Journal of Theoretical and Applied Information Technology
31st December 2023. Vol.101. No 24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT CYBER SECURITY AND DATA SCIENCE FOR ANALYZING BIG MEDICAL DATA

MOHAMMAD AL-OMAR[1], SALEH ALOMARI[2], TAMER BANI AMER[3]

[1,2,3] Faculty of Science and Information Technology, Jadara University, Irbid 21110, Jordan

m.alomar@jadara.edu.jo, omari08@jadara.edu.jo, t.baniamer@jadara.edu.jo

ABSTRACT

This study aims to the impact of the use of cyber security and data science in analyzing big medical data. The study sample comprised 120 participants, including hospital chief information officers, chief information security officers, and healthcare cyber security professionals, who were selected from all 33 government hospitals in Jordan connected to the Ministry of Health as the research sample. The primary independent variable, cyber security, was evaluated using information security, network security, operational security, and end-user education. massive amounts of medical data were used as the dependent variable. The study used SPSS to determine the impact of cybersecurity on the analysis of big medical data in Jordanian hospitals. The results found that 75% of participants confirmed that analyzing big data in the medical field will have a high impact on the evaluation of medical diagnoses and 63.3% of the participants agreed that analyzing big data in the medical field, it will have a high impact in predicting the incidence of diseases, the results also found the role of cybersecurity in protecting the storage of a large amount of data in hospital information systems (HIS), ranking first with an arithmetic mean of (3.73), The study recommends that future research should explore the benefits to medical organizations of analyzing structured and unstructured data in clinical and administrative fields, such as the limitations they face in these areas. Additionally, it is suggested that further research should also include medical institutions from outside Jordan borders to enable international comparative analyses.

Keywords: *Cyber Security; Big Medical Data; Data Analyzing; Jordan Hospitals*

1. INTRODUCTION

Currently, we find ourselves in a situation where we are bombarded with data from all areas of our lives, such as social relationships, science, work, health, etc. This abundance of data has been compared to a flood of information; Technological breakthroughs have enabled us to produce increasingly larger amounts of data to a point where it is no longer manageable with currently available solutions. As a result, the term "big data" has come to refer to this overwhelming amount of information. [1]. We need to develop new methods for organizing this data and extracting relevant information to meet our current and future social needs. Medical data is a unique social requirement. Healthcare firms, like all other industries, are producing data at an exponential rate, which simultaneously offers many benefits and issues [2]. All industries benefit from and rely on big data and the Internet of Things. Smart homes, smart healthcare, and other applications are beginning to harness the Internet of Things and big data. These applications based on the Internet of Things and big data are rapidly expanding [3]. However, every instance of cyber-attack against these technologies, which improve our lives and offer great applications, poses a threat. These applications are attractive targets for hackers due to the wealth of valuable data they contain [4]. Cybersecurity is a critical issue for these technologies. The development of these technologies can be halted by cyber security threats and attacks. Threats to cyber security make it harder to obtain user data with these technologies [5]. Currently, the healthcare industry is one of the most targeted industries. The findings draw attention to the increasing number of attacks and high levels of medical identity theft, which have resulted in the theft of millions of medical information worldwide breaches insider threats, malware, and hacking are some of its causes [6]. Hacking is the act of gaining access to a computer system without authorization to steal data or cause damage such as creating havoc viruses and ransomware are examples of dangers that fall under the category of malware ("malware") [7]. Malware is software that is intended to access systems without the users' permission threats from

within are problems that result from mistakes or purposeful staff activities (such as replying to phishing emails) [8].

The thousands of networked medical devices and frequently inconsistent business processes must be considered while implementing hospital cyber security. However, these gadgets are used all around the hospital and can even be used off-site, making connected medical devices multiple hospital cyber security concerns [9]. Hospital business processes can differ significantly from patient to patient, are mathematically challenging to model, and frequently need for openness (to allow for data exchange and emergency access to patient records) [10]. All industries may benefit from and using the Internet of Things and big data. Applications for smart homes, smart health care, and other areas are starting to exploit the Internet of Things and big data. That is why cyber security is essential to protect patient data in the medical sector because medical information is very sensitive, and disclosure can be inappropriate. Recovering it or losing it has a significant negative impact on patients [11]. It is much more crucial to comprehend and be aware of the potential hazards that may endanger different applications based on big data and the Internet of Things. For that reason, better safeguard these systems and applications against cybersecurity attacks by being aware of potential threats and attacks [12]. In order to better understand the connection between cybersecurity threats and the development of big data technologies, particularly medical data, this research highlights the significant effects of cybersecurity on big medical data. Numerous studies have examined the impact of cybersecurity on health and healthcare, without focusing on the abuse of big medical data analysis. However, the results are mixed [13], with cybersecurity having both a positive and a negative effect. Despite its importance, to the best of our knowledge, there are no studies on the impact of cybersecurity on the analysis of big medical data. Therefore, this study aims to determine the impact of cybersecurity on the analysis of big medical data in Jordanian hospitals.

The remainder of the study will be divided as follows. In Section 2, presenting the main a literature review and hypothesis development. In Section 3, explained data and methodology. In Section 4, discuss the results. Finally, the concluding comments are presented in Section 5.

2. RELAED BACKGROUND

In this field, many papers have been reviewed by researchers based on data science and its relationship to cybersecurity. For example, in [14] research on “Data Science” includes several forms of cutting-edge analysis techniques that can be used to improve application skills and intelligence by making Wise decisions in different situations. Considering intelligent computing and data-driven decision-making, it also examines and describes 10 potential real-world application areas, such as business, healthcare, cybersecurity, urban and rural data science, etc. In addition, in [15] paper outlines the cybersecurity and data privacy aspects of communication of patient data measured from wireless wearable biosensors to a nearby Cloudlet host server to facilitate complex, cloud-based primary analytics of big medical data. With regard to the role of cyber security in dealing with big data. [16] analyzed traditional technology/systems and security information and event management (SIEM) tools that show deficiencies in dealing with big data metrics and threats that will be successfully adopted in the cyber threat in The field of intelligence and cyber security to deal with complex data metrics.

In [17] A study on the development of a systemic and organizational perspective to examine the dynamics of the development of cyber security capabilities in hospitals and how these internal organizational dynamics interact to shape the hospital cyber security system in the United States. This was done through interviews with the hospital's Chief Information Officers, Chief Information Security Officers, and healthcare cyber security experts. The results show that the variable most influencing cyberattack risk in a hospital is endpoint complexity, followed by internal stakeholder alignment. It was recommended that policymakers should introduce policies that not only raise the target level of cyber security capabilities, but also reduce the variance in resource availability across the entire healthcare system

In [18], the improvement in information security in the adoption of digital patient records is highlighted based on the organization and standardization of providers and the increasing need for information sharing between patients, providers, and payers. In this paper, a cybersecurity framework based on big data analytics for security and privacy across healthcare applications is proposed. Electronic Health Records (EHR) can be shared by different users to increase the quality of healthcare services. In [19] the researchers also outline key cybersecurity challenges, solutions that the health

sector is adapting to, and areas for improvement needed to counter recent increases in cyberattacks (for example, phishing campaigns and ransomware attacks), which attackers have used to exploit vulnerabilities. Technology and people introduced by changes in work practices in response to the COVID-19 pandemic are identified as 9 key cybersecurity challenges and found that the most prominent and significant cyber-attack tactics that occurred during the pandemic were related to phishing, ransomware, distributed denial-of-service attacks, and malware.

In [10] analyzes numerous tools, features, and functions of cybersecurity in the health care industry, describes cybersecurity and its need in that industry, and specifies applications of cybersecurity in healthcare. A patient's collected data, which may include basic information, health patterns, family history, and financial information, is a gold mine for hackers. The significance of data access in the healthcare industry creates a vulnerability in the system for managing medical data. According to [20], not only do these types of attacks pose a threat to patients' identity and finances, but they can also disrupt hospital operations and put patients' health and well-being at risk. Hospitals in the UK's National Health System, which suffered from the WannaCry ransomware attacks in May 2017, have had to delay treatment plans and even redirect incoming ambulances because they have lost access to hospital information systems. Among these operational delays and the financial consequences of data breaches and ransomware attacks, cyberattacks have long-term detrimental effects on the reputation and revenues of hospitals and health facilities. In addition, [21] paper provides a detailed outline of how core values of health systems, such as principles of biomedical ethics, have a supportive or conflicting relationship with cybersecurity. The findings show that there are reasons to believe that the primacy of autonomy over benevolence and non-offending in contemporary medical ethics can be extended to include: Conflict of values in health-related cyber security.

3. RESRESEARCH QUESTION

To analyze this problem, our contribution aims to answer questions.

Q1. What is the role of cyber security in improving the quality of healthcare?

Q2. Does cyber security support the work of medical personnel and medical information?

Q3. What is the role of cyber security in maintaining business and management in medical hospitals?

Q4. What is the relationship between the values at risk in cybersecurity and the analysis of big medical data science?

4. RESEARCH METHODOLOGY

The research methodology will handle the most important things, Research Population and Sampling, Research Design, and measurement of research Variables.

4.1 Research Population and Sampling

The focus of the investigation will be significant public hospitals. All 33 of the government hospitals in Jordan that are connected to the Ministry of Health were chosen as the research sample. Hospital chief information officers, chief information security officers, and healthcare cyber security professionals are research participants. Convenience sampling, a non-probability sample approach, was adopted since it was difficult to define the research population precisely. With a questionnaire, determine the impact of cyber security on big medical data in the Jordanian healthcare industry.

4.2 Research Design

The questionnaire will be created with input from hospital chief information officers, chief information security officers, healthcare cybersecurity specialists, literature studies, and past survey analyses. It will be broken down into three parts to make it simpler for people to comprehend. In the first component of the survey, participants' demographic data will be sought, including their age, gender, years of experience, occupation, and educational background. The second part will be devoted to hospital cyber security. The third section of measurement will be concern the dependent variable (bulk medical data). The survey will utilize a 5-point Likert scale, with a rating of 1 for least important and 5 for most important. The selected sample consisted of the hospital's chief information officers, chief information security officials, and health care cyber security experts who understood the importance of cyber security in protecting medical information.

5. PREPARE YOUR PAPER BEFORE STYLING

In order to test hypotheses and provide usable results, the current research comprised a variety of factors that needed reliable measurement. The primary independent variable, cyber security, was evaluated using information security, network security, operational security, and end-user

education. Massive amounts of medical data were used as the dependent variable. The variables will be measured using key performance indicators and a standardized online questionnaire.

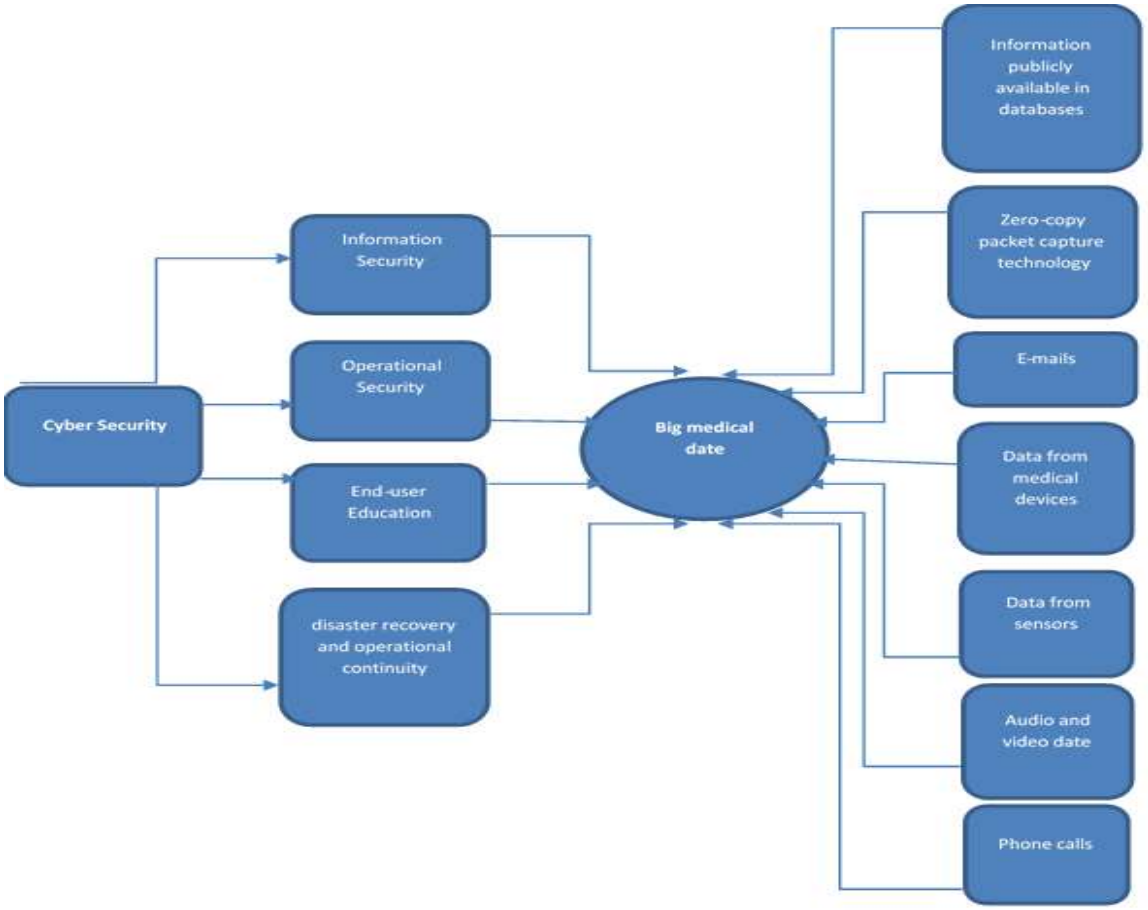

Figure 1:The proposed research model

As a result, the data was examined to calculate the mean and standard deviation. The study examined the reliability of variables, which is important and widely used in the social studies. The main aim of this test is to check the extent to which the measuring items of the variables are reliable for measuring the target factors, it is also called internal consistency [22]. Cronbach Alpha is the most common measure used to conduct reliability analysis for the measuring items validity. In general, the reliability coefficient is ranked between 0 to 1. Although the different assumptions are discussed regarding this issue and suggest different cuts-off acceptable values, but the most statisticians agree to accept at least 0.6 value to consider a reliable measure as stated by [23] The higher of coefficient value the higher the degree of measurements reliability. Table (1) shows the study's reliability results which mostly found great a threshold and met the cut-off of 0.70 and above.

Table 1:Reliability Results

Construct	Items numbers	Cronbach's Alpha	Status
cyber security related factors (independent variable)			
End-user Education	4	0.836	Reliable
disaster recovery and operational continuity	3	0.860	Reliable
Information Security	4	0.810	Reliable
Operational Security	9	0.808	Reliable
bulk medical data (dependent variable)	10	0.822	Reliable

6. THE RESULTS

6.1 Participant's Socio-Demographic Characteristics.

This study includes 120 participants from 33 of the government hospitals in Jordan that are connected to the Ministry of Health, the distribution of gender was male 75(62.5%) and female 45(37.5%), and the majority of them were in 31-39

years 31(25.8%) and 40-45 years (25%) with 6-10 years of experience 39(32.5%), 28(23.3%) with 0-5 years of experience and 27(22.5%) and 26(21.7%) more than 15 and 11-155 years of experience respectively, regarding the job title 53(44.2%) were chief information security officers, and healthcare, 37(30.8%) were chief information officers and 30(25%) were cyber security professionals, table (2) summaries participant's socio-demographic characteristics.

Table 2: Participant's socio-demographics characteristics (N=120)

Demographic	Frequency	Percent
Gender		
Male	75	62.5
Female	45	37.5
Age		
25-30	24	20
31-39	31	25.8
40-45	30	25
46-55	19	15.8
Above 55	16	15.3
Years of experience		
0-5	28	23.3
6-10	39	32.5
11-15	26	21.7
More than 15	27	22.5
Job title		
chief information officers	37	30.8
chief information security officers, and healthcare	53	44.2
cyber security professionals	30	25

6.2 The Role of Cyber Security in The Analysis of Big Medical Data

The study further aims to determine the impact of cybersecurity on the analysis of big medical data in Jordanian hospitals. The study examined the descriptive statistics of the main variables using the mean and standard deviation SD to conduct this analysis. The results about the normality distribution of the data showed a normal distributed dataset with a range of ±1.00 - ± 2.00 of the normality distribution measure of skewness and kurtosis respectively. To examine the role of cyber security in the analysis of big medical data, the means and standard deviations were calculated for the primary independent variable, cyber security, which was evaluated using information security, network security, operational security, and end-user education table (3) shows the results.

Table 3: The arithmetic means and standard deviations for the cyber security related factors

Cyber security related factors	Mean	SD	Degree of impact
End-user Education	3.44	0.783	High
disaster recovery and operational continuity	3.38	0.814	Medium
Information Security	3.52	0.735	High
Operational Security	3.50	0.519	High

To evaluate the above factors according to the benefits of analyzing big data in the medical field, the arithmetic means and standard deviations of the study sample estimates were calculated. Tables 4-7 show the results.

Table 4:Arithmetic means and standard deviations are the estimates of the study sample on end -user education.

No.	Statement	Mean	SD	Degree of impact
1	Evaluation of medical diagnoses	3.87	1.004	High
2	Lay out the path of disease treatment	3.23	1.136	Medium
3	Unearthing more effective methods, from a medical point of view	3.44	0.977	High
4	Unearthing more cost-effective ways to diagnose and treat patients	3.25	1.102	Medium
5	End-user Education	3.44	0.783	High

The results in Table (4) show that 64.2% of the participants agreed that by analyzing big data in the medical field, it will have a high impact in discovering more effective methods, from a medical point of view with a mean of 3.44 and standard deviation of 0.977 and 75% of them confirmed that analyzing big data in the medical field will have high impact in evaluation the medical diagnoses with a mean of 3.87 and a standard deviation 1.004, while53.3% and 50.9% agreed that by analyzing big data the path of disease treatment will be better determined and diagnose and treat patients in more cost-effective ways with a mean of 3.23 , 3.25 and standard deviation of 1.136,1.102 respectively.

Table 5: Arithmetic means and standard deviations are the estimates of the study sample on disaster recovery and operational continuity

No.	Statement	Mean	SD	Degree of impact
5	Identifying needs and introducing new health services and preventing and overcoming crises	3.43	1.018	High
6	prediction of the incidence of diseases,	3.42	1.001	High
7	analysis of the human genome for the introduction of personalized treatment.	3.30	1.034	Medium
	Disaster recovery and operational continuity	3.38	0.814	Medium

Regarding the disaster recovery and operational continuity the results in Table (5) show that 63.3% of the participants agreed that by analyzing big data in the medical field, it will have a high impact in predicting the incidence of diseases with a mean of 3.42 and standard deviation of 1.001 and 60% of them confirmed that analyzing big data in the medical field will have a high impact in identifying needs and introducing new health services and preventing and overcoming crises with a mean of 3.43 and a standard deviation of 1.018 ,while 47.5% of them agreed that analyzing big data have high impact in analysis of the human genome for the introduction of personalized treatment with mean 3.30 and standard deviation 1.034.

Table 6: Arithmetic means and standard deviations are the estimates of the study sample on Information Security

No.	Statement	Mean	SD
8	doctors compare recent medical cases to earlier ones in order to make better diagnoses and change treatments.	3.43	0.985
9	detection of diseases at earlier stages when they can be more easily and quickly cured, specifications	3.53	1.004
10	doctors' comparison of recent medical cases to earlier ones in order to improve diagnosis and therapy modification,	3.58	1.120
11	Identification of patients who are expected to be at greatest risk of disease	3.57	0.994
	Information security	3.52	0.735
No.	Statement	Mean	SD

The results presented in Table (6) also indicate that the analysis of big data in the medical field has a significant impact on the medical staff and the security of medical information, as 71.7% of the participants confirmed that through data analysis, it is possible to identify patients who are expected to be more at risk of contracting the disease with mean 3.57 and standard deviation 0.994. Furthermore, 64.2% of the respondents agreed that by analysis the medical information for the patients , doctors can more effectively compare recent medical cases to earlier ones to make better diagnoses and change treatments with mean 3.43 and standard deviation 0.985, also the results showed the high impact of analysis data in detection of diseases at earlier stages and doctors' comparison of recent medical cases to earlier ones in order to improve diagnosis and therapy modification with a mean of 3.53,3.58 and a standard deviation of 1.004 , 1.120 respectively .

Table 7: Arithmetic means and standard deviations are the estimates of the study sample on operational security

No.	Statement	Mean	SD	Degree of impact
12	Health management of the entire society and individual patient care	3.35	0.816	Medium

	(personalized medicine)			
13	Examining patient profiles to determine those who should be targeted for a prevention or preventive care strategy	3.49	0.698	High
14	the capacity to foresee the onset of particular diseases or the deterioration of patients' outcomes	3.34	1.008	Medium
15	detecting drug interactions and their side effects.	3.41	1.065	High
16	cost-saving measures, abuse prevention measures, and counseling techniques	3.49	0.935	High
17	speedier and more accurate detection of fraudulent financial activity to stop exploitation and fix mistakes	3.46	1.020	High
18	limiting pointless medical treatments and actions	3.49	0.830	High
19	Improve profitability by identifying patients who incur significant expenses	3.33	0.780	Medium
20	Increase profitability by identifying doctors whose work, procedures and methods of treatment are more expensive	3.48	0.907	High
	Operational Security	3.50	0.519	High

Regarding to the role of cyber security in maintaining business and management in medical hospitals all statements related to operational security came with averages from medium to high, as the results showed 70% of the respondents agreed that using cyber security in medical fields would effect on limiting pointless medical treatments and actions. The results also showed that 68.3% of the participants confirmed that cyber security can increase profitability by identifying doctors whose work, procedures, and methods of treatment are more expensive, also 67.5% of them ensured that cyber security increase detecting of drug interactions and their side effects, furthermore 65% of the sample agreed that cyber security will save cost and abuse prevention measures and detect fraudulent financial activity to stop exploitation and fix errors.

The findings also found a high agreement on the impact of cybersecurity in the medical field on the health management of the entire society and identifying those who should be targeted for a strategy of prevention or preventive care and the ability to anticipate the emergence of certain diseases or the deterioration of patient outcomes.

6.3 Cyber security in analyzing big medical data

To evaluate the implications of using cyber security in analyzing medical data, the arithmetic means and standard deviations of the study sample estimates were calculated in table (8)

Table 7: Arithmetic means and standard deviations are the estimates of the study sample on the implications of using cyber security in analyzing medical data

No.	Statement	Mean	SD	Degree of impact
1	The data preservation	3.63	0.831	High
2	Storing and restoring data stored in databases or other archives	3.54	0.943	High
3	Data exchange either within the hospital or between protected citizens	3.41	0.865	High
4	Interoperability for both healthcare	3.11	0.887	medium

	worker and citizen Exchange data between many systems and devices in a common and secure way			
5	Wireless communication for implantable devices to communicate with each other	3.26	0.825	medium
6	Protect patient data in PACS with privacy	3.43	0.775	High
7	Protect access to images for subsequent storage and sharing	3.08	1.175	medium
8	Protecting the storage of large amount of data in hospital information systems (HIS)	3.73	0.796	High
9	Defending IT infrastructures	3.25	0.748	medium
10	Download, upload and manipulate images securely	3.71	0.556	High
	Cyber security in analyzing big medical data	3.50	0.519	High

It is noted from Table (8) that the arithmetic means for the statements of the implications of using cyber security in analyzing medical data ranged between (3.08) and (3.73) with medium to high degrees, Where the role of cybersecurity in protecting the storage of a large amount of data in hospital information systems (HIS) came in the first rank with an arithmetic mean of (3.73) and a standard deviation(0.796) with a high degree of impact ,then the impact of cybersecurity in downloading, uploading and manipulating images securely with a mean of (3.71) and a standard deviation of (0.556) and a high degree impact, the data preservation with a mean of (3.63) and a standard deviation of (0.831) ,storing and restoring data stored in database or other archives with a mean of (3.54) and a a standard deviation of (0.943) , protect patient data in PACS with privacy with a mean of (3.43) and a standard deviation (0.775), data exchange either within the hospital or between protected citizens with a mean of (3.41) and a standard deviation of (0.865) and all with high degree impact ,while the role of cyber security in protect access to images for subsequent storage and sharing was ranked last in terms of its impact in analyzing medical data with a mean of (3.08) and a standard deviation (1.175), then the interoperability for both healthcare worker and citizen exchange data between many systems and devices commonly and securely with a of mean (3.11) and a standard deviation of (0.887),the wireless communication for implantable devices to communicate with each other and IT defending infrastructure with a means of (3.26) ,(3.25) and a standard deviations of (0.825) and (0.748) respectively and all with medium degree impact .

6.4 The relationship between the values at risk in cybersecurity and the analysis of big medical data science

To evaluate the relationship between the values at risk in cybersecurity and the analysis of big medical data science ,correlation coefficients were calculated between the independent variables and the dependent variables and the quality of the relationship model was tested using F, then calculating the percentage that each independent variable explains in the change obtained by analyzing the big medical data as a dependent variable by using R2 and making sure of the significance of the impact of these independent variables, which is the use of cybersecurity table (9) show the results.

Table 8: The calculation independent variable at the rick in cybersecurity between the R, F-Test, R2 and T-Test.

INDEPENDENT VARIABLE (CYBER SECURITY)	MASSIVE AMOUNTS OF MEDICAL DATA			
	R	F-TEST	R2	T-TEST
END-USER EDUCATION	0.586	61.974	0.344	7.861
DISASTER RECOVERY AND OPERATIONAL CONTINUITY	0.548	50.638	0.294	7.116
Information Security	0.649	85.745	0.421	9.260
OPERATIONAL SECURITY	0.851	310.637	0.725	17.625

Accordingly, the results in table (10) which confirm the existence of a positive direct relationship between the values at risk in cybersecurity and the analysis of big medical data science Where the correlation coefficients were statistically significant at the level of significance 0.01.

Table 9: the relationship between the values at risk in cybersecurity and the analysis of big medical data science

Variables	End-user Education	disaster recovery and operational continuity	Information Security	Operational Security
massive amounts of medical data	0.586**	0.548**	0.649**	0.851**

7. DISCUSSION

In the qualitative findings, it was evident that using cybersecurity in analysis of big medical data in Jordanian hospitals has created an opportunity for better research and patient care and detection of diseases at earlier stages. The results of the present study are supported by [24] [25]. It has resulted in consistent and large-scale patient diagnosis and monitoring. The perceived results confirmed that the analysis of big data sources that are generated by the health care system during the implementation of treatment plans, It helps in improving public health monitoring and provides a faster response through effective analysis of disease patterns, facilitating doctors to track the use of medicines, and monitor the patient's health status at any time, these findings agree with [26] which examined several big data frameworks concerning fundamental data sources, analytical capability, and application domains to present the numerous analytical options that exist in a patient-centered healthcare system from the perspective of various stakeholders.

The analysis of the latest data reveals that data analytics increase health management of the entire society, predict of the incidence of diseases, make better diagnoses and change treatments to unearthing more effective methods, from a medical point of view these finding are consistent with [27] [28] studies which confirmed that data analytics increase diagnostic accuracy, it enables doctors to use predictive algorithms to help them make more accurate diagnoses to prevent or mitigate many diseases. Regarding the impact of analyzing big medical data on improving profitability and measures of cost savings, The results found that identifying patients who incur significant expenses and identifying doctors whose work, procedures, and treatment methods are more expensive, which improves profitability in the medical sector which agreed with [29][30][31] studies that reveal that data analytics lowers healthcare costs and increases good outcomes and fewer resources used, including doctors' time. The cybersecurity in healthcare includes all the general actions employed both in the consumer and industrial sectors (information security, operational security, disaster recovery and operational continuity, end-user education) specialized for the medical field the results found that using cybersecurity in analyzing data protect patient data in PACS with privacy and data exchange either within the hospital or between protected citizens which agree with [32] study results which provided a review of the literature on what health care organizations are doing to protect patients' information privacy, how breaches and vulnerabilities occur, and the impact on healthcare organizations and the significance of enhancing information technology (IT) to protect it from electronic attacks from 2015 to 2020, 45 articles on cybersecurity, electronic attacks, and healthcare institutions were published, the study discussed the importance of cyber security in protecting patient information and avoiding the consequences of data theft, as well as how these institutions strengthen "information technology systems to protect them from electronic attacks".

The study's findings also agreed with [8] on the role of cybersecurity in facilitating data analysis programs for medical staff to communicate with others, even when they were working in different locations. This enables hospitals to communicate on the progress of various treatments, saving time and money while also assisting facilities in working more effectively together.

The results of the study showed that there is a significant impact of the use of cybersecurity in the preservation of patient data and the storage and recovery of data stored in databases or other archives, data exchange within the hospital and between protected citizens Possibility of interoperability for both the health care worker and the citizen exchange of data between many systems and devices in a common and secure manner, this results agreed with several studies that dealt with cyber security in the health sector, such as in [33] which presented the prerequisites that must be met for information sharing on recognized cyber images between people and proposed an orient-locate-

bridge-model (OLB) outlining how institutions can use educational techniques to empower both their leaders and cyber security personnel in order to effectively communicate situations relating to cyber security, and in [34] [35] [36] studies which emphasized the important role of cyber security in healthcare businesses that use modern technology, such as patient profile management software, cloud storage of healthcare data, and advanced medical equipment. Securing and protecting patient databank and enable healthcare businesses to enhance and monitor their whole ecosystem's cyber health while protecting patient privacy and health provider infrastructure.

8. LIMITATION

This study covered details of the use of cybersecurity and data science in analyzing big medical data, however we encountered some limitations. First, the research dealt with the positive effects of using cybersecurity and data science in analyzing big medical data, but it does not take into account the technical details related to implementation in terms of data analysis applications and cybersecurity applications applied in the medical sector. second, the sample size of 120 participants remains relatively underrepresented. As such, it is possible for the same survey with more participants can produce different results. third, since there are no currently published data comparing the use of cybersecurity in big data analytics among healthcare organizations globally, more needs to be done to generate data in this area. Finally, the availability of similar studies in the literature regarding the healthcare sector, especially recent ones, is not abundant in Arab countries, especially Jordan, and comparisons were made mainly against data from surveys conducted in hospitals in foreign countries.

9 CONCLUSION

In conclusion, the study confirms that there is a high impact of using cyber security and data science in the analysis of big medical data supported by quantitative evaluations from experts. This paper discussed the cybersecurity in healthcare including information security, operational security, disaster recovery and operational continuity, end-user education specialized for the medical field, evaluated these factors according to the benefits of analyzing big data in the medical field, the results found that using cybersecurity in analyzing data protect patient data in PACS with privacy and data exchange either within the hospital or between protected citizens and the role of cybersecurity in facilitating data analysis programs for medical staff to communicate with others and download, upload and manipulate images securely, the data preservation with mean storing and restoring data stored in database or other archives. The study recommends that future research explore the benefits to medical organizations of analyzing structured and unstructured data in clinical and administrative fields and the limitations they face in these areas. For this purpose, in-depth interviews will be conducted with medical personnel in Jordan who could provide additional data for experimental analyses based on their suggestions, additional research should also include medical institutions from outside Jordan's borders to enable international comparative analyses. Regarding the use of big data analytics to diagnose specific conditions big data analytics can also be used for studies on the prevalence of epidemics, the effectiveness of COVID treatment, or studies of psychology and psychiatry.

10 ACKNOWLEDGMENT

I would like to acknowledge the initial support received from Jadara University under grant number Jadara-SR-Full2023. This support played a vital role in facilitating this research.

REFERENCES

[1] Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: management, analysis and future prospects. Journal of Big Data, 6(1), 1-25.

[2] Ngiam, K. Y., & Khor, W. (2019). Big data and machine learning algorithms for health-care delivery. The Lancet Oncology, 20(5), e262-e273.

[3] Dumka, A., & Sah, A. (2019). Smart ambulance system using concept of big data and internet of things. In Healthcare data analytics and management (pp. 155-176). Academic Press.

[4] Alferidah, D. K., & Jhanjhi, N. Z. (2020, October). Cybersecurity impact over bigdata and iot growth. In 2020 International Conference on Computational Intelligence (ICCI) (pp. 103-108). IEEE.

[5] Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health care and cybersecurity: bibliometric analysis of the literature. Journal of medical Internet research, 21(2), e12644.

[6] Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working

towards mitigating the risks. BMC medical informatics and decision making, 20, 1-10.

[7] Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669-710.

[8] Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52.

[9] Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. Business horizons, 62(4), 539-548.

[10] Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: a comprehensive review of recent practices and trends. Cyber Security and Applications, 100016.

[11] Mijwil, M., Aljanabi, M., & Ali, A. H. (2023). ChatGPT: exploring the role of cybersecurity in the protection of medical information. Mesopotamian journal of cybersecurity, 2023, 18-21.

[12] Sreedevi, A. G., Harshitha, T. N., Sugumaran, V., & Shankar, P. (2022). Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review. Information Processing & Management, 59(2), 102888.

[13] Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10.

[14] Sarker, I. H. (2021). Data science and analytics: an overview from data-driven smart computing, decision-making and applications perspective. SN Computer Science, 2(5), 377.

[15] Javid, T., Faris, M., Beenish, H., & Fahad, M. (2020, September). Cybersecurity and data privacy in the cloudlet for preliminary healthcare big data analytics. In 2020 international conference on computing and information technology (ICCIT-1441) (pp. 1-4). IEEE.

[16] Rassam, M. A., Maarof, M., & Zainal, A. (2017). Big Data Analytics Adoption for Cybersecurity: A Review of Current Solutions, Requirements, Challenges and Trends. Journal of Information Assurance & Security, 12(4).

[17] Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: a systematic, organizational perspective. Journal of medical Internet research, 20(5), e10059.

[18] Zhu, S., Saravanan, V., & Muthu, B. (2020). Achieving data security and privacy across healthcare applications using cyber security mechanisms. The Electronic Library, 38(5/6), 979-995.

[19] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. Journal of medical Internet research, 23(4), e21747.

[20] Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. Bmj, 358.

[21] Loi, M., Christen, M., Kleine, N., & Weber, K. (2019). Cybersecurity in health–disentangling value tensions. Journal of Information, Communication and Ethics in Society.

[22] Alomari, Saleh Ali, Putra Sumari, Sadik AM Al-Taweel, and Ahmed M. Manasrah. "CUSTP: Custom Protocol for Audio and Video Conferencing System over P2P Networks." J. Digit. Content Technol. its Appl. 4, no. 3 (2010): 61-74.

[23] Mohammad Ibrahim Ahmed Al-Omar Tamer Bani Amer (2023)., The Impact of Cyber Security on Preventing and Mitigating Electronic Crimes in the Jordanian Banking Sector, International Journal of Advanced Computer Science and Applications, Vol. 14, No. 8, 2023.PP: 371-380.

[24] Basak, S. & Tamaghna, A. 2020. Spectrum-aware outage minimizing cooperative routing in cognitive radio sensor networks. Wireless Networks 26(2),1069-1084.

[25] Dhevi, B. Lakshmi, Vishvaksenan, K. S., Senthamil Selvan, K., Rajalakshmi, A. 2018. Patient monitoring system using cognitive internet of things. Journal of Medical Systems 42(11), 229.

[26] Palanisamy, V., & Thirunavukarasu, R. (2019). Implications of big data analytics in developing healthcare frameworks–A review. Journal of King Saud University-Computer and Information Sciences, 31(4), 415-425.

[27] Lerner I, Veil R, Nguyen DP, Luu VP, Jantzen R. Revolution in health care: how will data science impact doctor-patient relationships? Front Public Health. 2018;6:99

[28] Hampel HOBS, O'Bryant SE, Castrillo JI, Ritchie C, Rojkova K, Broich K, Escott-Price V. PRECISION MEDICINE-the golden gate for

detection, treatment and prevention of Alzheimer's disease. J Prev Alzheimer's Dis. 2016;3(4):243.

[29] Luthra, H., Nihith, T. A. S., Pravallika, V. S. S., Shree, R. R., Chaurasia, A., & Bansal, H. (2021, March). New paradigm in healthcare industry using big data analytics. In IOP conference series: materials science and engineering (Vol. 1099, No. 1, p. 012054). IOP Publishing

[30] Batko, K., & Ślęzak, A. (2022). The use of Big Data Analytics in healthcare. Journal of big Data, 9(1), 3.

[31] Doraisamy, Vaithegy, Saleh Ali Alomari, and Putra Sumari. "Video on demand caching system using NIPBCS over mobile ad hoc network." International Journal of Digital Content Technology and its Applications 5.6 (2011).

[32] Luthra, H., Nihith, T. A. S., Pravallika, V. S. S., Shree, R. R., Chaurasia, A., & Bansal, H. (2021, March). New paradigm in healthcare industry using big data analytics. In IOP conference series: materials science and engineering (Vol. 1099, No. 1, p. 012054). IOP Publishing

[33] Knox, Benjamin J., Øyvind Jøsok, Kirsi Helkala, Peter Khooshabeh, Terje Ødegaard, Ricardo G. Lugo, and Stefan Sütterlin. 2018. Socio-technical communication: The hybrid space and the OLB model for science-based cyber education. Military Psychology 30: 350–59

[34] Reagin, M. J., & Gentry, M. V. (2018). Enterprise cybersecurity: Building a successful defense program. Frontiers of health services management, 35(1), 13-22.

[35] Dullea, E., Budke, C., & Enko, P. (2020). Cybersecurity update: recent ransomware attacks against healthcare providers. Missouri Medicine, 117(6), 533.

[36] Nyakasoka, L., & Naidoo, R. (2022). Barriers to dynamic cybersecurity capabilities in healthcare software services., Proceedings of 43rd Conference of the South African Institute of Computer Scientists and Information Technologists, Vol. 85, pp: 231—242.