Cyber Threats Prediction System Using Artificial Intelligence

Dr. Md. Atheeq Sultan Ghori

Associate Professor, Department of Computer Science & Engineering, Telangana University, Nizamabad.

Received: 06.01.2024 Revised : 13.01.2024 Accepted: 24.01.2024

ABSTRACT
Worldwide digital goes after essentially influence the economy, society, associations, and people. Existing examination on digital assaults needs showing Man-made brainpower (simulated intelligence) based insightful answers for giving far reaching digital danger knowledge. Digital planners at a public level require man-made intelligence-based choice emotionally supportive networks for choosing a country's digital stance or readiness. This paper proposes a simulated intelligence-based arrangement that independently gathers multi-faceted digital assault information via virtual entertainment posts on digital related objection. The proposed framework gives basic logical capacity in the digital danger range and uses modern artificial intelligence-based calculations for peculiarity recognition, expectation, opinion examination, area discovery, interpretation, and so on.

Keywords: Cyber threat, intelligence Cyber threat prediction, Decision support system, Cyber anomaly detection,Cyber-attack dashboard, Social-media analysis.

INTRODUCTION

Overall Digital assaults had cost just about 1.5 trillion USD to worldwide economy in 2020 Cybercrimes are projected to cost as much as 12.6 trillion USD yearly by 2025. Bigger economies like China, Brazil, US, India, Mexico, France, Australia and, surprisingly, Joined Bedouin Emirates experience the ill effects of billions of dollars in customer misfortune through cybercrimes. For instance, China's purchaser misfortune through digital wrongdoing was 72.3 billion USD in 2017. Other than making monetary misfortunes, Digital assaults has adverse impact at social and mental level contacting the existences of person. For instance, as of late one of Australia's telecom monster, Optus have been presented to information break because of digital assault, which has made huge pressure and outrage on shoppers. Due to this digital assault, data of Optus clients have been uncovered causing trouble among 3.2 million buyers. Most as of late, touchy patient data that incorporate clinical determination and technique were taken by digital hoodlums from Australia's number 1 wellbeing guarantor. Consequently, digital wrongdoing is one of the most basic worries of current countries, states, associations, and people.

To decrease the effect of digital violations two basic commands are conglomeration of digital related information and modern scientific calculations to recognize and dissuade dangers. The necessities of digital information have been depicted in late exploration works. Then again, the necessity of Man-made brainpower based modern scientific calculations have been exhibited. While computer-based intelligence can be utilized to direct complex digital assaults, simulated intelligence can likewise be utilized in recognizing digital assault as exhibited. Notwithstanding, none of these current written works give country-level authentic digital insights, country level digital expectation, and irregularity location with artificial intelligence.

LITERATURE OF REVIEW

Existing written works in Digital Danger knowledge basically centered around an authoritative viewpoint, where digital assault affected a singular association for monetary or political advantage by the culprit 12]. While these viewpoint serves the worries of an individual hierarchical substance, this doesn't provide food the need of political heads of states having a wholistic view on their country. Public level worry on digital assault requires expansive digital danger knowledge that incorporates assault range covering a singular country alongside different nations in the globe for benchmarking reason. Utilizing this wholistic perspective on all the digital assault measurements for a country in correlation with different nations permits the political leader to decide their stance on digital safeguard. For instance, on the off chance that Australia is confronting surprisingly larger number of digital assaults contrasted with different countries like New Zealand, Joined Middle Easterner Emirates, Malaysia, then, at that point, Australia ought to put

their Digital protection pose at a more elevated level. Vast digital danger knowledge is basic for a country's Digital Readiness.

Existing exploration additionally experiences not using artificial intelligence based completely automated information obtaining procedures like Web Scratching, Element Discovery for Area Knowledge, Opinion Examination as their information prerequisites were essentially centered around interruption recognitions inside the organization. Accordingly, a large portion of the current examinations as shown in [16], were just getting Organization Traffic Information. Concentrate in [18] utilized mimicked sensor information on digital actual framework. Then again, scientist in [30] utilized overview information gathered from 294 members. None of these current examination works, acquired digital danger information from various sources like Digital assault measurements for every one of the nations from Against Infection Programming sellers or Digital related objection from live online entertainment posts. Virtual entertainment information on international pertinence requires artificial intelligence-based information obtaining and pre-handling as exhibited in our new papers [31]. As virtual entertainment contents were gotten, our clever philosophy showed in [34], applied artificial intelligence based Named Substance Acknowledgment (NER) for extricating geospatial knowledge, opinion examination for removing emotional pertinence of the substance, dynamic interpretation to comprehend web-based entertainment contents in 121 unique dialects.

Existing writing exhibits that there have been a developing interest utilizing man-made intelligence-based Inconsistency location and other profound learning procedures for distinguishing digital assault [16]. Nonetheless, inside these examinations Abnormality discovery has been utilized on Organization Traffic information for distinguishing interruptions. Peculiarity discovery calculations have never been accounted for to be utilized on far reaching digital assault insights.

At last, practically none of the current writing on digital assault supportive of vided intelligent dashboards that refreshes itself naturally for favorable to viding proof put together choices with respect to digital stance for key heads of a country. Since an essential leader needs to go with moment choices, the dashboards are expected to be accessible in a great many stages that incorporates versatile, tablet or conventional work areas. Existing exploration work on Digital assault portrayed in [13] were not accessible a large number of stages like Windows, iOS, or Android. It ought to be referenced that the necessity of key leaders to go with moment choice on a great many stages like cell phone running iOS or Android have been shown in [35]. Table 1, sums up the bottleneck of existing examinations and obviously exhibits how the arrangement introduced in this paper means to address these weaknesses.

MATERIAL & METHODS

Multi-layered Worldwide Digital Assault information is gained utilizing a mix of Work area Stream and Cloud Stream in Power Mechanize [31]. The Work area stream utilizes unattended Power Computerize Work area stream for mechanizing a progression of undertakings. This mechanization opens up program, goes to 8 unique connections [23] downloads 8 different assault insights documents, and saves these records into assigned One Drive for business envelope. With each new document creation, a trigger starts a different Microsoft Power Mechanize cloud stream that processes these assault measurements and stores them in Microsoft Dataverse [43]. In this way, by utilizing Work area stream and Cloud Stream, the introduced framework naturally and namelessly refreshes itself on an everyday timetable with day to day digital measurements gave by [22]. It ought to be noticed that the Kaspersky's locales in [24] doesn't give admittance to authentic information. Consistently, the everyday digital insights are supplanted with refreshed measurements. Consequently, the introduced framework fabricates verifiable digital measurements consistently (i.e., not progressively). Be that as it may, the introduced framework would uphold ongoing updates (utilizing a similar innovation pile of Microsoft Power Mechanize), when the digital assault measurements are given progressively (by the information sources).

Then again, web-based entertainment posts from Twitter are extricated utilizing Microsoft Power Robotize stream. During these extractions simulated intelligence-based Feeling Examination, NER, Interpretation is proceeded as portrayed in our latest exploration [35]. At last, these records are put away in Microsoft SQL Server Data set.

Microsoft Power BI acquires both these information sources (i.e., multi-layered digital danger information of Kaspersky and digital related web-based entertainment posts from Twitter) to give information examination and information perceptions for the essential leaders in iOS, Windows, and Android stages. Fig. 2 portrays this general interaction. Moreover, Table 2 give subtleties into different innovation parts utilized inside the proposed framework alongside legitimizations. Table 2 alludes to individual elements that was given inside Table 1 and guides those highlights to innovation parts.

As it shows in following table, man-made intelligence-based oddity discovery is the key innovation engaging the choice investigation. The oddity discovery adds extra component to line diagrams via

consequently recognizing abnormalities inside time-series information. It additionally gives Normal Language Handling (NLP) based [48] clarifications for the inconsistencies working with main driver investigation. In our latest review, we have involved computer-basedintelligence-based irregularity discovery for recognizing unusual instances of avalanches alongside the main drivers [39], irregularities of calamity occasions from virtual entertainment posts [36], peculiarities on worldwide occasions by observing 2397 worldwide news sources [31] and, surprisingly, on Coronavirus situational mindfulness [43]. Prior to digging into the subtleties of abnormality identification, we present the issue definition.

Table 1. Technology components used for automation

Technology component	**Purpose**	**Supported feature**
Microsoft Power Automate	• Capturing Tweets related to Cyber • AI-based Translation • AI-based Sentiment Analysis • AI-based Named Entity Recognition	• Feature 1 (Country-Wide) • Feature 2 (data acquisition) • Feature 3 (multisource data)
Microsoft Desktop Automate	• Unattended Robotic Process Automation for acquiring Cyber-attack data from 8 different sources and saving them as .xlsx files within Microsoft OneDrive	• Feature 1 (Country-Wide) • Feature 2 (data acquisition) • Feature 3 (multisource data)
Microsoft Power BI	• AI-Based Anomaly Detection • Exponential Smoothing Prediction • Dashboard for Windows • iOS App • Android App	• Feature 4 (Use of AI/CNN) • Feature 5 (Dashboard) • Feature 6 (Dashboard) • Feature 7 (Multi-Platform)
Microsoft Dataverse	• Storage of Daily Cyber Attack Statistics	• Feature 1 (Country-Wide) • Feature 2 (data acquisition)
Microsoft SQL Server	• Storage & Management of Tweets	• Feature 1 (Country-Wide) • Feature 2 (data acquisition)

Issue 1. Given a grouping of genuine qualities, or at least, $x = x_1, x_2, x_3, \ldots, xn$, the undertaking of time-series irregularity recognition is to create a result succession $y = y_1, y_2, y, \ldots, y_n$, where $y_i \in \{0, 1\}$ signifies whether xi is a peculiarity point.

The executed arrangement acquired the Ghastly Lingering (SR) from the visual saliency discovery space and afterward applied a Convolutional Brain Organization (CNN) to the outcomes delivered by the SR model [50]. The SR calculation comprises of three significant stages:

1. Perform Fourier change to acquire the log plentifulness range.
2. Ascertain the SR.
3. Perform reverse Fourier change, which changes the arrangement back to the spatial area.

$(f) = Amplitude\ (f\ (x))$ (1)

$P\ (f) = P\ hrase\ (f\ (x))$ (2)

$(f) = log\ ((f))$ (3)

$(f) = h_q\ (f)\ .L(f)$ (4)

$(f) = (f) - AL(f)$ (5)

$S\ (x) = \|\mathrm{f}^{-1}(\exp\ (R(f) + iP\ (f)))\|$ (6)

where f and f 1 signify the Fourier change and opposite Fourier change, individually; x is the information arrangement with shape nX1; $A(f\ )$ is the abundancy range of arrangement x; $P\ (f\ )$ is the relating stage range of arrangement x; $L(f\ )$ is the log portrayal of $A(f\ )$; what's more, $AL(f\ )$ is the typical range of $L(f\ )$, which can be approximated by tangling the info succession by $hq\ (f\ )$, where $hq\ (f\ )$ is a $q \times q$ lattice characterized as:

$$\mathrm{h_q(f)} = \frac{1}{\mathrm{q}^2}\begin{bmatrix} 1 & 1 & \cdots 1 \\ 1 & 1 & \cdots 1 \\ \cdots & \vdots & \ddots 1 \\ 1 & 1 \cdots & 1 \end{bmatrix}$$

( ) is the SR, that is to say, the log range $L(f)$ short the found the middle value of log range $AL(f)$. The SR fills in as a compacted portrayal of the grouping, while the development a piece of the first succession turns out to be more huge. Last, the succession was moved back to the spatial space utilizing a converse Fourier change. The resultant grouping $S(x)$ is alluded to as the saliency map [51]. The upsides of the abnormality focuses are determined as follows:
where x is the neighborhood normal of the first places, mean and var are the mean and fluctuation of all focuses inside the ongoing sliding window, and $r \sim N$ (0, 1) is haphazardly inspected. In this cycle, CNN is applied to the saliency map rather than to the crude information, hence expanding the proficiency of the general course of irregularity discovery [50,51]. As a matter of fact, we carry out oddity discovery in three stages utilizing Microsoft Power BI's Line Graph perception [40]:

- Distinguish every one of the peculiarities inside the time series (i.e., any qualities that lie outside the edge range). For the inconsistency discovery process, all the country explicit assault measurements (i.e., time-series information) was utilized. Microsoft Power BI's line outline perception utilizes CNN (counting Fourier change, SR, and opposite Fourier Change) to perform abnormality recognition on the country explicit assault insights.
- Distinguish the primary drivers of these irregularities. To get the principaldrivers both web-based entertainment information and digital assault insights from Kaspersky (i.e., [20]) were used.
- Make sense of the outcomes in a characteristic language (clarification of the underlying driver) utilizing NLP [48].

As seen in above table, the introduced framework utilizes a remarkable smoothing calculation for foreseeing nation level digital assaults. Remarkable smoothing is a noticeable and proficient time series determining strategy, dexterously adjusted to the domain of digital assault expectation [53, 54]. Through the guileful interaction of weighted midpoints, this calculation insightfully distinguishes patterns and dormant examples installed inside authentic digital assault information. By iteratively recalculating gauges and proficiently regulating the smoothing boundary, the calculation nimbly changes its prescient ability to oblige worldly priority while constricting the impact of authentic information [55]. With due perception of information quality and amount, and the faithfulness of hidden digital assault designs, the viability of this technique (i.e., dramatic smoothing) tries to enlighten the future scene of digital dangers with accuracy and intelligence.

4. RESULTS

The proposed procedure was conveyed and executed utilizing various parts of Microsoft Power Stage as depicted in the past segment from 11 October 2022 till 31 October 2022.

Table 2. Number of daily multidimensional cyber- threat statistics downloaded from 10January 2023 till 31January 2023 using the proposed system.

Exploit	Local infection	Malicious mail	Network attack	On-Demand scan	Ransomware	Spam	Web threat	Count of attack statistics
185	194	185	186	194	142	161	194	1441
185	194	185	186	194	142	161	194	1441
183	194	188	184	194	147	155	194	1439
178	194	191	185	194	151	159	194	1446
185	194	189	185	194	149	162	194	1452
181	194	186	184	194	139	162	194	1434
181	194	174	181	194	130	177	194	1425
180	194	173	173	193	128	176	194	1411
184	194	191	187	194	146	176	194	1466
184	194	191	187	194	146	176	194	1466
179	194	190	185	194	150	179	194	1465
181	194	188	184	193	143	169	194	1446
177	194	182	183	194	134	163	194	1421
176	194	170	178	194	138	163	193	1406
178	194	166	175	193	124	167	194	1391
183	194	188	187	194	144	175	194	1459
181	194	193	184	194	142	174	194	1456
182	194	186	188	194	146	160	194	1444
184	194	187	186	194	144	156	194	1439

185	194	186	186	194	143	168	194	1450
183	193	175	179	194	129	158	194	1405
3815	4073	3864	3853	4071	2957	3497	4073	30 203

Table 3. Number of daily cyber related tweets captured and processed with AI services from 12January 2023 till 31 January 2022 using the proposed system.

No. of twitter ID	No. of user ID	No. of locations	No. of tweet languages	Retweets	Average negative sentiments	Average neutral sentiments	Average of positive sentiments	No. of translations
52	51	29	7	80 707	0.398	0.422	0.180	12
211	189	122	15	77 089	0.399	0.402	0.199	67
219	208	116	18	408 635	0.292	0.461	0.247	74
208	205	111	18	428 407	0.312	0.442	0.246	67
221	208	122	14	188 791	0.295	0.464	0.240	60
186	180	101	18	49 255	0.315	0.492	0.193	56
226	219	133	18	132 222	0.354	0.421	0.225	55
216	215	123	17	231 915	0.321	0.469	0.210	51
206	204	129	17	533 082	0.434	0.413	0.152	37
219	209	118	14	134 067	0.409	0.401	0.190	46
223	207	116	18	34 249	0.333	0.466	0.200	69
226	218	128	16	88 944	0.440	0.353	0.206	59
227	219	118	20	200 700	0.434	0.403	0.164	46
219	205	113	13	30 097	0.375	0.413	0.211	48
222	219	121	14	175 143	0.339	0.423	0.238	47
218	212	124	14	287 112	0.388	0.377	0.235	48
224	215	126	14	176 450	0.414	0.356	0.230	41
222	215	114	12	217 949	0.351	0.457	0.208	48
209	205	113	18	252 942	0.322	0.480	0.199	55
3998	3607	1643	38	3 727 756	0.363	0.426	0.210	941

During this time, 30,203 records on worldwide digital assault measurements covering exploit, nearby disease, malevolent mail, network assault, on-request examine, ransomware, spam and web danger were naturally caught utilizing Microsoft Power Mechanize and Microsoft Dataverse. Table 3 gives nitty gritty insights on these 30K records. Every one of the segments Table 3, beginning from Exploit to Web Danger day to day insights consequently brought by the introduced framework from Kaspersky's statement measurements URL (i.e., https://statistics.securelist.com/) for 8 distinct kinds of digital dangers (i.e., Exploit, Neighborhood Contamination, Noxious Mail, Organization Assault, On-Request Output, Ransomware, Range, and Web Danger). The Day-to-day accumulation of these 8 sorts of dangers is given in ''Count of Assault Measurements'' segment of Table 3.

Also, our execution with Microsoft Power Robotize and Microsoft SQL Server, consequently gathered 3813 Tweets from 3513 unmistakable Tweet clients. As seen from above table, these tweets were automatically handled with simulated intelligence-based calculations to fathom Tweets in 37 unmistakable dialects. 893 Non-English Tweets were likewise deciphered powerfully. The segment ''No. of Interpretations'' shows the number of non-English Tweets that were caught every day with resulting interpretation and investigation (with opinion examination). This section (i.e., number of interpretation) connotes the ability and limit of the introduced sys-tem in fathoming multi-lingual tweets for a more thorough situational mindfulness. Point by point feeling examination uncovered that the most noteworthy pessimistic opinion (with a typical pessimistic feeling of 0.44) were noted on 24 October 2022, when many individuals were unglued about late digital assaults on Australia's telecom and medical coverage suppliers.

While Table 3 shows the insights relating to digital assault information, Table 4 exhibits measurements on the examined web-based entertainment information. The introduced framework began acquiring online entertainment information from 12January 2023 rather than 10January 2023. Consequently, the beginning date of both table contrasts by 2 days. It ought to be noticed that digital related data (either genuine assault information or information got through web-based entertainment) changes on an

everyday premise depending geo-political, social, military, and conciliatory elements. These changing elements of digital related information gives totally unique man-made intelligence driven experiences as detailed in late writings [56].

CONCLUSION

The predominant digital knowledge dashboards, as reported in trustworthy sources [11-19], are burdened with various deficiencies. Such impediments envelop the shortage of nation level verifiable digital assault insights, the inadequacy to anticipate country-explicit digital dangers, and failure of utilizing CNN put together irregularity recognition procedures with respect to country-level digital ranges. Considering these lacks, the introduced academic work presents a cutting edge and shrewd arrangement that successfully redresses all the previously mentioned deficiencies intrinsic in existing digital knowledge frameworks. The proposed arrangement outfits a widely inclusive appreciation of digital dangers across the globe. Utilizing a bunch of dashboards accessible in all stages (iOS, Android, and Windows), an essential leader can play out the accompanying:

- Examine and analyze the digital dangers among quite a few nations on the planet
- Break down and look at the digital danger of a nation by time
- Recognize or identify abnormalities inside the digital danger range for any nations
- Anticipate digital dangers for any nations
- Fundamentally Break down the perspectives via Virtual Entertainment clients on digital related issues

Utilizing the introduced framework, a vital digital expert would have the option to dissect multi-faceted digital dangers for any nations and as needs be suggest fitting digital stance. The general expectation blunder utilizing the real information till 3 August 2023 was estimated to be not as much as Root-mean-square deviation (RMSE) 0.19 utilizing Eq. (9). This shows somewhat more elevated level of forecast exactness's contrasted with existing frameworks digital danger expectation frameworks [54,56].

$$RMSE = \sqrt{\frac{\sum_{i=1}^{N} ||y(i) - \hat{y}(i)||^2}{N}} \quad (9)$$

Late exploration in artificial intelligence-based Twitter talk examination has uncovered that web-based entertainment investigation experiences different difficulties, including issues connected with information quality, falsehood, counterfeit client accounts, and moral worries [60]. In this review, it was expected that every one of the 30,203 tweets began from certified Twitter clients' records. In any case, it is essential to take note of that continuously, tweets can be created by counterfeit clients [61] and may contain misdirecting data [61].

Besides, while researching the constraints of Virtual Entertainment Investigation with a particular spotlight on Twitter, this concentrate intensely depended on the utilization of continuous Tweet Programming interface, Microsoft Power Stage, and Microsoft Purplish blue. Every one of these stages requires steady monetary venture, commonly worked with through Visa exchanges. For example, an essential membership to the Twitter Programming interface, which awards admittance to a month-to-month portion of just 10,000 tweets, causes an expense of $100 USD each month. Extending this remittance to cover 1 million tweets fundamentally expands the monetary obligation to a significant $5000 USD each month. Because of these monetary imperatives, the exploration's degree was definitely confined, focusing exclusively on a restricted example of tweets.

In future, we might want to foster imaginative calculations for creating country-wise digital danger files simply from the online entertainment information utilizing more vigorous and present-day toolset. For instance, Microsoft as of late sent off Microsoft Texture that will be that incorporates strong and high-level information warehousing, information designing, AI, information science, and perception capacity. Utilizing these inventive stages, we imagine to utilize profound learning procedures like Repetitive Brain Organization (RNN), Auto-encoders and others. Since this study began to catch digital related web-based entertainment posts from 13 October 2022, making of country-wise digital danger record would be an expansion to this examination. Consolidating the virtual entertainment driven digital danger lists alongside digital assault information from hostile to infection merchants would give substantially more complete perspective on worldwide digital dangers.

REFERENCES

[1] F. Cremer, B. Sheehan, M. Fortmann, A.N. Kia, M. Mullins, F. Murphy, S. Materne, Cyber risk and cybersecurity: A systematic review of data availability, Geneva Pap. Risk Insur. - Issues Pract. 47 (2022) 698–736.

[2] Cybercrime Magazine, Cybercrime to cost the world $10.5 trillion annually by 2025, 2020, [Online]. Available: Accessed152022.

[3] Statista Research Department, Consumer loss through cybercrime worldwide in 2017, by victim country, 2022, [Online]. Available: Accessed262022.
[4] M. Bada, J.R. Nurse, Chapter 4 - the social and psychological impact ofcyberattacks, in: V. Benson, J. Mcalaney (Eds.), Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press, 2020, pp. 73–92.
[5] BBC, News: optus: how a massive data breach has exposed australia, 2022, [Online]. Available: Accessed162022.
[6] Australian Securities & Investments Commissions, Guidance for consumers impacted by the optus data breach, 2022, [Online]. Available: Accessed192022.
[7] K. Merritt, Optus confirms 2.1 million customers affected by cyberattack, total telecom, 2022, [Online]. Available: Accessed232022.
[8] B. Kaye, Australia's (1) health insurer says hacker stole patient details, reuters, 2022, [Online]. Available: Accessed252022.
[9] A. Zibak, A. Simpson, Cyber threat information sharing: Perceived benefits and barriers, in: ARES '19: Proceedings of the 14th International Conference onAvailability, Reliability and Security, 2019.
[10] B. Guembe, A. Azeta, S. Misra, V.C. Osamor, L. Fernandez-Sanz, V. Pospelova, The emerging threat of ai-driven cyber attacks: A review, Appl. Artif. Intell. 36 (1) (2022) 36.
[11] M. Tetaly, P. Kulkarni, Artificial intelligence in cyber security – a threat or a solution, in: AIP Conference Proceedings, Vol. 2519, 2022.
[12] S. Xu, Y. Qian, R.Q. Hu, Data-driven network intelligence for anomaly detection, IEEE Netw. 33 (3) (2019) 88–95.
[13] M. Keshk, E. Sitnikova, N. Moustafa, J. Hu, I. Khalil, An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems, IEEE Trans. Sustain. Comput. 6 (1) (2021) 66–79.
[14] M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L.F. Capretz, S.J. Abdulkadir, Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review, Electronics 11 (2) (2022) 198.
[15] I.A. Gheyas, A.E. Abdallah, Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis, Big Data Anal. 1 (6) (2016).
[16] C.-W. Ten, J. Hong, C.-C. Liu, Anomaly detection for cybersecurity of the substations, IEEE Trans. Smart Grid 2 (4) (2011) 865–873.
[17] J. Yang, C. Zhou, S. Yang, H. Xu, Anomaly detection based on zone partition for security protection of industrial cyber-physical systems, IEEE Trans. Ind. Electron. 65 (5) (2018) 4257–4267.
[18] D. Shi, Z. Guo, K.H. Johansson, L. Shi, Causality countermeasures for anomaly detection in cyber-physical systems, IEEE Trans. Automat. Control 63 (2) (2018) 386–401.
[19] J. Kotsias, A. Ahmad, R. Scheepers, Adopting and integrating cyber-threat intelligence in a commercial organisation, Eur. J. Inf. Syst. (2022) 1–17, Available Online at https://www.tandfonline.com/doi/full/10.1080/0960085X. 2022.2088414.
[20] Kaspersky, Cyber threat statistics, 2023, [Online]. Available: Accessed32023.
[21] Kaspersky, Daily ransomware cyber threat statistics, 2023, [Online]. Available: Accessed32023.
[22] Kaspersky, Daily exploit cyber threat statistics, 2023, [Online]. Available: Accessed032023.
[23] Kaspersky, Daily web threats cyber threat statistics, 2023, [Online]. Available: Accessed32023.
[24] Kaspersky, Daily spam cyber threat statistics, 2023, [Online]. Available: Accessed32023.
[25] Kaspersky, Daily mailicious mail cyber threat statistics, 2023, [Online]. Available: Accessed32023.
[26] Kaspersky, Daily network attack cyber threat statistics, 2023, [Online]. Available: Accessed32023.
[27] Kaspersky, Daily local infections cyber threat statistics, 2023, [Online]. Available: Accessed32023.
[28] Kaspersky, Daily on-demand cyber threat statistics, 2023, [Online]. Available: Accessed32023.
[29] A.K. Dey, G.P. Gupta, S.P. Sahu, A metaheuristic-based ensemble feature selection framework for cyber threat detection in IoT-enabled networks, Decis. Anal. J. 7 (2023) 100206.
[30] N.F. Khan, N. Ikram, S. Saleem, S. Zafar, Cyber-security and risky behaviors in a developing country context: A pakistani perspective, Secur. J. (2022) 1–33, Available at https://link.springer.com/content/pdf/10.1057/s41284-022-00343- 4.pdf.
[31] F.K. Sufi, M. Alsulami, Automated multidimensional analysis of global events with entity detection, sentiment analysis and anomaly detection, IEEE Access 9 (2021) 152449–152460.
[32] F.K. Sufi, AI-GlobalEvents: A software for analyzing, identifying and explaining global events with artificial intelligence, Softw. Impacts 11 (2022) 100218.
[33] F.K. Sufi, M. Alsulami, A. Gutub, Automating global threat-maps generation via advancements of news sensors and AI, Arab. J. Sci. Eng. (2022) 1–18, Available at

https://link.springer.com/content/pdf/10.1007/s13369-022-07250-1.pdf.
[34] F.K. Sufi, Identifying the drivers of negative news with sentiment, entity and regression analysis, Int. J. Inf. Manag. Data Insights 2 (1) (2022) 100074.
[35] F. Sufi, M. Alsulami, A novel method of generating geospatial intelligence from social media posts of political leaders, Information 13 (3) (2022) 120.
[36] F. Sufi, I. Khalil, Automated disaster monitoring from social media posts using AI based location intelligence and sentiment analysis, IEEE Trans. Comput. Soc. Syst. (2022) 1–11, http://dx.doi.org/10.1109/TCSS.2022.3157142, Early Access.
[37] F. Sufi, M. Alsulami, AI-based automated extraction of location-oriented COVID-19 sentiments, Comput., Mater. Continua (CMC) 72 (2) (2022) 3631–3649.
[38] F. Sufi, I. Razzak, I. Khalil, Tracking anti-vax social movement using AI based social media monitoring, IEEE Trans. Technol. Soc. 3 (4) (2022) 290–299.
[39] F.K. Sufi, M. Alsulami, Knowledge discovery of global landslides using automated machine learning algorithms, IEEE Access 9 (2021).
[40] F.K. Sufi, AI-landslide: Software for acquiring hidden insights from global landslide data using artificial intelligence, Softw. Impacts 10 (100177) (2021).
[41] F. Sufi, E. Alam, M. Alsulami, Automated analysis of Australian tropical cyclones with regression, clustering and convolutional neural network, Sustainability 14 (2022) 9830.
[42] F. Sufi, A decision support system for extracting artificial intelligence-driven insights from live twitter feeds on natural disasters, Decis. Anal. J. 5 (2022) 100130.
[43] F. Sufi, Automatic identification and explanation of root causes on COVID-19 index anomalies, MethodX 10 (2023) 101960.
[44] S. Ainslie, D. Thompson, S. Maynard, A. Ahmad, Cyber-threat intelligence for security decision-making: A review and research agenda for practice, Comput. Secur. 132 (2023) 103352.
[45] Microsoft Documentation, Microsoft power automate, 2021, [Online]. Available: Accessed292021.
[46] Microsoft, Microsoft dataverse, 2022, [Online]. Available: Accessed252022.
[47] Microsoft, Microsoft power bi documentation, 2022, [Online]. Available: Accessed212022.
[48] Microsoft Documentation, Choosing a natural language processing technology in azure, 2020, [Online]. Available: https://docs.microsoft.com/en-us/azure/ architecture/data-guide/technology-choices/natural-language-processing.
[49] F.K. Sufi, AI-SocialDisaster: An AI-based software for identifying and analyzing natural disasters from social media, Softw. Impacts 11 (100319) (2022) 1–5.
[50] H. Ren, B. Xu, Y. Wang, C. Yi, C. Huang, X. Kou, T. Xing, M. Yang, J. Tong,Q. Zhang, Time-series anomaly detection service at microsoft, in: KDD '19: Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, New York, 2019.
[51] R. Zhao, W. Ouyang, H. Li, X. Wang, Saliency detection by multi-context deep learning, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition.
[52] Microsoft Documentation, Anomaly detection, 2023, [Online]. Available: Accessed32023.
[53] M. Ravinder, V. Kulkarni, Intrusion detection in smart meters data using machine learning algorithms: A research report, Front. Energy Res. 11 (2023)
[54] http://dx.doi.org/10.3389/fenrg.2023.1147431.
[55] F. Sufi, A new AI-based semantic cyber intelligence agent, Future Internet 15 (7) (2023) 231.
[56] C. Altintasi, Exponential smoothing of quadrature amplitude modulation for power quality disturbance detecting and classification, IEEJ Trans. Electr. Electron. Eng. 18 (8) (2023) 1245–1254.
[57] A. Yadav, A. Kumar, V. Singh, Open-source intelligence: A comprehensive review of the current state, applications and future perspectives in cyber security, Artif. Intell. Rev. (2023) 1–32, Avaliable Online at https://link.springer.com/article/ 10.1007/s10462-023-10454-y.
[58] D. Dale, K. McClanahan, Q. Li, AI-based cyber event OSINT via Twitter data, in: 2023 International Conference on Computing, Networking and Communications, (ICNC), 2023.
[59] T.A. Dempsey, Spreading Lies through the cyber domain, in: European Conference on Cyber Warfare and Security, 2023.
[60] C. Maathuis, R. Godschalk, Social media manipulation deep learning based disinformation detection disinformation detection, in: International Conference on Cyber Warfare and Security, 2023.
[61] F. Sufi, A new social media-driven cyber threat intelligence, Electronics 12 (5) (2023) 1242.
[62] F. Sufi, Social media analytics on Russia–Ukraine cyber war with natural language processing: Perspectives and challenges, Information 14 (9) (2023) 485.