Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.018048
Article

Tech Science Press

Machine Learning Based Framework for Maintaining Privacy of Healthcare Data

Adil Hussain Seh[1], Jehad F. Al-Amri[2], Ahmad F. Subahi[3], Alka Agrawal[1], Rajeev Kumar[4,*] and Raees Ahmad Khan[1]

[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, India
[2]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif P.O. Box 11099, Taif 21944, Saudi Arabia
[3]Department of Computer Science, University College of Al Jamoum, Umm Al Qura University, Makkah, 21421, Saudi Arabia
[4]Department of Computer Applications, Shri Ramswaroop Memorial University, Barabanki, 225003, India
*Corresponding Author: Rajeev Kumar. Email: rs0414@gmail.com

Received: 23 February 2021; Accepted: 13 April 2021

Abstract: The Adoption of Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), cloud services, web-based software systems, and other wireless sensor devices in the healthcare infrastructure have led to phenomenal improvements and benefits in the healthcare sector. Digital healthcare has ensured early diagnosis of the diseases, greater accessibility, and mass outreach in terms of treatment. Despite this unprecedented success, the privacy and confidentiality of the healthcare data have become a major concern for all the stakeholders. Data breach reports reveal that the healthcare data industry is one of the key targets of cyber invaders. In fact the last few years have registered an unprecedented rise in healthcare data breaches. Hacking incidents and privilege abuse are the most common threats and have exposed sensitive and protected health data. Experts and researchers are working on various techniques, tools, and methods to address the security issues related to healthcare data. In this article, the main focus is on evaluating the impact of research studies done in the context of healthcare data breach reports to identify the contemporary privacy and confidentiality issues of sensitive healthcare data. Analysis of the research studies depicts that there is a need for proactive security mechanisms that will help the healthcare organizations to identify abnormal user behavior while accessing healthcare data. Moreover, studies also suggest that ML techniques would be highly effective in securing the privacy and confidentiality of the healthcare data. Working further on this premise, the present study also proposes a conceptual framework that will secure the privacy and confidentiality of healthcare data proactively. The proposed framework is based on ML techniques to detect deviated user access against Electronic Health Records. Further, fuzzy-based Analytical Network Process (ANP), a multi-criteria decision-making approach, is used to assess the accuracy of the supervised and unsupervised ML approaches for achieving a dynamic digital healthcare data security environment.

Keywords: Healthcare; data security; machine learning; theoretical framework; fuzzy-ANP

1 Introduction

The Electronic health (e-health) is an advanced form of conventional paper-based health infrastructure that practices advanced healthcare information technology to enhance the care services. To provide efficient, reliable, and cost-effective service to the patients, various ubiquitous technologies namely the Internet of Medical Things, smart devices, web-based applications, wireless sensor devices, telemedicine devices, AI, ML, and cloud services have been adopted by the healthcare service providers. These technologies have significantly improved the dissemination of healthcare data among various interested entities and facilitated in providing online care services such as online patient monitoring and telemedicine, etc. Implementation of Electronic Health Record (EHR) systems is one of the major outcomes of health information technology [1,2]. The EHR systems store the medical and treatment histories of patients as records and make them accessible to the authorized users all the time. However, these health records are frequently breached by the hackers. The EHR automates access to information and has the potential to streamline the clinician's workflow. It improves the decision-making ability of the healthcare professionals and helps them in reducing the error rate in diagnosis.

Nevertheless, several potential hazards threaten the privacy and confidentiality of protected healthcare data. The inherent complex and dynamic nature of the healthcare industry make EHR systems potentially vulnerable to insider attacks that adversely affect the confidentiality of data. The healthcare sector is one of the top three sectors that are currently facing the highest number of breached incidents [3]. Authentic research studies and data breach reports reveal that the healthcare sector is highly susceptible to both internal and external intrusions. There have been 225 healthcare data breach episodes in the first half of 2020 itself. 130 of these breach instances were because of hacking/IT incidents which; i.e., 57.77% of the total number of breach cases [4], and 59 breaches were because of internal unauthorized access. Reports also cite that 3033 healthcare data breach incidents engineered during 2010 to 2019 exposed 255.18 million patients' records in the USA [5]. Out of the 3033 breach cases, 850 were disclosed because of hacking/IT incidents, and 843 were exposed because of internal unauthorized access. The healthcare data industry is being victimized by both internal as well as external threats. Healthcare data breaches also harm the reputation of the organizations and service providers, resulting in the loss of patients' trust and, consequently, loss of revenue [6]. One of the main reasons for the unprecedented rise in data breach cases is the selling value of health data records which is estimated to be ten to twenty times higher than the credit card data in the online market [7]. Facts and figures reveal that due to its' high sensitivity and valuable character, healthcare data has become the most sought-after entity for intruders. Such a scenario calls for immediate intervention mechanisms to eliminate the possibilities of healthcare data pilferage. To address the privacy and confidentiality issues of healthcare data, the authors of this study have provided a theoretical Machine Learning framework that will detect suspicious user access to an EHR system that holds the patients' health records.

Machine Learning, as a co-domain of Artificial Intelligence, ensures that historical data programs (intelligent models) can be enlisted to learn, achieve experience, and improve system's performance to classify, predict future trends and make decisions without human involvement [8,9]. Every correct future prediction or decision enhances the performance measure of the intelligent program. Artificial intelligence and machine learning have changed the way people think and play a significant role in different fields of life. ML-based models have been practiced in different areas to address real-life problems, and fortunately, in most of the areas, they have achieved the desired targets. Weather forecasting, disease analysis, and diagnosis, defense, sentimental analysis, marketing, traffic prediction, Fraud detection are some of the prominent examples of ML-based mechanisms. ML also has a significant role in cyber security because of its proactive character to detect misuse and anomalous behaviors such as intrusion, fraud, and email spam detection. Here we aim to address healthcare data's confidentiality and privacy issues through the ML approach. To achieve the stated objective, the study proposes a theoretical ML-based framework that will describe the normal users' behaviors of dynamic healthcare environment and detection of suspicious or abnormal user behaviors against the normal user profiles. This model will help the healthcare service providers to secure sensitive health data from suspicious accesses that result in healthcare data breaches.

The rest of the work has been organized as: the second section of this research endeavor presents the analysis of some important existing research studies; the third section discusses the healthcare data privacy and confidentiality issue in the contemporary scenario; part 3.1-the sub-section discusses the arrival rate and inter-arrival time of different data disclosures. The fourth section describes the ML-based theoretical framework for suspicious user access detection. Section 4.1 provides Fuzzy-ANP based idealness assessment of ML approaches. The final section concludes the proposed study.

2 Analyses of the Existing Research Studies

Research has an implicitly dynamic and a continuous character. It always starts with a problem and ends with a problem. The researcher identifies a problem and finds solutions for it and at the end of the research process, the determined results come up with some limitations as newly identified problems. This character of the research makes it an ongoing process. Hence, to identify the actual research gap and the objectives of a proposed research study, the researchers go through the existing literature relevant to the proposed theme. Thus, in this sub-section, we will summarize the results of some of the existing literature studies.

- The authors of this research endeavor implemented the Actor-Network Theory to address the complexity of dynamic healthcare environment and narrated the associations among the users who are concerned with the digital healthcare data [10]. In this study, the researchers showed that the complex network of individuals, service providers, and technologies that are involved in storing and processing protected health data make it more vulnerable to intruders.
- In this research endeavor, the market effect of healthcare data breaches has been examined from the patients' perspectives and actions [11]. This study shows that data breaches did not affect patients' short-term choices, but the overall effect of breach events over 3 years decreased the number of outpatient visits and admissions significantly.
- This research study depicts the monetary effects and consequences of cyber intrusions on healthcare organizations [12]. This study shows that though there is a variation in data breach cost reports, the healthcare data breaches adversely affect the overall healthcare organizations with special reference to Poland's health sector. The reasons behind the data breach cost variation are different cost estimation approaches, incomplete information, and insufficient disclosure of intrusions.
- In this comprehensive healthcare data breach study, the authors cite that with the advances in healthcare technology, healthcare data breaches have also increased rapidly [5]. This research endeavor depicts that hacking and other IT cyber incidents in the last five years have drastically affected the healthcare sector. Furthermore, the cost of healthcare breached records has increased rapidly as compared to the cost of breached records of other sectors. This study further reveals that privilege abuse is the second biggest cause behind healthcare data breaches. The authors of this work conducted an analytical study on healthcare data breaches from a digital forensic perspective [13]. The study cited that irrespective of the technological revolution in the healthcare sector, disclosure of protected health information is still at the peak. Most of the breached incidents show the same pattern and are attributed to internal actors. Privilege abuse is an alarming issue in the

healthcare sector and plays a significant role in illegal data disclosure. Various free and open source EMR systems have been examined in this study and it has been found that these systems do not provide a sufficient level of forensic logging needed to support investigations focusing on privileged abuse.

- In this research study, the authors analysed data breaches faced by various organizations from education to healthcare [14]. This study mainly focused on hacking incidents carried out on various organizations by the intruders. It revealed that healthcare and business organizations were the prime targets of the intruders and had very few mean inter-arrival times as compared to other organizations. This implies that healthcare and business organizations are more frequently attacked by the intruders because of the highly sensitive data.
- Authors of the study researched on the causes of the healthcare data breaches and concluded that the main causes for the breaches were theft, loss, unauthorized access/disclosure, improper disclosure, or hacking incidents [15]. This study also noted that the sources from where the healthcare data was exposed included networks, paper films, e-mail, portable devices, desktop computers, and laptops. The study observed that theft and loss compromised the largest data breaches as compared to hacking incidents.

From the analysis of some of the important existing studies, it was found that the healthcare sector is facing a major threat in the context of privacy and security breaches. Both the internal or external factors are responsible for data breach episodes. Loss, theft or tampering of health data impair the reputation, and business continuity of the healthcare organizations. Moreover, inaccurate information due to data breach can also lead to errors in treatment and medication, thus endangering the patients' health. Thus, the security experts and researchers need to address the privacy and security issues of healthcare data.

3 Data Privacy and Confidentiality Issues

A paradigm shift in the present day electronic healthcare records effected by the recent pandemic demand more foolproof security mechanisms [16]. As a result, in terms of sophistication, diversity, and timeliness, the healthcare sector is experiencing a massive expansion in the volume of data. In today's digital age, data is the most precious commodity. Every digitalized industry produces huge quantities of data. It is estimated that the amount of data produced each day throughout the world by 2025 will be 463 Exabyte and the number of IoT devices will reach up to 75 billion [17]. In 2018, 2.5 Exabyte data was produced each day. 90% of the aggregate data has been produced in the last two years alone [18]. Thus, safeguarding the privacy and the confidentiality of such huge data is, unambiguously, a serious and a challenging issue.

Data confidentiality defines the policies that ensure that customer-shared data is only used for the intended purpose and should be protected from unlawful, unauthorized access, disclosure, or theft [5]. The ability of the customers to monitor how their personal information is obtained and used ensures protection of the information. Privacy means ensuring that the health information of people is adequately protected. Privacy or rather the lack of it is one of the major hurdles in gaining patients' confidence and introducing completely functional e-health systems. Privacy can also be also defined as having the capacity to promote or encourage fundamental values such as personal autonomy. It also helps the individuals to monitor how clinicians and other consumers handle and use their e-health information in fields other than healthcare.

Major privacy and security challenges in e-healthcare are *access control and authentication, data Integrity, system Availability, Data Loss, and network security* [5,19,20]. Cyber-security risks to health care are frequently seen as primary instigators of data breaches, and while frequently real, this is not often the only aspect that protected companies and business associates need to plan. Further, from

2010 to 2019, 3033 data breach incidents were reported against the healthcare sector which collectively disclosed 255.18 million patients' records [5]. Furthermore, in the first nine months of the year 2020, 393 healthcare data breach incidents were reported that exposed 18.57 million patients' records [21].

Survey reports state that in 2010, the average cost of a breached record was $219, while the cost of healthcare breached record was $294. Interestingly, though the average cost of a breached record reduced to $150 in 2019, the cost of healthcare breached records increased to $ 429 [5]. This 45% increment in the value of breached healthcare data has been a major impetus for healthcare data predators who are constantly preying upon the privacy of patients' data. Tab. 1 given below represents the year-wise total number of healthcare data breaches, the number of data breaches with different disclosure types, and the number of exposed records from 2010 to 2020 [5, 21–25]. We have presented only the summarized data for the first 9 months of the year 2020 because of the unavailability of data for the last three months. The key issues in terms of healthcare data privacy and confidentiality are *Hacking/IT incidents (mainly includes ransomware, malware injection, and phishing), the unauthorized access (encompasses privileged abuse and internal disclosure), theft/loss, and Improper data disposal*. These issues have been identified from healthcare data breach analysis and their graphic representation is shown in Fig. 1. The illustration represents how different data disclosure types have affected the healthcare data industry year by year in an increasing or decreasing trend. The analysis also reveals that hacking related incidents followed by privileged abuse (internal disclosure) attacks are still growing abruptly and affect the healthcare industry adversely. As part of an efficacious solution to the pressing crisis, this study has devised an ML-based framework discussed in Section 4.

Table 1: Healthcare data breaches with different disclosure types

Year	Number of Data Breaches	Theft/ Loss	Hacking/ IT Incidents	Unauthorized Access/ Disclosure (Internal)	Improper Disposal	Unknown	Exposed Records in Millions
2010	199	148	8	8	10	25	5.530
2011	200	136	17	27	7	13	13.150
2012	217	138	16	25	8	30	2.800
2013	278	150	25	64	13	26	6.950
2014	314	143	35	76	12	48	17.450
2015	269	105	57	101	6	0	113.270
2016	327	78	113	129	7	0	16.400
2017	359	73	147	128	11	0	5.100
2018	365	55	158	143	9	0	33.200
2019	505	51	274	142	7	31	41.200
2020	393	37	262	77	13	4	18.57
Total	3426	1114	1112	920	103	177	273.62

3.1 Arrival Rate and Inter-Arrival Time of Different Data Disclosures

Arrival rate defines the number of arrivals of an event or object that occurred per unit of time whereas inter-arrival time specifies the time between two arrivals that occurred in a system. Arrival rate and inter-arrival time helps us to determine the frequency of different data disclosure types concerned with time and allows us to build a clear vision of the frequency of data breach attacks [14]. Such an analysis will help the healthcare organizations and security experts to prioritize and identify the most severe attack types, thus using the information to contain and minimise the impact of disclosures effectively. Arrival rate and inter-arrival time are inverse of each other and are mathematically calculated with the help of Eqs. (1) and (2).

$$Arrival\ Rate = \frac{1}{inter\ arrival\ time} \tag{1}$$

$$Inter\ Arrival\ Time = \frac{1}{arrival\ rate} \tag{2}$$

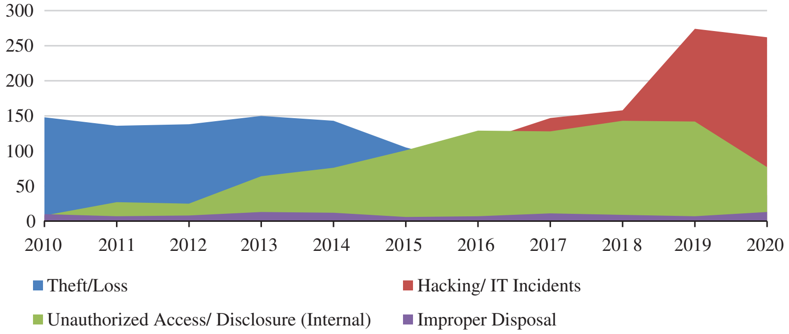

Figure 1: Different data disclosure types since 2010 to 2020

Time period mentioned in this study is 2010 to September 2020. And in most cases, the hour is considered as a unit. But data breach reporting is either carried out on a monthly or yearly basis. Thus, we also considered the unit here as either a month or a year. For a crisp and better analysis, we will consider month as a unit of time to calculate the arrival rate and inter-arrival time of the healthcare data breaches related to different disclosure types such as theft/loss, hacking/IT incidents, Internal disclosure, and Improper disposal. Therefore, the mentioned period (2010 to September 2020) consists of a total of 129 months. In this study, we will calculate the arrival rate and inter-arrival time of data breaches in three different cases:

- Case-I will determine these two parameters of the whole period.
- Case-II will calculate separately the first half (2020-2015) of the time period.
- Case-III will examine the inter-arrival time of the last half (2015-2020) of the period separately.

Different case analyses will help us to find out the trend of a data breach in three different scenarios and examine the pattern of change and the extent of the magnitude of the disclosure. Tab. 2, given below represents the above three cases separately with the final calculated results of arrival rate and inter-arrival time of different data disclosure attack types.

Results of Tab. 2 precisely reveal that in the last five or six years, the number of hacking related attacks increased rapidly whereas the cases of theft/loss show a sufficient decrement. However, privileged abuse (internal disclosure) type attacks also increased but not as much as the hacking related incidents. Improper disposal of unnecessary healthcare data does not show any significant change from case-II to case-III. In the II case of the study, the hacking/IT, incidents arrival rate was 2.194 per month, whereas in the III case it goes up to 14.652 breaches per month and its inter-arrival time reduces to 0.068 from 0.455. This makes it an alarming issue for both the healthcare organizations and researchers. Further, Privilege abuse (unauthorized internal disclosure) type attacks also grow from 4.180 to 10.432 in arrival rate with sufficient reduction in inter-arrival time from 0.239 to 0.095. Thus, privacy and confidentiality of healthcare data need the urgent focus of researchers and security experts who must find out strong technical solutions for the crisis. In the next section of this study, we have provided machine learning based proactive solution to ensure healthcare data's privacy and confidentiality.

Table 2: The Arrival rate and inter arrival time of different type's healthcare data disclosures

		Theft/Loss	Hacking/IT Incidents	Unauthorized Access/ Disclosure (Internal)	Improper Disposal
Case-I (2010-2020)	No of breaches	1114	1112	920	103
	Arrival Rate/Month	8.635	8.620	7.131	0.798
	Inter Arrival Time	0.115	0.116	0.140	1.253
Case-II (2010-2015)	No of breaches	820	158	301	56
	Arrival Rate	11.388	2.194	4.180	0.777
	Inter Arrival Time	0.087	0.455	0.239	1.287
Case-III (2015-2020)	No of breaches	399	1011	720	53
	Arrival Rate	5.782	14.652	10.434	0.768
	Inter Arrival Time	0.172	0.068	0.095	1.302

4 Theoretical Machine Learning-Based Framework

The theoretical framework provides concepts with their description of the study that is under consideration [25,26]. It provides demonstrations and understandings about the concepts that encompass the concerned work and convey a platform for a practical model that addresses the existing problem in a real life environment. The study aims to provide a theoretical ML framework that ensures the confidentiality of EHRs in the dynamic healthcare environment. It will provide a proactive mechanism for the detection of anomalous or suspicious user accesses against the protected health records and enhance the security attribute of healthcare data.

The advanced digital healthcare environment is predominantly concerned with the users that are patients, healthcare professionals who might be doctors, nurses, lab technicians, billers or system admins, and others (a user who can access on the behalf of a patient in an emergency). All these users' profiles have got different types of privileges to access healthcare data. The same levels of users usually get the same type of privileges such as all doctors, all nurses, all billers, all patients, and all other users. With the granted privileges, healthcare data is accessed in different ways by different types of system users. User accesses with different attributes such as user id, device id, patient id, time and duration, user action are recorded in the system log. Normal user accesses against the health information system repeats the same pattern by the same level of users [6]. Thus with the consultation of the concerned domain security experts, a labeled data set can be prepared from the historical log data to train and test the supervised ML model. And then it can be used in the healthcare environment to identify any abnormal or suspicious user access. But the preparation of a labeled data set is time consuming, costly, and expert dependent. Hence, the authors of the study have provided another scenario which is the implementation of an unsupervised ML-based model. The proposed model will distribute the historical log records in different clusters based on similarity and dissimilarity. The accuracy of the system will be determined on some part of the historical log data. After that, this model will be installed in the healthcare environment to detect the suspicious user access in future. For the identification of the abnormal user accesses against the system, log data will be provided to the model on specific time bases such as after every 24 h or once in a week.

In this way, the implementation of the proposed anomaly detection model will help the healthcare service providers to secure sensitive healthcare data in a better way. Moreover, the model will also aid in providing early information about the suspicious accesses against the system. This will also save time because then the security experts will investigate only those log records that are identified as suspicious because the investigation of thousands of log records is time consuming, hectic, uneconomical, and ineffective. Fig. 2 presents the conceptual view of an EHR system integrated with a machine learning model to identify deviated user behaviors while accessing healthcare data. Implementation of our proposed theoretical ML-based model will be considered in our future work. The next sub-section of the current section provides an assessment of supervised and unsupervised ML approaches by using the fuzzy-based ANP approach; a well-known and efficient multi-criteria decision-making technique.

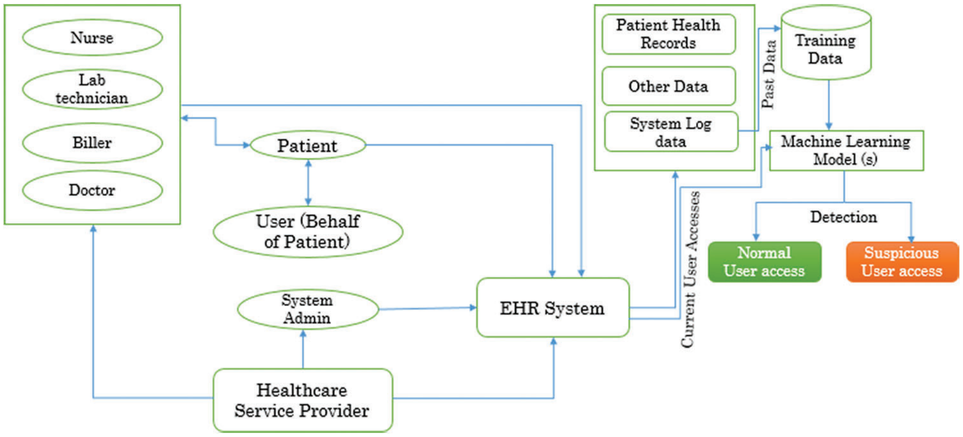

Figure 2: Conceptual EHR system with ML based anomaly detection model

4.1 Idealness Assessment of Supervised and Unsupervised Approaches

The Idealness assessment of two dominant ML approaches will help the researchers and healthcare service providers to select more ideal and suitable ML approach for healthcare data's privacy in a proactive fashion. The authors of the study assessed two dominant techniques of machine learning namely, the supervised and the unsupervised learning approaches through fuzzy-based Analytical Network Process (ANP). The analytical network process is an MCDM problem solving technique and is most suitable for addressing the problems that can produce multiple solutions. It can measure dependencies among criteria and also alternatives [26]. The numerical assessment of this work will provide a quantitative evaluation of two machine learning approaches and identified attributes. For that, a domain expert group is consulted to identify a criterion (attribute) set for this assessment. A set of five attributes has been selected to assess two different ML approaches against healthcare data security. These attributes are Nature of Data, Anomaly Detective, Misuse Decisive, Accuracy level, and Appropriateness. Fig. 3 given below presents the Network structure of these attributes with a pair of alternatives.

- *Nature of Data:* The nature of data defines the natural characteristic of the historical (past) data that is to be needed for the ML-based model. It can be either labeled or unlabeled data. The labeled data is very rare and needs more financial resources for its generation. Whereas, the unlabeled data is available in abundance and is utilized by unsupervised ML techniques only.
- *Anomaly Detection:* Anomaly detection defines an attribute of the ML-based approach to identify or detect unknown or newly generated attack types. The behavior of these attack types does not exist in

the supporting database of the model. An ML-based model analyzes the attack types and tries to predict its class based on its knowledge and experience.

- *Misuse Detective:* Misuse detection also ensures the characteristic of ML-based approaches to detect known attacks. The attack detection is based on signatures that are already known for the model. Approaches used for the misuse detection provide high accuracy but are ineffective for identifying unknown attacks.
- *Accuracy level:* Accuracy is one of the prominent characteristics of machine learning techniques. It is measure through various measuring scales such as precision, sensitivity, specificity, area under curve etc. It defines the performance accuracy of an ML-based model with respect to other models or techniques.
- *Appropriateness:* Appropriateness as a characteristic defines the suitability or fitness of a machine learning technique in a specified environment. It depicts how well an ML-based approach simulates the specified environment. Here, our specified environment is healthcare and its digital smart systems are used to store and process electronic health records.

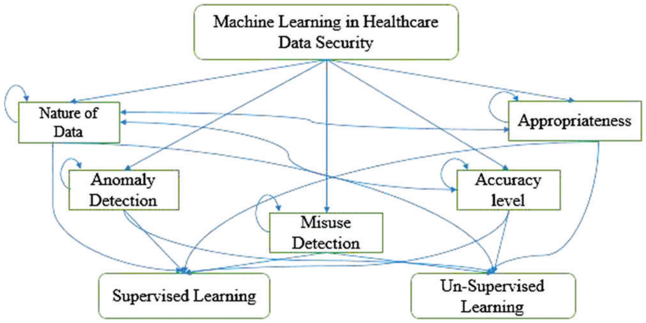

Figure 3: ANP based attributed and alternative structure

4.1.1 *Adopted Methodology*

The research methodology is based on a systematic, step-wise procedure to conduct the experiment of idealness assessment on the Supervised and the Unsupervised Machine Learning techniques. The proposed experiment will assess the overall idealness of both ML techniques with respect to the attribute set identified by various domain experts. The selected attribute set is considered from a healthcare cyber-security perspective. For that, the fuzzy Analytical Network Process (ANP) has been implemented to complete this work. ANP approach comes under the umbrella of the MCDM problem solving domain [27,28]. This research paper practically examines the ANP by using fuzzy logic so as to make it efficient and effective for deriving more accurate results. Fuzzy logic is considered as an advanced structure of classical logic and has acquired a major significance in those problems domains where a solution might vary between *absolute true* and *absolute false*. Such a solution might be *absolutely true, partially true, absolutely false, or partially false*. Such a varied range helps to categorise and address the uncertainty of the information [29]. Analytical network process is an MCDM problem solving technique and is the best technique for addressing the problems that can produce multiple solutions. It can measure dependencies among criteria and also the alternatives [28]. That makes it more efficient for depicting the real life problems and produce accurate results as compared to the analytical hierarchy process (AHP). Fuzzy-based ANP is applied, in this work for determining the weights of criteria (factors/attributes). Fig. 4 illustrates the step-wise working procedure of this work. Numerical formulas are discussed in the following subsections.

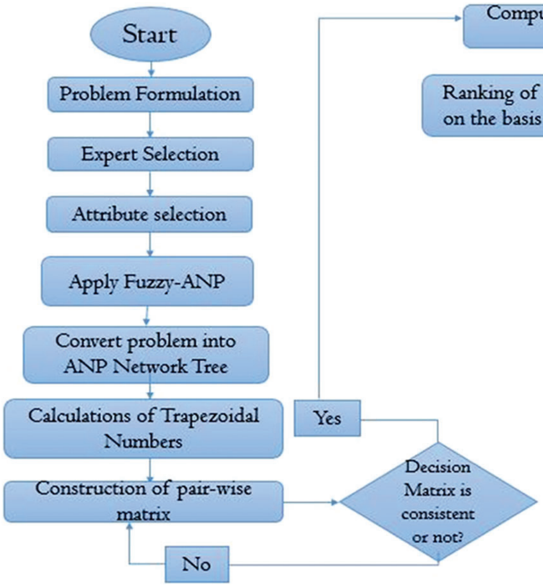
Start
Problem Formulation
Expert Selection
Attribute selection
Apply Fuzzy-ANP
Convert problem into ANP Network Tree
Calculations of Trapezoidal Numbers
Construction of pair-wise matrix
Decision Matrix is consistent or not?
Yes
No
Computing global weights of Attributes
Ranking of alternatives are determined on the basis of attribute global weights
End

Figure 4: Working diagram of fuzzy based ANP

Step_1: Triangular Fuzzy Number (TFN) is structurally as a triplet (f1, f2, f3) where f1 < f2 < f3 and f1 symbolize lower value, f2 middle one and < f3 symbolizes higher value. The membership function of the fuzzy number ~T is demonstrated with the help of Eqs. (3) and (4) and the number is known as TFN. Fig. 5 and Tab. 3 depict the structure of a TFN and scale, respectively.

$$\mu_T(\mathrm{x}) = \mathrm{F} \rightarrow [0, 1] \tag{3}$$

$$\mu_{\mathbf{T}}(\mathbf{x}) = \begin{cases} \dfrac{\mathbf{f1} - \mathbf{f2}}{\mathbf{f2} - \mathbf{f1}}, \mathbf{f}1 \leq \mathbf{x} \leq \mathbf{f}2 \\ \dfrac{\mathbf{f3} - \mathbf{x}}{\mathbf{f3} - \mathbf{f2}}, \mathbf{f}2 \leq \mathbf{x} \leq \mathbf{f}3 \\ 0, \mathbf{x} > \mathrm{f}3 \ \boldsymbol{Otherwise} \end{cases} \tag{4}$$

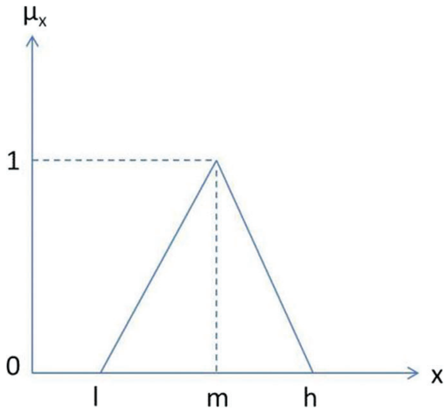

Figure 5: Structure of a TFN

Table 3: Linguistic-terms and respective TFNs

Saaty Scale Definition	Fuzzy Triangle Scale	
1	Equally important	(1, 1, 1)
3	Weakly important	(2, 3, 4)
5	Fairly important	(4, 5, 6)
7	Strongly important	(6, 7, 8)
9	Absolutely important	(9, 9, 9)
2	Intermittent values between two adjacent scales	(1, 2, 3)
4		(3, 4, 5)
6		(5, 6, 7)
8		(7, 8, 9)

After that fuzzy conversion is performed on these numeric values. To convert a numeric value into a TFN, Eqs. (5)–(8) are applied [27] and symbolized as (f1ij, f2ij, f3ij) where, f1ij presents low value, f2ij presents the middle one, and f3ij presents upper value. Further, TFN [ɳij] is defined as:

$$\eta_{ij} = \left(f1_{ij}, f2_{ij}, f3_{ij}\right) \tag{5}$$

$$\textit{where},\ f1_{ij} \le f2_{ij} \le f3_{ij}$$

$$f1_{ij} = \min\left(J_{ijd}\right) \tag{6}$$

$$f2_{ij} = \left(J_{ij1}, J_{ij2}, J_{ij3}\right)^{\frac{1}{x}} \tag{7}$$

$$\text{and } f3_{ij} = \max\left(J_{ijd}\right) \tag{8}$$

The relative importance of values among two attributes is denoted by Jijk with the help of expert opinions and above given equations, also attribute pairs are judged and denoted by i and j. Further, the operations on two TFNs are performed with the help of Eqs. (9)-(11). Suppose, T1 and T2 are two TFNs, T1= (f11, f21, f31) and T2= (f12, f22, f32). Then operational rules on them are as:

$$(\mathbf{f1_1}, \mathbf{f2_1}, \mathbf{f3_1}) + (\mathbf{f1_2}, \mathrm{f2_2}, \mathbf{f3_2}) = (\mathbf{f1_1} + \mathbf{f1_2}, \mathbf{f2_1} + \mathrm{f2_2}, \mathrm{f3_1} + \mathbf{f3_2}) \tag{9}$$

$$(\mathbf{f1_1}, \mathbf{f2_1}, \mathbf{f3_1}) \times (\mathbf{f1_2}, \mathbf{f2_2}, \mathbf{f3_2}) = (\mathbf{f1_1} * \mathbf{f1_2}, \mathbf{f2_1} * \mathbf{f2_2}, \mathbf{f3_1} * \mathbf{f3_2}) \tag{10}$$

$$(\mathbf{f1_1}, \mathbf{f2_1}, \mathbf{f3_1})^{-1} = \left(\frac{\mathbf{1}}{\mathbf{f3_1}}, \frac{\mathbf{1}}{\mathbf{f2_1}}, \frac{\mathbf{1}}{\mathbf{f1_1}}\right) \tag{11}$$

Step_2: Experts' responses are used to establish pair-wise comparison matrix and by applying Eq. (12), consistency Index (CI) is determined as follows:

$$CI = \frac{\gamma_{max} - q}{q - 1} \tag{12}$$

where, CI: Consistency Index and q: number of compared elements. The Consistency Ratio (CR) is calculated using a random index Eq. (13).

$$\mathbf{CR} = \mathbf{CI}/\mathbf{RI} \tag{13}$$

Generated matrix is reasonably called consistent if CR < 0.1. Here, the random index is specified by RI and is taken from Saaty [26].

Step_3: After the completion of step_2, the result is obtained in the form of a reasonably consistent matrix. Then by applying the defuzzification (alpha-cut) method taken from [28], TFN values are converted to quantifiable values. Defuzzification is determined through Eqs. (14)-(16).

$$\mu_{\alpha,\beta}(\eta_{\mathrm{ij}})=[\beta.\eta\alpha(\mathrm{f1_{ij}})+(1-\beta).\eta\alpha(\mathrm{f3_{ij}})] \tag{14}$$

Where, $0 \leq \alpha \leq 1$ and $0 \leq \beta \leq 1$

Such that,

$$\eta\alpha\left(f1_{ij}\right) = \left(f2_{ij} - f1_{ij}\right).\alpha + f1_{ij} \tag{15}$$

$$\eta\alpha\left(f3_{ij}\right) = f3_{ij} - \left(f3_{ij} - f2_{ij}\right).\alpha \tag{16}$$

The values of α and β lie between 0 and 1 and are used in the above equations.

Step_4: In this step, the process of paired comparisons is done in between groups including goal, attributes, sub-attributes, and alternatives in the form of priority vector that results in the formation of the super-matrix.

The systematic and step-wise methodology discussed above will be adopted in this work to carry out a case study on two dominant ML approaches for idealness assessment with respect to healthcare data security. In the next section of this work, we will provide numerical calculations with the results of this study.

4.1.2 Numerical Analysis and Results of Assessment

ANP under the fuzzy environment has been used in this work for greater accuracy and efficiency. To determine the overall idealness and performance nature of two different machine learning approaches, five above mentioned attributes have been considered for this experiment. These attributes are symbolized as *Nature of data (M1), Anomaly detective (M2), Misuse detective (M3), Accuracy level (M4), and Appropriateness (M5)* in the following tables. With the help of Eqs. (3)–(16), specified in the methodology section, assessment of the supervised and the unsupervised approaches under fuzzy-based ANP environment has been examined as follows:

Firstly, the linguistic-terms are converted into numeric values, and then these values are converted into aggregated TFNs by using the Saaty's scale, as shown in Tab. 3 and also by applying Eqs. (3)–(11). Conversion of crisp numbers into TFN values is carried out by using Eqs. (5)–(8). After that, for establishing a pair-wise comparison matrix for specified attributes, numerical calculations are carried out and the final results are depicted in Tab. 4. Then by applying Eqs. (12) and (13), CI and RI have been determined. For the consistency of the pair-wise comparison matrix, the consistency ratio (CR) should be < 0.1. Our generated calculations for CR also satisfy the criteria (CR = 0.07). Hence, our matrix is consistent. Further, by adopting Eqs. (9)–(11) addition, multiplication, and reciprocal operations on TFNs have been performed and those intermediate operation results become helpful in completing this study. However, their representation in this study is not necessary and will also increase the page limit of this study. By applying Eqs. (14)–(16) on pair-wise comparison matrix, the defuzzification process has been carried out by using the alpha-cut method. Thereafter, the normalized values and the defuzzified local weights of attributes are represented in Tab. 5. Taking help from the local attribute-weights, the attributes' weights and priorities have been determined. The results are represented in Tab. 6. And the graphical representation of the same is depicted in Fig. 6.

Table 4: Pair-wise comparison matrix

	M1	M2	M3	M4	M5
M1	1.00000, 1.00000, 1.00000	1.06210, 1.53110, 1.99110	0.51110, 0.62110, 0.86110	1.73110, 2.31110, 2.92110	1.69220, 2.41220, 3.15220
M2	0.51110, 0.65110, 0.94110	1.00000, 1.00000, 1.00000	1.18110, 1.47110, 1.87110	0.79110, 0.96111, 1.14111	1.46220, 1.86220, 2.22220
M3	1.16111, 1.67110, 1.96110	0.53110, 0.68111, 0.85110	1.00000, 1.00000, 1.00000	1.09211, 1.34110, 1.87110	1.61220, 2.34220, 3.15220
M4	0.34110, 0.43110, 0.58110	0.88110, 1.04110, 1.26110	0.53220, 0.74220, 0.53220	1.00000, 1.00000, 1.00000	1.50220, 1.93220, 2.35220
M5	0.32220, 0.41330, 0.59440	0.45220, 0.52220, 0.67777	0.32450, 0.43450, 0.63250	0.42750, 0.52750, 0.67750	1.00000, 1.00000, 1.00000

Table 5: Defuzzification by using alpha-cut method

	M1	M2	M3	M4	M5	Weightage
M1	1.000000	1.778150	0.892170	2.563180	2.667120	0.28811
M2	0.562140	1.000000	1.751180	1.212170	1.853180	0.18911
M3	1.121110	0.571710	1.000000	0.989170	2.606160	0.26511
M4	0.390210	0.825150	1.011140	1.000000	2.177140	0.24185
M5	0.375130	0.540710	0.384140	0.459140	1.000000	0.25732
CR = 0.07124420						

Table 6: Global weights of attributes

Attributes	Global Weights	Global Priorities
M1	0.1819500	5
M2	0.2119710	2
M3	0.1824960	4
M4	0.2427190	1
M5	0.1908640	3

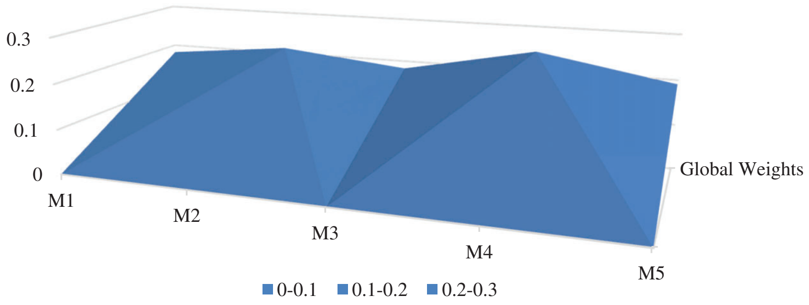

Figure 6: Graphic depiction of attribute weights

From the numerical analysis of the results, it was found that among the five identified attributes, the Accuracy level (M4) got the highest global weight (0.2427190) followed by the Anomaly detective (M2) with 0.2119710 global weight. The Misuse detective (M3) and Nature of Data (M1) got the lowest global weights. Thus, the prioritized order of these attributes, according to this assessment that is based on fuzzy-based ANP approach, is as: *Accuracy level (M4), Anomaly detective (M2), Appropriateness (M5), Misuse detective (M3), and Nature of Data (M1*). Therefore, the implications of this evaluation are that among the two specified techniques- supervised and unsupervised machine learning as alternatives- the unsupervised approach is more ideal for health data security as compared to the supervised approach. The results established that Accuracy, Anomaly detective, and appropriateness attributes have got the highest global weights. Hence, they are more ideal for an unsupervised approach because of the following reasons:

- Available healthcare log data is unlabeled; this feature better suits the unsupervised machine learning approach. This depicts the appropriateness (M5) attribute of the unsupervised learning approach.
- The anomaly detective (M2) attribute is also best depicted by the unsupervised approach as compared to the supervised approach because of independence on labeled data.
- The Accuracy level (M1) is better in the supervised approach but the unsupervised also provides good accuracy that is acceptable in dynamic environments.

5 Conclusion

The healthcare sector is one of the top data industries of the world that holds and processes sensitive and valuable data. Healthcare sector has become the most vulnerable target of intruders and the number of attacks against healthcare data is increasing rapidly. Healthcare data is being breached and exposed through Hacking (ransomware, malware, and fishing), and internal unauthorized access. The soaring cases of data theft call for more effective security mechanisms. The present research endeavor's theoretical framework for ensuring healthcare data confidentiality based on supervised and unsupervised machine learning is an attempt in this direction. Implementation of these models will help the healthcare organisations to identify suspicious user accesses against the protected healthcare data in a more robust manner. Moreover, the effective implementation of the model will also reduce the time spent in investigation and the cost incurred in the process. This work also depicts that the unsupervised machine learning approach is an ideal option for maintaining healthcare data security as compared to the supervised approach. Research is a dynamic process, thus we cannot claim that our identified attribute set is optimal but it is also an ideal choice. Moreover, the proposed assessment approach- fuzzy-based ANP is an effective MCDM approach but not optimal. So, researchers can practice other techniques for better results if possible. In our future work, we will focus on the implementation of the proposed theoretical framework.

Acknowledgement: This research was supported by Taif University Researchers Supporting Project number (TURSP-2020/211), Taif University, Taif, Saudi Arabia.

Funding Statement: This Project was funded by the Taif University Researchers Supporting Projects at Taif University, Kingdom of Saudi Arabia, under grant number: TURSP-2020/211.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] T. Sahama, L. Simpson and B. Lane, "Security and privacy in ehealth: Is it possible?," in *Proc. 2013 IEEE 15th Int. Conf. on e-Health Networking, Applications and Services*, Lisbon, Portugal, pp. 249–253, 2013.

[2] A. F. Subahi, “Edge-based IoT medical record system: Requirements, recommendations and conceptual design,” *IEEE Access*, vol. 7, no. 5, pp. 94150–94159, 2019.

[3] W. Hurst, A. Boddy, M. Merabti and N. Shone, “Patient privacy violation detection in healthcare critical infrastructures: An investigation using density-based benchmarking,” *Future Internet*, vol. 12, no. 6, pp. 100–105, 2020.

[4] June 2020 Healthcare Data Breach Report, *HIPAA Journal,* Jul. 24, 2020. 2021. [Online]. Available: https://www.hipaajournal.com/june-2020-healthcare-data-breach-report/.

[5] A. H. Seh, M. Zarour, M. Alenezi, A. K. Sarkar, A. Agrawal *et al.,* “Healthcare data breaches: Insights and implications,” *Healthcare*, vol. 8, no. 2, pp. 133–148, 2020.

[6] A. A. Boxwala, J. Kim, J. M. Grillo and L. Ohno-Machado, “Using statistical and machine learning to help institutions detect suspicious access to electronic health records,” *Journal of the American Medical Informatics Association*, vol. 18, no. 4, pp. 498–505, 2011.

[7] D. McGlade and S. S. Hayward, “ML-based cyber incident detection for Electronic Medical Record (EMR) systems,” *Smart Health*, vol. 12, no. 2, pp. 3–23, 2019.

[8] A. H. Seh and P. K. Chaurasia, “A review on heart disease prediction using machine learning techniques,” *International Journal of Management, IT and Engineering*, vol. 9, no. 4, pp. 208–224, 2019.

[9] E. Alpaydin, “Introduction to machine learning,” *MIT press*, vol. 9, no. 2, pp. 1–42, 2020.

[10] R. D. Stachel and M. DeLaHaye, “Security breaches in healthcare data: An application of the actor-network theory,” *Issues in Information Systems*, vol. 16, no. 2, pp. 1–14, 2015.

[11] J. Kwon and M. E. Johnson, “The market effect of healthcare security: Do patients care about data breaches?,” Vol. 16, no. 2, pp. 1–14, 2015.

[12] M. Meisner, “Financial consequences of cyber attacks leading to data breaches in healthcare sector,” *Copernican Journal of Finance & Accounting*, vol. 6, no. 3, pp. 63–73, 2018.

[13] M. Chernyshev, S. Zeadally and Z. Baig, “Healthcare data breaches: Implications for digital forensic readiness,” *Journal of Medical Systems*, vol. 43, no. 1, pp. 50, 2019.

[14] A. H. Seh and P. K. Chaurasia, “Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time,” *Procedia Computer Science*, vol. 151, pp. 1004–1009, 2019.

[15] S. B. Wikina, “What caused the breach? An examination of use of information technology and health data breaches,” *Perspectives in health Information Management*, vol. 11, no. 6, pp. 1–15, 2014.

[16] A. F. Subahi, “A model transformation approach for detecting distancing violations in weighted graphs,” *Computer Systems Science and Engineering*, vol. 36, no. 1, pp. 13–39, 2021.

[17] How Much Data Is Created Every Day? [27 Powerful Stats], Seed Scientific, Jan. 30, 2020. 2021. [Online]. Available: https://seedscientific.com/how-much-data-is-created-every-day/.

[18] How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read, 2021. [Online]. Available at: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#318c2c6d60ba.

[19] S. Bajrić, “Data security and privacy issues in healthcare,” *Applied Medical Informatics*, vol. 42, no. 1, pp. 19–27, 2020.

[20] Security and Privacy in the Medical Internet of Things: A Review. 2021. [Online]. Available at: https://www.hindawi.com/journals/scn/2018/5978636/.

[21] September 2020 Healthcare Data Breach Report: 9.7 Million Records Compromised, *HIPAA Journal,* Oct. 22, 2020. 2021. [Online]. Available at: https://www.hipaajournal.com/september-2020-healthcare-data-breach-report-9-7-million-records-compromised/.

[22] December 2019 Healthcare Data Breach Report. 2021. [Online]. Available at: https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.

[23] Largest Healthcare Data Breaches of 2016, *HIPAA Journal,* Jan. 04, 2017. 2021. [Online]. Available at: https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631/.

[24] January 2019 Healthcare Data Breach Report, *HIPAA Journal,* Feb. 25, 2019. 2021. [Online]. Available at: https://www.hipaajournal.com/january-2019-healthcare-data-breach-report/.

[25] January 2020 Healthcare Data Breach Report, *HIPAA Journal,* Feb. 21, 2020. 2021. [Online]. Available at: https://www.hipaajournal.com/january-2020-healthcare-data-breach-report/.

[26] U. Lechtenberg, "Research guides: Organizing academic research papers, theoretical framework," 2020. [Online]. Available at: https://library.sacredheart.edu/c.php?g=29803&p=185919.

[27] A. Agrawal, A. H. Seh, A. Baz, H. Alhakami, W. Alhakami *et al.,* "Software security estimation using the hybrid fuzzy ANP-TOPSIS approach: Design tactics perspective," *Symmetry*, vol. 12, no. 4, pp. 598–613, 2020.

[28] J. W. Lee and S. H. Kim, "Using analytic network process and goal programming for interdependent information system project selection," *Computers and Operations Research*, vol. 27, no. 6, pp. 367–382, 2000.

[29] A. Solangi, "An integrated Delphi-AHP and fuzzy TOPSIS approach toward ranking and selection of renewable energy resources in Pakistan," *Processes*, vol. 7, no. 118, pp. 1–18, 2019.