دوازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
12th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

کاربرد درخت خطا در تخصیص بهینه منابع در راستای کاهش ریسک حملات سایبری

محسن خرم[۱]، بابک امیدوار[۲]*، عباس یعقوبی اندرابی[۳]

۱- دانشجو دکتری مهندسی سوانح، دانشکده محیط زیست، دانشگاه تهران mohsenkhorram@ut.ac.ir

۲- دانشیار دانشکده محیط زیست، دانشکده محیط زیست، دانشگاه تهران

۳- دانشجو دکتری مهندسی سوانح، دانشکده محیط زیست، دانشگاه تهران

* نویسنده مسئول Email: bomidvar@ut.ac.ir

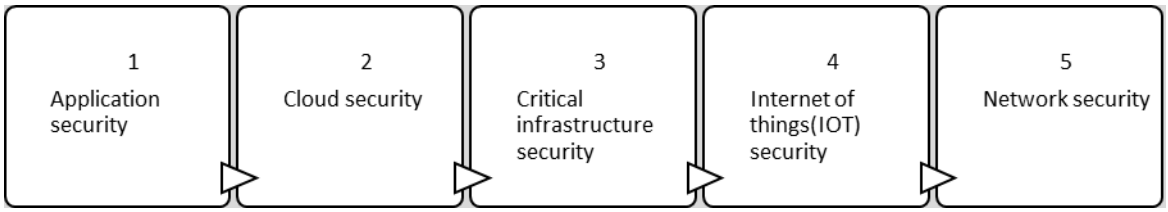
چکیده

افزایش دائمی حملات سایبری نشان می دهد که امنیت سایبری و دفاع در برابر تهدیدات سایبری بایستی در زمان مناسبی انجام شود. در عمل، مقابله به موقع با تعداد زیادی از حملات بدون بررسی عمیق ویژگی های حمله و انجام اقدامات دفاعی هوشمند مربوطه امکان پذیر نیست. در این تحقیق با بررسی تهدیدهای سایبری و دارایی ها، جفت های دارایی و تهدید، تعریف شد و در ادامه تحلیل ریسک تهدید سایبری با استفاده از درخت خطا صورت گرفت و مقدار کاهش ریسک با تخصیص منابع و هزینه کرد(بودجه) موجود مورد بررسی قرار گرفت. برای تحلیل ریسک، نرم افزار MBRA مورد استفاده قرار گرفت. حملات سایبری بسیار نامتقارن هستند، به این معنی که آنها ارزان بوده و به راحتی قابل استفاده هستند و منابع ما برای مقابله با حملات محدود می باشد. در یک مثال فرضی با استفاده از درخت خطا بهترین تخصیص منابع بررسی شد و مشخص گردید، زمانی که کل سرمایه گذاری ۵۰۰۰ دلار هزینه شود، ریسک از ۴۳۵۰۰ به ۲۷۸۰۴ کاهش می یابد.

کلمات کلیدی: امنیت سایبری، تهدید سایبری، تحلیل ریسک، درخت خطا

۱-مقدمه

اینترنت محیطی است که در زمان کنونی همه از آن استفاده می کنند و افرادی که دانش پیشرفته ای از اینترنت دارند، می توانند از افرادی که آنقدرها از فناوری آگاه نیستند سوء استفاده کنند[۱]. این موضوع گاهی اوقات منجر به حملات سایبری به کاربران آسیب پذیری می شود که دانش فنی کمی دارند. از آنجایی که اینترنت برای همه باز است، امنیت امری بسیار ضروری است[۲،۳]. امنیت سایبری[1] کاربرد فناوری‌ها، فرآیندها و کنترل‌ها برای محافظت از سیستم‌ها، شبکه‌ها، برنامه‌ها، دستگاه‌ها و داده‌ها در برابر حملات سایبری است و هدف آن کاهش خطر حملات سایبری و محافظت در برابر بهره برداری غیرمجاز از سیستم ها، شبکه ها و فناوری ها است[۳،۴]. در شکل ۱ پنج مورد از رایج ترین دامنه های امنیت سایبری که بسیار کارآمد هستند آورده شده است. در جدول ۱ نمونه هایی از اکسپلویت های انجام شده در جهان آورده شده است.



شکل ۱: انواع دامنه امنیت سایبری[۵]

جدول ۱: نمونه هایی از اکسپلویت های انجام شده در جهان[۶،۷]

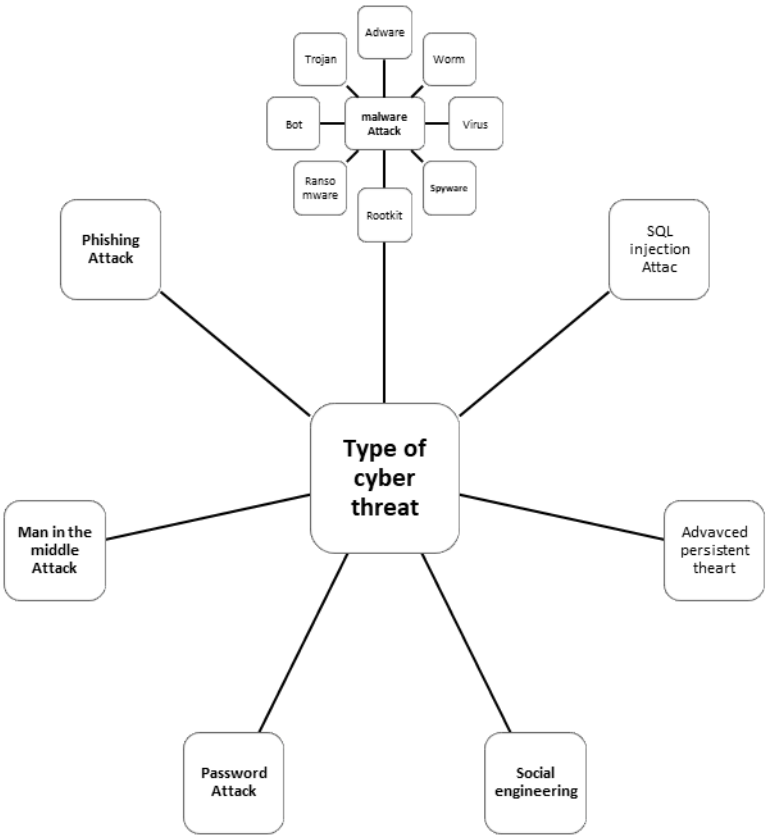
کشور	هدف	ماهیت تهدید	نوع	تاریخ
آمریکا	شبکه نیروگاه هسته ای اوهایو	Slammer Worm	Malware-DoS	۲۰۰۳
	خرابی نیروگاه برق آبی	Sensors Failure	Accident	۲۰۰۵
	تعطیلی نیروگاه هسته ای جورجینا	Installed Software Update	Undefined Software	۲۰۰۸
	شبکه برق ایالات متحده	Reconnaissance	Undefined Software Programs	۲۰۰۹
	ایستگاه پمپاژ اسپرینگ فیلد	Backdoor	Unauthorised Access	۲۰۰۱
	تصفیه خانه آب جورجینا	Physical Breach	Unauthorised Access	۲۰۱۳
	شرکتSolarWinds	security	Malwave	۲۰۲۰
	سیستم رای گیری	Ddos	Malwave	۲۰۲۲
ایران	تاسیسات هسته ای ایران	Stuxnet	Worm	۲۰۰۷
	نیروگاه ها و سایر صنایع	Stuxnet	Worm	۲۰۱۲
	شرکت های زیرساخت (هسته ای، نفتی) و ارتباطات ایران	DdoS	Disruptive	۲۰۱۲
	تاسیسات کلیدی نفت ایران	Computer Virus	Malware	۲۰۱۲
عربستان سعودی	زیرساخت های عربستان در صنعت انرژی	Shamoon	Malware	۲۰۱۲
	کامپیوترها و اهداف دولت عربستان	Shamoon	Malware	۲۰۱۶
	شرکت های پتروشیمی، شرکت ملی صنعتی، شرکت شیمیایی	Shamoon	Malware	۲۰۱۷

[1] Cyber security

قطر	سیستم گاز رسانی	Shamoon	Malware	۲۰۱۲
امارات	بخش انرژی امارات	Trojan Laziok	Malware	۲۰۱۵
استرالیا	بخش آب	Remote Access	Unauthorised Access	۲۰۰۰
کانادا	کمپانی Telvent	Security Breach	Exploited Vulnerability	۲۰۱۲
اوکراین	شرکت برق	BlackEnergy Malware	DdoS	۲۰۱۵
اوکراین	شرکت برق	Petya	Ransomware	۲۰۱۷

۲- تعاریف

تهدید سایبری[۲] به هرگونه حمله مخرب احتمالی اشاره دارد که به دنبال دسترسی غیرقانونی به داده ها، اختلال در عملیات دیجیتال یا آسیب رساندن به اطلاعات است[۸]. تهدیدهای سایبری می‌توانند از بازیگران مختلف، از جمله جاسوسان شرکت‌ها، هکریست‌ها، گروه‌های تروریستی، دولت‌های ملت متخاصم، سازمان‌های جنایتکار، هکرهای تنها و کارمندان ناراضی سرچشمه بگیرند[۹]. در شکل ۲ انواع تهدیدات سایبری بیان شده است.



شکل۲: انواع تهدیدات سایبری[۹]

[2] Cyber threat

همانطور که در شکل ۲ قابل مشاهده است حملات بدافزار به هشت گونه تقسیم شده است که در جدول۲ مورد بررسی قرار گرفتـه شـده اند.

جدول۲: انواع حملات بدافزار[۱۰،۱۱،۱۲]

Adware	یک برنامه رایانه‌ای است که جهت اهداف تبلیغاتی و نشان دادن پیام‌ها و آگهی‌های تبلیغاتی در رایانه افراد طراحـی شده‌اسـت. نحـوه کـار آگهی‌افزارهـا بدین‌گونه است که در پوشش یک نرم‌افزار به ظاهر سالم با اجازه کاربر بر روی سیستم نصب می‌شوند سپس بدون آنکه کاربر متوجه شود در هنگام اتصال به اینترنت به سرورهای خاصی متصل شده و پیام‌های تبلیغاتی را به صورت (pop-up) بر روی صفحه رایانه نمایش می‌دهند.
Trojan	بدافزاری که به نظر یک برنامه معتبر است یا بخشی از سیستم عامل کامپیوتر است، اما در واقع مخرب است. تروجان یک برنامه ی کامپیوتری تهاجمی یا همان بدافزار می باشد. این نوع بدافزار به شکل های مختلف و فریب کاربر وارد کامپیوتر کاربران می شود و به قسمت هایی از کامپیوتر کاربر که بـرای آن برنامه ریزی شده است حمله می کند.
Bot	به طور کلی Bot ها ایجاد شده اند که یک سری از فرایند ها را به صورت خودکار انجام دهند. زمانی که شخص سومی از دیتای یوزرها در دنیای Bot ها استفاده می کند به آن BotNet می گویند. در BotNet ها با حمله هایی همچون Ddos ، Spamها و تبلیغات مختلف به راحتی به سیسـتم شـما وارد می شوند.
Ransomware	نوعی از بد افزار است که اطلاعات کاربران را در داخل سیستم هایشان با ترفند های قفل گذاری کردن، بلاک می کند و با درخواست پول از مالکان دیتـا ها از آنها پول دریافت می کند تا دیتای کاربران را قفل گشایی کند. یکی از مهم ترین دلیلی که به این بد افزار یک باج افزار گفته می شود، همین روند دریافت پول اجباری است که از کاربران درخواست می کند، مهم ترین انگیزه ی این باج افزار پول است.
Rootkit	برنامه‌های کامپیوتری هستند که قدرت بالایی در اختفا دارند و قادر هستند در فایل‌ها، تنظیمات رجیستری یا پردازه‌ها پنهان شوند و به سرقت اطلاعات کاربران بپردازند. به‌طور کلی، روت کیت‌ها با هدف دسترسی از راه دور، کنترل سامانه‌های کـامپیوتری یـا شـبکه‌های کـامپیوتری و اسـتخراج اطلاعـات استفاده می‌شوند.
Spyware	نرم‌افزار جاسوسی یا spyware نوعی برنامه طراحی شده با اهداف خبیثانه است که خرابکار با استفاده از روش‌هایی آن را روی دسـتگاه قربـانی نصـب می‌کند. پس از آلوده شدن سیستم هدف، اطلاعات خصوصی مانند پیامک‌های ردوبدل شده، رمز دوم، شماره کارت، موقعیت مکانی و... ایشـان توسـط هکر برداشت می‌شود که می‌تواند از این اطلاعات برای اهداف خاصی بهره گیرد.
Virus	به صورت کلی ویروس را موجودی می دانند که قابلیت تکثیر شدن دارد و می تواند به راحتی خود را به تعداد زیادی منتشر کند. ویـروس هـا در داخـل برنامه، اسناد، اسکریپت، هارد، سی دی، فلش یا هر چیز دیگری که به سیستم متصل می شود، نفوذ می کند و از طریق همـان وارد سیسـتم کـاربر مـی شود. ویروس ها می توانند برای سرقت اطلاعات، از بین بردن دیتا، آسیب رساندن به سیستم کاربر و ... دیگر به کار گرفته شوند.ویروس قطعه ای از کد رایانه است که خود را در کد یک برنامه مستقل دیگر وارد کرده ، سپس آن برنامه را مجبور به اقدامات مخرب می کند و خود را گسترش می دهد.
Worm	کرم بخش مستقلی از نرم افزار مخرب است که خود را باز تولید کرده و از رایانه به رایانه پخش می شود. این بد افزار با استفاده از روزنه های آسیب پذیر سیستم، وارد آن می شود و به راحتی و بدون دخالت انسانی می تواند تکثیر شود، اما ویروس حتما می بایست با دخالت انسان تکثیر شود.

۳- روش تحقیق

تجزیه و تحلیل درخت خطا[3]یک ابزار گرافیکی برای بررسی دلایل شکسـت‌های سیسـتم اسـت. ایـن روش از منطـق بـول بـرای ترکیـب مجموعه‌ای از رویدادهای سطح پایین استفاده می‌کند و اساساً یک رویکرد از بالا به پایین برای شناسایی خرابی‌هـای سـطح جـز (رویـداد پایه‌ای) است که باعث بروز خرابی در سیستم (رویداد اصلی) می‌شود[۱۳]. در این تحقیق با بررسی تهدیدهای سایبری و دارایی ها، جفت های دارایی و تهدید، تعریف شد و در ادامه تحلیل ریسک تهدید سایبری با استفاده از درخت خطا صورت گرفـت و رابطـه مقـدار کـاهش ریسک با منابع و هزینه کرد(بودجه) موجود مورد بررسی قرار گرفت. برای تحلیل ریسک، نرم افزار MBRA مورد استفاده قرار گرفت.

۴- تحلیل ریسک سایبری

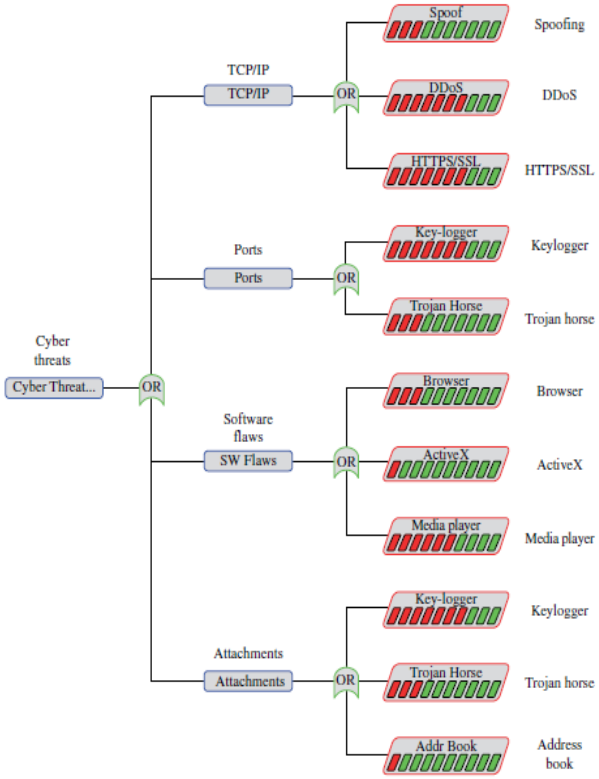
برای تجزیه و تحلیل ریسک سایبری، یک مدل کلی از تهدیدات سایبری که یک سیستم کامپیوتری با آن مواجه اسـت تهیـه شـد و ایـن مدل برای کاهش خطرات پیش روی یک کامپیوتر استفاده شد. با بررسی تهدیدهای سایبری و دارایی ها، جفـت هـای دارایـی و تهدیـد،

[3] Fault Tree Analysis

تعریف شد. دارایی ها شامل TCP/IP، Port، Software flaws و Attachments و تهدیدها شامل Spoofing، DDOS، HTTP/SSL، Keylogger، Trojan horse، Browser، Active X، Media player و Address book است و یک مدل درخت خطا از جفت های تهدید-دارایی تهیه شد(شکل۳). در ادامه تحلیل ریسک تهدید سایبری با استفاده از درخت خطا و در یک مثال فرضی مورد بررسی قرار گرفت. برای ریسک سیستم اینترنت بصورت فرضی دو هزار سیستم در اینترنت در نظر گرفته شد و

مورد تجزیه و تحلیل قرار گرفت.

دارایی(Asset)	تهدید(Threat)
TCP/IP	Spoofing
	DDOS
	HTTP/SSL
Ports	Keylogger
	Trojan horse
Software flaws	Browser
	Active X
	Media player
Attachments	Keylogger
	Trojan horse
	Address book



شکل۳: از سمت راست: مدل درخت خطا، جفت های تهدید و دارایی

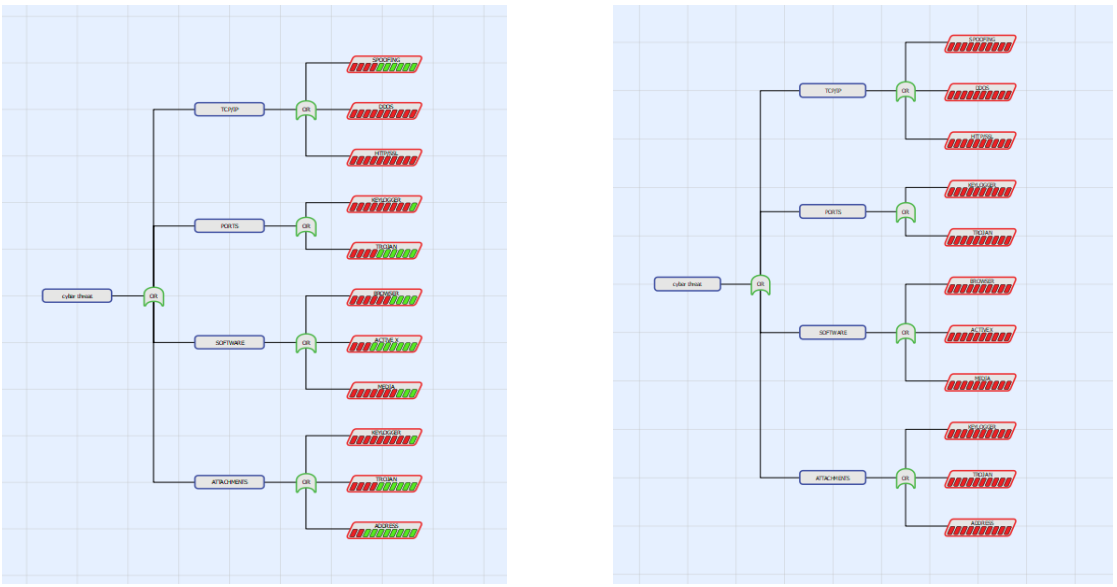
در جدول ۳ برای هر کدام از تهدیدها، احتمال رخ دادن(T)، مقدار آسیب پذیری(V)، مقدار هزینه و مقدار عواقب آن تهدید(C) آورده شده است. در حالت کلی ریسک از رابطه R=TVC محاسبه می شود. اگر حمله کننده رفتار منطقی داشته باشد، T به عنوان خروجی در نظر گرفته می شود. چون دقت می کند که کجا آسیب پذیرتر است و بنابراین در جهت حداکثر کردن ریسک قدم برمی دارد. اما چنانچه

رفتار حمله کننده منطقی نباشد، مثلاً ناشی از یک شرایط تصادفی یا حرکت حماقت آمیز و امثال آن باشد، از روش دیگری تحت عنوان Bayesian Network استفاده می کنیم، این روش بیشتر از آنکه مبتنی بر تحلیل باشد به شواهد تکیه دارد[۱۴].

جدول۳: مقادیر تهدیدات سایبری برای ورود در مدل درخت خطا

تهدید	احتمال تهدید (درصد)	آسیب پذیری (درصد)	هزینه (دلار)	عواقب (دلار)
Spoof	۱۰۰	۵۰	۲۵۰۰	۱۰۰۰۰
DDOS	۶۰	۵۰	۵۰۰۰	۱۰۰۰۰
HTTP/SSL	۸۰	۵۰	۵۰۰۰	۱۰۰۰۰
Keylogger	۹۰	۵۰	۵۰۰۰	۱۰۰۰۰
Trojan horse	۸۰	۵۰	۲۰۰۰	۱۰۰۰۰
Browser	۶۰	۵۰	۲۰۰۰	۱۰۰۰۰
Active X	۶۰	۵۰	۱۰۰۰	۱۰۰۰۰
Media player	۱۰۰	۵۰	۴۰۰۰	۱۰۰۰۰
Address book	۷۰	۵۰	۱۰۰۰	۱۰۰۰۰

در جدول۳ همه پیامدها ۱۰۰۰۰ دلار، همه آسیب پذیری ها ۵۰٪ فرض شده است، با توجه به شکل ۵ بهترین استفاده از منابع مالی هزینه شده برای کاهش ریسک در این درخت خطا مشخص شده است. زمانی که کل سرمایه گذاری ۵۰۰۰ دلار هزینه شد، ریسک از ۴۳۵۰۰ به ۲۷۸۰۴ کاهش می یابد. اطلاعات کلی درباره کاهش ریسک مربوط به تهدیدها در جدول۴ آورده شده است.



شکل۵: خروجی نرم افزار MBRA برای مدل درخت خطا: از راست: قبل از اعمال هزینه، بعداز اعمال هزینه ۵۰۰۰دلاری

جدول۴: اطلاعات کلی درباره کاهش ریسک مربوط به تهدیدها(خروجی نرم افزارMBRA)

Name	Threat	Vulnerability	Elimination Cost	Consequence	Risk Initial	Allocation	Vulnerability Reduced	Risk Reduced
SPOOFING	100	50	2500	10000	10000	1474.24	17.09	1709.17
DDOS	60	50	5000	10000	3000	0	50	3000
HTTP/SSL	80	50	5000	10000	4000	0	50	4000
KEYLOGGER	90	50	5000	10000	4500	18.24	49.58	4462.37
TROJAN	80	50	2000	10000	4000	702.6	22.27	1781.39
BROWSER	60	50	2000	10000	3000	452.07	29.71	1782.74
ACTIVE X	60	50	1000	10000	3000	527.24	14.85	891.01
MEDIA	100	50	4000	10000	5000	587.03	35.66	3566.25
KEYLOGGER	90	50	5000	10000	4500	17.63	49.6	4463.61
TROJAN	80	50	2000	10000	800	702.16	10	800
TROJAN	80	50	2000	10000	4000	702.16	22.28	1782.29
ADDRESS	70	50	1000	10000	3500	592.79	12.77	893.88

۵-نتیجه گیری

مجموعه وسیعی از تهدیدات حفاظت را بسیار دشوار وگران می کند. در واقع اکثر اپراتورهای سیستم کامپیوتری هرگز تحلیل ریسک دقیقی از سیستم های تحت مراقبت آنها انجام ندادند. با توجه به حرکت جوامع به سمت شبکه شدن و خودکار شدن فعالیت های روزانه وابستگی به سیستم های کامپیوتری راه دور افزایش یافته است. حملات سایبری بسیار نامتقارن هستند، به این معنی که آنها ارزان و به راحتی قابل استفاده هستند و منابع ما برای مقابله با حملات محدود می باشد. با استفاده از درخت خطا بهترین تخصیص منابع مدل شد و مشخص شد، زمانی که کل سرمایه گذاری ۵۰۰۰ دلار هزینه شد، ریسک از ۴۳۵۰۰ به ۲۷۸۰۴ کاهش می یابد.

۶-منابع

[1] Stevens T. Cyber security and the politics of time. Cambridge University Press; 2016.

[2] Goutam RK. Importance of cyber security. International Journal of Computer Applications. 2015 Jan 1;111(7).

[3] Sun CC, Hahn A, Liu CC. Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems. 2018 Jul 1;99:45-56.

[4] Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. 2021 Nov 1;7:8176-86.

[5] Ghelani D. Cyber security, cyber threats, implications and future perspectives: A Review. Authorea Preprints. 2022 Sep 22.

[6] Al-Mhiqani MN, Ahmad R, Abidin ZZ, Yassin WM, Hassan A, Mohammad AN, Clarke NL. A new taxonomy of insider threats: an initial step in understanding authorised attack. International Journal of Information Systems and Management. 2018;1(4):343-59.

[7] Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. 2021 Nov 1;7:8176-86.

[8] Conti M, Dargahi T, Dehghantanha A. Cyber threat intelligence: challenges and opportunities. Springer International Publishing; 2018.

[9] Tanwar S, Paul T, Singh K, Joshi M, Rana A. Classification and imapct of cyber threats in India: a review. In2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) 2020 Jun 4 (pp. 129-135). IEEE.

[10] Rieck K, Holz T, Willems C, Dussel P, Laskov P. Learning and classification of malware behavior. Lecture Notes in Computer Science. 2008 Jul 10;5137:108-25.

[11] McLaughlin N, Martinez del Rincon J, Kang B, Yerima S, Miller P, Sezer S, Safaei Y, Trickel E, Zhao Z, Doupé A, Joon Ahn G. Deep android malware detection. InProceedings of the seventh ACM on conference on data and application security and privacy 2017 Mar 22 (pp. 301-308).

[12] Ab Razak MF, Anuar NB, Salleh R, Firdaus A. The rise of “malware”: Bibliometric analysis of malware study. Journal of Network and Computer Applications. 2016 Nov 1;75:58-76.

[13] Vesely WE, Goldberg FF, Roberts NH, Haasl DF. Fault tree handbook. Nuclear Regulatory Commission Washington DC; 1981 Jan 1.

[14] Scutari M, Denis JB. Bayesian networks: with examples in R. Chapman and Hall/CRC; 2021 Jul 28.