Integrated Computer-Aided Engineering -1 (2022) 1–21 1
DOI 10.3233/ICA-220689
IOS Press

Vulnerability prediction for secure healthcare supply chain service delivery

Shareeful Islam[a,*], Abdulrazaq Abba[b], Umar Ismail[b], Haralambos Mouratidis[c] and Spyridon Papastergiou[d]
[a]*School of Computing and Information Science, Anglia Ruskin University, UK*
[b]*School of Architecture Computing and Engineering, University of East London, UK*
[c]*Institute for Analytics and Data Science, School of Computer Science and Electronic Engineering, University of Essex, UK*
[d]*Department of Informatics, University of Piraeus, Greece*

Abstract. Healthcare organisations are constantly facing sophisticated cyberattacks due to the sensitivity and criticality of patient health care information and wide connectivity of medical devices. Such attacks can pose potential disruptions to critical services delivery. There are number of existing works that focus on using Machine Learning (ML) models for predicting vulnerability and exploitation but most of these works focused on parameterized values to predict severity and exploitability. This paper proposes a novel method that uses ontology axioms to define essential concepts related to the overall healthcare ecosystem and to ensure semantic consistency checking among such concepts. The application of ontology enables the formal specification and description of healthcare ecosystem and the key elements used in vulnerability assessment as a set of concepts. Such specification also strengthens the relationships that exist between healthcare-based and vulnerability assessment concepts, in addition to semantic definition and reasoning of the concepts. Our work also makes use of Machine Learning techniques to predict possible security vulnerabilities in health care supply chain services. The paper demonstrates the applicability of our work by using vulnerability datasets to predict the exploitation. The results show that the conceptualization of healthcare sector cybersecurity using an ontological approach provides mechanisms to better understand the correlation between the healthcare sector and the security domain, while the ML algorithms increase the accuracy of the vulnerability exploitability prediction. Our result shows that using Linear Regression, Decision Tree and Random Forest provided a reasonable result for predicting vulnerability exploitability.

Keywords: Healthcare supply chain service, ontology, vulnerability exploitability prediction, machine learning, cyber security

1. Introduction

Healthcare supply chain services aim to deliver critical healthcare services where multiple healthcare entities of the healthcare ecosystem are involved. A healthcare ecosystem can be defined as a globally distributed, interconnected set of entities (i.e., hospital and healthcare operators), processes and services that rely upon an interconnected web of ICT infrastructures and cyber networks to leverage the flows of services and information. The increased usage of information technology in modern healthcare ecosystem means that they are becoming more vulnerable to the activities of threat actors and susceptible to potential security attacks. Due to the type of information at risk and the consequences related to patient safety, securing the health care sector is recognized as a priority. For instance, when a credit card number is stolen, the financial institution can reissue the card and the consequences are just financial. On the other hand, if a patient's health care record is stolen, this can have significant personal and societal consequences [1]. Even worst, if a medical device is compromised that might result in loss of life if the device is used for example surgery. A recent survey by

*Corresponding author: Shareeful Islam, School of Computing and Information Science, Anglia Ruskin University, UK. E-mail: shareeful.islam@aru.ac.uk.

ISSN 1069-2509/$35.00

HIMMS reveals that there is a lack of budget in the healthcare sector related to the security of the health care IT infrastructure [2]. Additionally, medical devices are increasingly interfaced with other equipment, and vulnerabilities of the devices can be propagated into the other part of the network within the healthcare supply chain. This poses service disruption as well as unintended consequences. There are approximately 20 new cyber vulnerabilities released and reported every day [3], which makes it very challenging task for healthcare practitioner to determine which are relevant for a specific healthcare context [3]. Additionally, according to Kenna research only 2% of the published vulnerabilities have observed exploits in the wild [4]. It is therefore necessary to prioritise relevant vulnerabilities, based on the prediction of the individual vulnerabilities' exploitability.

Within this context, the paper aims to enhance secure healthcare supply chain service delivery. The proposed approach includes three main components: a conceptual view, an ontology and vulnerability exploitability prediction. Our work considers a number of industry specific standards and data sets for vulnerabilities such as the Common Vulnerabilities and Exposures (CVE), the Common Vulnerability Scoring System (CVSS3.1), machine learning models such as Linear Regression (LR), Decision Tree (DT) and Random Forest and ontology methodology such as OWL [5].

The main novelty of the work is to ensure security of the healthcare service delivery based on the understanding of the modern healthcare ecosystem and its decomposition using a number of concepts and ontological views and predict exploitation of vulnerabilities that can pose any risks on the overall system context. This provides an early warning of possible disruption so that appropriate measurements can be taken for the overall business continuity. Our work makes three important contributions. Firstly, we consider the healthcare ecosystem and its decomposition to understand the overall system context. The whole ecosystem is contextualized to include relevant constructs, a conceptual model and an ontology. The ontology provides semantic mapping and explicit representation of knowledge which is necessary for a holistic analysis of vulnerabilities in the healthcare domain. Secondly, we provide machine learning models that support the analysis and discovery of security vulnerability patterns and make predictions as to whether they can become usable exploits. This allows us to prioritize vulnerabilities according to an exploitability rating, and more importantly, determine necessary control actions. Finally, we have designed and carried out an experiment to determine the usable exploit for the vulnerability prioritisation. Our experimental result shows that our work provides higher accuracy with Random Forest than other algorithms, e.g. Decision Tree (DT) and Linear Regression (LR).

The rest of the paper is structured as follows. Section 2 presents the existing works related to our work from two dimensions, i.e., vulnerability and ontology, vulnerability exploitability, and healthcare sector cyber security. Section 3 explains the healthcare ecosystem and its decomposition. In Section 4, we introduced the proposed approach in terms of conceptual view, three ontological views including Healthcare supply chain service delivery ontology, Vulnerability Assessment Ontology and Base Score Vulnerability Metrics Ontology and vulnerability prediction method using the Machine Learning Models. Section 5 explains the experiment and results. A discussion of the work is added in Section 7. Finally, Section 7 concludes the paper and provides limitation and directions for the future works.

2. Related works

This section provides an overview of existing works which are relevant to our work. In particular, we examine the areas of security vulnerability, ontologies and healthcare sector cyber security.

2.1. Vulnerability and ontology

Välja et al. [6] introduced an ontology framework for improving automatic threat modelling, where they proposed a framework that is developed with conceptual modelling, which is validated using different datasets from water utility control network and university IT environment. The goal of the framework is to support the automation of threat modelling by improving the comparability and completeness of data from multiple sources based on specific data type elements such as software products, operating systems, and data flows. However, the contributions in this research have failed to consider the relevance and essentiality of vulnerability for enhancing threat modelling processes. Vorozhtsova and Skripkin [7] presented an ontological analysis of vulnerability in the energy sector. The ontology reflects the interrelationship between commonly used terminologies concepts in the energy sector and cyber security concepts. The authors developed a classification of vulnerabilities and possible control measures for ensuring security of cyber asset in the energy sector. The ontological analysis scheme presented in the paper facilitates the classification of vulnerabilities, their causes and methods of elimination. However, the authors neither provided a solid argument on either the sources of vulnerabilities or purported control actions used in the approach. Dimitrov and Kolev (2020) presented an ontology based on information from the common weakness enumeration's (CWE) top 25 most dangerous software errors [50]. The methodology used in the research adopted the National Vulnerability Database (NVD) and Common Vulnerability Scoring System (CVSS). The authors argued that newly discovered vulnerabilities are sometimes registered as old entries in CVE, thereby hindering investigation process and creating inconsistencies because vulnerabilities are classified as old entry. Similarly, Syed et al. [49] introduced the Unified Cybersecurity Ontology that provides a common structure for describing cyber security domain. The approach incorporates some of the widely used standards, best practices, vocabularies and ontologies such as CVE and CVSS. It also supports reasoning and inferring of new information from existing data sources in addition to capturing of security analysts' specialized knowledge.

2.2. *Vulnerability exploitability*

There are a number of recent works in the literature that focus on the vulnerability exploitation for the security improvement. A notable work is done by Jacob which focuses on existence of proof-of-concept exploit code or weaponized exploits from the vulnerability database [8]. The work aims to estimate the probability of exploits in the next 12 months. Various vendors such as Microsoft, HP, Adobe and IBM are used for the experiment. The result shows that there is a strong correlation between proof of concept exploits being published and weaponized for the vulnerability exploitation. Recorded future considers NVD and Exploit DB data sets for anticipating cyber vulnerability exploits based on the SVM Linear and Naïve Bayes [9]. The work investigates a number of common words, vendor products, and references for the better accuracy. The result concludes that CVSS scores, and CWE-numbers are redundant when a large number of common words are used for the exploitation. Keena research shown that 2% of published vulnerabilities have observed exploits in the wild and vulnerability prioritisation is the biggest challenge for the vulnerability management [4]. It is necessary to determine the relevant vulnerabilities that need remediation in a cost-effective manner. The research result also shows that 77% of CVEs does not include any exploit code or observed exploitations associated with them. CVSS score 7 or more shows higher percentage of exploited CVEs than CVEs with no known exploit code or observations. Deqiang and Sujuan [10] consider the vulnerability chain based on the assumption that vulnerabilities do not always exploit in isolation and there is a link between the vulnerabilities which can be exploited by an attacker. The work considers the CVSS vector to determine the score of a chain based on the privilege required for an exploitation [50]. For instance, if two vulnerabilities are linked, one requires no privilege then the attack can exploit the other vulnerability intendent of access vector. Another related work [11] investigated using ML in predicting cybersecurity incidents with specific focus on Small and Medium Enterprises (SME) in South Korea. However, their work uses text mining, such as n-gram, bag-of-words and ML algorithms, such as Naïve Bayes (NB) and Support Vector Machine, to find a pattern from their collected data of cyber incidents on SME for classifying cyber incidents and the corresponding response. However, unlike our work, which uses ML and ontology on the CVE data set. Other works that are using ML in healthcare sector include investigating ML in predicting pneumonia mortality, which includes using DT in developing their prediction technique [12]. Similarly, ML was used successfully in the prediction of progressive cancer to help effectively provide control measures at the early stage of the cancer onset. Also, recently, ML was used in various works for the prediction of COVID-19 diagnosis to help provide control measures to reduce the spread of the virus [13]. In the literature [14], there are additional collections of recently collected related works for using ML to improve the security of healthcare system. Additionally, there are several recent works that focus on the supervised machine learning model. Rafiei presents a Neural Dynamic Classification algorithm (NDC) that aims to identify the optimal features and most effective feature space [15]. The proposed NDC is compare with a number of existing algorithms, such as PNN, EPNN, and SVM. The result shows that NDC provides the most accurate classification for both standard and large classification problem compared to the other algorithms. NDC considers classification as a dynamic problem and obtained results certainly demonstrate NDC as a robust classification algorithm. Pereira presents finite element machine classifier framework, where whole training set is modelled as a probabilistic manifold for classification purposes [16]. The result is compared with the nine other supervised pattern recognition techniques with both small and medium-to-large-sized datasets. FEMa is a superior technique for almost all small datasets and it is the third best classifier for the other data sets. Alam designs a NN ensemble and present a dynamic ensemble learning (DEL) algorithm that aims to automatic determination of NN ensemble architecture and size of individual NN [17]. It also improves the accuracy and diversity of neural network. There are eight distinct steps followed by DEL and experiment analysis is performed based on different medical and non-medical datasets. The result shows that DEL obtained better diversity comparing to the existing ensemble learning methods and avoid using trial-and-error process. Gao proposes balanced semi-supervised GAN (BSS-GAN) approach that aims to address the data deficiency and class imbalance to support the wider adoption of deep learning (DL) algorithm [18]. Several experiments were performed including crack detection, spalling detection, Damage pattern recognition, failure cases and synthetic image quality. The results from these experiments show that BSS-GAN is able to achieve better damage detection, specifically its outperformed others in both binary crack and spalling detection under low-data and imbalanced-class settings. Dong considers flood vulnerability assessment and prediction using Bayesian modelling [19]. The work adopts data-driven probabilistic vulnerability assessment and cascades characterization of flood control infrastructure failure. The approach is applied to 4,023 km of flood control network in Houston and failure cascades simulation achieves more than 80% accuracy.

2.3. *Healthcare sector cybersecurity*

A review by [20] concluded that healthcare industry lacks comparing to the other sectors for securing patient sensitive data. Rapid technological advancement and evolving federal policy are considered two main drivers for the exposing healthcare to cyber threats. A security report observed that implantable cardiac device gets security features associated with the system architecture [21]. This device often uses device-to-device authentication schemes such as hardcoded credentials on home monitoring devices for authenticating to patient support networks. An attacker can exploit this credential to access the network. The Centre for Internet Security (CIS) highlights a number of attacks such as ransomware, data breaches, DDoS, inside threats and business email compromise which are commonly used by the attacker in the healthcare sector [22]. The report mentions that the Personal Health Information (PHI) is much more valuable comparing to the Personally Identifiable Information (PII) because cybercriminal can use PHI data to target victim with frauds and scam and fake insurance claim. Argaw review cyber-attacks that can threaten various healthcare services, including surgery and medicine delivery, by targeting medical devices such as imaging equipment, automated drug dispensers and electronic health record [1]. The work recommends a number of action points such as risk-based approaches, vulnerability and patch management, and Incident response plans for improving cyber security in Hospitals. Wagner uses graph modelling to measure the vulnerabilities in supply chain and recommends possible mitigations [23]. The work develops supply chain vulnerability index (SCVI) based on relationships among the supply chain drivers and applied in real world scenario. SCVI considers four steps and determines the graph weight and directed edge. The result shows that automotive industries are exposed to the highest supply chain vulnerability. Dobrzykowski investigates healthcare supply chain network and provides a contextual view of the downstream healthcare delivery supply chain and its relationship with the regulatory compliance [24]. The work considers downstream of the healthcare supply chain context because of its important for the coordination of the service delivery. Several issues such as finance model, data privacy, investment in technology are discussed and highlight the necessity of decentralised healthcare supply chain. Nguyen reviews the existing Deep Reinforcement Learning (DRL) approaches for cyber security based on the cyber physical system, intrusion detection system, and game theory [25]. DRL is applied in various applications actors a number of sectors including cyber physical and autonomous system, intrusion and phishing detection. The review provides several important observation and future directions for the adoption of DRL in cyber security.

All the above-mentioned works and study reports contribute to the overall cyber security including knowledge presentation through ontology, vulnerability exploitability, and risk factors in healthcare domain. However, there is a lack of consideration to improve cyber security for the overall healthcare ecosystem considering vulnerabilities exploitability. This research fills this gap by providing methods for understanding the overall healthcare sector and predicting the exploitability of vulnerabilities.

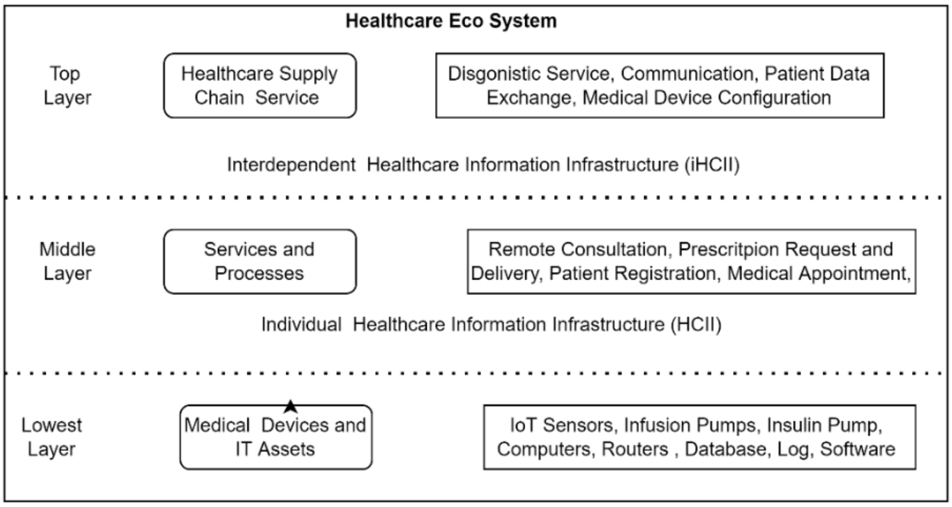

Fig. 1. Healthcare ecosystem and its decomposition.

3. Healthcare ecosystem

The healthcare sector has experienced a technical evolution over the past decade and undergone dramatic changes in the past several years, primarily spurred by the adoption of new medical devices and technologies including insulin pump, health care information management system, IoT, and Cloud Computing. Healthcare ecosystem is the core area of the context that consists of a heterogeneous set of actors, entities, and systems such as hospitals and general practitioners organisations, service providers, medical equipment suppliers, patients, doctors, nurses who are actively participating to delivery healthcare service delivery [26]. There is a significant increased interdependencies between the physical and cyber level for the overall healthcare service delivery. Cyber security is a cross cutting concern from each dimension of the ecosystem. The ecosystem consists of three main components:

– Healthcare ecosystem: Healthcare ecosystem, as stated previously, interconnects a set of entities with healthcare information infrastructure for the healthcare service delivery. The overall healthcare ecosystem consists of four distinct hierarchical areas of considerations from healthcare devices, ICT infrastructure, healthcare services, interconnect healthcare information infrastructure. To ensure security and resilience, the ecosystem demands a number of capabilities, i.e., a thoroughly performed assessment of the vulnerabilities of all interconnected cyber assets; a continuous evaluation of the corresponding risks; and of detection and analysis of incidents.
– Healthcare entities: The Ecosystem includes healthcare entities such as hospital, clinic, and agents who are responsible for performing specific tasks relating to the security capability. For instance, an agent identifies the vulnerabilities related to the specific healthcare devices and assesses the identified vulnerabilities or detects an ongoing cyber threat without knowing how this may affect the others.
– Security-related information: This component presents the knowledge of cyber-attacks, vulnerabilities, and risks which need to be analysed for the overall cybersecurity improvement. Healthcare entities are the key stakeholder who receive this security-related information. This information is used as an input for performing tasks relating to security analysis. Security related information considers details of attacks and incidents of specific assets such as CVEID, vulnerability description, causes, asset type, attack, impact, and other relevant properties. If required, security related information also needs to review the healthcare supply chain services and underlying Healthcare Information Infrastructure (HCII).

3.1. Healthcare ecosystem decomposition

It is necessary to decompose the ecosystem to understand the main areas so that vulnerabilities can be discovered from all these areas. This research follows a bottom-up hierarchy structure to decompose the ecosystem into three different levels as presented in Fig. 1.

These levels are related with each other and necessary for the healthcare service delivery. The lowest level relates to the individual patient health care devices and underlying ICT infrastructure that support the patient healthcare service delivery and processes. Hence, this lowest layer considers all IT and medical devices related assets such as infusion pump, routers, IoT sensors, and many more. The middle level relates with the healthcare services and process within a Heath Care Information Infrastructure (HCII) of a specific healthcare institute such as a hospital or clinic. HCII requires the components of overall IT infrastructure and medical devices necessary to delivery healthcare services including the patient healthcare devices, communication networks, information system, and other relevant ICT infrastructure. A health care entity relies on this infrastructure to deliver the services and support the business process. Finally, the highest level relates with the interdependent HCIIs (iHCII) for the supply chain health care service deliver and underlying infrastructure. The iHCII connects the individual HCII to delivery supply chain healthcare services and composes the whole health ecosystem. For instance, a clinic as HCII exchange patient diagnostic report with a Hospital for the treatment. Therefore, security of iHCII depends on the individual HCII security status. The interdependency among the HCIIs is characterized by the distribution of services, data sharing, collaboration among the activities for the informed decision making.

4. The proposed approach

This work aims to ensure secure healthcare supply chain service delivery by analysing and prioritizing the vulnerabilities so that an informed decision can be taken to tackle any issues relating to security. It considers security from the context of healthcare ecosystem and other related components. The proposed approach uses a conceptual view to represent the concepts and the relationship between, and an ontological view that provides a common language and a knowledge base of healthcare ecosystem. The integration of these important elements would help healthcare institutions to understand emerging vulnerabilities and to identify suitable controls to mitigate the risks to a secure and resilient healthcare ICT infrastructure. In addition, the proposed approach considers evidence-based data for the security analysis and adopts a vulnerability exploitability prediction model. The reason for considering vulnerability exploitability is that there are significant confirmed vulnerabilities published every month, and it is challenging for healthcare entities to fix a reasonable proportion of these vulnerabilities. Therefore, it is necessary to prioritize the relevant vulnerabilities based on potentiality of exploitation within a specific healthcare entity. Additionally, we have also integrated an ontology for providing a common understanding, reusing of domain knowledge and making assumptions for security considerations in the overall healthcare ecosystem more explicit. In addition, an ontology is machine-readable, it can make inferences, enables consistency checking and specifies semantic relationship between diverse set of constructs or concepts. This will make it easier for healthcare entities and actors to perform analytical tasks, understand vulnerability exploitability and correlate potential risks with control actions.

4.1. *Conceptual view*

This section presents the concepts used in constructing the conceptual model of the proposed approach. The point of the conceptual view is to highlight specific construct from the broader perspective of vulnerability analysis, which will support practitioner's ability to connect different perspectives and mapping the concepts, and more importantly, promote a meaningful interpretation of the concepts according to healthcare-based systems. Hence, the concepts are derived from multiple domains including cybersecurity, healthcare ecosystem, threat intelligence and vulnerability. The rationale behind the inclusion of these concepts is based on the analysis and elicitation of healthcare-based systems considering security and privacy requirements.

– Actor: is an entity who derives benefit or interacts with a healthcare infrastructure or system, participates in a process, performs a task, or supports other entities within the healthcare ecosystem to perform a task. Actor is characterised by type and role. For instance, healthcare practitioner is responsible for the patient treatment. There are other actors such as IT professionals who are responsible for managing the overall ecosystem.
– Cyber asset: implies any form of medical device, patient data or ICT component that supports for the healthcare service delivery. The assets within the healthcare ecosystem are dependent upon each other for the healthcare service delivery. In particular, assets within the healthcare system are connected for the specific service delivery. For instance, the data from the home infusion pump as medical device are transferred to the pump server

as IT device. The server correlates the data for making clinical decision. Assets comprise hardware, software, information, and includes various properties as types, values, criticality, sensitivity and required level of protection.

- Threat actor: represents an individual or groups that participate in hostile actions or operate with malicious intents to compromise the availability, integrity or confidentiality of a healthcare delivery system or the information it contains. Threat actors are identified based on their distinctive characteristics and motives (such as goals, motivation, tactics, and procedure). In particular, threat actor aims for patient data leak and health care service disruption. Threat actor needs certain profile to exploit specific vulnerability for an attack.
- Goal: represents strategic interest of an actor. Goals are mainly introduced to realize security constraints that are imposed to an actor. Goal consists of attributes as type and purpose, for example, authentication and authorisation controls could be the goal of an asset whose purpose is to ensure security protection.
- Vulnerability: a weakness or a flaw in an asset, either from implementation, design, or other processes, that can be exploited or triggered by a threat agent. Each asset may link with single or multiple confirmed vulnerabilities published by Common Vulnerabilities and Exposures (CVE) which are required to consider for an attack. Vulnerability considers properties published in common vulnerability scoring system (CVSS 3.1). For instance, Infusion Pump medical device lacks input validation that provides command line access and privilege escalation (CVE-2021-33886) and insulin pump lacks security (authentication and authorization) in RF communication protocol with other devices (CVE-2019-10964).
- Risk: a potential loss, harm or consequence to assets as a result of a threat actor exploiting a vulnerability. In other words, a risk can affect an asset when asset vulnerabilities are exploited by a threat actor. The purpose of this concept is to identify the risks facing an asset. Risk contains properties such as type, likelihood and severity. The main risk in healthcare ecosystem focuses on the service disruption and patient data leak.
- Control mechanism: refers the implementation of technical safeguards, systems, or other administrative processes that are used to prevent or mitigate risks, and to ensure the overall protection of healthcare systems. Control mechanisms include several properties such as type, functionality, effectiveness level.
- Cyber course of action: comprises a set of security controls that can be executed by an actor in response to cyber incidents in healthcare systems. In other words, cyber course of action are those ancillary procedural actions and technical measures that are used to defend against threat actors and their tactics, techniques and procedures. It is characterised by procedural and technical courses of action.
- Cyber incident: implies a security-related event or a series of events that may result in unanticipated consequences, or interruption of essential healthcare systems and functions. Cyber incidents are characterized by type, affected asset, severity and access vector. For instance, misconfiguration of insulin pump could be an incident.
- Effect: determines the measurable implications or consequences caused by a security incident to healthcare systems. The intention is to measure the potential severity of adverse effect or compromise caused by a security incident. Impact contains attributes such as affected asset and severity.
- Security and privacy requirement: imply specific qualities or restrictions relating security and privacy measures that must be present and maintained in healthcare systems. These requirements aim to support the protection and privacy of cyber assets, as well as the overall picture of mitigating risks.
- Dependency: signifies the connection, linkage or connection that exists between two or more assets, by which the state of one asset influences or is reliant upon the state of the other. A dependency exists if the operation of a cyber asset depends on data or services processed by another cyber asset.

Figure 2 provides a meta model consisting of the concepts and the relationship between them. The aim of the meta model is to offer a simplified view and to render and abstraction of how such concepts can be used in the context of vulnerability analysis in healthcare-based systems. Put differently, the meta-model is presented so that the concepts can be recognized and the dependencies, properties, inheritance and association between them can be easily traced. Therefore, concepts are represented with rectangular shape. The top section displays the concept name, while the middle section inside the rectangular shape contains the concepts' properties (attributes) as properties. Lines are used to represent association, inheritance, multiplicity and relationship

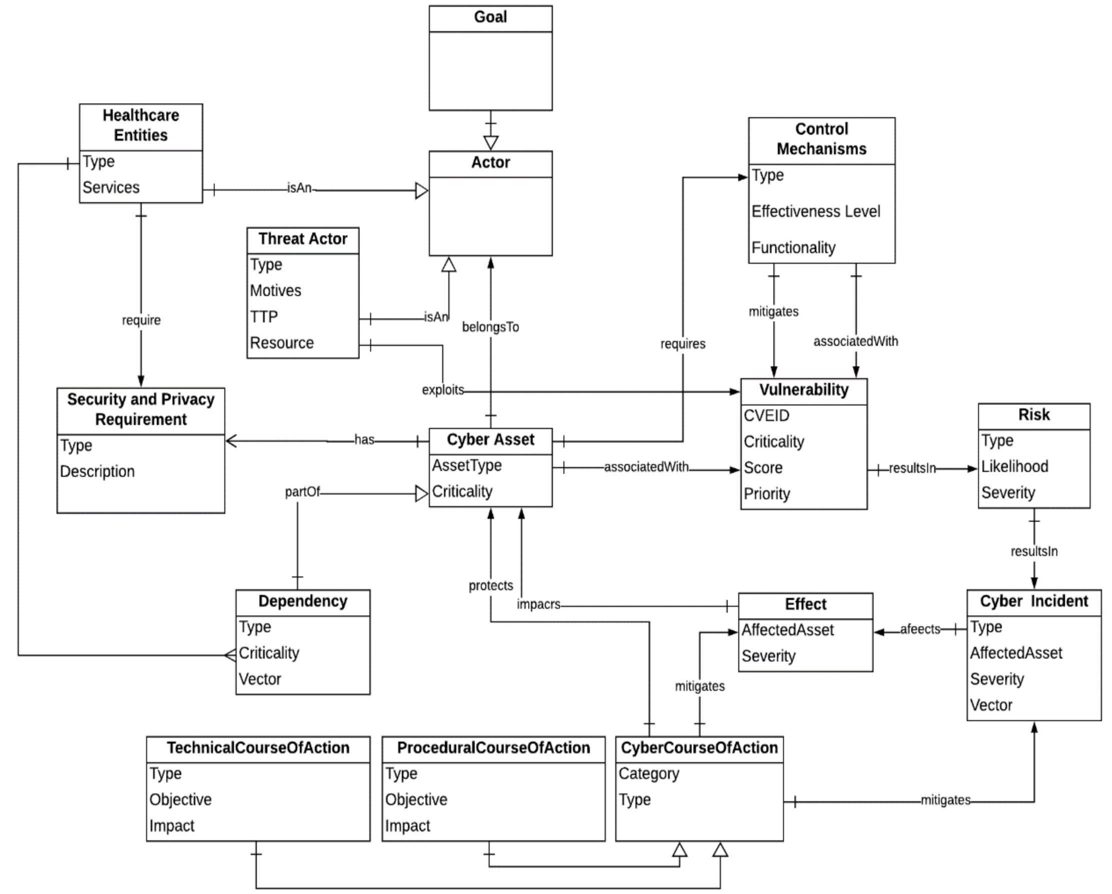

Fig. 2. Meta model.

between concepts. On the one hand, solid arrow lines indicate an association between two concepts where one concepts interact with the other. On the other hand, shallow arrow lines indicate inheritance between two concepts where one concept is a sub-class of another.

Essentially, healthcare functions and operations are supported by cyber assets. Such assets are operated, managed, controlled, and used by different actors with varying set of goals. Each cyber asset is associated with specific security and privacy requirements that elaborate performance characteristics that must be preserved in by healthcare entities such as processing or transmission of personal health information by General Practitioners (GPs). Further, each cyber asset has a specific level of criticality based on its operational value or consequences of failure and could be exposed to various forms of common vulnerabilities.

Vulnerabilities are related to cyber asset implementation weakness, security misconfigurations or lapses in vendor products, and they can be subject to exploitation by a threat actor. However, each vulnerability has a different impact – some need to be addressed urgently while others are less of a priority – hence they are assessed according to exploitability metrics (criticality, score and priority). A threat actor possesses different skillsets, resources and goals for compromising cyber asset or access sensitive information. Also, the manifestation of a threat actor activities could result in a risk such as the interruption of healthcare functions, which that may lead to a certain degree of effect to one or more cyber assets and dependencies. In addition, control mechanisms are implemented to address vulnerabilities and protect cyber assets. Control mechanisms can be implemented according to detective, preventive and corrective actions for various functions such as detecting and minimising the potential effect of vulnerability, and/or restoring cyber assets to a prior state. On the other hand, the Cyber course of action expresses additional countermeasures to mitigate the impact of an incident and offer more protection to cyber assets.

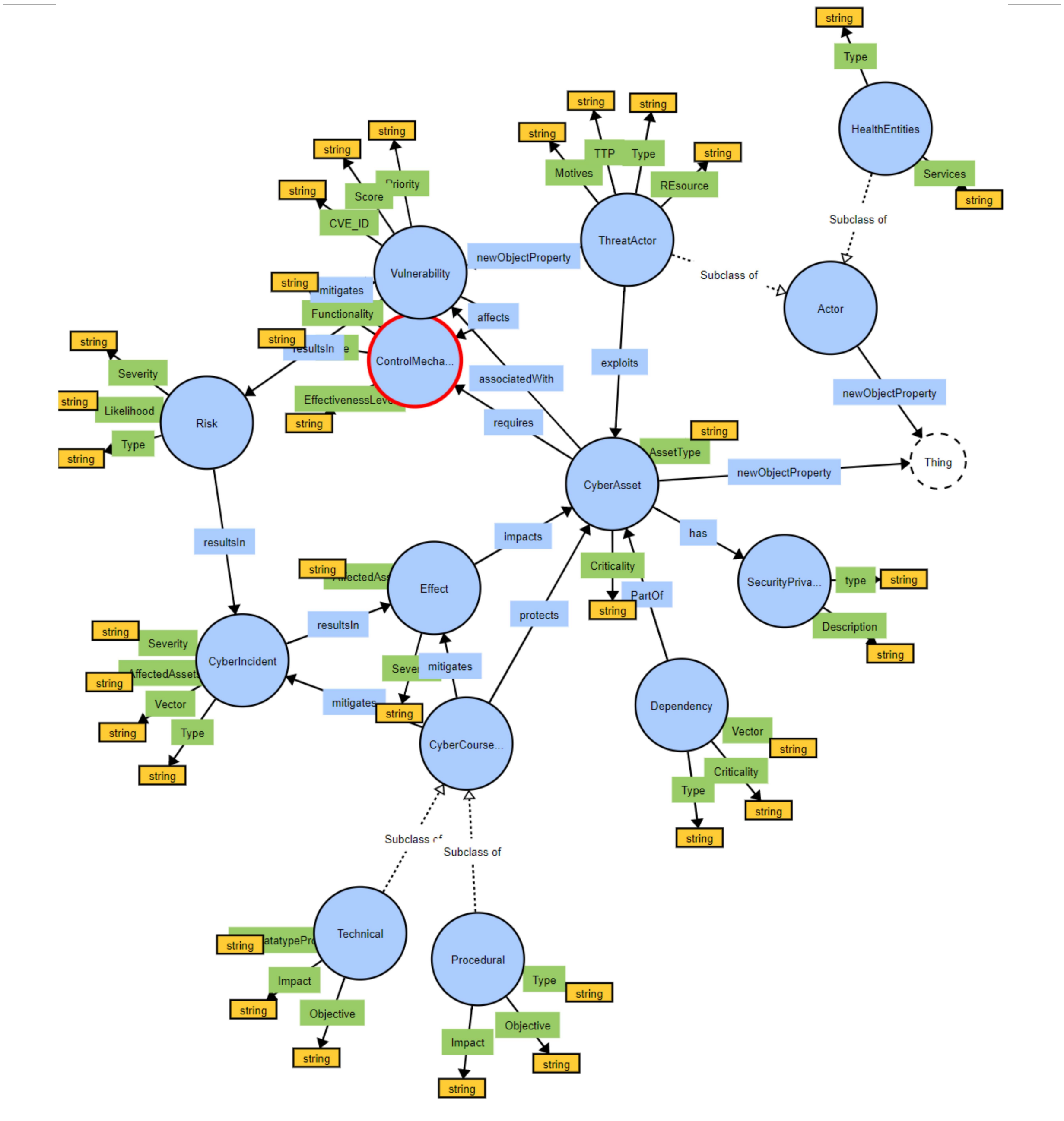

Fig. 3. Healthcare supply chain ontology.

The cyber course of action also improves the existing control mechanisms and the overall security posture of cyber assets.

4.2. Ontological view

This section presents ontological views based on the concepts. The ontology is created based on the well-established Web Ontology Language (OWL) methodology, which allows the specification of concepts, relationships, as well as characteristics of concepts and relationships in a human and machine understandable. This makes it ideal to explicitly represent the meaning of terms in vocabularies and the relationships between those terms [5]. Therefore, the ontology consists of Classes (concrete representation of concepts), instances

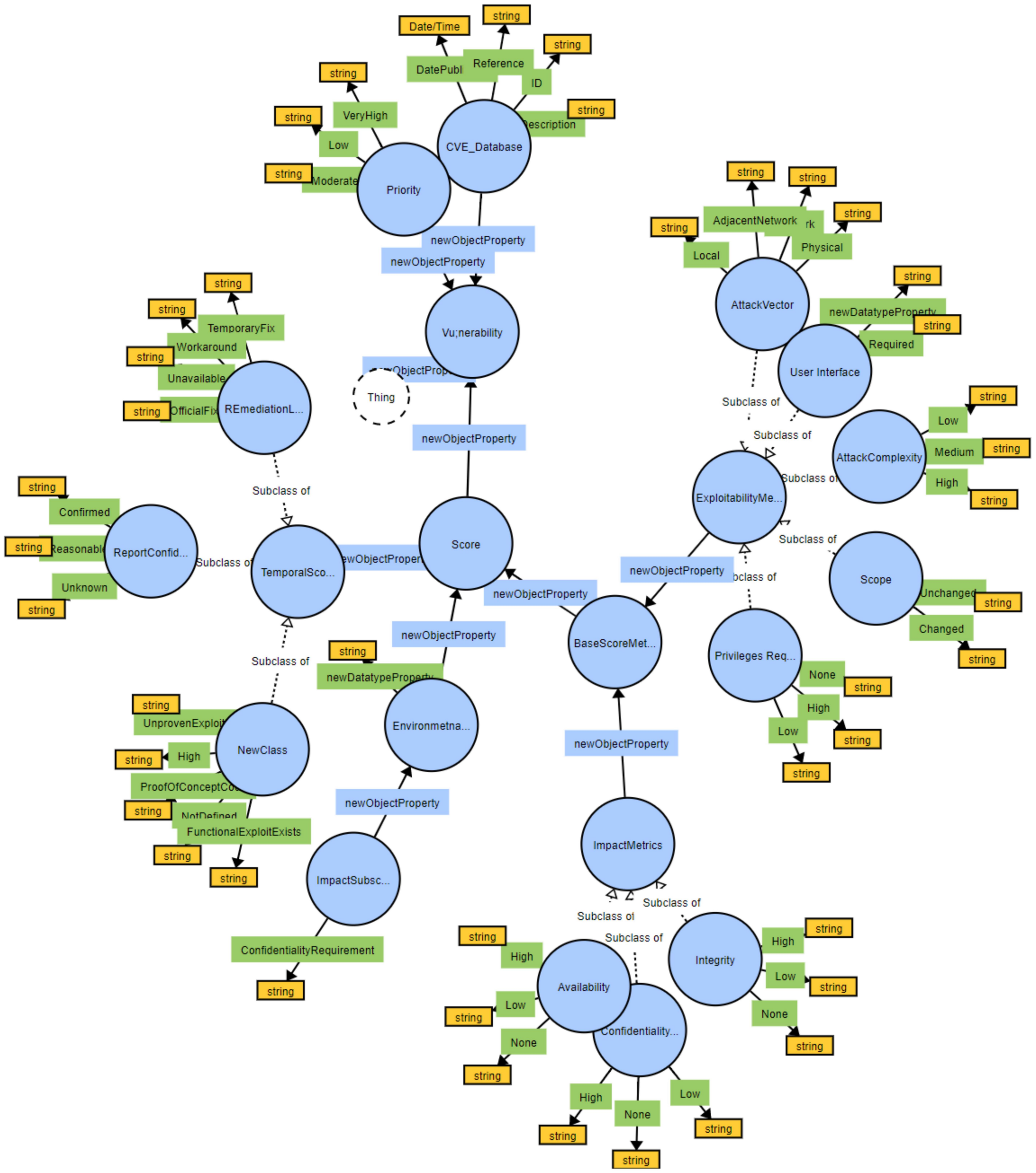

Fig. 4. Vulnerability assessment ontology.

(individuals of classes) and properties. Instances specify the conditions that must be met, while properties imply relationships between classes and individuals. The aim of the ontological views is to establish a formalized and structured representation of the concepts that constitute vulnerability assessment, as well as their association with other concepts for analysing vulnerabilities in the context of healthcare cyber systems. In other words, three different ontologies are generated as:

– Healthcare supply chain service delivery ontology
– Vulnerability assessment ontology
– Base Score vulnerability Metrics Ontology

4.2.1. Healthcare supply chain service delivery ontology

An explicit formal specification of the concepts in healthcare domain and the relationships between them are expressed as an ontology in Fig. 3. according to

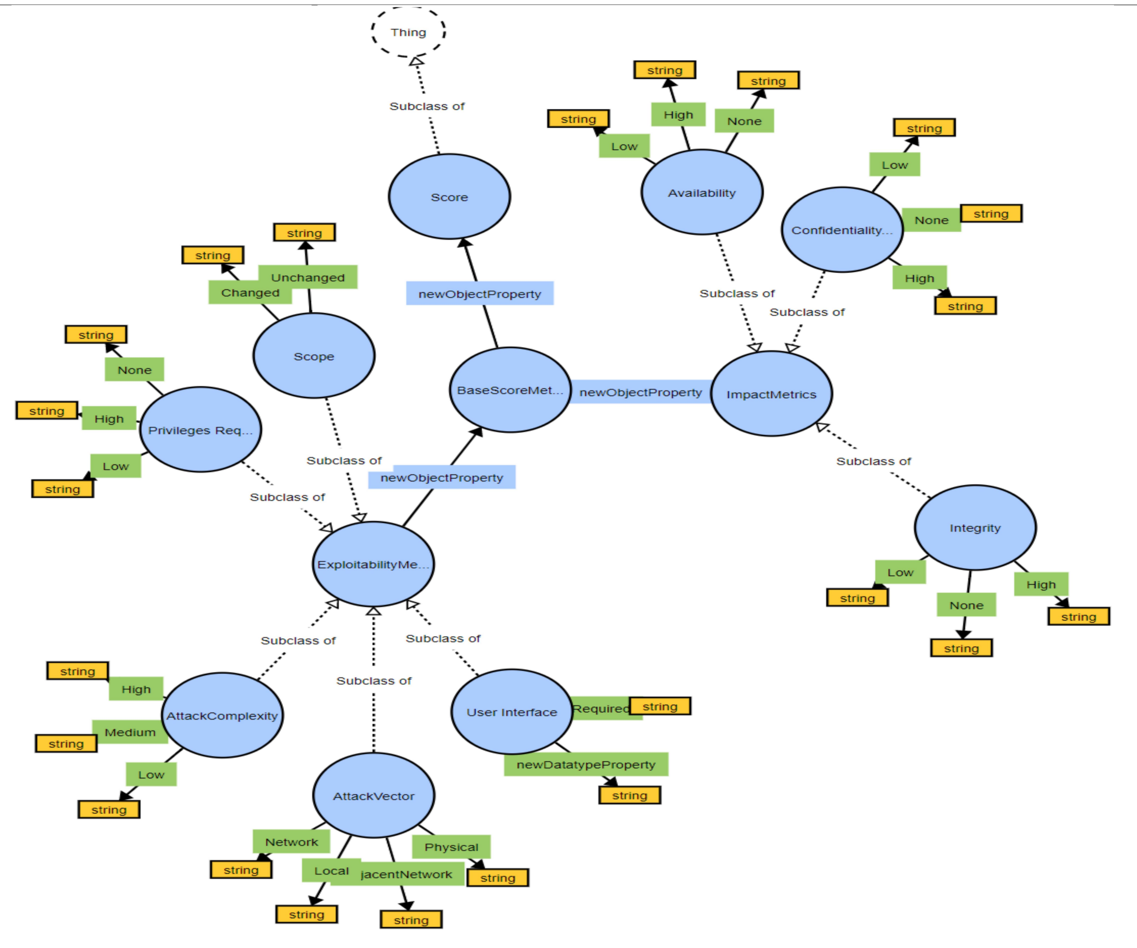

Fig. 5. Detailed view of base score metrics ontology.

the concepts and their properties presented described in the previous section, which aims to provide general knowledge base for healthcare supply chain service. It consists of concepts, object properties, and data properties. Concepts are represented in bright-blue circles. Object properties are represented in green rectangles, and datatypes in yellow rectangles. With the creation of this ontology, healthcare entities can efficiently develop a shared understanding of critical vulnerabilities, exposures and exploitability that may result in substantial harmful consequences. Therefore, based on the terminologies in OWL, the core concepts are represented as classes, relations are implemented as properties and accompanying datatype.

4.2.2. Vulnerability assessment ontology

A vulnerability assessment ontology is developed in order to highlight the concepts, their association and properties in a more formal representation of knowledge for describing vulnerabilities in the context of healthcare-based systems. In other words, this ontology is designed to provide a structured representation and efficient assessment of vulnerabilities in healthcare domain. The basis of this ontology is implemented according to all the three fundamental scoring metrics specified in Common Vulnerability Scoring System (CVSS) as Base Metric, Temporal Metric and Environmental Metric.

The scoring metrics are represented as classes including their properties as shown in Fig. 4. For example, vulnerability assessment properties such as “priority”, “scope”, “attack vector” etc. are essential in characterizing vulnerabilities in healthcare systems. Specifically, the ontology characterizes the Base metric as consisting of specific vulnerabilities that are constant across healthcare systems over time. It consists of subclasses as exploitability metrics and the impact metrics. The Temporal metric consists of other subclasses and properties to represent vulnerabilities that are likely to change over time but not across all healthcare systems. Similarly, Environmental metric consist of subclasses that characterize vulnerabilities that are unique and relevant to healthcare systems only. This allows us to analyse the concepts in further depths, for example, analysing the vulnerabilities associated to a specific asset, the threats that could exploit a vulnerability and the implementable control actions.

4.2.3. Base score vulnerability metrics ontology

Although three different vulnerability assessment ontologies are presented, it is important to mention that only Base Score Metric and its properties are adopted in our approach for assessing vulnerabilities in healthcare supply chain cyber systems. The rationale behind the choice of Base Score Metrics is that it can measure severity based on the characteristics of a vulnerability that are constant over time. It is also capable of assuming reasonable worst-case scenario of a successful attack across different deployed environment of healthcare systems. This is essential in extending the knowledge base, as well as flexibility and adaptability for vulnerability assessment for healthcare supply chain service. Therefore, Fig. 5 focuses on the "Base Score Metrics". It contains the main class "Score" that provides the numerical representation of the severity of a vulnerability. "Score" is associated with the "Base Score Metric", which further comprises other sub-classes elements (sub-scoring) as "Exploitability Metric", "Scope Metric" and "Impact Metric" subclasses.

In addition, all the sub-classes contain other subclasses, property, and datatype accordingly. The central interpretation of the ontology is that a vulnerability is assessed and scored according to the properties of "Base Metrics" i.e. exploitability, scope and impact metrics. The "Exploitability Metric" is made up of four further sub-classes (Attack Vector, Attack Complexity, Privileges required, and User Interface), and contains a set of defined property (high, medium, and low) and data type (string). "Attack Vector" subclass is aims to measure the level of access required to exploit a vulnerability; "Attack complexity" assesses the factors outside of the threat actor's control that are required to exploit the vulnerability; "Privileges required" measures the privileges required for the threat actor to conduct the exploit; and "User Interface" is based on whether the threat actor must recruit another participant in order to complete the attack. Scope relates to whether a vulnerability that exists in one component of a healthcare system can propagate to other components (dependencies). Impact metrics is used to assess the actual outcome of an attack as a result of a vulnerability being exploited – consisting of subclasses as confidentiality, integrity, and availability. The subclass "confidentiality" measures the amount of data that a threat actor gains access to; "integrity" scores the ability of a threat actor to alter or change data on the affected healthcare system; "availability" measures the loss of availability of the exploited healthcare system. Each subclass contains an "object property" classified according to "high, none or low." For example, the score of "Confidentiality" measurement will be "High" if all data on the healthcare system impacted is accessible by the threat actor and "Low" if data is not accessible to the threat actor.

4.3. Prediction of vulnerability exploitability

This component focuses on the identified vulnerabilities which are applicable for the healthcare sector. Out approach advocates to use the National Vulnerability Database which contains over detailed entries relating to vulnerabilities in a structured format [27]. The NVD includes information for all Common Vulnerabilities and Exposures (CVEs). The vulnerabilities are based on the assets and products that are used in the healthcare system including hardware, operating systems, healthcare devices, or applications and listed with a unique CVE ID. A detailed list of the vulnerabilities can be obtained from the CVE detailed. At the time of this work, there are 164463 recorded confirmed vulnerabilities and almost 20 new cyber vulnerabilities are released and reported every day (CVE). Common Vulnerability Scoring System (CVSS) is used to evaluate the severity and prioritise of each vulnerability. CVE contains a database of publicly known cybersecurity vulnerabilities including an identification number, a description, and at least one public reference. It is widely used across the sectors to evaluate the coverage of the security tools. Hence, it allows one to search for known attack signature and possible remediations if the vulnerability is exploitable. CVE list feed NVD, therefore NVD is fully synchronized with CVE. But NVD provides enhanced information for each recorded vulnerability in CVE including remediation guideline, impact rating.

Due to the huge information in CVE, it is therefore really challenging for a healthcare entity to determine which of these vulnerabilities are relevant for a specific healthcare context. Hence, it is a daunting task for healthcare practitioner to prioritise the relevant vulnerabilities. The proposed work attempts to predict which vulnerabilities are relevant and should be prioritised for the specific context. Hence, we aim to predict which vulnerabilities are likely to exploit so that healthcare entity can implement right level of control to mitigate the risk that can pose from the vulnerability. It is worth mentioning that not all vulnerabilities can be easily exploited due to the nature of the specific product or vulnerability. Therefore, predicting exploitability is an effective means to prioritise the vulnerability. The trend of disclosing software vulnerabilities has become a serious concern. Keeping up with these vulnerabilities in providing control requires a huge investment in resources and personnel. However, ML has a potential contribution in predicting vulnerabilities that will help in saving both cost and life, by predicting vulnerability and providing appropriate control measures.

4.3.1. Vulnerability exploitability

The approach follows the Common Vulnerability Scoring System Version 3.1 and its metrics to determine the exploitation (CVSS-3.1). CVSS computes the severity of a vulnerability as a function of its characteristics, and the impact on the confidentiality, integrity, and availability of the system. The CVSS score ranges from 0–10, and is an official severity measurement, with 10 being the most critical vulnerabilities. It is a widely used methodology for vulnerability management that considers three vectors concerning vulnerabilities, i.e., Base, Temporal, and Environmental, to qualitatively rate a vulnerability. The CVSS 3.1 provides for more accurate scoring estimation. We consider the Base vector for the purpose of this work. Base score aims to provide an inherent characteristic of a vulnerability, which is constant over time and across user environments. The base vector composes of two sets of metrics: The Exploitability metrics and the Impact metrics. Exploitability metrics represent the teaching means by which a vulnerability can be exploited based on the characteristics of an asset which are vulnerable. Impact metrics reflect the direct consequence of the successful exploitation of a vulnerability as possible worst outcome. An overview of the metrics is given below.

- Attack vector: This indicator reflects the context by which vulnerability exploitation is possible and level of access required by an attacker to exploit the vulnerability. The higher the metric value means there is more likely an attacker can be to exploit the vulnerable component remotely. It includes four possible values: Network (N) as vulnerability can remotely exploitable, Adjacent (A) as requires network adjacency for exploitation, Local (L) as are not exploitable over a network, Physical (P) as physically interaction with the target system is required.
- Attack complexity: This metric indicates the necessary conditions beyond the attacker's control that must exist to exploit the vulnerability. Such conditions may require the collection of more information about the target, or computational exceptions. It includes two possible values: Low (L) as no specific pre-conditions and High (H) as conditions beyond the attackers' control for successful attack.
- Privileges required: it indicates the necessary privileges or access an attacker must possess before successfully exploiting the vulnerability. The no privileges give an attack opportunity to successfully execute an attack. It includes three possible values: None (N) as no privilege or special access required, Low (L) as basic user level privileges to leverage the exploit, and High (H) as Administrative or similar access privileges.
- User interaction: This indicates the involvement of user, besides an attacker, necessary for the exploitation. It can be none when no interaction is required or required for a successful exploitation.
- Scope: It indicates whether a vulnerability in one vulnerable component can impact on another system or component. It can be unchanged or changed.
- Confidentiality: It measures the impact on the confidentiality of the information resources managed by specific application. In general confidentiality ensures that only authorised user can access specific information. A vulnerability aims user with no right to access certain information. It is one of the main impacts due to the exploitation and severely effect on the overall business continuity. It can be high, medium or none.
- Integrity: It measures the impact to integrity of a successfully exploited vulnerability. Integrity ensures to protect data or application from unauthorised modification. Reliability of delivering services and accurate data is key for integrity. Similar to the confidentiality, it also considers three scales.
- Availability: This metric measures the impact on the availability of network services resulting from a successfully exploited vulnerability. Availability ensures information or service available as per the requirements. Confidentiality and integrity is prerequisite for availability. This metric measures the impact on availability due to the exploitation of a vulnerability.

4.3.2. Machine learning model for predicting vulnerability exploitability

The Machine Learning (ML) models allow us to correlate the vulnerability data and determine which vulnerability would likely be exploited. It is used for building a predictive model for classification in addressing real-world problems [28]. In this work, we consider three different ML models, Linear Regression (LR), Decision Tree (DT) and Random Forest (RF) in developing the prediction model. The reason for choosing these models is part of our research for finding the most suitable fitting model for the selected dataset CVE. This is because we want to optimize our techniques in terms of higher accuracy and less complexity. In addition to taking advantage of these three models in getting a clear insight into the data with high efficiency. For instance, LR provides an initial insight into the data because of its linear fitness capability, handling over-fitting excellently, and extrapolation capability [29]. With the added advantages of handling multiple output problems in DT, we get additional insights into the data beyond LR, efficiently [30]. We are able to understand the multiple dimensions of data. Going further, we consider additional advantages of RF to improve our work, using the capability of RF, such as turning single parameter, improving efficiency, and the possibility of generalizing errors that may arise [31]. These helped us to improve the accuracy and precision of our work Thus, we start with LR that is less complex, then improve the result with DT and then improve further with RF.

– LR is based on a linear predictor function commonly used for prediction among multiple factors or predictors. Nowadays, LR is one of the popular simple techniques for analysing the effect of multifactor data against the interesting factor (predicted values). This is because LR has a conceptual logical process for expressing relationships between the interesting factor and the related predictors in the form of a simple mathematical equation. This provides a good foundation for developing a theoretical basis that can easily apply to real-world data, particularly in making projections [32]. In ML, LR is commonly used as the first choice for developing learning models from a data set.
– A decision tree is another model in the form of a tree-like structure for analysing options and their corresponding factors in making a decision and understanding the consequences of each decision [33] This provides a visual tool for analysing decisions among competing alternatives (multiple covariates) that provides a good basis for developing predictions algorithm. As of today, DT is one of the most effective techniques for identifying patterns in a data set, in addition to being easy to use for communication and also robustness in accommodating various types of data. As a result of that, DT is used not only in ML, but also in Business, and currently is becoming popular in processing health data for making predictions. For example, in analysing patterns of symptoms to predict medical conditions. The advantages of a decision tree include handling missing values, assessing the relative importance of variables, as well as variable selection in selecting the most relevant factors for the learning model.
– Random forest is another multifactor decision technique that constructs multiple trees to aggregate their decision from random features, thereby forming a suitable decision model from the learning data to predict the targeted interesting factor [34]. RF is an extension of DT that is being used successfully for general-purpose classification, by combining these multiple random decision trees with random factors and aggregating their predicted values. This is similar to the common approach of majority wins, so the most popular predictions will be selected. A combination of random inputs and random features reduce both the aggregated error and over fitness of the learning model. This makes it a suitable choice for real-world applications in diverse domains. In addition, the advantages of RF include high performance, adapting ad hoc learning tasks and also flexibility for large scale data sets such as CVE, the data set we used in this experiment [35].

The base score is important to capture the fundamental properties of a vulnerability. Additionally, it also specifies the impact due to the exploitation. Kenna research shown that there is a positive correlation between CVSS scores and exploitation [4]. Temporal metrics require up-to-date information about the vulnerability, which is difficult to obtain in many cases. Additionally, it is also difficult to obtain the evidence of exploit data. For the suitability of the selected ML models, we consider in this work, from the attributes of the data set, as explained in Section 4.3.1, we selected six suitable features for our planned experiment: Attack/Access Vector, Attack Complexity, Privileges Required, Confidentiality, Integrity and Availability:

– Authentication/Privileges Required – required credentials before the vulnerability can be exploited: None, Low, and High.

– Availability – the impact of the general availability of the system: None, Low, and High.
– Confidentiality – impact underlying system exploited vulnerability: None, Low, and High.
– Integrity – measures whether an exploit would affect the system's level of trustworthiness: None, Low, and High.
– Attack/Access Vector – level of access to the vulnerable system: Local Access, Adjacent Access, or Network (Remote) Access.
– Attack Complexity – extenuating circumstances required to exploit the vulnerability: Low or High.

5. Experiments

This section describes the experimental process we follow in using ML models for predicting vulnerability exploit using the CVE dataset. The purpose of this experiment is illustrating the suitability of using ML models in predicting vulnerabilities, and also investigate a suitable fitted model for predicting vulnerability exploit using the provided information in the CVE database. The experiment includes the following steps:

– Data preparation: the data set is considered from the widely used CVE data. The data set is divided into two parts: training set and testing set.
– Feature selection: we select the six suitable features to feed the selected ML algorithms and implemented the selected three ML algorithms, LR, DT and RF. The choosing algorithms were selected based on the increasing suitability and complexity, LR followed by DT and then RF.
– Run the experiment on Google Collab platform, were we setup a separate notebook for each of these three algorithms, LR, DT and RF and collect the results.
– Evaluation: the result was evaluated using the elements of confusion matrix, sensitivity measure and specificity measure as shown in Figs 8–15 with additional details in the following subsequent subsections.

5.1. *Dataset description*

The dataset used for this experiment is the popular CVE database CVE that provides a rich catalogue of disclosed vulnerabilities, which contain a total of 164512 entries [3,36]. Organisations partnered with CVE submit their discovered vulnerability to make it publicly available. Here, we summarised the data set in

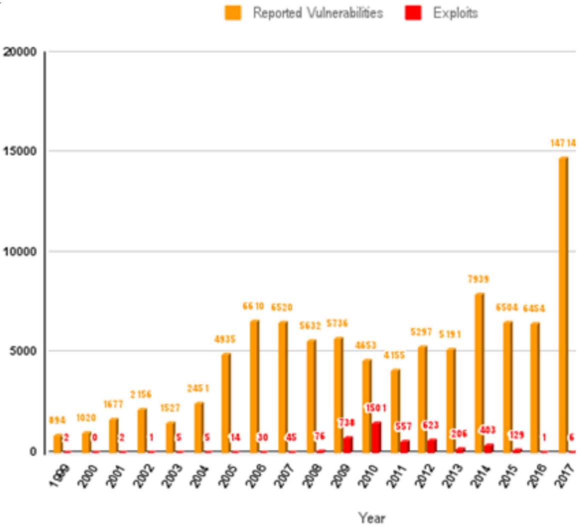

Fig. 6. Trends in vulnerabilities disclosure.

Fig. 6 with the highest disclosed vulnerabilities from the CVE data set. In particular, the figure depicts the Trends in Vulnerabilities Disclosure as it continues to increase from 1999 to 2021, with a sharp rise from 2017, which indicates the increasing demand for investigating novel approaches to address the problem of software vulnerability. The reported vulnerability trend creates the need for an automated approach to support the selection of prioritizing the likelihood of exploiting a vulnerability in the nearest future, to help prioritize which vulnerability need priority patching or control to protect the system. There are strong correlations between the number of reported vulnerabilities and exploitations. Although there is a large number of published vulnerabilities in public databases, like CVE and OSVDB. In practice, this is just a fraction of the vulnerabilities that exist because some vulnerabilities are never disclosed to protect the integrity of the system. The same applies to the published exploitations, large fractions of exploitations remain private to protect the integrity of the exploited system. In this work, we initially consider data sets covering the disclosed vulnerabilities from 1988 to 2018, totaling 111,520 data point that has suitable categorical attributes for the three algorithms we used in this work where we consider limiting the datasets to cover three decades as summarise in Fig. 6. Later on, we have added new data from 2019 and 2022 as there are new supply chain vulnerabilities across the sector after 2018. The outcome of the experiment shows that there is a high correlation among the data set, based on the recorded attributes of the vulnerabilities we used in this work, with additional details in Section 4.

5.2. *Feature selection and implementation*

We have selected a number of features for the exploitability prediction using the published vulnerability data sets. Once the data is collected, the preprocessing stage extract the features in the JSON format organized into data frame. For the suitability of the selected three ML models, we used in this work, we chose suitable attributes of the data set that will help us predict exploitation, as explained in Section 4.3.1. We selected six suitable features for our planned experiment: Attack/Access Vector, Attack Complexity, Privileges Required, Confidentiality, Integrity and Availability:

- Authentication/Privileges Required – required credentials before the vulnerability can be exploited: None, Low, and High.
- Availability – the impact of the general availability of the system: None, Low, and High.
- Confidentiality – impact underlying system exploited vulnerability: None, Low, and High.
- Integrity – measures whether an exploit would affect the system's level of trustworthiness: None, Low, and High.
- Attack/Access Vector – level of access to the vulnerable system: Local Access, Adjacent Access, or Network (Remote) Access.
- Attack Complexity – extenuating circumstances required to exploit the vulnerability: Low or High.

The data set is split into two parts: training set and testing set, using the function *train_test_split* from the *sklearn* library [37]. Each ML algorithm is implemented on a separate notebook in the Google Collaboratory (Collab) platform [38], mainly for the purpose of getting high performance, in addition to providing GPU access as well as flexibility for sharing the work. Initially, we started using Jupiter platform, to increase the speed, we moved to Google Collaboration platform, on the cloud, where we run the experiment in higher speed efficiently.

5.3. *Evaluation*

In evaluating the selected models, first, we consider the prediction usefulness [39] in evaluating the developed technique for predicting the exploitation. Here, we report the prediction usefulness of the three algorithms in Figs 7–9. Figure 7 depicts the prediction usefulness of LR that assess the performance of the LR models by comparing the 'ratio of predicted True/actual true' with actual true. We retrieve the actual true data from the training dataset and compare it with predicted true from testing dataset in evaluating the prediction usefulness.

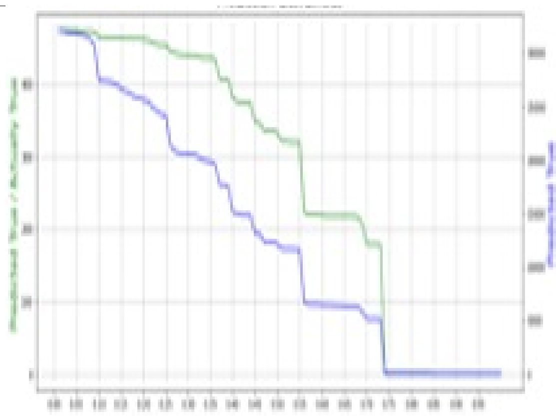

Fig. 7. Prediction usefulness of linear regression.

Fig. 8. Prediction usefulness of decision tree.

This help us to compare the predicted true data with the actual true data in the LR model. The gap between the two graphs (blue and green lines) indicate the closeness of the predicted true and actual which shows the usefulness of the prediction.

Figure 8 depicts the prediction usefulness of DT that assess the performance of the DT models in making prediction. This is by comparing the actual true data from the training set with the predicted true data from the testing dataset. Here, also the narrow area between the two graphs indicate the predictions usefulness of the DT that is closer to LR.

Finally, Fig. 9 depicts the prediction usefulness of RF that assess the performance of the RF models by comparing the training set with testing dataset, to evaluate the predicted true data with the actual true data used to train the model. The graph also follows a similar patterns as LR and DT. For the three graphs, we find that they behave well in a similar pattern with an acceptable threshold that can be improved further. However, here we observe that each of the algorithm drop sharply just before the points 0.55 and 0.75. This is an interesting

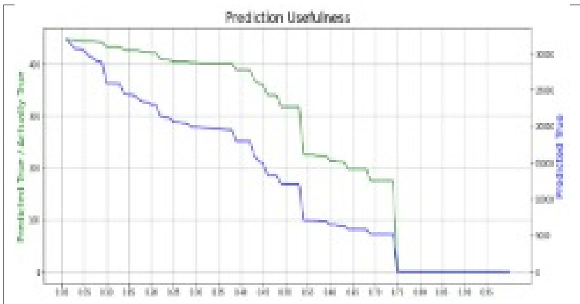

Fig. 9. Prediction usefulness of random forest.

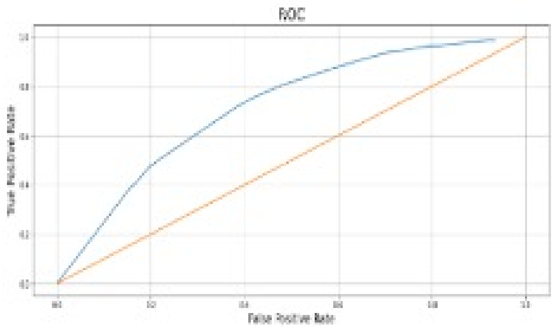

Fig. 10. ROC of linear regression.

observation that we would like to investigate further by using another data set, which will be suitable for expanding the accuracy of the prediction technique.

Receiver Operating Characteristic (ROC) is used to assess the discrimination threshold of the three algorithms. The purpose of ROC is comparing the rate of the two operating characteristics *True-Positive* and *False-Positive*, to measure the performance of a classification model. The higher the area under the curve, the better the performance of the classifier. In the field of ML, ROC quantify the predictive power of the selected models, represented in the area under curve of a graph between the True Positive Rate and False Positive Rate [40].

In this work, as shown in Figs 10–12, the three models form a curve above the diagonal, and cover higher area under the curve which indicates that each of the three ML models performs well in the classification. We find that the ROC of the three ML models resembles one another, which means that the difference between the three algorithms in the discrimination threshold is not significant, as seen in the area under curve of the three algorithms Figs 10–12, for the CVE dataset we used in this work. This is an interesting result that we would like to explore further as part of the recommended direction of expanding this work towards generalising the result.

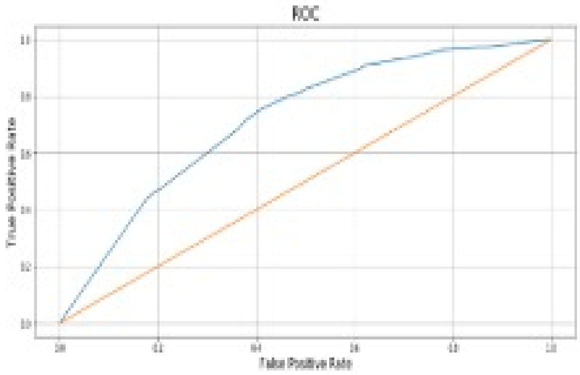

Fig. 11. ROC of decision tree.

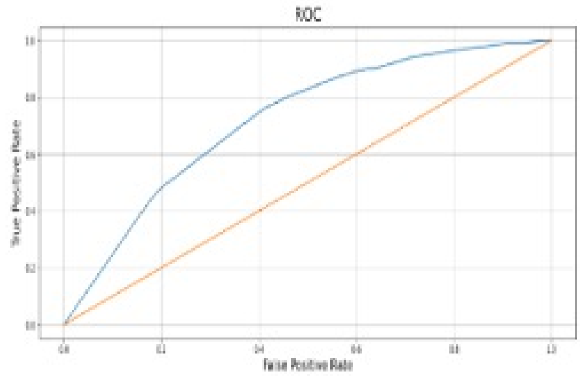

Fig. 12. ROC of random forest.

Likewise, Figs 11 and 12 depict the ROC curve of DT and RF, which also follow a similar pattern in generating a curve above the diagonal covering more area under the curve. Thus, in terms of using ROC to assess descrimination, we find that the three ML models follow similar patterns in prividing useful result by generating a curve above the diagonal and covering more area under the curve.

To find a way of reducing False-Positives and increase the True-Positive result, we consider combining recall and precision to calculate the F-beta scoring system [41], using the scores 2, 4, 6, 8, 10, 12, 14, 16, 18, and 20, as shown in Figs 9–11. The F-Beta score has a positive real number as its factor β for adjusting the weight of recall and precision for an experimental test [42]. The value of β is chosen as an integer value such that recall is considered β times as important as precision, expressed as follows:

$$F_\beta = \left(1+\beta^2\right) * \frac{Precision * Recall}{(B^2 * Precision) + Recall}$$

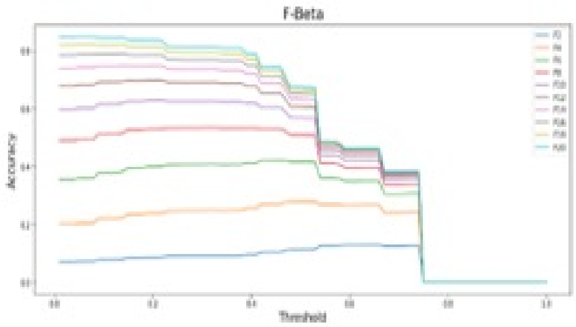

Fig. 13. F-Beta graph of linear regression.

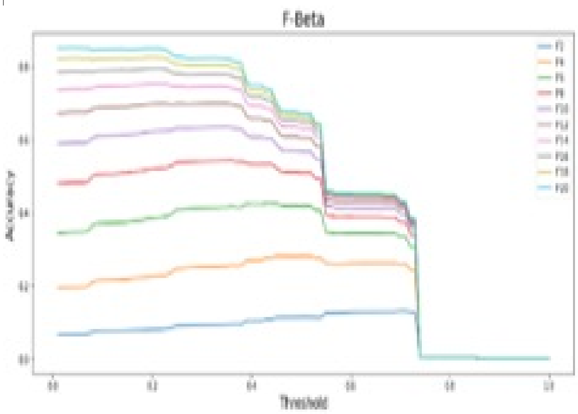

Fig. 14. F-Beta graph of decision tree.

The results allow us to measure the effectiveness of the models by adjusting the recall over the corresponding precision. Thus, after developing the F-Beta graph of the three ML models, we find that in each case, the F-Beta scores drop between 0.5 to 0.6 and between 0.7 to 0.8. This result indicates that in terms of F-Beta measurement three models behave the same.

The results allow us to measure the effectiveness of the models by adjusting the recall over the corresponding precision. For instance, Figure 13 shows the F-beta graph of LR, for F2, F4, F6…F20. In similar way, we develop the F-beta graph of the remaining two ML models, DT and RF. Thus, after developing the F-Beta graphs of the three ML models, we find that in each case, the F-Beta scores drop in between 0.5–0.6 and also between 0.7–0.8, as shown in Figs 14 and 15. The result confirms that three models behave in similar manner, in terms of F-Beta measurements.

The LR has the lowest accuracy of 61% in predicting exploitation, while DT improves the result to 62% and RF improve it further to 63%. Thus, the results get better with the increasing complexity of the algorithms;

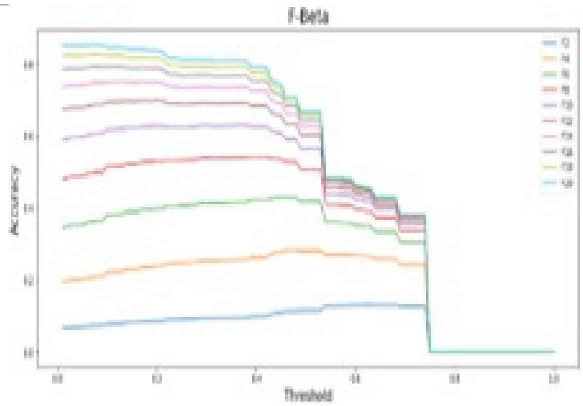

Fig. 15. F-Beta graph-random forest.

from the simple algorithm LR to DT with higher complexity but better result, and also better result in using RF with the cost of increasing complexity. Although we expect better results than the reported results, considering the increasing complexity, as recommended in the literature [43]. RF provides better results compared to DT, especially with increasingly large datasets like CVE. However, our concern here may be due to the structure of the input data set, in the form of textual data that is regarded as one of the weaknesses of RF. This is an interesting observation that we will explore further as part of our future work. Also, we will investigate additional algorithms that will help us improve the accuracy of the prediction to be able to provide precise control for the predicted vulnerability.

6. Discussion

The health care sector is now primary target for information theft and service disruption due to the lack of security measure. The cyber attack can pose any security risks that have the potential to the overall eco system. Patient healthcare information is handled by almost every healthcare entities including hospital, clinic and diagnostic centre. The actors of the entities such as doctors, nurses, pharmacists, and technicians use this sensitive information for patient treatment and other related service delivery. Therefore, cybersecurity needs to consider holistically from every aspects of the overall ecosystem. However, understanding vulnerabilities which are relevant for the specific context is a challenging task. This work presents a conceptual view to represent the concepts and ontological view that provides a common language and a knowledge base related to the health care and cyber security domain. This certainly

Table 1
False precision measures

ML model	False-negative	False-positive	Sum
Linear regression	12266	125	12391
Decision tree	11938	128	12066
Random forest	11777	130	11907

help in identifying the relevant vulnerabilities from all aspect of the concepts. Finally, we have considered the possible vulnerabilities exploitability using three ML models to prioritise the vulnerabilities which needs adequate attention. The experimentation result provided high accuracy with the LR. We have made the following observations.

– Determine the applicability of using ML in predicting exploitation – the result shows that exploitability prediction provides an early warning of the potential attack so that appropriate control measures can be taken into consideration.
– Improving the Accuracy of the result – in comparing the three algorithms, we see clear progress in improving the accuracy of predicting the vulnerability exploitability, with decision tree at 61%, linear regression at 62% and Random Forest at 63%.

Determine the rate of false predictions – there is additional progress in the accuracy of the predicted result by minimising both the false-negative and false-positive, as summarise in Table 1. For the LR, the false-negative is 12266 while false-positive is 125, resulting in 12391. For DT, the false-negative is 11938 while false-positive is 128, resulting in 12066. For RF, the false-negative is 11777 while false-positive is 130, resulting in 11907. So, there is good progress in reducing the negative results, 12391, 12066 and 11907.

We have compared our findings with the existing works in the literature for the general observations. In particular, the work [44] is closer to our approach of using ontology and ML in cybersecurity. The work illustrates using an ontology on the structured NVD data and proposes a TRONTO system that gathers information about vulnerabilities from social media and supported queries using BERT classifier. However, our work uses the CVE data sets in a broader context of healthcare vulnerabilities, without restricting the work to specific systems or applications or area. We have also considered three ML to demonstrate the advantages of each model for the prediction of exploitability. Another work [11] considers using ML in predicting cybersecurity incidents focusing specifically on Small and Medium Enterprises (SME) in South Korea. However, the context of our work is not specific to SMEs, hence we focus the broader healthcare system with CVE database. There is another work [45] that illustrates using social media, news articles and open-source data to predict vulnerabilities in cybersecurity, using two ML models: Vector Machines and fine-tuned BERT. The result indicates that the model BERT performs better than Vector Machine. In comparison to our work, we use different datasets from CVE and different ML models which expand the literature. But it will be interesting to investigate the performance of BERT on the CVE, which is the dataset we used for this experiment. Also, [46] considers different ML models to predict risk types, which shows that different algorithms provide different accuracy level in predicting various risk types including Cyber Espionage and Denial of Service. Our work differs from this work as we focus on vulnerability exploitability prediction, but both focus on critical infrastructure.

The healthcare entities are still using a number of legacy applications and devices that are running outdated software or operating systems without upto date patch. Additionally, third party services providers are in many cases responsible to manage the overall system. Vulnerabilities in medical devices such as CT scanners, pacemakers, and drug infusion pumps are also growing concern. Therefore, it is necessary for the healthcare entity to actively search out vulnerabilities relevant in their systems and maintain ongoing vulnerability management for the overall security. It is also necessary not to overemphasis on zero-day vulnerabilities, rather the probability of the exploitability of vulnerabilities which are relevant within the context.

The proposed work can effectively support in determining the exploitability of the relevant vulnerabilities so that a list of vulnerabilities can be prioritised for suitable controls. Our work advocates to consider the center for internet security control (CIS) as baseline to understand the various areas where controls are required based on the exploitable vulnerability. The controls are classified according to basic, foundational and organizational with twenty different classes of controls. For instance, encryption need to be implemented in various data states including both at rest and in transit as well as the third-party service providers that have access to healthcare networks or databases. Security awareness and training is also required for all healthcare actors on handling the healthcare data to prevent data breach and service disruption.

7. Conclusion

The health care sector is constantly an attractive target for cybercriminals due to the sensitivity of the healthcare data and potential financial gain. As a result, cyberattacks are increasing across the Health Care Information Infrastructure (HCII). This work integrates relevant concepts for a common understanding of cyber security of the healthcare sector and uses ontology that provides knowledge base for the domain. Three different ontological views are considered including Healthcare supply chain service delivery, Vulnerability assessment, and Base Score vulnerability Metrics Ontology. We consider three ML models to predict vulnerability exploitability which effectively support the prioritisation of relevant vulnerabilities. In particular, a list of features from the CVSS is considered for the prediction. The results show that the ML is able to anticipate which vulnerabilities can be exploitable with 63% accuracy.

Our work has some limitations. In particular, the scope of this work is limited to the CVE dataset. However, CVE does not fully provide up-to-date exploitability related information for a specific vulnerability. Therefore, in future, we are planning to adopt other dataset including ExploitDB for the purpose of prediction. Extending the dataset has a good potential for improving the accuracy of the research that will also help in generalising our findings. The approach considers three algorithms, i.e., LR, DT and RF. The vulnerability description is in textual format, which includes related information that could link with exploitation. Therefore, Natural Language Processing (NLP) can help improve the result by extracting additional features from the text description of the vulnerabilities. We are planning to include NLP for this purpose. Finally, the current work focuses on base metric properties for the exploitation. The temporal metric also provides other information related to the exploitation such remediation level and report confidence. This information can change over the time and indicates the possibility of exploitation. The addition of temporal metric value could be an interesting future direction as well. Part of the recommended future work should investigate the possibility of addressing both false positives and false negatives, considering the provided six features used in the predictions.

Acknowledgments

This work was partially supported by the AI4HEALTHSEC EU project, funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273.

References

[1] Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, Burleson W, Vogel JM, O'Leary C, Eshaya-Chauvin B, Flahault A. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC medical informatics and decision making. 2020; 20(1): 1-10.

[2] HIMSS. Cybersecurity Survey. https//www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf. 2020 (accessed 22 April 2022).

[3] CVE. Common Vulnerabilities and Exposures CVE. https://cve.mitre.org/. 2021.

[4] Cyrntia Institute. Kenna security, prioritization to prediction volume 1: Analyzing vulnerability remediation strategies. Leesburg, USA; 2018.

[5] McGuinness DL. OWL web ontology language overview. W3C recommendation. 2004; 10(10).

[6] Välja M, Heiding F, Franke U, LagerstrÃűm R. Automating threat modeling using an ontology framework. Cybersecurity. 2020; 3(1): 1-20.

[7] Vorozhtsova T, Skripkin S. Ontological analysis of vulnerabilities in the energy sector. In: Vth International workshop Critical infrastructures: Contingency management, Intelligent, Agent-based, Cloud computing and Cyber security (IWCI. 2018.

[8] Jacobs J, Romanosky S, Adjerid I, Baker W. Improving vulnerability remediation through better exploit prediction. Journal of Cybersecurity. 2020; 6(1).

[9] Recorded Future. Threat Intelligence Report | Recorded Future. https://www.recordedfuture.com/threat-intelligence/#:text=Recorded%20Future%20users%20identify%20risks,where%20even%20seconds%20can%20matter. 2022 (accessed 22 April 2022).

[10] Qiu D, Qin S. Vulnerability chain assessment for multiple vulnerabilities. In: 3rd International Conference on Materials Engineering, Manufacturing Technology and Control. 2016.

[11] Mohasseb A, Aziz B, Jung J, Lee J. Predicting cyberSecurity incidents using machine learning algorithms: A case study of Korean SMEs. In: ICISSP. 2019. pp. 230-237.

[12] Cooper GF, Aliferis CF, Ambrosino R, Aronis J, Buchanan BG, Caruana R, Fine MJ, Glymour C, Gordon G, Hanusa BH, Janosky JE. An evaluation of machine-learning methods for predicting pneumonia mortality. Artificial intelligence in medicine. 1997; 9(2): 107-138.

[13] Zoabi Y, Deri-Rozov S, Shomron N. Machine learning-based prediction of COVID-19 diagnosis based on symptoms. NPJ digital medicine. 2021; 4(1): 1-5.

[14] Qayyum A, Qadir J, Bilal M, Al-Fuqaha A. Secure and robust machine learning for healthcare: A survey. IEEE Reviews in Biomedical Engineering. 2020; 14: 156-180.

[15] Rafiei MH, Adeli H. A novel unsupervised deep learning model for global and local health condition assessment of structures. Engineering Structures. 2018; 156: 598-607.

[16] Pereira DR, Piteri MA, Souza AN, Papa JP, Adeli H. FEMa: A finite element machine for fast learning. Neural Computing and Applications. 2020; 32(10): 6393-6404.

[17] Alam KM, Siddique N, Adeli H. A dynamic ensemble learning algorithm for neural networks. Neural Computing and Applications. 2020; 32(12): 8675-8690.

[18] Gao Y, Zhai P, Mosalam KM. Balanced semisupervised generative adversarial network for damage assessment from low-data imbalanced-class regime. Computer-Aided Civil and Infrastructure Engineering. 2021; 36(9): 1094-1113.

[19] Dong S, Yu T, Farahmand H, Mostafavi A. Bayesian modeling of flood control networks for failure cascade characterization and vulnerability assessment. Computer-Aided Civil and Infrastructure Engineering. 2020; 35(7): 668-684.

[20] Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care. 2017; 25(1): 1-10.

[21] Rios B, Butts J. Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies. WhiteScope, sl. 2017.

[22] CIS. Cyber attacks: In the healthcare sector. https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/. 2022 (accessed 22 April 2022).

[23] Wagner SM, Neshat N. Assessing the vulnerability of supply chains using graph theory. International Journal of Production Economics. 2010; 126(1): 121-129.

[24] Dobrzykowski D. Understanding the downstream healthcare supply chain: Unpacking regulatory and industry characteristics. Journal of Supply Chain Management. 2019; 55(2): 26-46.

[25] Nguyen TT, Reddi VJ. Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems. 2019.

[26] Islam S, Papastergiou S, Mouratidis H. A dynamic cyber security situational awareness framework for healthcare ICT infrastructures.25th Pan-Hellenic Conference on Informatics. 2021; 334-339.

[27] Booth H, Rike D, Witte GA. The national vulnerability database (NVD): Overview ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD. https//tsapps.nist.gov/publication/get_pdf.cfm?pub_id=915172. 2013 (accessed April 22 2022).

[28] Jordan MI, Mitchell TM. Machine learning: Trends, perspectives, and prospects. Science. 2015; 349(6245): 255-260.

[29] Montgomery DC, Peck EA, Vining GG. Introduction to linear regression analysis. John Wiley & Sons. 2021.

[30] Rokach L. Decision trees. In: Data mining and knowledge discovery handbook. Springer, Boston, MA. 2005. pp. 165-192.

[31] Cutler A, Cutler DR, Stevens JR. Random forests. In: Ensemble machine learning. Springer, Boston, MA. 2012. pp. 157-175.

[32] Montgomery DC, Peck EA, Vining GG. Introduction to linear regression analysis. John Wiley & Sons. 2021.

[33] Song YY, Ying LU. Decision tree methods: Applications for classification and prediction.Shanghai archives of psychiatry. 2015; 27(2): 130.

[34] Breiman L. Random forests. Machine learning. 2001; 45(1): 5-32.

[35] Biau G, Scornet E. A random forest guided tour. Test. 2016; 25(2): 197-227.

[36] Martin R, Christey S, Baker D. The Common Vulnerabilities and Exposures (CVE) Initiative. MITRE Corporation. 2002.

[37] Trappenberg TP. Machine learning with sklearn. In: Fundamentals of Machine Learning. Oxford University Press. 2019. pp. 38-65.

[38] Carneiro T, Da Nóbrega RVM, Nepomuceno T, Bian GB, De Albuquerque VHC, Reboucas FPP. Performance analysis of google colaboratory as a tool for accelerating deep learning applications. IEEE Access. 2018; 6: 61677-61685.

[39] Kappen TH, van Klei WA, van Wolfswinkel L, Kalkman CJ, Vergouwe Y, Moons KG. Evaluating the impact of prediction models: lessons learned, challenges, and recommendations. Diagnostic and Prognostic Research. 2018; 2(1): 1-11.

[40] Fawcett T. An introduction to ROC analysis. Pattern recognition letters. 2006; 27(8): 861-874.

[41] Frolov N, Kabir MS, Maksimenko V, Hramov A. Machine learning evaluates changes in functional connectivity under a prolonged cognitive load. Chaos: An Interdisciplinary Journal of Nonlinear Science. 2021; 31(10).

[42] Van Rijsbergen CJ. Information retrieval. 2nd. Newton, MA. 1979. p. 37.

[43] Ali J, Khan R, Ahmad N, Maqsood I. Random forests and decision trees. International Journal of Computer Science Issues (IJCSI). 2012; 9(5): 272.

[44] Aranovich R, Wu M, Yu D, Katsy K, Ahmadnia B, Bishop M, Filkov V, Sagae, K. Beyond NVD: Cybersecurity meets the Semantic Web. In: New Security Paradigms Workshop. 2021. pp. 59-69.

[45] Iorga D, Corlătescu D, Grigorescu O, Săndescu C, Dascălu M, Rughiniş R. Early detection of vulnerabilities from news websites using machine learning models. IEEE 19th RoEduNet Conference: Networking in Education and Research (RoEduNet). 2020; 1-6.

[46] Kure HI, Islam S, Mouratidis H. An integrated cyber security risk management framework and risk prediction for the critical infrastructure protection. Neural Computing and Applications. 2022; 1-31.

[47] Kappen TH, van Klei WA, van Wolfswinkel L, Kalkman CJ, Vergouwe Y, Moons KG. Evaluating the impact of prediction models: lessons learned, challenges, and recommendations. Diagnostic and Prognostic Research. 2018; 11.

[48] Fawcett T. An introduction to ROC analysis. Pattern Recognition Letters. 2006; 861-874.

[49] Syed Z, Padia A, Finin T, Mathews L, Joshi A. UCO: A Unified Cybersecurity Ontology. AAAI Workshop on Artificial Intelligence for Cyber Security. 2016.

[50] Dimitrov V, Kolev I. An Ontology of Top 25 CWEs. http//ceur-ws.org/Vol-2656/paper9.pdf. 2020.