gg03

by GANG GAO

Submission date: 09-Sep-2022 07:07AM (UTC+0100)
Submission ID: 185823280
File name: 287186_GANG_GAO_gg03_6305014_842035133.pdf (1.47M)
Word count: 12785
Character count: 76378

University of Nottingham
UK | CHINA | MALAYSIA

Cyber Threat Intelligence-based Risk Assessment in Healthcare

Submitted 9th September 2022, in partial fulfilment of
the conditions for the award of the degree **MSc Computer Science.**

GANG GAO

20373079

Supervised by Ying He

School of Computer Science

University of Nottingham

I declare that this dissertation is all my own work, except as indicated in the text

Signature _____

Date _____ / _____ / _____

Contents

List of Figures

List of Tables

Abstract

In the current cyber and information age, the healthcare sector is constantly exposed to a variety of cyber threats and attacks, which cause negative effects that people do not want to confront, such as equipment corruption and patient privacy breaches, especially irreversible loss of assets and health. This project combines Cyber Threat Intelligence (CTI) with Risk Assessment (RA) and proposes a novel CTI-RA model that is designed to help healthcare organisations make more informed risk decisions.

In addition, this research has implemented a python-based web data visualisation, the results of which demonstrate the trends of cyber threats or risks in healthcare, and present organisations with a series of mitigations corresponding to threats.

Keywords – cyber security, healthcare, CTI, risk assessment, visualisation, python

Acknowledgements

During this enriching and meaningful project, I would like to thank my supervisor - Professor Ying He, for broadening my horizons in the field of cyber security and for her patient guidance and advice in pointing me in the right direction. Furthermore, I have learnt from my supervisor to think with an open mind in the process, which will be of great assistance to me in my future studies and research.

I would also like to thank my girlfriend Yue, and family from afar, whose company and support gave me the courage and hope to face the challenges in my studies.

Finally, I would like to thank my friends in this country, who have made my life so much richer, for their companionship and struggle together. Wish them all the best in their future life

Chapter 1: Introduction

With the spread and widespread use of information technology and the Internet of Things, the high importance of cyber security in the healthcare sector is no longer in doubt. When a malicious hacker or organisation launches a cyber-attack on healthcare organisations, not only can it lead to financial, reputational, and various other losses to the organisations, more importantly, but it can also pose risks and negative impacts on the safety and health of patients, some of the effects and losses would even be irreparable.

In order to better understand the details of threats and implement more effective defences, organisations can use cyber security intelligence (CTI) and risk assessment (RA) to support decision-making. However, there are numerous existing works with best practices, but most of them independently study CTI or RA and do not associate CTI with RA. Organisations are overwhelmed by the sheer volume of CTIs and cannot find the most relevant CTI for RA, particularly in healthcare where organisations require clear defence strategies and mitigation measures in the event of threats. This project is intended to integrate CTI and RA to facilitate more effective risk prevention, control, and decision-making in healthcare organisations.

1.1 Motivation and Aims

When faced with vast amounts of CTI, organisations cannot find the most relevant information to them for risk prevention and control, while existing researches only focus on building CTI models for cyber threats, or applying attacks to risk assessment frameworks. This implies that a bridge is lacking between CTI and organisational risk assessment, and healthcare organisations need an effective risk prevention framework and strategy guidelines to improve their overall cybersecurity and reduce the financial loss caused by cyber-attacks.

With the requirements of the current situation as a motivation, the objective of this research is to create a novel CTI-RA model that can map CTI into RA framework and, through data visualisation, achieve the goal of making some contributions to healthcare. The overall project can be divided into the following aims:

- Identify key challenges relevant to cyber security in healthcare, focusing primarily on the combined CTI and CRA aspect.
- Propose a novel model or framework to assist healthcare organisations in decision-making regarding cyber security.
- Successfully visualise data and present possible recommendations and mitigations for healthcare organisations.
- Test and evaluate the validity or accuracy of results through related industry standards.

1.2 Overview of the dissertation structure

The dissertation contains chapters as follows.

Chapter 2 reviews and analyses some of the existing technologies and research on CTI and RA, as well as presenting some background on cyber security in healthcare.

In Chapter 3, the techniques and frameworks that will be used in this study are presented, and the elements of the proposed novel CTI-RA model are described and analysed in detail.

Chapter 4 focuses on the process of data analysis and the related code implementation, describing the difficulties and challenges involved. Additionally, the principles and results of the implementation of data visualisation are illustrated in this chapter.

Chapter 5 contains the analysis of some of the limitations and shortcomings of this study, through testing results and comparing with generic standards.

Finally, conclusions of this project and perspectives for future works are given in Chapter 6.

Chapter 2: Literature Review

The purpose of this section is to identify tools and methodologies available in the existing works, in order to create a more robust framework to improve cybersecurity in the healthcare sector and facilitate risk-based decision making. This review will also create a gap in the literature that indicates an opportunity to design a CTI-based risk assessment model in healthcare. Meanwhile, readers will be provided with needed background knowledge on cyber security, CTI, and risk assessment, which are associated with my work.

2.1 Cyber security in healthcare

While medical devices and systems are becoming increasingly networked and computerised, which brings various benefits to the healthcare sector, the growth in information flow also poses risks to healthcare, particularly in terms of privacy breaches and security risks due to the massive cyber-attacks. The medical systems of Hammersmith Medicines Research (HMR) in the UK were attacked by a ransomware attack that led to the disclosure of the personal and private information of thousands of former COVID-19 patients after the company refused to pay the ransom (Goodwin, 2020). More seriously, when critical medical devices become the target of cyber-attacks, it can directly have a detrimental impact on patient health and even lead to death. Researches have proven that some embedded medical devices, such as pacemakers, can turn into assassination weapons, when they are accessed remotely and modified for operation, which could pose a health threat to the patients involved (Beavers and Pournouri, 2019; Rehman et al., 2020). Additionally, Al-Mhiqani et al. (2019) found that a defective pacemaker, which could be attacked to cause alteration or complete shutdown, would result in disastrous outcomes. This means that other potentially vulnerable infusion pumps used to deliver antibiotics, chemotherapy and other medicines to patients could also suffer from serious security problems in that they could be remotely and secretly hacked to change the original dose of drugs dispensed to the patient. In this case, any security breach could have serious implications for the patient, even causing death in some situations (Seh et al., 2020).

To cope with the healthcare data leakage problem and improve the security of medical devices, existing works have made a significant contribution that cannot be ignored. For instance, Rughoobur and Nagowah (2017) proposed a lightweight framework that can detect replay attacks on medical IoT devices by combining universally unique identifiers, timestamps, and a self-learning battery depletion rate monitor. A new prototype application was built for testing, with successful detection results. Although the diversity of types for cyber-attacks, the reliable framework proposed in this research would be defended against replay attacks and would contribute to the healthcare field.

As the development of IoT technology brings the potential risk of medical devices being attacked, research on related attack prevention has followed suit. Ahmed et al. (2018) developed a tool called IoT-Flock for generating normal and malicious IoT traffic. Afterwards, the authors applied different machine learning (ML) techniques to the generated dataset for detecting and protect the healthcare system from cyber-attacks, and the results showed that the Random Forest classifier achieved an accuracy of 99.5123%, demonstrating that the framework would be helpful in developing more robust context-aware security solutions, especially for IoT healthcare. It can be noted that artificial intelligence (AI) appears to be an inspiring area of research that provides an important enhancement to security detection in cyberspace. Similarly, a Cognitive Machine Learning assisted Attack Detection

Framework (CML-ADF) model was proposed by AlZubi et al. (2021) to detect anomalies and attacks in healthcare networks. This design approach is based on patient-centric to safeguard the information on trusted devices, such as end-user mobile phones and end-user-controlled data sharing access. The results of the study showed that the model created by the authors achieved 98.2% accuracy and 96.5% attack prediction, effectively securing patient data to overcome attack behavior.

Furthermore, artificial intelligence-based heuristic health management systems (AI-HHMS) have been investigated (Al-Maitah, 2019; Meng et al., 2020). This system uses health datasets from IoT-assisted sensors to prompt staff, supervisors, and experts to make more rational and effective cyber security decisions using an AI health system, which could reduce the risk of cyber-attacks and protect the privacy and security of the patient database. The results of the study reported that the system, implemented by MATLAB, achieved 99.66% in accuracy, 98.6% in detail, and 99.75% in precision.

2.2 Cyber Treat Intelligence (CTI)

Dandurand and Serrano (2013) contributed to define requirements for a CTI sharing platform among the first, and with the development and refinement of CTI, many organisations that suffer from malicious cyber threats could prevent security breaches before they would be attacked (Kao and Hsiao, 2018) thus effectively preventing the compromise of an organisation's private data. In order to decompose standards, and analyse interoperability and dependencies within the current CTI sharing community, Burger (2014) presented a taxonomy that classified threat sharing standards by using an abstraction framework, an approach that would contribute to the development of shared automation of CTI in general. However, the CTI field also exists with its own challenges. Serrano et al. (2014), for example, recommended that organisations should install quality control procedures to provide various measurable quality values, due to the lack of support for quality control and management in existing CTI sharing platforms. Though the authors suggested the need for quality assessment, they did not describe the concrete methods to implement it on the platform.

Therefore, with the aim of improving the quality of CTI and helping organisations make better decisions, Abu et al. (2018) stated that CTI on the platform should have three elements including relevance, timeliness and actionability to ensure threat data can be analysed and processed in a timely way and produce actionable intelligence. Also, Riesco et al. (2020) suggested applying standards such as the W3C Semantic Web standard and Structured Threat Information Exchange (STIE), to create a knowledge workspace relevant to behavioural threat intelligence models to describe tactics, techniques and procedures (TTP), these are the attributes defined in Structured Threat Information Expression (STIX) which is defined and maintained by the OASIS consortium (Barnum, 2012).

A well-established and comprehensive case of CTI platform is the malware information sharing platform (MISP) (Wagner et al., 2016), one of the most used open source platforms since 2016, would deploy 20 to 40 new instances each day and share data with a size of about 100K md5 hashes a month, which demonstrated the real demand of the end users. On the other hand, the authors suggested new possible research directions regarding data quality, since it is usually not reliable.

In the meantime, cyber threats are in a constant state of dynamic change, and threats are evasive, resilient and complex, so traditional static security approaches based on heuristics

and signatures cannot match the dynamic nature of the new generation of threats (Tounsi and Rais, 2018). Accordingly, Conti et al. (2018) defined a much-needed concept of CTI to further advance the understanding of the CTI concept, not only improving communication between the different intelligence teams, but also the company's defence posture and overall cyber security. Meanwhile, as described by Riesco and Villagrá (2019), working dynamically in the risk domain could be a promising approach, because it would always keep risks at an acceptable level. To achieve that, they proposed to use cyber threat intelligence for a Dynamic Risk Management (DRM) framework that allowed the representation of contextual behaviour patterns, such as the representation of TTP. Their concept which combined CTI with risk assessment is similar to my work.

However, the numerous and varying standards of current CTI platforms, coupled with the sheer volume and complexity of CTI information, have led organisations to be overwhelmed by the massive amount of CTI and unable to find the most relevant intelligence to handle risk. As pointed out by Liu et al. (2022), effectively using the large numbers of CTI security technicians is becoming significantly more difficult, given the current situation where the amount of cyber security reports is growing dramatically. This is also one of the problems that this study is dedicated to addressing. Consequently, they developed trigger-enhanced actionable CTI discovery system (TriCTI) and extracted actionable CTIs from cybersecurity reports using natural language processing (NLP) techniques. To tackle the lack of annotation of CTI datasets, the authors also devised a data augmentation method, which demonstrated a higher accuracy of 86.99% for TriCTI compared to other state-of-the-art models, such as the BERT text classification model.

2.3 Risk Assessment (RA)

A traditional framework was developed on enterprise risk management with scalability and adaptability features that included four phases (as in Fig. 1), respectively, risk assessment, mitigation, validation, and audit (Kabanov, 2016). This framework tends to be a formal approach, which focused on evolving an analytic foundation towards the designs, specifications, implementations, executions, and evaluations of secure systems. Such a can improve the effectiveness of the analysis management process, but the probable challenge may be that after the risks have been identified, skilled technical professionals would be required to perform some key security controls such as application encryption and key management, identity and access management, security assessment and decision management. Based on the afore-mentioned requirements of security risk assessment, some renowned risk assessment methods are frequently applied, mainly consisting of qualitative and quantitative analysis.

Fig. 1: Traditional risk management framework

2.3.1 Qualitative methods in RA

Research in qualitative methods would contribute to the improvement of risk assessment, because qualitative methods of researches tend to focus more on social factors beyond mathematical analysis. A typical example as, the RITE model explored by Dhillon and

Backhouse (2000) explored social issues, apart from technical solutions, other social elements like responsibility (R) of different roles, integrity (I) of employees, trust (T), and ethicality (E) coupled with technology issues, to offer a general view of the vulnerability and risk recognition in organisations. After in-depth interviews with information technology (IT) leaders from different organisations, the authors concluded a value-focused approach (VFA) to information security. It was revealed that social, human, and interpersonal issues could also contribute to IS security, and it is significant to consider these issues in an appropriate RA strategies (Dhillon and Torkzadeh, 2006). Another approach to risk qualitative analysis (Williams, 2020) is introduced by OWASP, by following the steps in the method, the severity of the threat impact on the business would be estimated and it would be helpful in risk decision making, thereby ensuring critical businesses would not fail to function properly due to the threat.

2.3.2 Quantitative methods in RA

On the other hand, quantitative methods, which involve the computational analysis of various attributes of risk assessment, are often used to quantify risk. Relevant examples such as DREAD (DOMARS, 2018), one of the prevalent risk/threat assessment approaches, considers five properties: damage potential, reproducibility, exploitability, discoverability, and affected users. The final score of the risk assessment is graded for each category and then the mean value is derived. Regarding further, an effort to minimize economic losses due to risk, Mukhopadhyay et al. (2019) presented a CRAM framework to evaluate the likelihood of an attack by using generalized linear models (GLM), called logit and probit, the framework was a quantitative model to quantify the probability of a cyberattack and the expected loss to business. The researchers also modelled the percentage of security factors that need to be implemented when an organisation intends to minimize security breaches to a certain level. Besides, they also provided the chief technology officers (CTOs) of organisations with decision on the proportion of risk based on premium estimations, which proved the effectiveness and practicality of their framework. Moreover, Ekelund and Iskoujina (2019) built a mathematical model for risk assessment and mitigation strategies, which is based on cost benefits. This means that while evaluating the risk, the cost of the risk could also be calculated and demonstrated. Consequently, this would assist security decision makers in the organisation to determine whether it is worthwhile to invest into risk mitigation actions, and if at the cost of high expenses, then mitigation strategies might not be adopted for non-critical risks.

In this study, the quantitative RA framework used is the Factor Analysis of Information Risk (FAIR) (Jones, 2006; Le, 2017; Park et al., 2018), which is widely recognised and applied for its taxonomy of risk analysis. In the smart grid domain, for instance, Le et al. (2019) combined FAIR's loss event frequency (LEF) with Bayesian networks (BN) to derive the numerical assessments to rank the threat severity, resulting in the BN probabilistic relations from the FAIR lookup tables to reflect and preserve the FAIR appraisal. Their study enhanced the prevention and control of cyber threats in the smart grid sector, and lacked a more in-depth evaluation and analysis of FAIR's model, though it extended some of FAIR's capabilities. However, Wang et al. (2020) pointed out the shortcomings of the FAIR algorithm, that is, the restriction in both the type of useful statistical distributions and the expandability of the model structure. Consequently, they suggested a FAIR-BN approach that imported Bayesian networks into FAIR and improved the accuracy of risk assessment by employing Monte Carlo (MC) methods. In addition, the authors applied process-oriented and game-theoretic methods to demonstrate the flexibility and scalability of FAIR-BN.

This section reviewed the work of the different supportive solutions proposed to address cybersecurity problems suffered by the healthcare sector, and discussed the importance of various CTI and CRA frameworks for organisations to control and prevent network risks. These existing efforts have made significant efforts to provide a deeper understanding of threats and to make protection and security decisions. However, despite these notable contributions, most of the current studies focus on CTI or risk assessment independently, and lack a bridge between CTI and CRA, particularly in healthcare, resulting in organisations unable to find the most relevant information among the numerous CTIs to conduct CRA. Hence, building on existing works, this project fills this gap with the novelty of combining CTI at the technical level with CRA at the managerial level and applying it to security decisions at the strategic level. The research in this paper considers the use of CTI information to improve the visibility of CRA, so that healthcare organisations will gain better insight in risk recognition and analysis, prevention and decision-making when faced with concealed and complex threats, thus helping organisations to manage risk effectively and make better-informed decisions.

Chapter 3: Approaches and Methodology

In this section, methods to achieve the final model building and possible measures to facilitate the resolution of cyber security issues in the healthcare sector will be discussed. The focus is on the analysis and creation of highly relevant, and novel, CTI-based risk assessment model and framework for the healthcare sector. Additionally, it will describe and analyse relevant methods or techniques, such as Python and FAIR frameworks, to implement the objectives in different processes, and the reasons and requirements for the choice of approaches will also be discussed.

3.1 Python

Python, as one of those numerous computer programming languages, is an object-oriented programming with polymorphism and inheritability. Despite the fact that Python may run more slowly than other languages such as C/C++, due to its dynamically typed interpreted features rather than statically typed compilation (VanderPlas, 2014), its integration of a variety of powerful libraries and modules makes Python stand out in many areas, especially in the field of artificial intelligence (AI) and big data, and its convenience and strength in data analysis is one of the reasons why I chose it. In this study, the main techniques employed are crawling in Python for data collection and the Streamlit framework for web visualisation data analysis.

3.1.1 Python Crawler

There are a wide range of crawling techniques and methods involved in Python, and common libraries include urllib, requests, pandas etc. Where permissions allow, in order to retrieve information from a particular web page, automatic extraction definitely provides a significant advantage compared to manual extraction. By writing a python script, it is feasible to query a web server, request data, and parse complex html pages, ultimately automating the extraction of the required data and information. In general, the web crawling mechanism consists of three steps: requesting information from the web server, processing the server response, and extracting the data by automatically interacting with the site (Mitchell, 2018).

The "pandas" package has been imported into the python script as the preferred library file for this study, since "pandas" not only can automatically fetch multiple pages of data from web pages and update them in real-time, but also incorporates a large number of libraries and standard data models with functions and methods that enable fast and efficient data storage, cleaning and leveraging (Chen, 2018), which are essential to make Python become a powerful and efficient data analysis environment.

3.1.2 Streamlit framework

As one of the large amounts of open-source libraries in Python, Streamlit (https://streamlit.io/) makes it easier and more efficient to create and share custom web applications, especially in recent years for data science and ML applications (Lee et al., 2022; Kiss et al., 2022). Data scientists can use Streamlit to build web pages seamlessly and quickly. Also, Streamlit provides many different APIs that support real-time data requests from a database to be loaded to a custom visual dashboard (see Fig. 2).

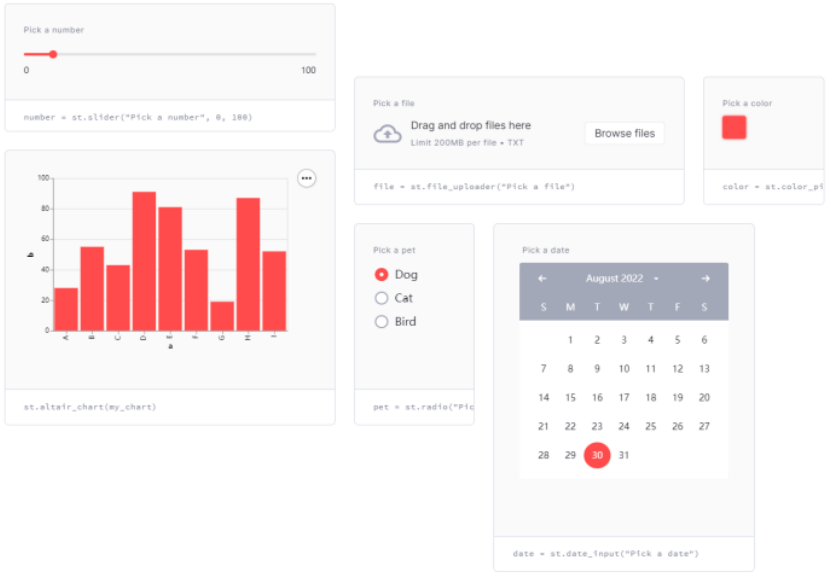

Fig. 2: Streamlit dashboard example

Considering the high efficiency of Streamlit in data visualization and its potential to become a future trend in data science, this research applies this framework to the statistical analysis of CTI data and the visualization of CTI-RA models.

3.2 The FAIR Model Overview

3.2.1 Structure of the FAIR model

The classification model structure of Factor Analysis of Information Risk (FAIR) (The Open Group, 2018; Jones, 2006) is shown in Fig. 3, where the "RISK" is classified and defined as Loss Event Frequency (LEF) and Loss Magnitude (LM) of future loss (also called "loss exposure") that will be incurred by major stakeholders over a defined period. On the one hand, LEF refers to the probable frequency of an asset being harmed by a threat agent, which could be any agent (human, object, or substance) that takes harmful action against an asset, at a particular time and consists of the Threat Event Frequency (TEF), which represents the possible frequency of a threat agent acting on an asset at a specified time, and the Vulnerability (V), which is the probability of a threat event becoming a loss event. After an asset comes into contact with a threat agent there exist two scenarios, classified as being acted upon and not acted upon, so a statistic of the frequency of contact events (Contact Frequency (CF)) and the chance of success (Probability of Action (PoA)) yields the TEF, In the meantime, the likelihood of vulnerability (V) can be assessed after analysing the Resistance Strength (RS) and the Threat Capacity (TC) of an event.

On the other hand, the LM is the magnitude of the loss that may be caused by the loss event, which is the sum of the Primary Loss (PL) and the Secondary Loss (SL) from the risk event, rather than a separate one-time assessment of the LM. PL could be interpreted as the magnitude of the possible loss that occurs directly, based on the actions of the threat agent on the asset, and contains a maximum and a minimum value; however, SL takes PL as premise, which is derived from losses caused by secondary stakeholders, such as regulators, customers,

organisational environment, etc., reacting negatively to the primary threat event. In addition, the percentage of time that the analyst assesses for the expected secondary impact arising from a certain situation results in the Secondary Loss Event Frequency (SLEF), which is estimated together with the Secondary Loss Magnitude (SLM) to constitute the SL.

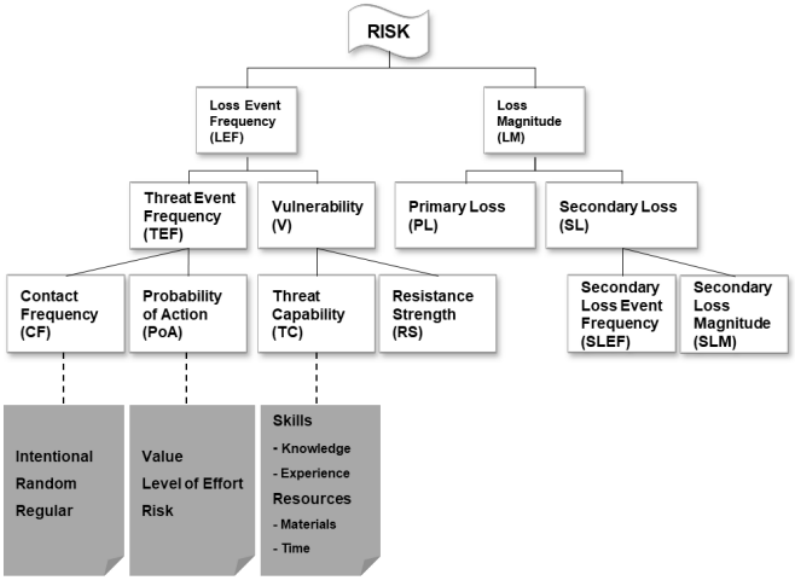

Fig. 3: The FAIR model structure

It can also be observed from Fig. 3 that if further subdivision is performed, when a threat agent contacts an asset, regardless of whether the contact is physical (e.g., theft) or logical (e.g., network), the types of possible contacts can be classified as: deliberate, random and periodic. While the level of CF can be influenced by three factors in the PoA, respectively value, effort and risk. Further interpretation is that an organisation's assets are more likely to be deliberately contacted by a threat agent if a) the higher the value of the asset itself to the threat agent; b) the lower the difficulty of completing the threat action on the asset; and c) the lower the negative outcomes of the threat action to the threat agent. Furthermore, TC and RS as two factors in assessing V. the former represents the likely level of force exerted on an asset by a threat agent, in the form of skills, resources and time, which can be mapped to TTP (tactics, techniques, procedures) in CTI, which will be elaborated in the CTI-RA model. Whereas the latter RS indicates the level of resistance compared to the attacker's percentage of power, like the password complexity of an asset. Hence, organisations in the healthcare sector need to evaluate and measure these sub-factors comprehensively to implement a risk assessment of the relevant threats.

3.2.2 Total loss/risk assessment and calculation

With regard to the FAIR model described above, a series of these risk factors could be quantitatively analysed and modelled, that is, factors and sub-factors can be treated as dependent variables and independent variables, which would be expressed as probabilistically or statistically different functional relationships (The Open Group, 2018). The summarised variables and functions are shown in Table 1.

Step	Independent Variable	Dependent Variable	Function
1	Contact Frequency (FC), Probability of Action (PoA)	Threat Event Frequency (TEF)	*TEF=FC*PoA*
2	Threat Capability (TC), Resistance Strength (RS)	Vulnerability (V)	*V=TC*RS*
3	Primary Loss Event Frequency (PLEF), Chance of Secondary Loss (CSL)	Secondary Loss Event Frequency (SLEF)	*SLEF=Binomial (n=PLEF, p=CSL)*
4	Threat Event Frequency (TEF) Vulnerability (V)	Mean of PLEF (MPLEF)	*MPLEF=TEF*V*
5	Mean of PLEF (MPLEF)	Primary Loss Event Frequency (PLEF)	*PLEF=Poisson(λ=MPLEF)*
6	Loss Event Frequency (PLEF/SLEF), Loss Magnitude (PLM/SLM)	Primary/Secondary Loss (PL/SL)	*PL=RA(PLEF, PLM), SL=RA(SLEF, SLM)*
7	Primary Loss (PL), Secondary Loss (SL)	Total Loss (TL)	*TL=PL+SL*

Table 1: Variables and functions in the FAIR model

It can be observed that the first 5 steps of assessing risk in the FAIR model are associated with the frequency of loss events, and the last 2 steps are for calculating the magnitude of loss, therefore the whole risk assessment process can be divided into two procedures: steps 1-5 for calculating the frequency of loss events and steps 6-7 for assessing the total magnitude of loss. Each variable in the model is one of the risk factors and the functions can be calculated using SIPmath (The Open Group, 2019), a plug-in example generation tool, and building the model in Excel. Also, the sample distribution of each dependent variable can be derived not only by calculating the independent variables, but also by random simulation based on a user-specified triangular distribution.

This section describes the risk factors that pose a threat to the organisation and the relationship between them in terms of their influence, including primarily an assessment of the likely frequency of loss events and the possible magnitude of losses. Although the variability of risk factors may be reflected in different categories or scales of organisations, the risk taxonomy and assessment process for each risk factor in FAIR can still be worthy of application by organisations, and equally applicable to the healthcare organisations focused on in this paper, as it could be a significant contribution to mitigating risk and controlling financial losses.

3.3 CTI- based RA Model

With a view to promoting the implementation of effective security risk assessments in healthcare, it is essential to develop an understanding of and familiarity with the risks themselves before evaluating threat risks. Nevertheless, the amount and variety of CTI information currently available on the Internet is so vast that organisations are likely to be overwhelmed by it, especially in the healthcare sector. Therefore, the CTI-based risk assessment methodology proposed in this study provides healthcare organisations with a

comprehensive and targeted view of CTI-RA that will help organisations identify the most relevant CTI information to them, including the motivations, resources and skills of threat agents, as well as the tactics, techniques and procedures (TTP), etc used to execute the threat, Not only could this information be used to effectively assess risk and loss, but it would also assist healthcare organisations to improve their perception of the vulnerability of threatened assets and the effectiveness of controls, ultimately achieving the objective of contributing to more effective risk control and decision making by the organisation (board of directors or security specialists).

This research suggests the CTI-based RA model (as shown in Fig. 4), which integrates some widely adopted frameworks and practices. This model takes into account CTI and RA at three levels - technical, strategic and decision-making to support healthcare organisations in securing their assets and reducing financial losses from risk so that they can robustly achieve their operational and business goals. The technical level involves identifying attributes such as TTPs, objects, and indicators of threat events, which are contained in STIX (a structured and standardised CTI specification). After analysing and accessing this information, organisations could more fully understand the types of threats they are defending against and the associated characteristics, and can then develop arrangements related to targeted strategic perspectives. For example, organisations may use threat trend analysis to enhance the direction of corresponding technology developments; in addition, according to the object or target of the threat, they can protect specific assets and conduct vulnerability patching or strategy defence. For the decision-making level, this study recommends that healthcare organisations refer to the Centre for Internet Security's Critical Security Controls (CIS-CSC) principles and measures, which are authoritative and comprehensive controls for the cyber security domain and will guide organisations to make more informed decisions.

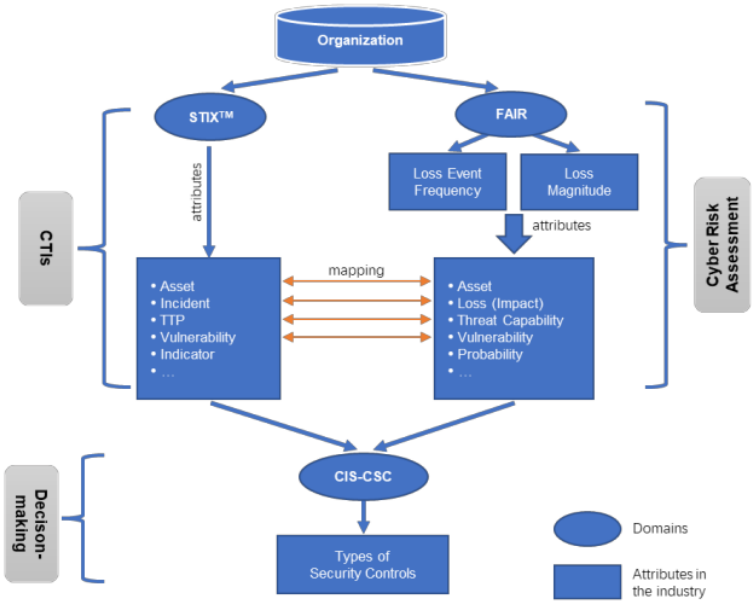

Fig. 4: The CTI-based RA model

3.3.1 CTI Model

Considering that in addressing threats, regardless of risk assessment and security control, organisations may not be expected to make informed security decisions if they do not have detailed information on the characteristics of the threat, therefore, the STIX model has been selected as the recommended CTI specification for organisations in this study, due to its comprehensive and structured presentation of threat information, which encompasses all dimensions of current CTI (Barnum, 2012).

STIX provides a normative and standard information structure for cyber threats, which is a language developed collaboratively by all cyber security stakeholders. A common mechanism is defined in the STIX model in order to structure CTI and improve efficiency, consistency, interoperability, and overall situational awareness in threat analysis. Besides, the flexibility and extensibility benefits of STIX are the reason why it is being adopted by more and more organisations, since organisations are given the flexibility to select any element of this structured language to construct security use cases that are strongly correlated to the threat they are suffering from to control the risk. Notably the various elements and attributes in the STIX unified architecture, such as TTP, assets, vulnerabilities, metrics, etc., of which this study focuses on elements that could be mapped to the attributes in risk assessment (RA), by combining them with RA to improve the application of RA in the healthcare sector.

3.3.2 CTI Mapping Risk Assessment (RA)

In order to facilitate more comprehensive risk control and decision-making in healthcare organisations, one of the objectives of this study is attempting to map CTI to an organisational risk framework, that is, to combine CTI with RA and establish a bridge between CTI and RA, which is the novelty of the study, with the aim of helping healthcare organisations to improve their overall cyber security and reduce the financial losses caused by cyber-attacks.

One of the challenges during the process of this part of the research has been the requirement to identify the common features between CTI and RA if the two are to be mapped or linked. After in-depth analysis, it can be found that among the various attributes contained in the CTI (STIX), there are many points that could be matched with the attributes of risk assessment, despite the differences in the definitions and characteristics of their various attributes. Consequently, this study takes this as an entry point, focusing on the same or similar attributes in the CTI and RA by correlating them and mapping them one-to-one or one-to-many. Through this approach, organisations could consider both CTI and RA when faced with a threat or risk, to quickly identify and locate the risk and then implement effective and informed decision-making or control tools. The design and analysis of the CTI and RA mapping framework is outlined below (Fig. 5).

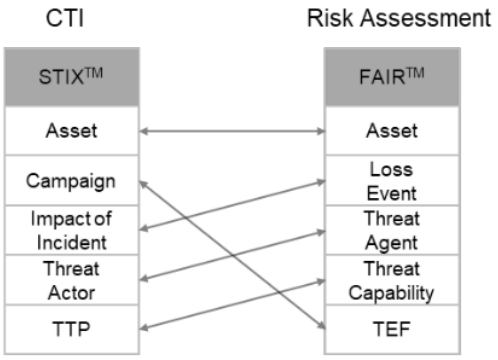

Fig. 5: Mapping relationship between CTI and RA

- Asset - Asset. The assets in CTI may be people, facilities or data that may be subject to attack by a threat agent. When assets are threatened or compromised, organisations have to bear the risk of loss, in both financial and non-financial terms, and for healthcare organisations in particular, this is a strike they do not expect to suffer. Similarly, assets in FAIR are information, components or systems that could be destroyed or impaired by threat agents and the value of the asset would be diminished or have a negative impact on stakeholders.

  The study found that healthcare organisations' assets, which mainly include medical equipment, web servers and electronic medical records, etc., once targeted by threat agents, would not only result in the loss of the assets of organisations, but more importantly, the leakage or even tampering of patients' personal privacy data, which is a matter of health and safety for patients and thus deserves to be treated seriously.

- Attack Pattern, Infrastructure, Malware – Threat Capability. TTP was defined in early CTI as tactics, techniques, or procedures, representing modus operandi, which are the resources or actions of a threat agent to execute an attack. One example of a tactic could be the use of malware by a cyber hacker to steal patients' medical data privacy; a technique might be an attacker using network protocols and commands to send an email with malicious code to an organisation's employees, and once someone clicks on it, the malicious code would automatically execute and obtain private information such as credit card accounts, passwords, etc. that the employee types from a keyboard; employing a procedure as a resource for an attack could be reflected in an attacker developing an open source software with specific vulnerabilities or backdoors that are difficult to discover and as users use it, they would unwittingly expose their personal privacy. Through development and optimisation, in STIX version 2.1, TTP has been further categorised into attack pattern, infrastructure, and malware, but its essence remains the same.

  The attribute in FAIR that can be mapped to TTP is threat capability (TC), which stands for the level of force an attacker has to exert the threat, and the manifestation also includes technology and resources, as well as time. Based on the mapping of these two, organisations could understand more details about the threat agent and the threat itself, which in turn allows them to rate the capabilities of the threat agent at a percentile and judge the probability of loss. Since threat agents with different

capabilities could attack different assets and cause different losses, it is recommended for healthcare organisations to categorise threats and assets and implement a targeted strategy.

- Campaign - Threat Event Frequency (TEF). Campaign, also called wave, is described in STIX 2.1 as a set of malicious attacks or activities executed by threat agents against a specific target over a certain period of time, and it is correlated with the TEF in FAIR, which contains two factors: contact frequency (CF) and probability of action (PoA). In comparison, PoA quantifies the campaign, allowing organisations to calculate and assess risk events more effectively. Moreover, it is essential to note that a threat event is not the same as a loss event (The Open Group, 2021), because an attack launched by a threat agent is not necessarily a successful event; only a successful event would cause a loss to the organisation. This will therefore provide a reminder to healthcare organisations of the increased necessity to focus on loss events and loss targets, with prevention and control measures in place.
- Impact of Incident – Loss Event. In the incident description or summary of threat events in CTI, the threatened assets and the (expected) impact or impact magnitude caused are usually involved. Likewise, in FAIR, these impacts are referred to by the loss event, and the process of assessing the loss magnitude actually quantifies the impact, with the final total loss being derived by calculating the primary loss (PL) and secondary loss (SL) (as in Table 1). The Open Group (2021) has defined six forms of loss (as in Fig. 6), with primary loss comprising three possible forms, and secondary losses could account for 4 of them.

  It can thus clearly show that when an organisation experiences a threat, it is not necessarily the financial aspects that are lost, but also the non-financial aspects such as loss of reputation. Accordingly, the recommendation from this study is that healthcare organisations can integrate CTI and RA and carry out some quantitative analysis and classification when faced with the impact of a threatening event. Also, prioritisation of losses can be performed to prioritise the primary forms of major losses, reducing as much as possible the negative impacts and losses due to the risk and avoiding unnecessary secondary losses.

- Threat Actor – Threat Agent. Both are those people, organisations or objects that have malicious intent and may take any action to harm the assets of the organisations.

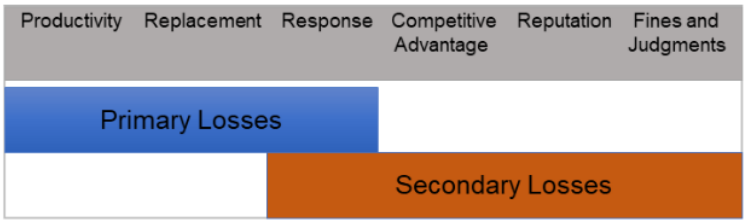

Fig. 6: Forms of Loss

Above lists and analyses the mapping framework between CTI and RA, and explains the mapping relationship. In healthcare, CTI can be mapped to an organisational risk framework, which helps organisations to make a quantitative assessment of risk based on a full

understanding of threat details. Given the demand to protect assets and mitigate various losses, organisations need proper and effective risk assessment, which will promote more informed control or mitigation measures based on the assessment results.

3.3.3 Decision-making (Controls)

Cyber security risk control is a general methodological recommendation and technical strategy for dealing with cyber threats and attacks.

The CIS-CSC is intended for organisations to carry out maintenance of data confidentiality, usability, and integration by providing some basic technical specifications and methods. The CIS-CSC has now been upgraded to version 8.0, with 18 controls including hardware and software authorisation management and attack defence, and emphasises employee security awareness and skills development, etc. Some of the priority control actions in the CIS-CSC could help organisations to respond effectively to common cyber-attacks and reduce losses, so it can be applied to the healthcare sector, where organisations can analyse the risks and take relevant controls to defend or mitigate the attack.

Chapter 4: Design and Implementation

The objective of this section is to visualise specific CTI data and risk mitigation measures in the healthcare field, with the aim of giving organisations the most relevant and intuitive view of the various threats and risks that exist in healthcare, assisting them with effective asset protection and clear risk prediction, ultimately taking control of risk and making decisions based on the authoritative mitigation measures provided by the industry.

In addition, the major steps consist of data collection, integration, processing, and visualisation of the results, which will focus on analysing some of the difficulties or challenges during the study, as well as strategies and rationale for solving them.

4.1 Data collection

4.1.1 Dataset

As so far there is no independently accessible public dataset in the CTI field that is strongly relevant to healthcare, one of the challenges of this study is to filter and merge several different, general cybersecurity-related data sources into a CTI dataset specific to the healthcare industry, and then analyse and process the data.

The first dataset chosen comes from one of the National Institute of Standards and Technology's (NIST) products: the National Vulnerability Database (NVD), an official and authoritative standards-based public database for vulnerability management, security measurement and compliance automation. The NVD is a cybersecurity vulnerability database that "integrates all publicly available U.S. government vulnerability resources and provides a reference to industry resources" (Booth et al., 2013), and is based on and synchronised with CVE, a directory of data for identifying and classifying publicly disclosed cybersecurity vulnerabilities. The NVD has been used in a wide range of research applications for vulnerability analysis and cyber threat prediction (Zhang et al., 2011; Zhang et al., 2015; Williams et al., 2018). Organisations or individuals can browse relevant vulnerability entries by filtering through search keywords and conditions (e.g., Fig. 7). If the keyword "healthcare" is typed in, part of the query results are shown in Fig. 8, where it can be found that the data table structure has three columns, which are the vulnerability ID, the vulnerability summary, and the CVSS severity rating (the full name of the Common Vulnerability Scoring System, an open framework for representing the features and severity of vulnerabilities). In addition, the NVD will display 20 entries per page, and the value of the vulnerability ID is unique.

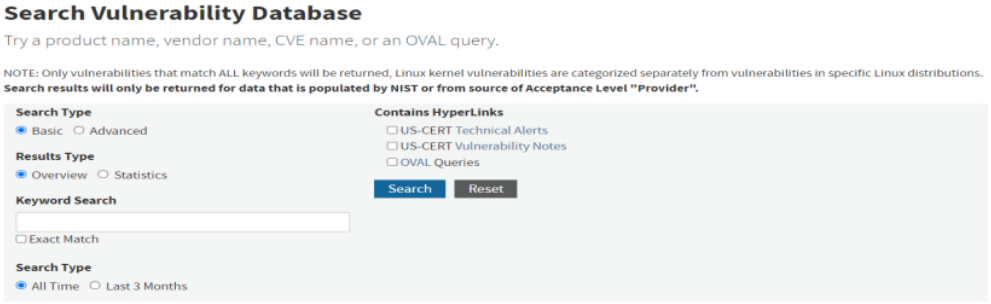

Fig. 7: Homepage of NVD

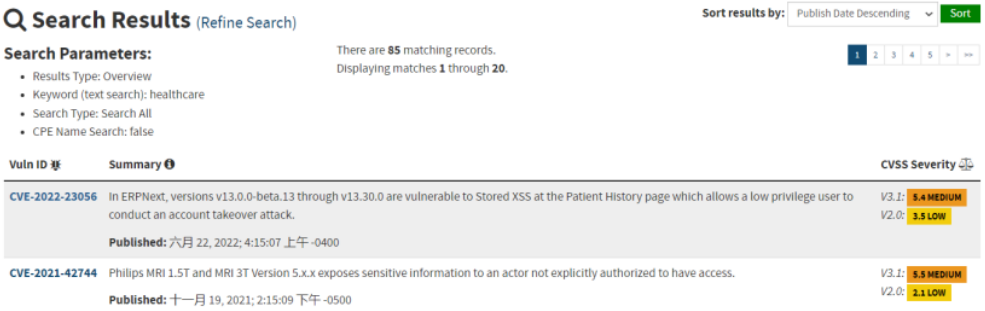

Fig. 8: Data of NVD

Another source of data is the healthcare-related information breach report (hhs.gov) published by the US Department of Health and Human Services (HHS), which is focused on protecting the health of all Americans. This report is used to record data breaches in different states in the US in the form of a table, which currently contains almost 5,000 data entries and is still being updated. Similarly, information could be filtered based on criteria such as time, type of breach, etc. (as in Fig. 9), and the table contains information on when, where, and what type of data breach occurred. In addition, the dataset allows to be downloaded locally in excel, csv and pdf format, making it easier for users to carry out data analysis.

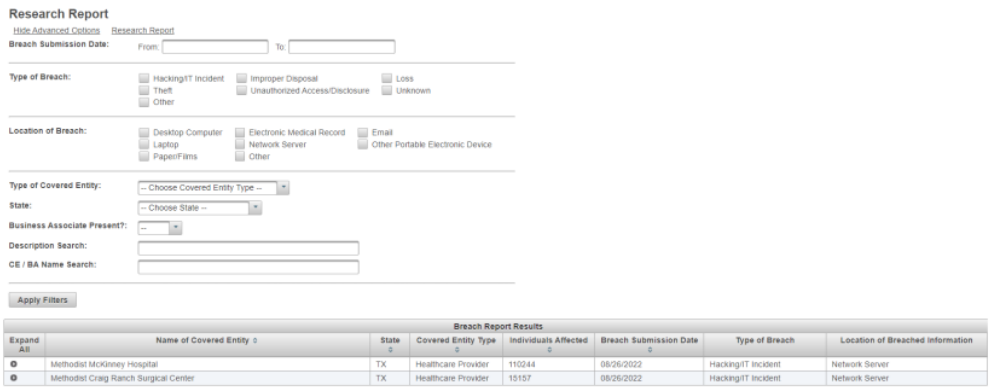

Fig. 9: Data breach report from HHS

These two data sources are selected not only because they can be filtered for public and authoritative data specific to the healthcare sector, but more importantly, on the one hand, patient privacy data breaches are known to be one of the major cybersecurity issues in healthcare, and breach reports from HHS could facilitate more effective data protection for organisations; and on the other hand, vulnerabilities in medical devices or software could also lead to privacy breaches and loss of organisational assets, and data analysis of the NVD would potentially be beneficial for organisations to fix major vulnerabilities and achieve targeted attack prevention and asset protection.

4.1.2 Data crawling

As the data from the HHS leak report can be downloaded directly from the official website in csv format, this paper focuses on the implementation process of crawling data from the NVD using python crawler technology.

Considering that the NVD is a generic vulnerability database with vulnerabilities from various industries, this study requires three data crawls of the NVD using the keywords healthcare, hospital, and patient as query criteria respectively. Taking healthcare as the keyword for example, Fig. 10 shows the results of a manual search in the webpage, and it can be found that filtering for the keyword healthcare resulted in a query of 85 records, 20 records per page, 5 pages in total. As such when implemented via python code, multiple pages of data crawling are involved. Moreover, the query results are in a tabular form on the web page and is the only table in the web interface. After clarifying these web pages and data characteristics, the process of crawling the data through the "pandas" library in python is shown in Fig. 11. To confirm the accuracy of the crawling process, a printer is added to the code, printing "crawl complete" and a prompt for the crawled data entry for each page of data fetched. Upon completion of each page, a new csv file will be created and saved to a local csv file, with the save mode set to "a+", indicating incremental saving, which will not overwrite previously saved data.

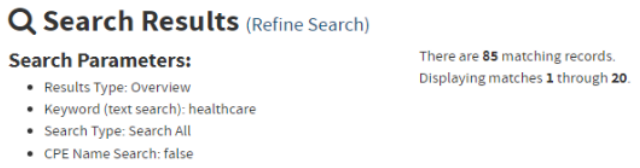

Fig. 10: A manual search from NVD

```
import pandas as pd

p1 = 1
for i in range(0,81,20):  # Crawl all 5 pages of data
    url = 'https://nvd.nist.gov/vuln/search/results?isCpeNameSearch=false&query=healthcare&results_type=o
    tb1 = pd.read_html(url)[0]   #The required table is the 1st table in the website
    tb1.to_csv('Vuln.csv', mode='a+', encoding='utf_8_sig', index=False)
    print("Page " + str(p1) + " crawl completed! " + str(len(tb1)) + " rows.")
    tb = pd.read_csv("Vuln.csv")
    p1 += 1
print(tb.shape)
# print(tb.head())
```

✓ 11.7s

```
Page 1 crawl completed! 20 rows.
Page 2 crawl completed! 20 rows.
Page 3 crawl completed! 20 rows.
Page 4 crawl completed! 20 rows.
Page 5 crawl completed! 5 rows.
(89, 3)
```

Fig. 11: Data crawling from NVD

According to the results, 85 records have been crawled, because each page contains a table header, the data saved to the csv file is 89 rows and 3 columns, with 4 extra rows of table headers. Similarly, for the hospital and patient keywords, only a few variables need to be

changed in the code to achieve a different data crawl. The result is a total of 530 rows and 3 columns of data crawled and saved to a csv file (as in Fig. 12). Although there may be some duplicate items in the query results for the different keywords, this will be de-duplicated in the data pre-processing section below.

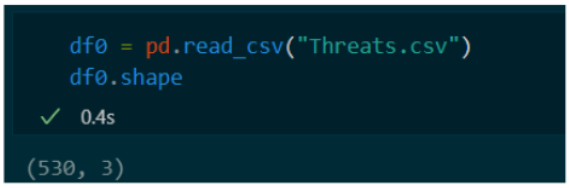

Fig. 12: Results of the data crawl from NVD

4.2 Data pre-processing

Data pre-processing, also known as data cleansing, is a process that involves replacing or removing missing values, duplicate values, outliers, etc. from the data. For a clearer follow-up data analysis, this study also performs data sorting. It should be noted that since there is only a summary of vulnerabilities in the NVD, neither a classification of vulnerabilities or threats nor corresponding mitigation measures are available, so one of the contributions of this study is the extraction and classification of keywords for the summary of vulnerabilities, and the addition of matching possible impacts and mitigations for different types of vulnerabilities or threats through data aggregation.

The whole data processing can be divided into the following two phases: data filtering, and keyword matching & data aggregation.

4.2.1 Data filtering

As the NVD data is obtained through crawlers, while the HHS data is a directly downloaded csv file, more data processing steps are required for the NVD dataset. The following data filtering operations are based on the NVD dataset as an example, and the processing of the HHS dataset is similar.

The first step of data filtering is to check whether missing values exist in the dataset. The NVD dataset is queried by the built-in missing value judgment functions *isna()* and *isnull()* in python, and the results are both False, indicating that there are no missing values in the dataset. The next step is to delete the duplicate values in the dataset, using the built-in function *duplicated()*, the execution result is shown in Fig. 13, which shows that 70 duplicate values exist in total, and the dataset after deletion is 460 rows and 3 columns. To improve retrieval efficiency, the *drop_duplicates()* function is used here to retrieve only the "Vuln ID" column in the dataset, as the value of this column should be unique, and then the parameters are set to reserve the first duplicate entry. What is likely to be ignored in the data filtering process is that two header rows still exist in the current dataset, one is the real header and the other is kept as a data entry, so perform another deletion step and the result can be seen in Fig. 14, remaining 459 rows and 3 columns. Due to the index values remaining unchanged after data de-duplication, which would result in a discontinuous index, a third step is performed: sorting. After sorting the "Vuln ID" in descending order using the *sort_values()* function,

save the dataset as a new CSV file so that when the csv file is read again, the index values become ascending from 0.

Fig. 13: Data de-duplication 1

Fig. 14: Data de-duplication 2

The final step is outlier handling, but the useful CTI information is only described in the "Summary" variable, which is a categorical variable and cannot determine outliers. Given that the subject of this study is healthcare and that the data is crawled using healthcare-related keywords, as a consequence, this study decides to treat irrelevant values as outliers, meaning that data entries that are not relevant to healthcare will be removed. It was observed that several data items contain the "non-medical device" field in Summary, which means that the vulnerability is not related to healthcare and thus they need to be removed, otherwise the final statistics would be affected. The code implementation is as follows.

```
# Removing outliers
df1 = pd.read_csv("Threats_new.csv")
noOutlier = df1.copy(deep = True)     # Copy both the index and data of the object
row_remove = []
for row in range(len(df1)):
    if df1.loc[row, "Summary"].casefold().find("non-medical device") == -1:
        continue
    else:
        # print(row)
        row_remove.append(row)
        noOutlier.drop([row], inplace = True)
```

4.2.2 *Keyword matching & Data aggregation*

When data from a single source does not meet the statistical requirements of the data, it becomes necessary to collect data from multiple sources and further aggregate and process them. In this study, one of the challenges is that the collected NVD and HHS datasets include only basic CTI information, which is not enough for healthcare organisations to master, they also need to extract valid elements from the CTI, moreover, some authoritative and standard mitigation measures or recommendations are also required. Therefore, one of the contributions of this project is in this aspect.

Most of the data processing work in this study is for the NVD dataset, as the CTI information is only included in its summary. Therefore, before obtaining data on mitigation measures from other sources, keyword matching and extraction operations are made on the NVD dataset. The keywords are collected from The Web Application Security Consortium (WASC) (2010), a non-profit organisation established by international cyber security experts and organisations that have currently developed a wide range of security standards and best practices for the Internet. In the WASC, a series of threat vulnerabilities and attacks are classified, such as buffer overflows, denial of service, SQL injection, insufficient authorisation and so on. Sixteen of these commonly used keywords are used in this study and stored in a list variable, by comparing and matching them with the fields in the NVD dataset "Summary", if a data entry is successfully matched, the keyword will be extracted and stored as the value of the new column "Threat Type", otherwise its value will be set to "Other vuln". The implementation codes are shown below.

```
df2 = pd.read_csv("Threats_new.csv")
df2.shape          # (450, 3)
kwList=[]
threatList = []
def kwordMactching(df):
    for row in range(len(df)):
        for i in range(len(kwordMap)):
            if df.loc[row][1].casefold().find(kwordMap[i].casefold()) != -1:
                kwList.append(kwordMap[i])
                threatList.append(threatMap[i])
                break
            else:
                if i==len(kwordMap)-1:
                    kwList.append(kwordMap[-1])
                    threatList.append(threatMap[-1])
    return threatList
threat=kwordMactching(df2)
```

```
pd.value_counts(threatList)
✓ 0.4s
Insufficient Authorization         169
SQL Injection                       82
Insufficient Authentication         44
XSS Attack                          39
Other vuln                          25
Brute Force                         25
Denial of service                   19
Insufficient Process Validation     18
SSL Injection                       10
Buffer Overflow                      8
Improper Input Handling              6
Information Leakage                  5
dtype: int64
```

Fig. 15: Results of keyword matching

The statistics for keyword matching are shown in Fig. 15. Also, to analyse the prevalence of vulnerability threats, the year field contained in the "Vuln ID" is extracted, using the split function *split()*. As a next step, mitigations for these vulnerability threats are gathered from different sources at the Cybersecurity and Infrastructure Security Agency (CISA), the official US website dedicated to providing cybersecurity-related best practices and various resources. Since the relevance of mitigations information for different threats needs to be determined, a manual data aggregation approach is adopted for this study. For instance, in Fig. 16, threat keywords are searched from CISA first, and then mitigations data can be collected from the most relevant results saved to a new csv file. Similarly, this study also collects healthcare specific mitigations and authoritative recommendations on threat vulnerabilities and data breaches from other security organisations and CTI platforms, such as AVERTIUM, CIS (Center for Internet Security), MITRE, with the data categorised and integrated into different csv files, in order to prepare for later data visualisation

Fig. 16: Information retrieval from CISA

4.3 Data visualization in web

The data visualisation in this subsection focuses on the application of the Streamlit framework in Python, which implements the visualisation of CTI data analysis results and mitigations corresponding to threats or risks. The goal of the visualisation is to help individuals or organisations in the healthcare sector to gain a deeper understanding of CTI, identify potential threats or risk trends in the current field, and provide some targeted and practical risk mitigations and recommendations that may assist organisations in making more effective risk control and more informed decision making.

4.3.1 Interface layout design

The overall layout of the visualisation interface is designed as a sidebar and a main interface, with the sidebar containing mainly optional conditions such as drop-down and selection boxes, and the main interface containing the results and text of the data statistics, displayed in multiple columns or segments.

The implementation of the sidebar layout is accomplished through the interface component in streamlit, such as *selectbox()*, *checkbox()*, *button()*. The partial codes are:

```
import streamlit as st
# Sidebar
st.sidebar.header("Please select here:👇")
risk = st.sidebar.selectbox(
   "Please choose Risk Type:",
   ("Data Breach", "Vulnerability")

CISA = st.checkbox("CISA (General Mitigations)")
button1 = st.form_submit_button()
```

The multi-column design of the main interface uses the *columns()* function with the following code.

```
# Columns layout
col1, col2, col3, col4 = st.columns(4)
# Info
with col1:
    st.subheader("Year:")
with col2:
    st.subheader("Type of threats:")
with col3:
    st.subheader("Number of threats:")
with col4:
    st.subheader("Country:")
```

The general layout implemented is shown in Fig. 17.

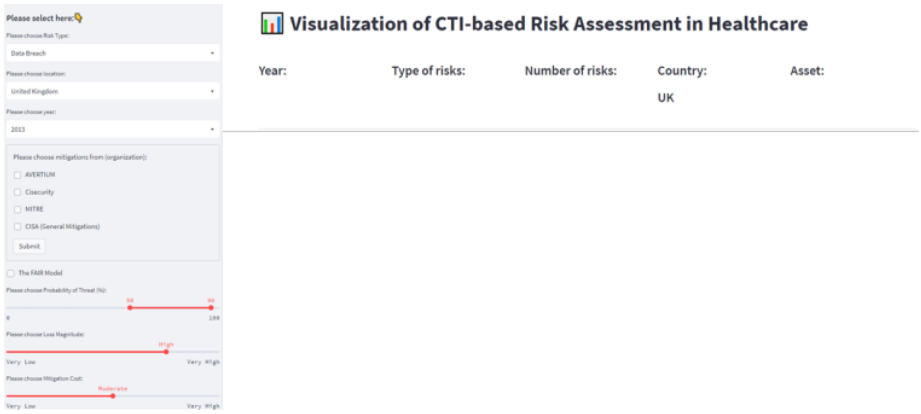

Fig. 17: Overall layout for visualisation

4.3.2 Data analysis visualisation

The data analysis visualisation includes two aspects: statistical distribution, and data recall from datasets.

Before visualising the statistical distribution on the web, the distribution graphs (e.g., bar and line graphs) need to be drawn by "pyplot" library in Python, and then call the plot to display on the web via Streamlit. The partial codes are:

```
def bar(year):
    fig = plt.figure()
    df = df_breach[["Year","Breach Type"]][df_breach.Year==year]
    df["Breach Type"].value_counts().sort_index().plot.bar(color=colors,width=0.8)
    plt.ylabel('Number')
    plt.xlabel('Risk Type')
    plt.title("Risk distribution in " + str(year))
    st.pyplot(fig)
    return

def line(threat):
    fig = plt.figure()
    plt.ylabel('Number')
    plt.title(threat)
    breachGroup[threat].T.plot(kind="line",marker="o")
    # st.line_chart(threatGroup[threat])
    st.pyplot(fig)
    return
```

Statistical distribution graphs mainly include bar, line, and pie charts. Bar charts analyse the distribution of different threats or risks in a certain year, line charts show how the magnitude of a particular threat changes over the years, and pie charts illustrate the proportion of various threats to a particular asset of organisations. Fig. 18 presents the final graphs on the web after coding by "pyplot".

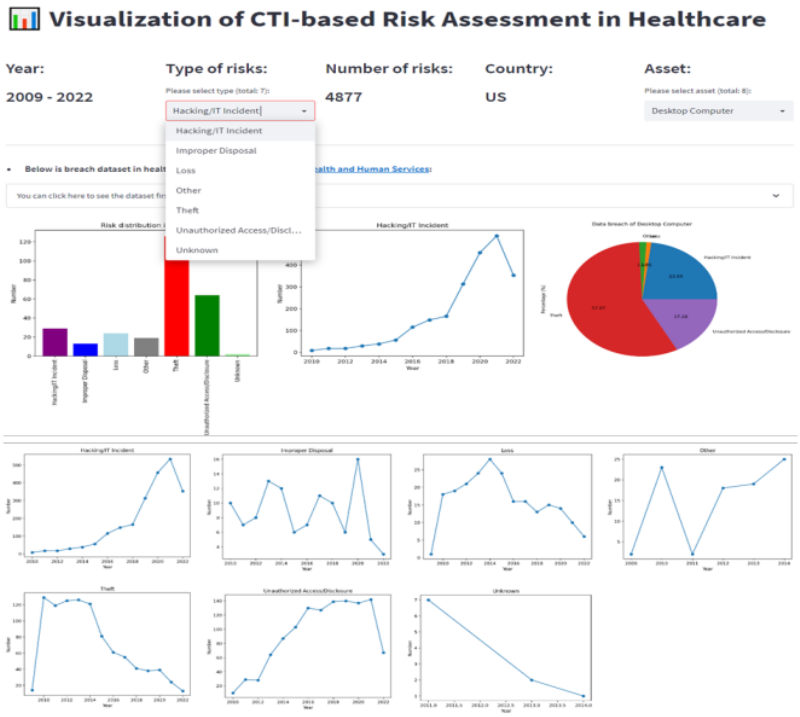

Fig. 18: Visualisation of statistical distribution

For the FAIR model, this study currently only briefly implements some basic functionality that allows organisations to further determine which security institution's mitigation recommendations to select according to the base situation when faced with a threat, which consists of the two elements of the FAIR model, Threat Event Frequency (TEF) and Loss Size (LM), coupled with the organisation's budget for the cost of mitigations that can be carried out. The visualisation result is shown in Fig. 19.

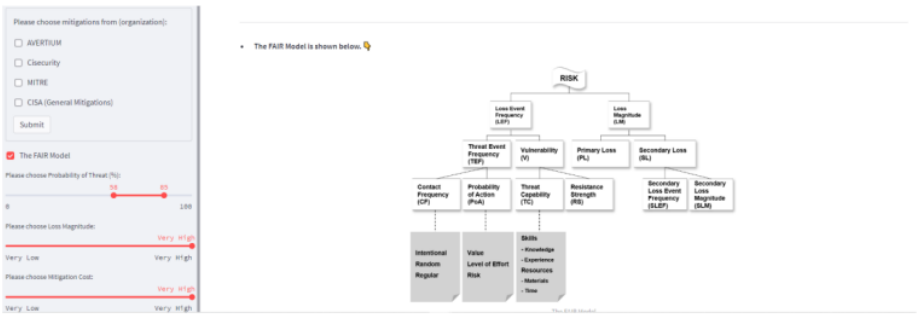

Fig. 19: FAIR visualisation

Furthermore, this study also provides the visualisation of controls or mitigations from different sources for various risks by calling different csv files, with some filters through python commands, and finally presents the query results on the web by Streamlit, partial code

implementation is given below. This is also a process of data aggregation, which is similar to SQL data queries. The visualised result is shown in Fig. 20.

```
breachType=st.multiselect(
    f"Please select data breach type (total: {len(breachMap)}) to see mitigations in
healthcare:",
    options=breachMap
    )
for item in breachType:
    if item == "Unknown":
            mitigation=df_mitigation.Mitigations[df_mitigation["Threat/Breach Type"]==item]
        # mitigation=df_mitigation.loc[df_mitigation["Threat/Breach Type"]==item]
        mitigation.index=np.arange(1,len(mitigation)+1)
        st.markdown(f"- Mitigations for **{item}**: ")
        st.write(mitigation)
    else:
        df_m0=df_mitigation.Mitigati[df_mitigation["Threat/Breach Type"]==item]
        df_m0.index=np.arange(1,len(df_m0)+1)
        df_m1=df_m0[1]
        df_m2=M1["Mitigations"][M1.Object==df_m1]
        df_m2.index=np.arange(1,len(df_m2)+1)
        st.markdown(f"- Mitigations for **{item}**: ")
        st.write(df_m2)
```

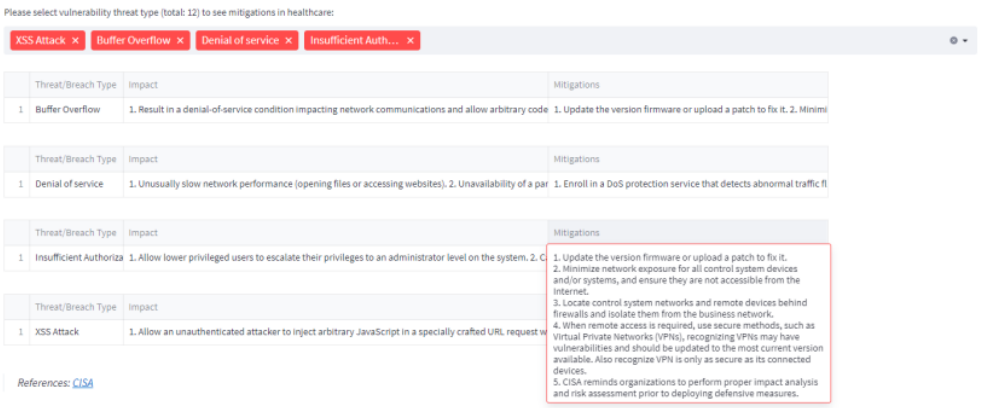

Fig. 20: Visualisation of mitigations

Chapter 5: Testing and Evaluation

This section will test and evaluate the results of the data visualisation. The testing will focus on the functionality and overall performance of the various modules that have been implemented in the current web visualisation, while the evaluation will be wider in scope, mainly involving comparisons with common visualisation standards and with the work of other researchers, so as to analyse the strengths and limitations of this study.

5.1 Testing

The testing process for this study included the following elements:

No.	Test element	Description	Result
1	Single select box	The single select boxes can drop down and select elements normally.	*Success*
2	Multi-select box	The multi-select boxes can drop down and select single or multiple elements normally.	*Success*
3	Button	The "Submit" button can be clicked normally	*Success*
4	Bar chart	Bar charts display normally.	*Success*
5	Pie chart	Pie charts display normally.	*Success*
6	Line chart	Line charts display normally.	*Success*
7	Text display	Text of all charts display correctly.	*Success*
8	Dataset display	Dataset display normally.	*Success*
9	Interaction	All interactable objects are normal and quickly responsive.	*Partial success* *(When the year is selected as "past-now", the line chart results are displayed slowly, and the same line charts are reloaded slowly while other operations are performed.)*
10	Error warnings	Any unreasonable operation should trigger an alert or warning.	*Success*

Table 2: Test items and results

5.2 Evaluation

This subsection will evaluate the results in three perspectives, firstly by comparing the results of the study with some common standards, for example from Google (2022) and IBM (2021), and secondly by comparing them with the existing work of other researchers, and moreover, a scenario simulation study will also be considered for evaluation.

5.2.1 Standards from Google and IBM

Source	Standards	Result
Google	Accurate	*Considered*
	Helpful	*Partly considered*
	Scalable	*Not considered*
IBM	Set the context	*Not considered*
	Know your audience(s)	*Considered*
	Choose an effective visual	*Partly considered*
	Keep it simple	*Considered*

Table 3: Visualisation standards from Google and IBM

No.	Element	Description	Result
1	Environment	Surfaces/Elevation/Light and shadows	*Not involved*
2	Layout	Predictable/Consistent/Responsive	*Considered*
3	Navigation	Navigation transitions/Search	*Not considered*
4	Colour	Consistent/Distinct/Intentional	*Considered*
5	Typography	Font/Language	*Partly considered*
6	Sound	Informative/Honest/Reassuring	*Not involved*
7	Iconography	Product icons/System icons/Animated icons	*Partly considered*
	Shape	Size/ Morphing/Components	*Not considered*
8	Motion	Informative/Focused/Expressive	*Not involved*
9	Interaction	Gestures/Selection/States	*Partly considered*
10	Communication	Alert dialog/Date and time/. etc	*Considered*
11	Machine learning	Object detection/Barcode scanning	*Not involved*

Table 4: Visualisation elements from Google

5.2.2 Comparison with other research works

By comparing this study with other research works, some analytical findings are as follows. A taxonomy on CTI was suggested by Burger (2014), which facilitates the shared automation of CTI; and Planqué (2018) proposed a CTI model for intelligent creation processes, but the model only stayed at the conceptual level. Further, a trigger-enhanced actionable CTI discovery system (TriCTI) incorporating natural language processing (NLP) techniques was created by Liu et al. (2022) to enable accurate discovery and exploitation of CTI, but these studies share the commonality of not caring about RA. Mukhopadhyay et al. (2019) proposed a quantitative CRAM model for calculating risk probabilities and predicting losses, but the model did not involve CTI. However, combining CTI would be more effective in conducting assessments of the risks to organisations, as CTI can provide an in-depth understanding of the details of the threat.

Studies with similar research themes as this paper, for example, Kure and Islam (2019) also integrated concepts related to CTI and CSRM (Cyber Security Risk Management), though the objective of the study was also to assess risk to protect cyber security, but unlike this study, their target domain was critical infrastructure (CI). In addition, the researchers used more CSRM standards than this paper, such as Common Weakness Enumeration (CWE), NIST SP800-30, ISO 27005, etc. However, they did not consider presenting visualisations of CTIs and risks to organisations. Healthcare, as a dynamic environment where human life and health are of concern, requires a comprehensive threat handling and risk control solution, and by mapping CTI into RA as well as visualising the data presentation, it will be more beneficial to provide guidance strategies to the organisation.

5.2.3 Scenario simulation study

Due to the lack of realistic healthcare scenarios in practice, this study also evaluates the results through a basic simulation scenario.

Assuming a scenario exists where a healthcare organisation is experiencing a cyber-attack, this visualisation interface allows the organisation to compare year-on-year risk trends, determine the current type of risk and quickly identify compromised assets. The FAIR model can then be used to assess risk factors and make decisions based on the mitigations corresponding to the assets.

It can be found in this process that although some mitigations may help organisations to make effective decisions, a detailed risk assessment cannot be made through this web interface, which is one of the shortcomings of this project.

5.3 Limitations

Comprehensive analysis of the above tests and evaluations reveals that there remain significant points to be optimised, such as speed of interaction, interface layout, components, navigation, and typography, although some basic criteria have been considered or partially considered. Also, since the data in this study is all called via csv rather than database, this may limit the system performance to some extent. Furthermore, the data visualisation only implements part of the CTI-RA model and does not integrate all the algorithms of the FAIR model into the input and output system of the visualisation.

Therefore, in order to make more effective contributions in healthcare, more functional and practical visualisation implementations would be required, combined with richer CTI and RA frameworks, to promote more informed safety decisions in healthcare organisations.

Chapter 6: Conclusion and Future Work

This study has analysed the gap that could currently exist in the field of cyber threat intelligence (CTI) combined with risk assessment (RA) in healthcare, and has designed a novel CTI-based RA model that can be used to facilitate organisations to conduct risk assessment and loss control more effectively. Moreover, another contribution of this work is the data visualisation of healthcare-specific CTI-RA as well as the presentation of relevant risk mitigations and recommendations for healthcare organisations. Consequently, the integration of technical-level CTI with management-level RA and its application to strategic-level security decisions is accomplished, thus promoting effective risk identification and assessment and more informed decision-making in healthcare organisations.

However, the protection of cyber security in the healthcare sector will not stop here, and future work on this research could optimise the CTI-RA model, for example by integrating more CTI and RA frameworks to it. Also, improving the user interface design of data visualisation systems, adding input-output settings of the FAIR model, and using machine learning algorithms to provide more practical mitigations for healthcare organisations would also be a promising endeavour.

From the perspective of the wider healthcare industry, the future direction can be a combination of big data and artificial intelligence technologies to accurately identify and locate risks, contributing to rapid response strategies and enhanced cyber security for organisations.

References

Abu, M. S. *et al*. (2018) 'Cyber threat intelligence-issue and challenges', *Indonesian Journal of Electrical Engineering and Computer Science*, 10(1), pp. 371–379.

Ahmed, A. *et al*. (2018) 'Malicious insiders attack in IoT based Multi-Cloud e-Healthcare environment: A Systematic Literature Review', *Multimedia tools and applications*, 77(17), pp. 21947–21965. doi: 10.1007/s11042-017-5540-x.

Al-Maitah, M., AlZubi, A. A. and Alarifi, A. (2019) 'An optimal storage utilization technique for IoT devices using sequential machine learning', *Computer networks (Amsterdam, Netherlands : 1999)*, 152, pp. 98–105. doi: 10.1016/j.comnet.2019.01.025.

Al-Mhiqani, M. N. *et al*. (2019) 'Review of cyber attacks classifications and threats analysis in cyber-physical systems', *International Journal of Internet Technology and Secured Transactions*, 9(3), pp. 282–298.

AlZubi, A. A., Al-Maitah, M. and Alarifi, A. (2021) 'Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques', *Soft computing*, 25(18), pp. 12319–12332. doi: 10.1007/s00500-021-05926-8.

Barnum, S. (2012) 'Standardizing cyber threat intelligence information with the structured threat information expression (stix)', *Mitre Corporation*, pp. 1–22.

Beavers, J. and Pournouri, S. (2019) 'Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions', in *Blockchain and Clinical Trial*. Cham: Springer International Publishing, pp. 249–267.

Booth, H., Rike, D. and Witte, G. A. (2013) *The national vulnerability database (nvd): Overview*.

Burger, E. *et al*. (2014) 'Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies', in *Proceedings of the 2014 ACM Workshop on information sharing & collaborative security*. ACM, pp. 51–60. doi:10.1145/2663876.2663883.

Chen, D. Y. (2017) *Pandas for everyone: Python data analysis*. Addison-Wesley Professional.

Conti, M., Dargahi, T. and Dehghantanha, A. (2018) 'Cyber Threat Intelligence: Challenges and Opportunities', in *Advances in Information Security*. Cham: Springer International Publishing, pp. 1–6.

Dandurand, L. and Serrano, O. S. (2013) 'Towards improved cyber security information sharing', in *5th International Conference on Cyber Conflict*. IEEE, pp. 1–16.

Data visualization (2022) *Google Material Design*. Available at: https://material.io/design/communication/data-visualization.html (Accessed: 8 September 2022).

Dhillon, G. and Backhouse, J. (2000) 'Technical opinion: Information system security management in the new millennium', *Communications of the ACM*, 43(7), pp. 125–128.

doi: 10.1145/341852.341877.

Dhillon, G. and Torkzadeh, G. (2006) 'Value-focused assessment of information system security in organizations', *Information systems journal*, 16(3), pp. 293–314. doi: 10.1111/j.1365-2575.2006.00219.x.

DOMARS (2018) *Threat modeling for drivers*, *Microsoft.com*. Available at: https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers (Accessed: 8 September 2022).

Ekelund, S. and Iskoujina, Z. (2019) 'Cybersecurity economics – balancing operational security spending', *Information technology & people*, 32(5), pp. 1318–1342. doi: 10.1108/itp-05-2018-0252.

Goodwin, B. (2020) 'Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack', *Computer Weekly*.

IBM Cloud Education (2021) *What is data visualization?*, *Ibm.com*. Available at: https://www.ibm.com/cloud/learn/data-visualization?mhsrc=ibmsearch_a&mhq=visualization (Accessed: 8 September 2022).

Jones, J. (2006) 'An introduction to factor analysis of information risk (fair)', *Norwich Journal of Information Assurance*, 2(1), p. 67.

Kabanov, I. (2016) 'Scalable Frameworks for Application Security and Data Protection', in *Global Security, Safety and Sustainability - The Security Challenges of the Connected World*. Cham: Springer International Publishing, pp. 82–95.

Kao, D. Y. and Hsiao, S. C. (2018) 'The dynamic analysis of WannaCry ransomware', in *20th International conference on advanced communication technology (ICACT). IEEE*, pp. 159–166.

Kiss, S. *et al.* (2022) 'Early prediction of acute necrotizing pancreatitis by artificial intelligence: a prospective cohort-analysis of 2387 cases', *Scientific reports*, 12(1), p. 7827. doi: 10.1038/s41598-022-11517-w.

Kure, H. and Islam, S. (2019) *Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure*.

Le, A. (2017) *Assessing loss event frequencies of smart grid cyber threats: encoding flexibility into fair using bayesian network approach Smart Grid Inspired Future Technologies*. Springer.

Le, A. *et al.* (2019) 'Incorporating FAIR into Bayesian network for numerical assessment of loss event frequencies of smart grid cyber threats', *Mobile networks and applications*, 24(5), pp. 1713–1721. doi: 10.1007/s11036-018-1047-6.

Lee, C. *et al.* (2022) 'StarGazer: A hybrid intelligence platform for drug target prioritization and digital drug repositioning using Streamlit', *Frontiers in genetics*, 13, p. 868015. doi: 10.3389/fgene.2022.868015.

Liu, J. *et al*. (2022) 'TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network', *Cybersecurity*, 5(1), pp. 1–16. doi:10.1186/s42400-022-00110-3.

Meng, W. *et al*. (2020) 'Detecting insider attacks in medical cyber–physical networks based on behavioral profiling', *Future generations computer systems: FGCS*, 108, pp. 1258–1266. doi: 10.1016/j.future.2018.06.007.

Mitchell, R.E. (2018) *Web scraping with Python : collecting more data from the modern web*. 2nd edition. O'Reilly.

Mukhopadhyay, A. *et al*. (2019) 'Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance', *Information systems frontiers: a journal of research and innovation*, 21(5), pp. 997–1018. doi: 10.1007/s10796-017-9808-5.

Park, M. (2018) 'Situational awareness framework for threat intelligence measurement of android malware JoWUA', *JoWUA*, 9(3), pp. 25–38.

Rehman, M. M. U., Rehman, H. Z. U. and Khan, Z. H. (2020) 'Cyber-attacks on medical implants: A case study of Cardiac Pacemaker vulnerability', *International Journal of Computing and Digital Systems*, 9(6), pp. 1229–1235.

Riesco, R., Larriva-Novo, X. and Villagra, V. A. (2020) 'Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and Smart contracts to foster the cyber threat and risk intelligence exchange of information', *Telecommunication systems*, 73(2), pp. 259–288. doi: 10.1007/s11235-019-00613-4.

Riesco, R. and Villagrá, V. A. (2019) 'Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (STIX™, SWRL and OWL)', *International journal of information security*, 18(6), pp. 715–739. doi: 10.1007/s10207-019-00433-2.

Rughoobur, P. and Nagowah, L. (2017) 'A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare', in *2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS)*. IEEE.

Seh, A. H. *et al*. (2020) 'Healthcare data breaches: Insights and implications', *Healthcare (Basel, Switzerland)*, 8(2), p. 133. doi: 10.3390/healthcare8020133.

Serrano, O., Dandurand, L. and Brown, S. (2014) 'On the Design of a Cyber Security Data Sharing System', in *Proceedings of the 2014 ACM Workshop on information sharing & collaborative security*. ACM, pp. 61–69. doi:10.1145/2663876.2663882.

The Open Group (2018) *Open FAIR™ tool with SIPmath™ distributions: Guide to the theory of operation*, *Opengroup.org*. Available at: https://publications.opengroup.org/g181 (Accessed: 8 September 2022).

The Open Group (2019) *The Open FAIR™ Risk Analysis Tool Beta (90-day Beta evaluation*

license), *Opengroup.org*. Available at: https://publications.opengroup.org/i181 (Accessed: 8 September 2022).

Tounsi, W. and Rais, H. (2018) 'A survey on technical threat intelligence in the age of sophisticated cyber attacks', *Computers & security*, 72, pp. 212–233. doi: 10.1016/j.cose.2017.09.001.

VanderPlas, J. (2014) *Why Python is Slow: Looking Under the Hood*, *Github.io*. Available at: https://jakevdp.github.io/blog/2014/05/09/why-python-is-slow/ (Accessed: 8 September 2022).

Wagner, C. (2016) 'MISP: The design and implementation of a collaborative threat intelligence sharing platform', in *Proceedings of the 2016 ACM on workshop on information sharing and collaborative security (WISCS '16*. New York, NY, USA: ACM, pp. 49–56.

Wang, J., Neil, M. and Fenton, N. (2020) 'A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model', *Computers & security*, 89(101659), p. 101659. doi: 10.1016/j.cose.2019.101659.

Williams, J. (2020) *OWASP Risk Rating Methodology*, *Owasp.org*. Available at: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology (Accessed: 8 September 2022).

Williams, M. A. *et al.* (2018) 'Analyzing evolving trends of vulnerabilities in national vulnerability database', in *2018 IEEE International Conference on Big Data (Big Data)*. IEEE.

Zhang, S., Caragea, D. and Ou, X. (2011) 'An empirical study on using the national vulnerability database to predict software vulnerabilities', in *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 217–231.

Zhang, S., Ou, X. and Caragea, D. (2015) 'Predicting cyber risks through national vulnerability database', *Information Security Journal A Global Perspective*, 24(4–6), pp. 194–206. doi: 10.1080/19393555.2015.1111961.

gg03

ORIGINALITY REPORT

9%	5%	5%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Nottingham Student Paper	2%
2	link.springer.com Internet Source	1%
3	oa.upm.es Internet Source	<1%
4	Jiali Wang, Martin Neil, Norman Fenton. "A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model", Computers & Security, 2020 Publication	<1%
5	epub.uni-regensburg.de Internet Source	<1%
6	qmro.qmul.ac.uk Internet Source	<1%
7	wrap.warwick.ac.uk Internet Source	<1%
8	Submitted to The Hong Kong Polytechnic University Student Paper	<1%

9	Paavan Rughoobur, Leckraj Nagowah. "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare", 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), 2017 Publication	<1 %
10	cve.mitre.org Internet Source	<1 %
11	cybersecurity.springeropen.com Internet Source	<1 %
12	dokumen.pub Internet Source	<1 %
13	hdl.handle.net Internet Source	<1 %
14	"Information Technolog: New Generations", Springer Science and Business Media LLC, 2016 Publication	<1 %
15	Submitted to University of Sunderland Student Paper	<1 %
16	Wiem Tounsi, Helmi Rais. "A survey on technical threat intelligence in the age of sophisticated cyber attacks", Computers & Security, 2018	<1 %

Publication

17	Jian Liu, Junjie Yan, Jun Jiang, Yitong He, Xuren Wang, Zhengwei Jiang, Peian Yang, Ning Li. "TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network", Cybersecurity, 2022 Publication	<1 %
18	Submitted to University of Adelaide Student Paper	<1 %
19	lib.dr.iastate.edu Internet Source	<1 %
20	Submitted to Institute of Technology, Tralee Student Paper	<1 %
21	Submitted to Ohio University Student Paper	<1 %
22	docs-aliyun.cn-hangzhou.oss.aliyun-inc.com Internet Source	<1 %
23	scholarbank.nus.edu.sg Internet Source	<1 %
24	Hyochang Baek, Minhee Joo, Won Park, Youngin You, Kyungho Lee. "Android Application Risk Indicator Based on Feature Analysis Utilizing Machine Learning", 2019 International Conference on Platform Technology and Service (PlatCon), 2019 Publication	<1 %

25	Varun M Deshpande, Ashwath Desai. "Smart Secure: A Novel Risk based Maturity Model for Enterprise Risk Management during Global Pandemic", 2021 6th International Conference for Convergence in Technology (I2CT), 2021 Publication	<1 %
26	dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn. Internet Source	<1 %
27	Freund, Jack, and Jack Jones. "Thinking about Risk Scenarios Using FAIR", Measuring and Managing Information Risk, 2015. Publication	<1 %
28	repository.sustech.edu Internet Source	<1 %
29	Chang-Joo Kim, Sangkyung Sung. "Efficient ST Techniques for Nonlinear Optimal Control Analyses Using a Pseudospectral Framework", IEEE Transactions on Control Systems Technology, 2015 Publication	<1 %
30	Submitted to Colorado State University Fort Collins Student Paper	<1 %
31	acikbilim.yok.gov.tr Internet Source	<1 %
	eprints.nottingham.ac.uk	

32	Internet Source	<1%
33	globalinitiative.net Internet Source	<1%
34	repository.tudelft.nl Internet Source	<1%
35	www.hindawi.com Internet Source	<1%
36	Submitted to Federation University Student Paper	<1%
37	Jeongeun Seo, Minhee Joo, Kyungho Lee. "Chapter 2 Turn On the Lights: User Behavior in Game Environment Using CPTED", Springer Science and Business Media LLC, 2020 Publication	<1%
38	Jerry M. Couretas. "An Introduction to Cyber Modeling and Simulation", Wiley, 2018 Publication	<1%
39	Minhee Joo, Junwoo Seo, Junhyoung Oh, Mookyu Park, Kyungho Lee. "Situational Awareness Framework for Cyber Crime Prevention Model in Cyber Physical System", 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), 2018 Publication	<1%

40	Ross Anderson. "Security Engineering", Wiley, 2020 Publication	<1 %
41	Submitted to Victorian Institute of Technology Student Paper	<1 %
42	api.intechopen.com Internet Source	<1 %
43	jultika.oulu.fi Internet Source	<1 %
44	www.diva-portal.org Internet Source	<1 %
45	www.science.gov Internet Source	<1 %
46	Bi, Chao, Lei Zhang, Miao Qi, Caixia Zheng, Yugen Yi, Jianzhong Wang, and Baoxue Zhang. "Supervised Filter Learning for Representation Based Face Recognition", PLoS ONE, 2016. Publication	<1 %
47	"Information Security Practice and Experience", Springer Science and Business Media LLC, 2017 Publication	<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography On