Data-Driven and Artificial Intelligence (AI) Approach for Modelling and Analyzing Healthcare Security Practice: A Systematic Review

Prosper Kandabongee Yeng[1], Livinus Obiora Nweke[1], Ashenafi Zebene Woldaregay[2], Bian Yang[1] and Einar Arthur Snekkenes[1]

[1]Norwegian University of Science and Technology, Technolgien 22, 2815 Gjøvik, Norway
[2]University of Tromsø, The Arctic University of Norway, Hansine Hansens veg 18, 9019 Tromsø, Norway
Prosper.yeng@ntnu.no

Abstract. Data breaches in healthcare continue to grow exponentially, calling for a rethinking into better approaches of security measures towards mitigating the menace. Traditional approaches including technological measures, have significantly contributed to mitigating data breaches but what is still lacking is the development of the "human firewall," which is the conscious care security practices of the insiders. As a result, the healthcare security practice analysis, modeling and incentivization project (HSPAMI) is geared towards analyzing healthcare staffs' security practices in various scenarios including big data. The intention is to determine the gap between staffs' security practices and required security practices for incentivization measures. To address the state-of-the art, a systematic review was conducted to pinpoint appropriate AI methods and data sources that can be used for effective studies. Out of about 130 articles, which were initially identified in the context of human-generated healthcare data for security measures in healthcare, 15 articles were found to meet the inclusion and exclusion criteria. A thorough assessment and analysis of the included article reveals that, KNN, Bayesian Network and Decision Trees (C4.5) algorithms were mostly applied on Electronic Health Records (EHR) Logs and Network logs with varying input features of healthcare staffs' security practices. What was found challenging is the performance scores of these algorithms which were not sufficiently outlined in the existing studies.

Keywords: Artificial Intelligence, Machine Learning, Healthcare, Security Practice

1 Introduction

The enormous increase in data breaches within healthcare is frightening and has become a source of worry for many stakeholders such as healthcare providers, patients, national and international bodies. In 2018, the healthcare sector recorded about 15 million records which were compromised in about 503 data breaches [1, 2]. This was a triple of 2017 data breaches in healthcare [1, 2]. In the middle of 2019, the number of compromised records in healthcare were more than 25 million, implying that by the end of 2019, the number of compromised records might have sky rocketed [2]. Greater

proportion of the breaches (59%) were perpetrated by insiders [1] who are authenticated users of the systems [3]. Most of the adversaries were motivated by financial gains (83%) and other motives such as convenience (3%), grudges (3%), industrial espionage (2%) [1]. The number of data breaches in healthcare has substantially exceeded that of the financial sector and almost caught up with other public sector entities [1].

The tremendous increase in data breaches in recent time within healthcare, have therefore left many to ponder about the possible causes. The healthcare data is comparatively richer and has become "honey-port", thereby attracting malicious actors [4, 5]. Health data has vast scientific, societal, and commercial values, which cause cyberattacks and black market targeting of this data. Healthcare data can be used to commit multiple dark activities in the dark web as detection of breaches, related updates and correction of the compromised data takes a longer time. Another angle of thought is that, the healthcare personnel are busy with their core healthcare duties and are less experienced in information security conscious care behavior. This leaves room for adversarial attacks. The technological measures (such as firewall, intrusion detection or prevention systems, antiviruses and security governance configurations) have been strengthen [6] and making it difficult for external cyber criminals to inappropriately access data [7, 8]. But there is no related development of "the human firewall" [9]. The human firewall is the information security conscious care behavior of the insiders [9, 10]. The human firewall has not gained equal attention, and this is the vulnerability which cyber criminals tend to exploit for easy entry [11]. By virtue of their access privileges, healthcare insiders are "double-edged sword". While their privileges enable them to provide therapeutic care to patients, healthcare staffs' errors and deliberate actions can compromise the confidentiality, integrity and availability (CIA) of healthcare data. Additionally, an attacker can masquerade as insiders to compromise healthcare data through various ways, including social engineering methods [3].

Furthermore, the healthcare environment is relatively complex and delicate, making it hard for healthcare information security professionals to design stricter access control policies. So, access control mechanisms in healthcare are mostly designed with a degree of flexibility to enable efficient patient management. While such design considerations are very important and meets the availability attribute of the CIA, the healthcare systems remain vulnerable. The broad range of access flexibility can be abused by the insiders. This can also be a dream for cyber criminals to adopt various diabolic means of gaining insiders credentials to enable them to equally have larger access. The incidence of data breaches could bring various consequences including denial of service for timely medical services, negative impact on mutual thrust between patient and healthcare providers, breaches to individual's privacy and huge finds to healthcare providers by national and international regulatory bodies.

The general objective of this study was to therefore to identify, assess, and analyze the state-of-the-art in artificial intelligence strategies and their hybrid aspects which can be used to efficiently detect anomaly and malicious events in healthcare staff's security practices in their access related data towards improving counter-measures for healthcare staffs related security breaches.

Specific objectives include;

- Identifying AI learning algorithms which can be used to efficiently profile healthcare staff security practices, for anomalies detection.

- Assess and analyzed the design considerations of the methods (such as the tolerance ranges or thresholding mechanisms provided to accommodate non-treacherous user behaviors i.e., new users, mistakes and during emergencies) towards mitigating false positives.
- Assess and analyze their performance metrics and other suitable evaluation methods
- Determine associated challenges in the usage of the algorithms and how these challenges can possibly be overcome.

1.1 Motivation, Scope and Problem Specification

Healthcare Security Practice Analysis, Modelling and Incentivization (HSPAMI), is an ongoing research project in which an aspect involves modelling and analyzing data with AI methods to determine the security practices of healthcare staffs, towards improving their security conscious care behavior. In analyzing healthcare related data, there is the need to consider details of the methods and data sources in view of the unique and critical nature of the sector. In a related study, Walker-Roberts et al., conducted a systematic review of "the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure" [12]. Among various teams few machine learning methods were identified to be used for intrusion detections and preventions. The methods that were identified are Petri net, Fuzzy logic, K-NN, K-Decision tree(RADISH system) [12-14] and inductive machine learning methods[12, 13, 15]. In a similar way, Islam et al conducted a systematic review on data mining for healthcare analytics [16]. Categories such as healthcare sub-areas, data mining techniques, type of analytics, data and data sources were considered in the study. Most of the data analysis were for clinical and administrative decision making. The data sources were mostly human generated from electronic health records. Other studies which explored for related methods includes [17] and [18].

Even though, the studies [12, 16] were in healthcare context, details of the algorithms and data sources were not considered. For instance, the features of the data sources and algorithm performance methods, were not deeply assessed in their studies. Additionally, the studies of [17] and [18] were general and not healthcare specific. So unique challenges within healthcare environment were not considered in their study. To this end, the study aimed to explore in detail, AI methods and data sources in healthcare that can be efficiently used for modeling and analyzing healthcare professionals' behavior. Healthcare professionals and healthcare staffs were used interchangeably in this study to include but not limited to nurses, physicians, laboratory staff and pharmacies who access patients records for therapeutic reasons.

2 Background

Security practice of healthcare staffs includes how healthcare professionals respond to the security controls and measures towards achieving the CIA goals of the healthcare organizations. Healthcare professionals are required to conduct their work activities in a security conscious manner to maintain the CIA of healthcare environment. For

instance, borrowing of access credentials could jeopardize the purpose of access control for authorized users and legitimate accesses. Additionally, the inability to understand social engineering scammers' behavior can lead to healthcare data breaches.

Various ways can be adopted to observe, model and analyze healthcare professionals' security practices. Perception and socio-cultural context can be adopted by analyzing the healthcare staffs' security perception, social, cultural and socio-demographic characteristics with their required security practices. Also, Attack-Defense simulation can be used to measure how healthcare staffs understand social engineering related tricks. Furthermore, data-driven approach with artificial intelligence (AI) methods could be adopted to understand the security risk of each healthcare professions. The findings can then help decision makers to introduce appropriate incentive methods and solve issues which are hindering sound information security practice towards enhancing conscious care behavior. But this study is focused on exploring for appropriate AI methods and data sources that can be used to modeled and analyzed healthcare security practices. Therefore, psycho-socio-cultural context and attack-defense simulations are beyond the scope of this paper.

2.1 Data-Driven and Artificial Intelligence in healthcare security practice analysis

Advances in computational and data sciences along with engineering innovations in medical devices have prompted the need for the application of AI in the healthcare sector [19]. This has the potential of improving care delivery and revolutionizing the healthcare industry. AI can be referred to as the use of complex algorithms and software to imitate human cognitive functions [20]. It involves the application of computer algorithms in the process of extracting meaning from complicated data and to make intelligent decisions without direct human input. AI is increasingly impacting every aspects of our lives and the healthcare sector is not an exception. In recent years, the healthcare sector is experiencing massive deployments of AI in the bid to improve the overall healthcare delivery. There is currently no consensus on the classification of the applications of AI in healthcare. However, we rely on the classification of the application of AI in healthcare described in [21] to briefly discuss deployment of AI in healthcare.

The deployment of AI in healthcare sector has been classified in [21] to include; expert systems, machine learning, natural language processing, automated planning and scheduling, and image and signal processing. Expert systems are AI programs that have been trained with real cases to execute complicated tasks [22]. Machine learning employs algorithms to identify patterns in data and learn from them and its applications can be grouped into three, namely; supervised learning, unsupervised learning, and reinforcement learning [21]. Natural language processing facilitates the use of AI to determine the meaning of a text by using algorithm to identify key words and phrases in natural language [21]. For automated planning and scheduling, it is an emerging field in the use of AI in healthcare that is concerned with the organization and prioritization of the necessary activities in order to obtain desired aim [21]. And image and signal processing involve the use of AI to train information extracted from a physical occurrence (images and signals) [21].

The common characteristics of all these applications is the utilization of massive data that is being generated in the healthcare sector to make better informed decisions. For instance, the collection of healthcare staffs' generated data, has been used for disease surveillance, decision support systems, detecting fraud and enhancing privacy and security [23]. In fact, the code of conduct for healthcare sector of Norway require the appropriate storage and protection of access logs of healthcare information systems for security reasons [24]. The healthcare staffs' accesses within the network or electronic health records (EHR), leaves traces of their activities which can be logged and reconstructed to form their unique profiles [24]. The healthcare staffs' accesses within the network or electronic health records (EHR), leaves traces of their activities which can be logged and reconstructed to form their unique profiles [25]. So, the appropriate AI methods can then be used to mine in such logs to determine the unique security practices of the healthcare staffs. Such findings can support management to adopt to the suitable incentivization methods towards improving on the security conscious care behavior in healthcare. Therefore, this study aims to explore for the appropriate AI methods and data sources that can be used to observe, model and analyzed the security practices of healthcare staffs.

3 Method

The objective of this study was to identify, assess and analyze the state-of-the-art data-driven and artificial intelligence (AI) algorithms along with their design strategies, and challenges. The study is towards analyzing healthcare professionals' security practices in the context of big data or human generated data in Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI) project.

A literature search was conducted between June 2019 and December 2019 through Google Scholar Science Direct and Elsevier, IEEE Explore, ACM Digital. Different key words such as "Healthcare", "staff", "employee", "Information security", "behavior", "Practice", "Threat", "Anomaly detection", "Intrusion detection", "Artificial Intelligence" and "Machine Learning ", were used. For a good quality searching approach, the key words were combined using Boolean functions of 'AND', 'OR' and 'NOT'. Peer reviewed journals and articles were considered. The inclusions and exclusions criteria were developed based on the objective of the study and through rigorous discussions among the authors. Basic selection was done by initially skimming through the titles, abstracts and keywords to retrieve records which were in line with the inclusion and exclusion criteria. Duplicates were filtered out and articles, which seems relevant, based on the inclusion and exclusion criteria, were fully read and evaluated. Other appropriate articles were also retrieved using the reference list of accepted literatures. Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) flow diagram was used to report the article selection and screening [26].

3.1 Inclusion and Exclusion Criteria

For an article to be included in the review, the study has to be an anomaly detection or intrusion detection in healthcare using artificial intelligence methods in healthcare

professionals' generated access logs data or patterns. Any other article outside the above stated scope (such as articles in medical cyber-physical devices, body area networks etc.) including literatures in other languages, except English, were excluded.

3.2 Data Collection and Categorization

The data collection and categorization were developed based on the objective and through literature reviews and authors discussions. The categories have been defined exclusively to assess, analyzed and evaluate the study as follows:

Type of AI method: This category includes explicit machine learning methods such as, Support Vector Machine (SVM), Bayesian network, etc.

Type of Input: This category includes the features which were used by the algorithm. This could include access location, time, log in failed attempts etc.

Input Sources: This attribute refers to the kind of access logs data, which was used in the study. Such sources include browser history, network logs, host-based activity logs and electronic health records logs

Data Format, Type, Size, and Data Source: This category could include file format such as XML, CSV

Input Preprocessing: Defines how the data was preprocessed from unstructured to structured, and how missing and corrupted input data were handled.

Application Scenario: This category defines the context of which the algorithm was implemented such as intrusion or anomaly detection.

Ground Truth: Refers to the kind of training set used in training the model.

Privacy approach: This defines the privacy method used to safeguard the privacy right of individuals who contributed to the data source.

Performance Metrics or Evaluation Criteria: This includes the measures used to assess the accuracy of the study. It includes metrics such as specificity, sensitivity, receiver operating characteristic (ROC) curves, and others

Nature of Data Sources: This category specifies if the data used was synthetic or real data.

3.3 Literature Evaluation and Analysis

The selected articles were assessed, analyzed and evaluated, based on the above defined categories. The analysis was performed on each of the categories (Type of AI method, type of input, input source, preprocessing, learning techniques, performance methods etc.) to evaluate the state-of-the-art approaches. Percentages of the attributes of the

categories were calculated based on the total number of counts (n) of each type of the attribute. Some studies used multiple categories, therefore, the number of counts of these categories exceeded the total number of articles of these systems presented in the study.

4 Results

After searching in the various online databases, a total of 130 records were initially identified by following the guidelines of the inclusion and exclusion criteria in the reading of titles, abstracts, and keywords. A further assessment of these articles through skimming of the objective, method and conclusion sections led to a further exclusion of 77 articles which did not meet the defined inclusion criteria. After removing duplicates, 42 articles were fully read and judged. After the full text reading, a total of 15 articles were included in the study and analysis as shown in the Fig. 1. As shown in the Figure 2 & 3, the topic of data-driven and AI for analyzing healthcare security practice has seen consistent interest.

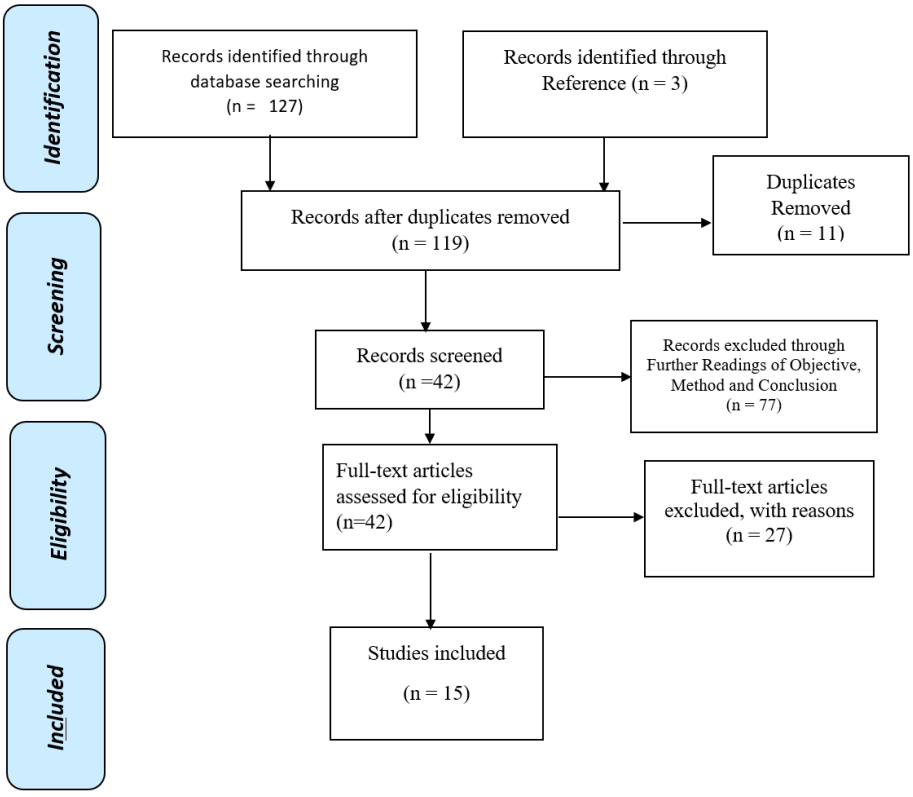

Fig.1. Flowchart of the systematic review process

As shown in Fig. 2, most of the literatures were identified in google scholar and followed by IEEE Explore and ACM Digital Library.

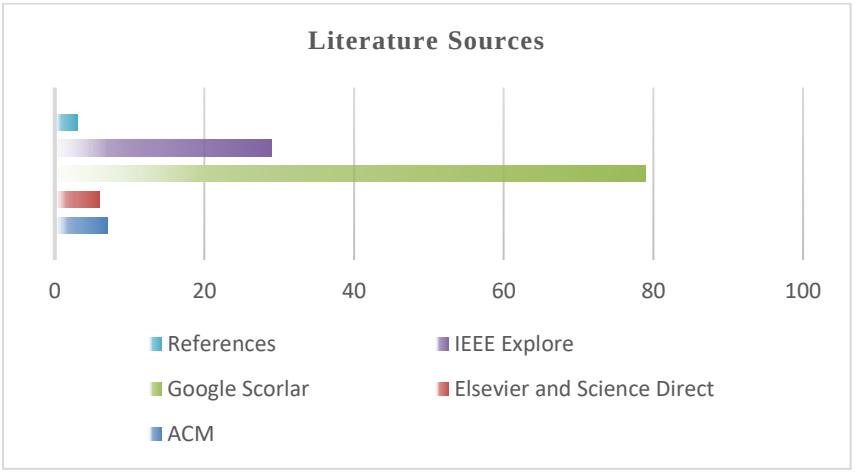

Fig. 2. Literature Sources

The articles were published between 2010 and 2019 as shown in Fig. 3

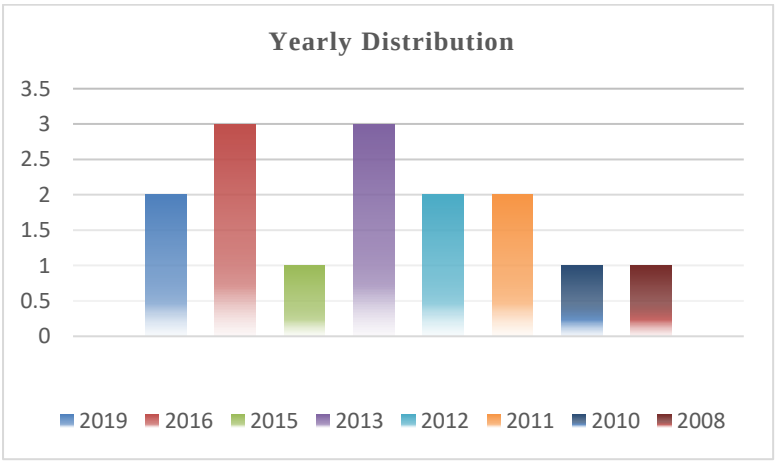

Fig. 3. Yearly Distribution

4.1 Evaluation and Analysis

Evaluation and analysis of the articles were carried out as described above, and the main finds are presented below**.**

Articles in the Study

The articles and their related categorizations, such as algorithms, features and data sources are shown in Table 1.

Table 1. Algorithms, Features, their related Data Sources and application domain

Study	Algorithms						Features							Data Sources				Application Domain	
	K-NN	Bayesian Network	Random Forest	J48	SVM	C4.5	User ID	Patient ID	Device ID	User Actions	Date and Time	Route	Location	EHR Logs	Host System Log	Network Logs	Key Stroke D.	Anomaly	Intrusion
[27]							■	■	■		■	■		■				■	
[28]							■			■					■				■
[29]							■	■			■			■					■
[30]							■			■									■
[31]							■	■	■		■	■	■	■				■	
[32]							■	■	■		■		■	■				■	
[33]							■	■	■		■					■			■
[34]							■	■	■	■	■					■			■
[35]							■		■							■		■	
[36]								■			■		■	■					■
[37]										■	■	■		■				■	
[38]							■	■	■	■	■			■				■	
[3]							■	■	■		■	■	■	■				■	
[39]																	■	■	
[40]							■	■	■		■			■				■	

I. Algorithms

The algorithms which were found in the review are as shown in Table 2. KNN method was mostly used (17%), followed by Bayesian Network (14%) and C4.5 decision tree (10%).

Table 2: Algorithms and their respective proportions

Algorithm	Count	%
K-Nearest Neighbors (KNN)[27, 30, 31, 38, 40]	5	17
Bayesian Network (BN)[27, 30, 33, 39]	4	14
C4.5[34, 37, 39]	3	10
Random Forest[34, 39]	2	7
J48[37, 39]	2	7
Principal Component Analysis(PCA) [40]	2	7
Spectral Project Model[40]	1	3
SVM[39]	1	3
k-Means[28]	1	3
Spectral Project Method	1	3
Ensemble averaging and a human-in-the-loop model [35]	1	3
Partitioning Around Medoids with k estimation (PAMK) [34]	1	3
Distance Based Model [32]	1	3
White-box anomaly detection system[29]	1	3
C5.0	1	3
Hidden Markov Model (HMM) [32]	1	3
Graph-Based[3]	1	3

II. Features

With reference to Table 3, the features which were mostly used include Users ID (19%), Date and Time attribute (17%), Patient ID (16%) and Device Identification (DID)(14%).

Table 3. Features used

Feature	Count	%
User Identification (UID)	12	19
Patient Identification (PID)	10	16
Device ID(DID)	9	14
Access Control (AC)	5	8
Date and Time	11	17
Location	4	6
Service/Route	5	8
Actions (Delete, Update, Insert, Copy, View)	3	5
Roles	3	5
Reasons	1	2

III. Data Sources

Most of the data sources were EHR logs (60%) and Network logs (20%) as shown in Table 4.

Table 4. Data Sources Used

Data Source	**Count**	**%**
Electronic Health Records logs (EMR) Logs	9	60
Host-Based Logs	1	7
Network Logs	3	20
Key-Stroke Activities	1	7

IV. Performance Methods

Regarding performance methods as shown in Table 5, FP (23%), TP (20) % and Recall (13%) were mostly used to assess the studies.

Table 5. Performance Methods

Performance Methods	**Count**	**%**
True Positive (TP)	8	20
False Positive (FP)	9	23
False Negative (FN)	5	13
Receiver Operating Characteristic ROC Curve	5	13
Area Under ROC (AUC) curve	3	8
Recall (Sensitivity)	5	13
Precision	3	8
Accuracy	2	5

V. Application Scenario

The studies in the review were mostly applied for anomaly detection (60%) and Intrusion detection (40%) as shown in Fig. 4.

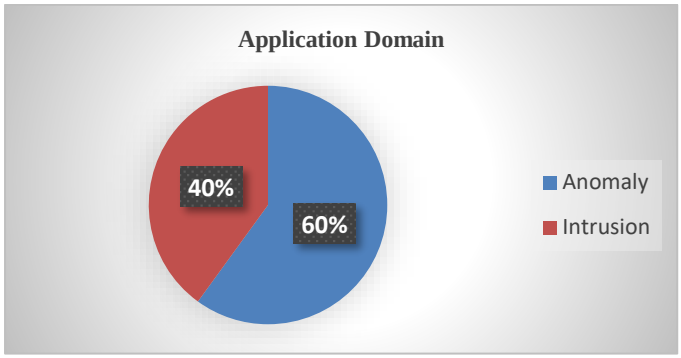

Fig. 4. Application domain

VI. Data Format

Regarding file format, Comma separated values (CSV) was commonly used as the file format [27, 28]. Some studies also used SQL file format[29, 41].

VII.Ground Truth

In the review, the ground truth was being established with similarity measures, observed and controlled practices and historical data of staffs' practices as shown in Table 6.

Table 6. Ground Truth

Ground Truth	Count	%
Similarity Measures	3	38
Observed practices	3	38
Historical data	2	25

VIII. Privacy preserving data mining approach

Privacy preserving methods which were adopted in study are tokenization [27], deidentification[31] and removal of medical information[37].

IX. Nature of Data Source

With reference to Fig. 5, the nature of the data sources which were used in the studies were mostly Real data (80%) and synthetic data (20%).

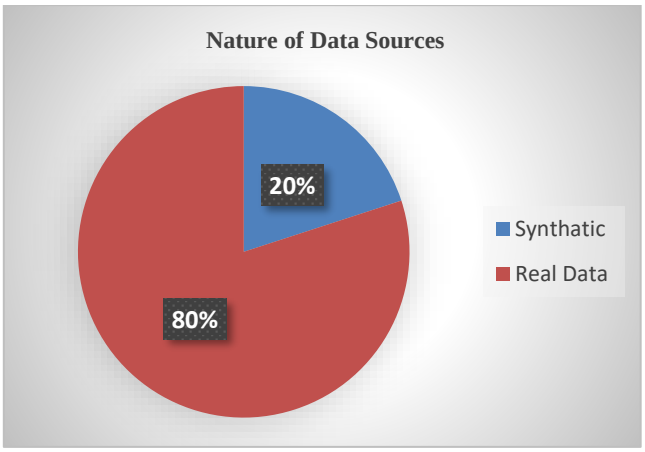

Fig. 5. Nature of Data Sources

5 Discussion

The main purpose of this systematic review was to find details of Artificial Intelligence (AI) methods and suitable healthcare staffs' generated security practice data, that can be efficiently mined to determine the status of healthcare security practices with respect to required security practices. The main findings in the study are as shown in Table 7.

With reference to Figure 1, 2 and 3 and Table 1, there were 15 studies which met the inclusion and exclusion criteria. Recently, a related systematic review for countermeasures against internal threats in healthcare also found about 5 machine learning methods, [12] which were fit for such measures. This suggests that the adoption of AI methods for modeling and analyzing healthcare professionals' generated security practice data, is still an emerging topic of academic interest.

Table 7. Principal findings

Category	**Most Used**
Algorithms	KNN and Bayesian Networks
Features	User IDS, Patient IDs, Device ID, Date and Time, Location, Route and Actions
Data sources	Electronic health Records (EHR) logs and Network logs
Application Domain	Anomaly Detection
Performance Methods	True Positive, False Positive, False Negative, ROC curve, AUC
Data Format	CSV
Nature of Data Sources	Real Data logs

Ground Truth	Similarity measures and observed data
Privacy preserving approaches	Tokenization and deidentification

5.1 AI methods

As shown in Table 2 and Table 7, various algorithms were identified in the study, but the most used methods were KNN and BN algorithms. K-Nearest Neighbors (kNN) is a supervised learning -based classification algorithm [30] which gets its intelligence from labeled data. The KNN then tries to classify unlabeled data item based on the category of the majority of most similar training data items known as K. The similarity between two data items in KNN, can be determined with the Euclidean distance of the various respective feature vectors of the data item. Another method which was mostly used is Bayesian Network (BN). BN is a probabilistic classifier algorithm, based on the assumption that, related pair of features used for determining an outcome are independent of each other and equal[30]. There are two commonly used methods of BN for classifying text, thus the multi-variant Bernoulli and multinomial models. KNN and BN algorithms were mostly used based on their comparatively higher detection accuracy. For instance, in an experimental assessment of KNN and BNN for security countermeasures of internal threats in healthcare, both KNN and BN had over 90% accuracy. BN performed better (94%) than the KNN (93%). In a related study[12], the KNN method was found to have higher detection rate with high true positive rates and low false positive rate.

The major issue with KNN in the context of healthcare staff security generated data is the lack of appropriate labeled data [42][23][35]. Within the healthcare setting, emergencies often dictate needs. In such situations, broader accesses for resources are normally allowed, making it challenging for reliable labeled data [42][23][35]. Therefore, in adopting KNN for empirical studies, the availability of appropriate labeled data should be considered but, in the absence of labeled data, unsupervised clustering methods such as K means clustering could also be considered [26].

5.2 Input data, features, sources, Ground Truth, data format and nature of data

The input data which was mostly used include EHR logs and Network data. A study which was conducted by Yeng et al., for observational measures towards profiling healthcare staffs' security practices, identified various sources including EHR logs, browser history, network logs, and patterns of keystroke dynamics [25]. Most EHR systems uses an emergency access control mechanism, known as "break the glass "or self-authorization" [43]. This enables healthcare staffs, to access patients' medical records during emergency situations without passing through conventional procedures for access authorization. A study into access control methods in Norway [43] revealed that about 50% of 100,000 patients records were accessed by 12,0000 healthcare staffs (representing about 45% of the users) through self-authorization. In such a scenario, EHR remains a vital source for analyzing for deviations of required healthcare security practices.

Regarding Ground Truth, it refers to the base-line, often used for training algorithms [44]. The detection efficiency of the algorithms can be negatively impacted if the accuracy of the ground-truth is low. As shown in Table 6, various methods such as similarity measures, observed data and historical methods were used. Similarity measure compares security practices with other healthcare professionals who have similar security practices. Observed measure is a control approach of obtaining the ground truth whereby some users were observed to conduct their security practices under a supervised, required security practices [39]. But the historical data basically relied on past records with a trust that, the data is reliable enough for training set. These methods can be assessed for adoption in related studies.

EHR contains most of the features which were identified in this review as shown in Table 7. Features such as patients ID, Actions, and User ID are primary features in EHR logs. The actions of the users such as deletion, inserting, updating and various routes such as diagnosis, prescriptions, and drugs dispensing can be tracked in EHR logs [43].

5.3 Application Scenario and Privacy preserving log analysis

The application of AI methods to analyze big data, generated by healthcare professional security practice, is a reactive approach. With such approaches, the primary aim is to determine deviations or outliers in healthcare security practices and further process these anomalies for possible malicious activities. As most of the algorithms were applied for anomaly detection (60%), such methods can be used to initially detect outliers. Deep leaning methods such as BN can then be used to further analyze the outliers for possible intrusions. This would help in privacy preserving at the same time while saving resources. Privacy preserving in data mining provides method to efficiently analyze data while shielding the identifications of the data subjects in a way to respect their right to privacy. For instance, limited number of less sensitive features can be used with KNN-based algorithms and if there exist outliers, BN methods can then be applied on only large number of the outliers to further assess these anomalies. In the review, deidentification, tokenization and sensitive data removals were some of the methods adopted to preserve privacy.

5.4 Conclusion

Based on the galloping rate of data breaches in healthcare, Healthcare Security Practice Analysis, Modeling and Incentivization (HSPAMI) project was initiated to observe, model and analyze healthcare staffs' security practices. One of the approaches in the project is the adoption of AI methods for modeling and analyzing healthcare staffs' generated security practice data. This systematic review was then conducted to identify, asses and analyze the appropriate AI methods and data sources. Out of about 130 articles which were initially identified in the context of human-generated healthcare data for security measures in healthcare, 15 articles were found to meet this inclusion and exclusion criteria. After the assessment and analysis, various methods such as KNN, Bayesian Network and Decision Trees (C4.5) algorithms were mostly applied on Electronic Health Records (EHR) Logs and Network logs with varying input features of healthcare staffs' security practices.

With these algorithms, security practice of healthcare staffs, can then be studied. Deviations of security practices from required healthcare staffs' security behavior can

be examined to define appropriated incentives towards improving conscious care security practice. Analyzing healthcare staff security practice with AI seems to be a new research focus area and this resulted into the inclusion of only 15 articles in this study. Among these included articles, there were no adequate recorded performance scores. As a result, the study could not adequately perform a comparative assessment of the performance of the identified algorithms. Future work would include development of a framework and a practical assessment of the performance of these methods towards implementation in real healthcare staffs' generated logs.

References

1. Verison. Data Breaches Report. 2019.
2. HealthITSecurity. The 10 Biggest Healthcare Data Breaches of 2019, So Far. @SecurityHIT; 2019.
3. Zhang H., Mehotra S., Liebovitz D., Gunter C., Malin B. Mining Deviations from Patient Care Pathways via Electronic Medical Record System Audits. ACM Transactions on Management Information Systems (TMIS). 2013;4.
4. Caroline Humer, Finkle J. Your medical record is worth more to hackers than your credit card. 2014.
5. C. Humer, Finkle J. Your medical record is worth more to hackers than your credit card. Reuters. 2014 2014-09-24.
6. Lena Yuryna Connolly M. L., John Gathegi, Doug J. Tygar,. Organisational culture, procedural countermeasures, and employee security behaviour. https://doiorg/101108/ICS-03-2017-0013. 2017.
7. Tetz E. Network Firewalls: Perimeter Defense - dummies. 2018.
8. Predd J., Pfleeger S. L., Hunker J., Bulford C. Insiders Behaving Badly - IEEE Journals & Magazine. of Publication: 05 August 2008.
9. Cannoy S. D., Salam A. F. A framework for health care information assurance policy and compliance. Commun ACM. 2010;53(3):126-31.
10. Safa N. S., Sookhak M., Von Solms R., Furnell S., Ghani N. A., Herawan T. Information security conscious care behaviour formation in organizations. Computers & Security. 2015;53:65-78.
11. Prosper Kandabongee Yeng A. S., Bian Yang, Einar Arthur Snekkenes. Framework for Healthcare Staffs' Information Security Practice Analysis: Psycho-Socio-Cultural Context. journal of Medical and Internet Research. 2019.
12. Walker-Roberts S., Hammoudeh M., Dehghantanha A. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access. 2018;6:25167-77.
13. Böse B., Avasarala B., Tirthapura S., Chung Y., Steiner D. Detecting Insider Threats Using RADISH: A System for Real-Time Anomaly Detection in Heterogeneous Data Streams. IEEE Systems Journal. 2017;11(2):471-82.
14. Gafny M. a., Shabtai A., Rokach L., Elovici Y. Detecting data misuse by applying context-based data linkage2010. 3-12 p.
15. Chen Y., Nyemba S., Zhang W., Malin B. Specializing network analysis to detect anomalous insider actions. Security Informatics. 2012;1(1):1-24.
16. Islam S., Hasan M., Wang X., Germack H. D., Noor-E-Alam. A Systematic Review on Healthcare Analytics: Application and Theoretical Perspective of Data Mining. Healthcare (Basel). 2018;6(2):54.

17. Gheyas I., Abdallah A. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Analytics. 2016;1.
18. Ghafir I., Husák M., Prenosil V. A Survey on Intrusion Detection and Prevention Systems2014.
19. Shaban-Nejad A., Michalowski M., Buckeridge D. Health intelligence: How Artificial Intelligence Transforms Population and Personalized Health. Nature Medicine. 2018;50.
20. Jiang F., Jiang Y., Zhi H., Dong Y., Li H., Ma S., et al. Artificial intelligence in healthcare: past, present and future. BMJ (Clinical research ed). 2017;2:svn-2017.
21. Wahl B., Cossy-Gantner A., Germann S., Schwalbe N. Artificial intelligence (AI) and global health: How can AI contribute to health in resource-poor settings? BMJ Global Health. 2018;3:e000798.
22. Vihinen M., Samarghitean C. Medical Expert Systems. Current Bioinformatics. 2008;3(1):56-65.
23. Chandra S., Ray S., Goswami R. T. Big Data Security in Healthcare: Survey on Frameworks and Algorithms2017. 89-94 p.
24. Code of conduct for information security and data protection in the healthcare and care services sector, (2018).
25. Yeng P., Yang B., Snekkenes E., editors. Observational Measures for Effective Profiling of Healthcare Staffs' Security Practices. 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC); 2019 15-19 July 2019.
26. PRISMA. PRISMA 2018 [Available from: http://www.prisma-statement.org/.
27. Boddy A. J., Hurst W., Mackay M., Rhalibi A. e. Density-Based Outlier Detection for Safeguarding Electronic Patient Record Systems. IEEE Access. 2019;7:40285-94.
28. Tchakoucht T. A., Ezziyyani M., Jbilou M., Salaun M., editors. Behavioral appraoch for intrusion detection. 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA); 2015 17-20 Nov. 2015.
29. Costante E., Fauri D., Etalle S., Hartog J. D., Zannone N., editors. A Hybrid Framework for Data Loss Prevention and Detection. 2016 IEEE Security and Privacy Workshops (SPW); 2016 22-26 May 2016.
30. García Adeva J. J., Pikatza Atxa J. M. Intrusion detection in web applications using text mining. Engineering Applications of Artificial Intelligence. 2007;20(4):555-66.
31. Gupta S., Hanson C., Gunter C. A., Frank M., Liebovitz D., Malin B., editors. Modeling and detecting anomalous topic access. 2013 IEEE International Conference on Intelligence and Security Informatics; 2013 4-7 June 2013.
32. Li X., Xue Y., Malin B., editors. Detecting Anomalous User Behaviors in Workflow-Driven Web Applications. 2012 IEEE 31st Symposium on Reliable Distributed Systems; 2012 8-11 Oct. 2012.
33. Amálio N., Spanoudakis G., editors. From Monitoring Templates to Security Monitoring and Threat Detection. 2008 Second International Conference on Emerging Security Information, Systems and Technologies; 2008 25-31 Aug. 2008.
34. Pierrot D., Harbi N., Darmont J., editors. Hybrid Intrusion Detection in Information Systems. 2016 International Conference on Information Science and Security (ICISS); 2016 19-22 Dec. 2016.
35. Boddy A., Hurst W., Mackay M., Rhalibi A. E., editors. A Hybrid Density-Based Outlier Detection Model for Privacy in Electronic Patient Record system. 2019 5th International Conference on Information Management (ICIM); 2019 24-27 March 2019.
36. Asfaw B., Bekele D., Eshete B., Villafiorita A., Weldemariam K., editors. Host-based anomaly detection for pervasive medical systems. 2010 Fifth International Conference on Risks and Security of Internet and Systems (CRiSIS); 2010 10-13 Oct. 2010.

37. Ziemniak T., editor Use of Machine Learning Classification Techniques to Detect Atypical Behavior in Medical Applications. 2011 Sixth International Conference on IT Security Incident Management and IT Forensics; 2011 10-12 May 2011.
38. Chen Y., Nyemba S., Malin B. Detecting Anomalous Insiders in Collaborative Information Systems. IEEE transactions on dependable and secure computing. 2012;9:332-44.
39. Wesołowski T., Porwik P., Doroz R. Electronic Health Record Security Based on Ensemble Classification of Keystroke Dynamics. Applied Artificial Intelligence. 2016;30:521-40.
40. Chen Y., Malin B. Detection of Anomalous Insiders in Collaborative Environments via Relational Analysis of Access Logs2011. 63-74 p.
41. Asfaw B., Bekele D., Eshete B., Villafiorita A., Weldemariam K. Host-based anomaly detection for pervasive medical systems2010. 1-8 p.
42. Gates C., Li N., Xu Z., Chari S., Molloy I., Park Y. Detecting Insider Information Theft Using Features from File Access Logs2014. 383-400 p.
43. Røstad L., Edsberg O. A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs2006. 175-86 p.
44. Smyth P., Fayyad U., Burl M., Perona P., Baldi P. Inferring Ground Truth from Subjective Labelling of Venus Images. Advances in Neural Information Processing Systems. 1996;7.