Social media data analysis of IoT risks in smart cities

Abdullah Alajmi
School of Engineering
Cardiff University
Cardiff, UK.
E-mail(s): alajmia6@cardiff.ac.uk

Ioan Petri
School of Engineering
Cardiff University
Cardiff, UK.
E-mail(s): petril@cardiff.ac.uk

Yacine Rezgui
School of Engineering
Cardiff University
Cardiff, UK.
E-mail(s): rezguiy@cardiff.ac.uk

Fodil Fadli
College of Engineering
Qatar University
Doha, QATAR.
E-mail(s): f.fadli@qu.edu.qa

2023 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) | 979-8-3503-1517-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICE/ITMC58018.2023.10332268

***Abstract*— Social media has emerged as the most popular *platform* for individuals from all walks of life who wish to connect with one another to discuss recent news or events that have taken place all over the globe. Twitter, in particular, is among the most important social networks with users that produce real time content. Users can also create a new hashtag or a particular topic to attract other users to enter a discussion. Within the scope of this research project, our goals are to gain an understanding of the effect that social media data has on the Internet of Things (IoT) in smart cities, to provide a description of the risks that have been posed, and to determine whether each individual tweet is neutral, positive, or negative in relation to evaluation criteria. We have conducted research by studying the effects of weather and temperature and how they affect the Internet-of-Things. We use data and scenarios using the World Cup event that took place in Qatar as a prominent example because of the large number of people, services and assets allocated and associated data.**

Keywords*— *Natural Language Processing, Social media, Data analysis, IoT Risks, Smart cities.

I. Introduction

Social media data and users generate increased volumes of data that have a certain value when analysed in relation to relevant scenarios. Social networks in particular, were presented to the public after having been used privately as a messaging service by a select group of people. These systems quickly developed into a microblogging and social networking portal services that enables users to post brief messages, reviews, and write-ups, which are commonly referred to as "tweets." While non-registered users are only able to view tweets, registered users have access to a platform that allows them to post tweets, and retweet tweets generating data and information. Events can be extracted from social media data based on relevance within a smart city context and often prediction models can be developed to obtain historical correlations between variables. In particular, Twitter is a social media platform that generate significant data and information from users posting valuable information that can used in analysis such as natural language or semantical processing. Such analysis include scenarios related to crime identification, based on geolocated tweets into a density model that can help authorities to assess risks and allocate resources. Social media provides

capabilities for predicting events related to smart cities based on a taxonomy of risks that can be defined a-priori. The semantical value of an event can be determined based on assessment of positive and negative implications whereas related statistical models can be used to predict public events and risks occurring in a smart cities context [1]. The collection of Twitter data can be often unstructured because it lacks a predetermined format, which is one of the main difficulties of interpreting the data. Natural language processing (NLP) can help to address this problem based on filtration and clearing of the tweets which can be tokenised into words. The tokenised text data can then be analysed to extract value based on selected scenarios.

The combination of NLP and social media provides an opportunity to capture real-time evolution of states and events that take place in a smart city related to buildings, traffic, vehicles and assets analysis. Energy and cost evaluations can be conducted as well as comfort, security and performance models. Social media analytics can be utilised to determine the status of users allowing the discovery of relationships between weather patterns and smart cities services and operations. Social media can be utilised to help professional to design models for future smart cities as well as tracking assets or monitoring the status of services. Some smart cities will publish digital representations of their development plans and solicit comments from citizens and tourists via social media. This increases the possibility to have citizens as active users involved in the process of decision making in cities. Such models leverage on the concept of "users as active sensors" that generate data with semantical value to inform decision-making [2].

Internet of Things (IoT) threats are already starting to occur. Because smartphones, computers, and tablets are so widely available, people can now communicate in real time about the IoT threats they face. Consequently, Twitter has become a popular medium or channel of communication during emergencies and disasters. Therefore, many data-analytic IT companies and governance bodies are attempting to monitor tweets in real time to discover any IoT-related threats originating from tweets. This would help millions of ordinary people to avoid threats in smart cities [9]

In this paper, we used methods from Natural Language Processing (NLP) to analyse social media data for identifying IoT security and privacy risks in a smart city application. The key objective of this work is to identify IoT related risks in the context of a mega-sports event in Qatar with a view to understand the implications of IoT risks and their subsequent role for decision-making.

The remainder of the paper is as follows: Section II presents related contributions in the field of IoT risks in smart city. The methodology is presented in Section III. The results are presented in Section IV and additional analysis around the

correlation between IoT risks and weather factors in Section V. Section VI presents the conclusions of the research.

II. Related Work

Smart cities are complex systems that combine operations, services, and data processing to make smarter and safer interventions. ICT, electronic sensors (RFID, laser scanners, IR, GPS), geospatial technologies, AI, and blockchain may all make a city smarter. However, IoT is the most crucial technology because it enables intelligent (1) recognition, (2) tracking, (3) location, (4) monitoring, and (5) control and administration of devices, as well as real-time data analysis and insights [5,12]

However, serious security issues must be addressed in IoT. The bulk of the literature cites explicit security and privacy risks. For example, in an IoT-enabled smart city, "the modelling of information dissemination patterns in wireless sensor networks, and the invention of efficient preventative procedures" in the run-time environment would limit virus proliferation [3,4]. The need for better regulatory frameworks to update, improve, and sustain security standards has also been stressed. Thus, frequent update installations, interoperability, and optimised network security protocols are essential for rigorous monitoring and security of complex IoT devices [11,16].

Automated sensing and control systems may aid smart cities because more devices are connected to the Internet. IoT-powered real-time data collection and processing has improved civic services. Smart city infrastructure integrates low-cost sensors and actuators with physical objects, internal and/or remote IT systems, human systems, and the Internet to benefit residents through a range of urban applications. Most sensing and actuation applications include smart transit, structural health monitoring, intelligent traffic control, rapid emergency response, smart street lighting, waste management, smart parking, environmental monitoring, and smart grids. Although the smart city notion is attractive, the highly instrumented, networked, and intelligent aspects of IoT present significant scientific and technological challenges that require industry and academic research projects [13]. Privacy and security aspects are also important in smart cities to ensure authentication, identification, and device heterogeneity incurring increased IoT security and privacy issues [17,10]. Comprehensive regulatory frameworks, new protocols, and designs are needed to protect data privacy and secure smart city infrastructure [15]. A number of studies and articles have focused on machine learning and NLP of social media data to identify any potential security and privacy risks that are associated with the deployment of IoT devices in urban environments [14].

Cities are experimenting a variety of governance models required by the increase of urbanised and digital environments as guided by decision support systems that use (near) real-time information, including social media sources, to improve their sustainability and resilience [8]. A smart city model therefore aims to raise the living standards of its citizens. A new analytical approach has gained popularity for assessing whether the creation of smart cities is in line with sustainable development objectives. Several studies [18, 19] described smartainability as a methodology focused on assessing how sustainable smart cities become from the perspective of smart technologies and infrastructure using both qualitative and quantitative measures and the overall efficiency.

On the other hand, there is a drive towards the adoption of IoT in smart cities that appears to be one of convenience, comparable to the use of other smart technology solutions. However, the integration of IoT-driven smart technological capabilities within a city's infrastructure is intended to attain some important goals, such as efficient infrastructure management, enhancing resident safety, street lighting, cutting administrative costs, and facilitating efficient energy usage [6]. To help understand the rise of smart cities, provides arguably one of the most compelling descriptions of the drivers behind the rapid adoption of smart city technology, including (1) infrastructure management and maintenance, (2) data privacy and security, (3) improved commuter and communication capabilities, (4) reduction in energy usage, and (5) traffic flow and congestion prevention.

The real-time collection and processing of information powered by IoT have enabled urban authorities to deliver smarter services to citizens. Smart city infrastructures are characterised by the synergetic integration of multiple low-cost sensors and actuators with physical objects, internal and/or remote IT systems, human systems, and the Internet to benefit citizens through a wide range of applications in urban areas. Some examples of the most popular privacy and security aspects related to sensing and actuation applications in buildings and infrastructure where an array of devices and controllers sense and actuate based on parameters selected based on performance management strategies [7].

In this paper, social media is used as a source of information for the identification of IoT security and privacy risks in a smart city context. Natural language processing is applied to capture events related to security threats of IoT devices in the context of a mega-sport event involving an increased number of users, devices, and services.

III. Methodology

In this research, we focused on the identification of social media events linked to IoT risks in smart cities (see Fig 1). We separated the investigation into four different scenarios so that we could cover all of the IoT risks in smart cities that were reported by different users.

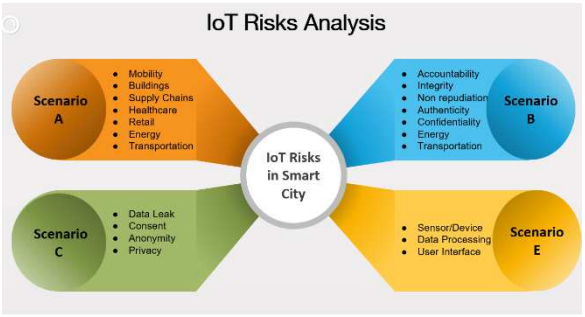

Fig 1. Tweets of IoT risks analysis scenario

The first possible outcome of the tweet analysis is that IoT risks are linked to various services. The second possible outcome is the examination of tweets pertaining to IoT security. The third outcome is the analysis of tweets related to potential risks associated with IoT privacy. The fourth outcome focuses on the analysis of tweets relating to risk associated with components of IoT.

This work leverages on the increased data generated by Twitter users that produce content periodically in the form of news, stories and events. In this study we gathered information from Twitter users using Twint, a Python module [1]. Twint is a sophisticated Twitter scraping tool that is written in Python, which can extract tweets from Twitter profiles without utilising

Twitter's API. Twint can also extract tweets related to particular topics, hashtags, and trends. It can also scrape tweets that contain sensitive information, such as e-mail addresses and phone numbers. The advantages of Twint are that there is no retrieval cap on the number of tweets, no login requirement, and it has a quicker API scraping process. The tweets' content regarding IoT risks in smart cities were either neutral, negative, or positive.

A. Filtering

The goal of this research is to identify the threats to the IoT. Consequently, our queries revolved around terms such as "crack IoT," "black hole attack IoTs," "IoT device failed," "IoT networks do not work", " insecurity IoT ", and so on. The search queries resulted in over 125090 tweets.

B. Preprocessing

Datasets must be prepared before the analysis can start. To prepare tweets for analysis, the following procedures are taken,

- www.*** or https URL conversion.
- Converted @username to AT USER.
- Replace two or more dots with spaces.
- Elimination of RT retweets.
- Two or more letters repeated to two letters are transformed.
- Recognise specific negation indications.
- Remove any further white spaces.
- Separate hashtag words.
- Substitute #word for word.
- Replace SMS slang phrases.

The column names of the collected data together with their missing data are shown in Table 1. Because the vast majority of the column includes empty data, we eliminated it before doing the analysis.

TABLE 1. COUNTS OF MISSING DATA

Column	Number of missing data	Column	Number of missing data
Id	0	Cashtags	85525
conversation_id	0	link	85525
created_at	0	retweet	85525
date	0	quote_url	124293
time	0	video	85525
timezone	0	Thumbnail	116260
user_id	0	near	125090
username	0	geo	125090
Name	6	source	125090
Place	125090	user_rt_id	125090
Tweet	0	user_rt	125090
Language	0	retweet_id	125090
Mentions	0	reply_to	85525
Urls	28575	retweet_date	125090
Photos	33180	translate	125090
replies_count	33665	trans_src	125090
likes_count	33665	trans_dest	125090
hashtags	33665	year	0

The given data are primarily disorganised tweets, which need to be pre-processed before an NLP classifier can be developed from them. One of the most popular Python libraries for analysing text data is called Text Blob, which is based on the NLTK. Emotion analysis and typo fixes are two of the additional capabilities that come with Text Blob. Within the context of this endeavour, the data are pre-processed in three stages, as follows:

a) Tokenization NLP

Tokenization is a mechanism for breaking an input text into individual tokens. Tokens can be differentiated through the use of whitespace and punctuation characters. Meanwhile, text may be tokenised into a variety of words or phrases using Text Blob's capabilities. This makes it much simpler to understand the context [2].

b) Normalisation

The fact that an abbreviation was used within a tweet is noted for the purpose of the normalisation process. Subsequently, the abbreviations are reconstructed according to their actual meaning, and various problems involving terms that have the same significance as a regular word are resolved with the help of Lexicon normalisation.

c) Part of Speech

POS-tagging refers to the process of assigning a tag to each phrase that identifies the part of speech to which it belongs through the use of a tagging system. We also used Text Blob to denote the many components of speech that are contained inside a phrase.

C. Model selection and vectorisation

Even before the information can be used for training, the quantitative characteristics of the pre-processed data must be represented. There are two well-known methods for vectorising words in the field of language processing: counting vectorisation and the Bag-of-words conversion. To supply a machine learning algorithm with this information, the string information is converted to a numeric number. The Naive Bayes classifier is commonly used in NLP, and is therefore used in this project to solve the classification challenge. In addition, technologies based on machine learning pipelines are used to save a considerable amount of time and computational power.

D. Clustering

There were approximately 125090 tweets made by various users, with each tweet emphasising the risks posed by IoT devices. The main goal was to determine if the content of the tweet should be labelled as favourable, negative, or neutral. We were able to achieve this goal thanks to the deployment of a Text Blob sentiment technique that included a polarity measure. The polarity indicates how strongly the author feels about the topic being covered in the text.

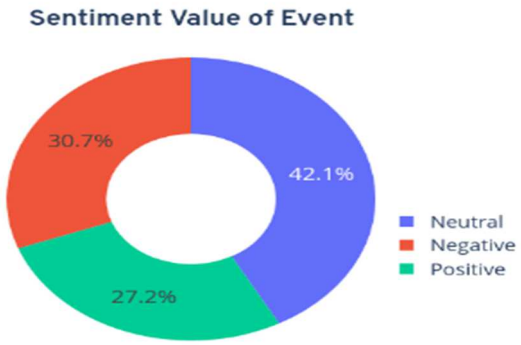

Fig .2 The frequencies of sentiments

Polarity is represented as a decimal number ranging from -1 to 1, which can be interpreted as follows: text with negative feelings was coded with a polarity less than zero, text with neutral feelings was coded with a polarity equal to zero, and text with positive feelings was coded with a polarity greater than zero. Figs 2 and 3 show that the clustering produced roughly 38399 negative events, 34051 positive events, and 52640 neutral events.

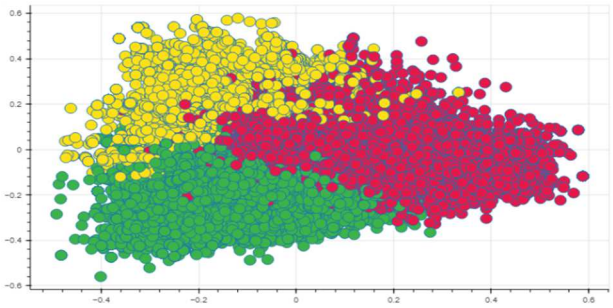

Fig. 3 Positive, Negative, Neutral Clusters of Events.

IV. THE RESULT OF ANALYSIS

In this section, we present the results associated with several scenarios relevant for smart city IoT based event detection.

A. Scenario A: Analysis of IoT risks related to services infrastructure in smart cities.

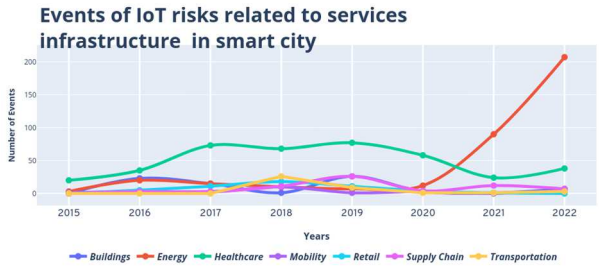

Fig. 4. Scenario A- Events of IoT risks related to services infrastructure in smart cities.

Based on the seven-year research period, there were significant fluctuations in the events of various terms. The term "Energy" showed the highest increase, with a minimum negative tweet of 3 in the first year and a maximum of 207 in the last year. This indicates an increasing interest in the topic of energy over the years. Meanwhile, "Retail" showed a decline, with a maximum of 18 negative events in one year and a minimum of 0 in two other years. The negative events in "Healthcare" also showed an upward trend, with a range of 20 to 77 events. "Mobility" and "Supply chain" had a more moderate range, with "Mobility" ranging from 0 to 10 and "Supply chain" ranging from 0 to 26. The negative events of "Buildings" varied greatly, with a range of 1 to 26 events.

Finally, the negative events in "Transportation" showed the least range, with only three events in the last year and zero events in the first six years. This suggests that transportation was not a significant topic in the events over the past seven years. This research highlights the varying levels of interest in different topics on Twitter, with energy and healthcare showing the most growth and retail and transportation showing the least interest (see Fig. 4).

B. Scenario B: Analysis of risk events related to IoT security in smart cities.

This scenario examined the rate of some of the involved keywords in the analysed events over time. The primary terms are "Accountability," "Authenticity," "Confidentiality," "Non-repudiation," and "Integrity".

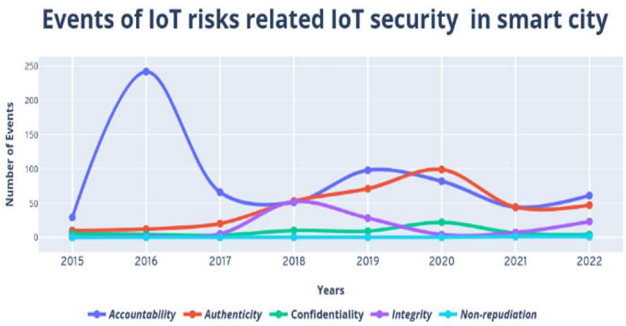

Fig. 5.Scenario B- Risk events related IoT security in smart cities.

In 2015, the frequency of negative events for this factor was around 30 to 45. The frequency rapidly rose to approximately 250 events in 2016. However, in 2017, there was a decline with the most frequent term, "Non-repudiation," having close to 100 events.

Starting in 2018, brief terms such as "Non-repudiation," "Confidentiality," and "Authenticity" began to appear more frequently in events. "Confidentiality" and "Authenticity" reached their peaks at 200 and 180 negative events, respectively, in 2020, while "Non-repudiation" remained consistent. All terminologies saw a decline in 2021 and 2022, with most common terms scoring around 100 and 125 negative events, respectively. The least frequent term "Accountability" had the fewest positive and negative events, with approximately 45 positive and 55 negative events (see Fig 5).

C. Scenario C: Analysis of risk events related IoT privacy in smart cities

This scenario analysed events regarding the disclosure of personal data and looked at key terms such as "Anonymity," "Consent," "Privacy," and "Data Leak." "Privacy" was the most frequently discussed term, with varying levels of frequency over the years. "Anonymity," "Consent," and "Data Leak" were not widely mentioned between 2015 and 2017 but became more prevalent in later years, with "Consent" appearing in 2018-2020 and "Data Leak" peaking in 2021.

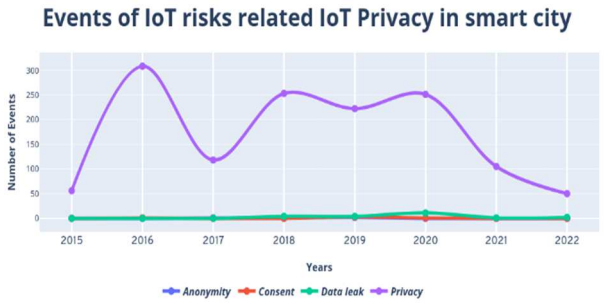

Fig. 6. Scenario C- Events of IoT risks related IoT Privacy in smart city.

Despite its frequency, "Privacy" was a sensitive topic and received negative attention, starting with 25 negative events in 2015 and reaching its highest peak in 2017 with over 300 negative events. Between 2019 and 2021, there was another peak with 250, 230, and 255 negative events, respectively. However, there was a significant decline in the following two years, with 100 and 50 negative events (see Fig 6).

D. Scenario E: Analysis of events IoT risks related to components of IoT in smart cities

This scenario examined the frequency of some of the involved keywords in the collected events over time. The prominent terms are "sensor/device", "data processing", and " User interface".

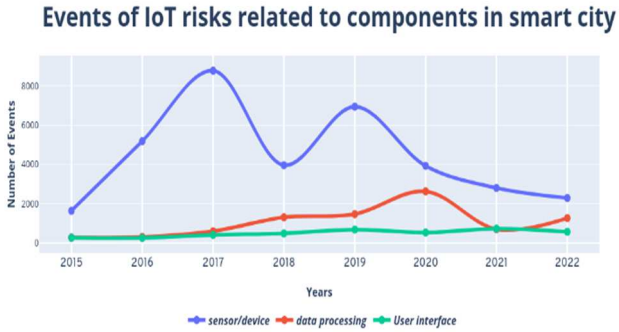

Fig .7.Scenario E- Risk events related to components of IoT in smart cities

This graph depicts trends in the frequency of the phrases that people used in discussions about potential threats posed by IoT between 2015 and 2022.

In general, "data processing" and "user interface" have lower frequencies than "sensor/devices." The latter has gradually climbed since 2016, while the increase for "data processing" peaked at roughly 2900 words in 2020 before rapidly decreasing in the following year. However, "user interface" declined somewhat in 2020 before increasing slightly again in 2021. By 2022, the terms "data processing" and "user interface" were almost identical in frequency, with only 500 words separating them (see Fig 7).

V. IOT RISKS EVENTS VS TEMPERATURES: QATAR2022 AS A CASE STUDY

IoT devices in smart cities may be adversely affected by environmental conditions such as heat, sunlight, and humidity. The extent of this influence has been examined by pulling events from various months of the year and contrasting them.

Several factors led us to select Qatar as our case study country. First, Qatar is one of the countries where temperatures soar during the summer. Second, the 2022 FIFA World Cup that was hosted there used the most recent accomplishments of IoT, including smart stadium and transportation technology designed from the ground up for this event. Third, the sheer volume of fans in attendance during the month of December when the World Cup was held speaks to their enthusiasm for the chance to voice their opinions on the impact of these technologies. The total number of events that we generated through Twint scrapping for the entire year of 2022 was around 18901 (see Table 2).

Taking the average for the country of Qatar into account, we found that in 2022 there were over 8388 positive events from various cities in Qatar. Positive events were lower at the start of the year in winter months with low temperatures than in summer months, as shown in Fig 8. When the temperature remained constant, there was a high watermark in July. By October, we can see that the increase in events occurred as the weather began to cool. The increase in December events could be attributed to the World Cup FIFA 2022 organisation having a large influence on people's perceptions at the end of 2022.

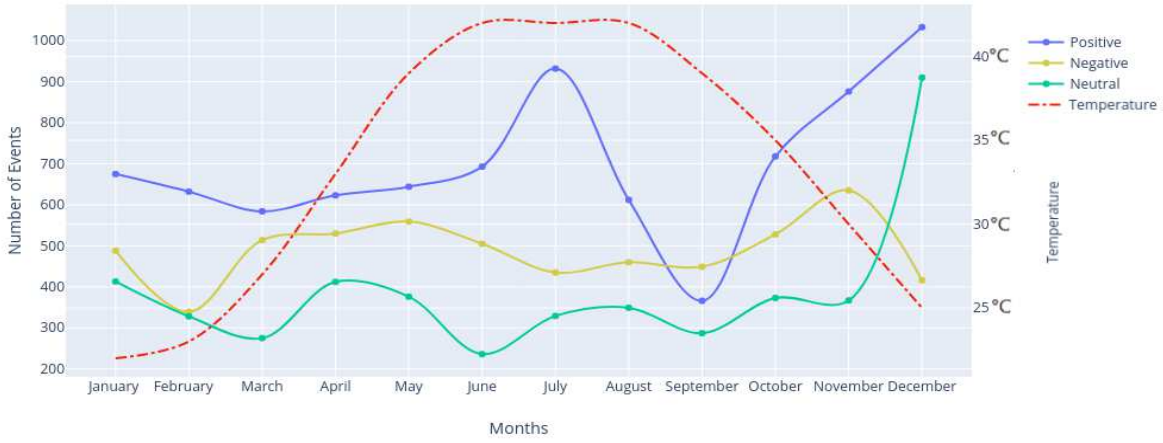

Fig. 8. A comparison of events with Qatar's temperature over months in the year of 2022.

TABLE 2. RESULTS OF SENTIMENT ANALYSIS FOR MONTHS

MONTH	TEMPERATURE	POSITIVE	NEUTRAL	NEGATIVE
JANUARY	22	675	413	488
FEBRUARY	23	632	328	339
MARCH	27	584	275	514
APRIL	33	623	412	530
MAY	39	644	376	559
JUNE	42	693	236	505
JULY	42	932	329	435
AUGUST	42	612	349	460
SEPTEMBER	39	366	287	449
OCTOBER	35	718	373	528
NOVEMBER	30	876	367	635
DECEMBER	25	1033	910	416

More than 4,655 events were neutral in tone. There seems to be no correlation between the temperature in Qatar and the number of neutral events, although there is a noticeable decrease in the number of events in June when the weather starts to settle down. We may also connect the about +900 events of neutral sentiment that were sent in December to the 2022 FIFA World Cup.

There were more than 6346 negative events throughout 2022 as shown in Fig 8. This demonstrates a correlation between the increase in temperature and the growth in the number of negative events. The falsely alleged claims raised up by some European countries about Qatar's capacity to host the World Cup, as well as the fact that the tournament took place in the midst of the football season, have had a considerable influence on the number of unfavourable events, especially during the month of November.

VI. CONCLUSION

Social media analysis with sentiment analysis examines how individuals express themselves online. However, unstructured social media data makes evaluation difficult. Our model varies from past work in this field because it uses real-time Twitter data, the TextBlob module from the Python library, and other approaches to produce the best positive, negative, and neutral sentiment findings. In the sentiment analysis procedure, Twitter API events have been cleaned and discovered. The data was then put into training models. Each tweet was analysed based on its semantic values related to IoT risks. We studied how factors affect categorisation accuracy, with the observation that clearer data means more accurate outcomes.

The results of the research indicated that the users have a significant amount of contact with reports of risks associated with the IoT in all its forms and varieties of services and devices, in addition to concerns regarding security and privacy. As a result, individuals who are in a position to make decisions and those who are interested in IoT should take this into account while resolving previously established issues, as well as covering and elaborating on potential future solutions. It is necessary to develop an advanced system to monitor all events directly and link it to the pre-warning centre in the management of smart cities to ensure that there is a quick response to risks and to prevent the occurrence of the threat or its spread.

The possibility to engage citizens in the creation of smartainable cities empowers people to work towards more effective and high-quality urban systems. The effect of moving users closer to decision making has been demonstrated to increase civic involvement in cities. As such smart cities required more sustainable decision making and assessment of risks in order to improve quality of solution for the citizens and to offer a more direct involvement of users in the process of decision making.

Match and Contribution:

The paper "Social Media Data Analysis of IoT Risks in Smart Cities" aims to understand the impact of emerging technologies on urban environments. The research focuses on the interplay between social media data and the Internet of Things (IoT) in smart cities. The study examines the effects of weather and temperature on IoT systems and employs Natural Language Processing techniques to evaluate sentiments expressed by users in social media data. The findings have implications for shaping the future of smart cities, as urban spaces become more connected and data-driven. The research contributes valuable insights to the ongoing dialogue on leveraging social media data analysis to enhance the sustainability and security of smart cities. The article will arouse debates among academics, decision-makers, and business professionals interested in using social media data for improved urban planning, risk management, and technological integration.

VII. ACKNOWLEDGMENTS

This publication was made possible by NPRP grant No. NPRP12S- 0222-190128 from the Qatar National Research Fund (a member of Qatar Foundation). The findings achieved herein are solely the responsibility of the authors.

VIII. REFERENCES

[1] Goswami, S., & Raychaudhuri, D. (2020). Identification of Disaster-Related Tweets Using Natural Language Processing: International Conference on Recent Trends in Artificial Intelligence, IOT, Smart Cities & Applications (ICAISC-2020).

[2] Al-Turjman, F., Zahmatkesh, H., & Shahroze, R. (2019). An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies, e3677.

[3] Zhang, J., Wang, Y., Li, S., Shi, S. (2020). An architecture for IoT-enabled smart transportation security system: A geospatial approach. IEEE Internet of Things Journal, 8(8), 6205–6213.

[4] Cui, L., Xie, G., Qu, Y., Gao, L., Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. IEEE access, 6, 46134–46145.

[5] Kim, T.-h., Ramos, C., Mohammed, S. (2017). Smart city and IoT. Elsevier.

[6] Aqeel-ur Rehman, S.U.R., Khan, I.U., Moiz, M., Hasan, S. (2016). Security and privacy issues in IoT. International Journal of Communication Networks and Information Security (IJCNIS), 8(3), 147–157.

[7] Williams, M., Axon, L., Nurse, J.R., Creese, S. (2016). Future scenarios and challenges for security and privacy. 2016 ieee 2nd international forum on research and technologies for society and industry leveraging a better tomorrow (rtsi) (pp. 1–6).

[8] Hodorog, A., Petri, I., & Rezgui, Y. (2022). Machine learning and Natural Language Processing of social media data for event detection in smart cities. Sustainable Cities and Society, 85, 104026.

[9] Aiswarya, M. K. (2021). Sentiment analysis of Twitter using machine learning. Journal of Research Proceedings, 1(2), 216-225.

[10] Abosaq, N. H. (2019). Impact of privacy issues on smart city services in a model smart city. International Journal of Advanced Computer Science and Applications, 10(2), 177-185.

[11] Ahad, M. A., Paiva, S., Tripathi, G., & Feroz, N. (2020). Enabling technologies and sustainable smart cities. Sustainable cities and society, 61, 102301.

[12] Al-Turjman, F., & Alturjman, S. (2018). Confidential smart-sensing framework in the IoT era. The Journal of Supercomputing, 74(10), 5187-5198.

[13] AlDairi, A., & Tawalbeh, L. (2017). Cyber security attacks on smart cities and associated mobile technologies. Procedia Computer Science, 109C(2017), 1086-1091.

[14] Alhirabi, N., Rana, O., & Perera, C. (2021). Security and privacy requirements for the Internet of Things: A survey. ACM Transactions on Internet of Things, 2(1), 1-37.

[15] Alshehri, M. D. (2019). Intelligent trust management methodology for the internet of things (IoT) to enhance cyber security (Doctoral dissertation).

[16] Ande, R., Adebisi, B., Hammoudeh, M., & Saleem, J. (2020). Internet of Things: Evolution and technologies from a security perspective. Sustainable Cities and Society, 54, 101728.

[17] Aqeel-ur-Rehman, S. U. R., Khan, I. U., Moiz, M., & Hasan, S. (2016). Security and privacy issues in IoT. International Journal of Communication Networks and Information Security (IJCNIS), 8(3), 147-157.

[18] Shad, M. H., Rezgui, Y., Hodorog, A. and Petri, I. 2021. Digitalising risk of fire resilience for UK buildings. Presented at: 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Cardiff, Wales, 21-23 June 2021 (10.1109/ICE/ITMC52061.2021.9570247)

[19] Ahmed, U., Petri, I. and Rana, O. 2022. Edge-cloud resource federation for sustainable cities. Sustainable Cities and Society 82, article number: 103887. (10.1016/j.scs.2022.103887)