greatness of their harm. The procedure introduced right now be embraced or adjusted to examine datasets of a comparative sort. There are many open issues that are left for future research. For instance, it is both interesting and testing to examine how to anticipate the amazingly huge qualities and how to manage missing data (i.e., breach incidents that are not reported). It is likewise worthwhile to assess the specific happening times of breach incidents. At last, more research should be led towards understanding the consistency of breach incidents (i.e., the upper bound of expectation precision.

References

[1]. P. R. Clearinghouse. Privacy Rights Clearinghouse's Chronology of Data Breaches. Accessed: Nov. 2017.
[2]. ITR Center. Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout. Accessed: Nov. 2017.
[3]. C. R. Center. Cybersecurity Incidents. Accessed: Nov. 2017.
[4]. IBM Security. Accessed: Nov. 2017.
[5]. NetDiligence. The 2016 Cyber Claims Study. Accessed: Nov. 2017.
[6]. M. Eling and W. Schnell, "What do we know about cyber risk and cyber risk insurance?" J. Risk Finance, vol. 17, no. 5, pp. 474– 491, 2016.
[7]. T. Maillart and D. Sornette, "Heavy-tailed distribution of cyber-risks," Eur. Phys. J. B, vol. 75, no. 3, pp. 357–364, 2010.
[8]. R. B. Security. Datalossdb. Accessed: Nov. 2017.
[9]. B. Edwards, S. Hofmeyr, and S. Forrest, "Hype and heavy tails: A closer look at data breaches," J. Cybersecur., vol. 2, no. 1, pp. 3– 14, 2016.
[10]. S. Wheatley, T. Maillart, and D. Sornette, "The extreme risk of personal data breaches and the erosion of privacy," Eur. Phys. J. B, vol. 89, no. 1, p. 7, 2016.
[11]. P. Embrechts, C. Klüppelberg, and T. Mikosch, Modelling Extremal Events: For Insurance and Finance, vol. 33. Berlin, Germany: Springer-Verlag, 2013.
[12]. R. Böhme and G. Kataria, "Models and measures for correlation in cyber-insurance," in Proc. Workshop Econ. Inf. Secur. (WEIS), 2006, pp. 1–26.
[13]. H. Herath and T. Herath, "Copula-based actuarial model for pricing cyber-insurance policies," Insurance Markets Companies: Anal. Actuarial Comput., vol. 2, no. 1, pp. 7–20, 2011.
[14]. A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, and S. K. Sadhukhan, "Cyber-risk decision models: To insure it or not?" Decision Support Syst., vol. 56, pp. 11–26, Dec. 2013.
[15]. M. Xu and L. Hua. (2017). Cybersecurity Insurance: Modeling and Pricing.
[16]. M. Xu, L. Hua, and S. Xu, "A vine copula model for predicting the effectiveness of cyber defense early-warning," Technometrics, vol. 59, no. 4, pp. 508–520, 2017.
[17]. C. Peng, M. Xu, S. Xu, and T. Hu, "Modeling multivariate cybersecurity risks," J. Appl. Stat., pp. 1–23, 2018.
[18]. M. Eling and N. Loperfido, "Data breaches: Goodness of fit, pricing, and risk measurement," Insurance, Math. Econ., vol. 75, pp. 126–136, Jul. 2017.
[19]. K. K. Bagchi and G. Udo, "An analysis of the growth of computer and Internet security breaches," Commun. Assoc. Inf. Syst., vol. 12, no. 1, p. 46, 2003.
[20]. E. Condon, A. He, and M. Cukier, "Analysis of computer security incident data using time series models," in Proc. 19th Int. Symp. Softw. Rel. Eng. (ISSRE), Nov. 2008, pp. 77–86.