sustainability

MDPI

Article

Security Risk Assessment Framework for the Healthcare Industry 5.0

Abdullah Baz [1], Riaz Ahmed [2,*], Suhel Ahmad Khan [2,*] and Sudesh Kumar [2]

[1] Department of Computer and Network Engineering, College of Computers, Umm Al-Qura University, Makkah 21955, Saudi Arabia; aobaz01@uqu.edu.sa
[2] Department of Computer Science, Indira Gandhi National Tribal University, Amarkantak 484886, Madhya Pradesh, India; sudesh.kumar@igntu.ac.in
* Correspondence: riazchoudharyk786@gmail.com (R.A.); suhelak@igntu.ac.in (S.A.K.)

Abstract: The relevance of Industry 5.0 confirms the collaborative relationship between humans and machines through an inclusive automation process. The healthcare industry at present is facilitated by the use of these emerging technologies, which promise a more personalized, patient-centric approach, enabling more prompt, cost-effective, and efficacious medical care to the affected. However, managing enormous data volumes, lack of standards, risks to data security, and regulatory obstacles, such as regulatory compliance, are critical issues that must be addressed to ensure that Industry 5.0 can be effectively integrated into the healthcare industry. This research assumes significance in the stated context as it seeks to reveal the gaps between security risks and threats assessments for personalized healthcare services based on Industry 5.0. The study's investigations cite that the identification of security risks and various threats is an imperative need and must be prioritized so as to ensure optimal security for the healthcare system. Furthermore, the study peruses various security threats and security risk assessments for enhancing and safeguarding the healthcare industry. Moreover, the study also proposes a framework for security risk assessment based on Industry 5.0 ($SRVF^{HI5.0}$) for the healthcare security system. A step-wise procedure is applied to validate the proposed framework and provide support for designing feasible security evaluation criteria and tools for future research. Statistical analysis was performed to evaluate the measure of the applicability of multiple criteria, the tool's reliability, and factor analysis. This offers an adequate basis for accepting the suggested risk assessment methodology based on Healthcare Industry 5.0 for implementation as well as further research and analysis.

Keywords: Industry 4.0; Industry 5.0; healthcare security issues; security threats; risk assessment

Citation: Baz, A.; Ahmed, R.; Khan, S.A.; Kumar, S. Security Risk Assessment Framework for the Healthcare Industry 5.0. *Sustainability* **2023**, *15*, 16519. https://doi.org/10.3390/su152316519

Academic Editors: Maurizio Faccio, João Reis and Yuval Cohen

Received: 6 October 2023
Revised: 20 October 2023
Accepted: 31 October 2023
Published: 3 December 2023

1. Introduction

The Fifth Industrial Revolution, termed "Industry 5.0", is an emerging concept with the capacity to satisfy each consumer's demands with its inclusiveness in nature and co-operative working environment. Prior to Industry 5.0, mass customization was possible with the help of automation and the use of advanced digitalized technologies, including artificial intelligence, the Internet of Things, and Machine Learning, but more was needed. In the present context, the end users prefer mass personalization with the human touch. Thus, Industry 5.0 offers them the choice of mass personalization against bulk customization. It affords the consumers a product that is tailored to their personalized requirements. The industrial revolution refers to the interplay between humans and machinery that has improved and enhanced human capabilities without replacing them while economizing on the time invested in doing so. Robots are now fast replacing the hitherto labor-intensive jobs of loading, unloading, painting, welding, etc. [1].

Personalization is the most crucial component of Industry 5.0. It stipulates the strategy and manufacturing of numerous sensor data directly integrated to provide team members

with real-time customized facilities [2]. Industry 5.0 endeavors to strengthen global cyber infrastructure by establishing a secure and confidential atmosphere for innovative practices. The use of artificial intelligence in various applications, artificial neural network concepts under the realm of deep learning, peer-to-peer decentralized access via block chain, big data concepts, and machine learning experiences based on AI techniques are prioritized technological aspects to strengthen Industry 5.0. Information extraction through sensors and actuators in IoT, open-source software for application development and service access, meaningful information extraction through data science, on-demand services through cloud computing, and virtual, augmented, and mixed reality are the most relevant technological advancements proposed to fulfill the goals of Industry 5.0 [3–7].

Figure 1 depicts digital transformation and its links to Industry 5.0, which refers to the expansion of new technological platforms that have significantly transformed the quality processes. This necessitates a high level of adaptability in order to satisfy the demands of patients and provide realistic, innovative solutions [8,9]. Industry 5.0 provides enhanced service design for controlling health hazards and meeting diverse organizational objectives. A case in point here is the manufacturing of tailored PPE kits during COVID-19. This is an example of personalization wherein the firms could fulfill the burgeoning demand for PPE kits easily by employing the current manufacturing technology [10].

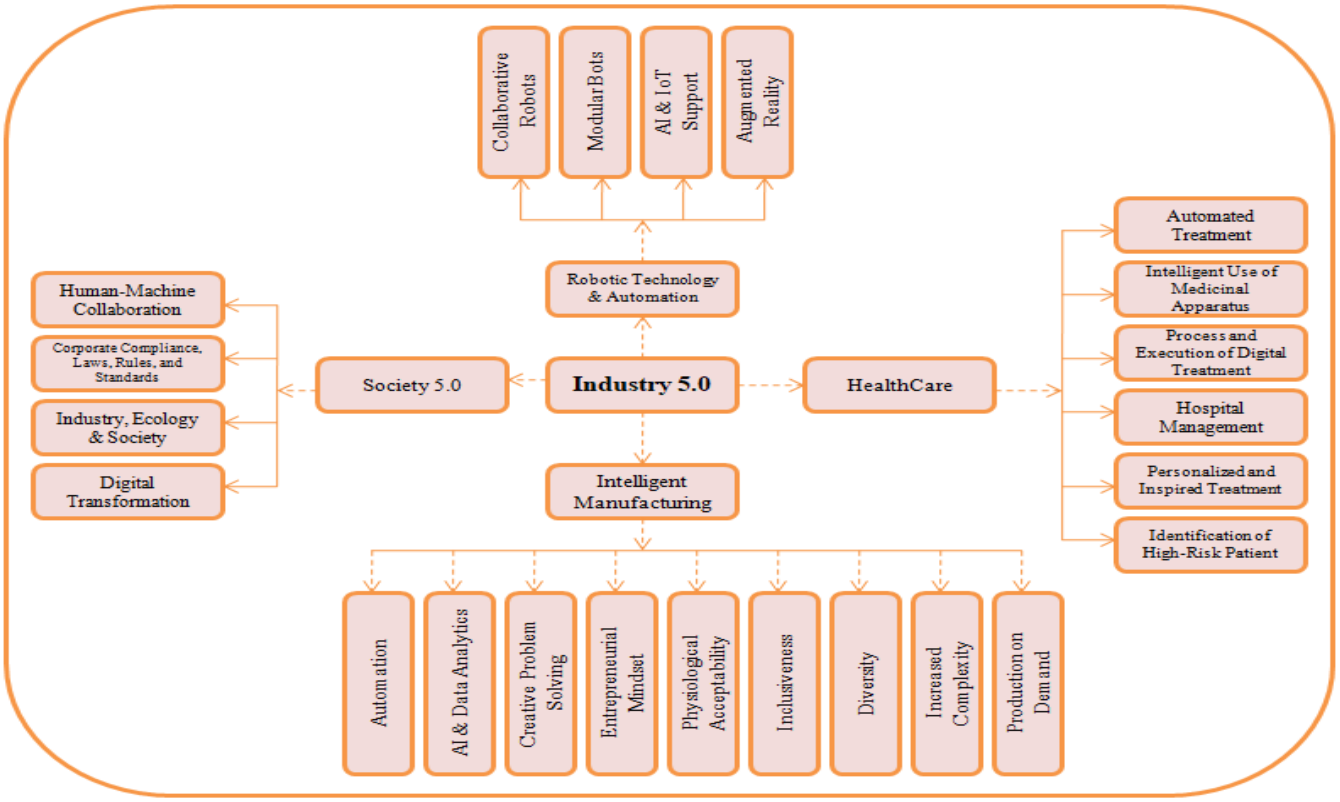


Figure 1. Linking the digital transformation of Industry 5.0.

Industry 5.0 goes one step further by combining increasingly precise and powerful machinery with the distinctive creative capacity of human beings. More specifically, this article also highlights personalized services in pandemic situations while focusing on personalization and risk assessment in healthcare concerning Industry 5.0. One of the crucial phases of the risk management process is risk assessment, which is more focused on mass personalization. The purpose of risk analysis is to recognize and comprehend the risk better. The sources of risk, their effects, and the possibility of how these effects would materialize are all considered during risk analysis in healthcare. Hence, the authors of this

study targeted the risk assessment at the initial level with a strong strategic intention for a better, safe, and risk-free life for the patient [11].

The risk estimation process is responsible for delivering an ideal path to protect the assets. In this league, the proposed methodology for risk profiling in the present study has been envisioned to achieve the following:

- The identification of the basic functionality and risk factors in the healthcare system based on Industry 5.0, considering security standardization and systematic evaluation process.
- Assessment requires possible standard threats to quantitatively assess to measure the impact and future possibilities for healthcare systems.
- Mitigation is the remedy of risk by comparing the proper scaling of impact. It allows for the establishment of a proper correlation between various attributes of Industry 5.0 with healthcare security factors.
- Prevention promotes proper countermeasures and preventive techniques for identifying and mitigating risks with respect to healthcare Industry 5.0.

Furthermore, the paper has been meticulously structured as follows: Section 2 provides contextual findings and the research gap. Section 3 profiles an in-depth discussion on the need for and importance of Industry 5.0. It also focuses on the urgent requirement of transition from Industry 4.0 to Industry 5.0 in healthcare services. Section 4 provides a detailed data analysis of security breaches related to the healthcare industry. Section 5 tabulates the generation of diverse security risk assessment factors and threats pertinent to their related attributes in the healthcare industry 5.0. It also provides a symmetrical solution based on past research experiences aligned with the proposed problem statement. Section 6 outlines the proposed methodology concerning the necessity of Industry 5.0 in healthcare perspectives and further elucidates the development of the Security Risk Assessment Framework for Healthcare Industry 5.0 ($SRVF^{HI5.0}$). Section 7 details the validation of the proposed framework and statistical analysis that was performed to achieve objectivity. Finally, Section 8 entails a concise yet comprehensive analysis and discussion to conclude this study.

2. Contextual Findings and Research Gap

Achieving improved healthcare goals, including patient care support, drug manufacturing, digital healthcare data analysis, and healthcare data security, requires incorporating innovative practices and support from all stakeholders to strengthen the healthcare system. In this league, Industry 5.0 is spreading rapidly into the health systems in India, motivated by a goal to decrease costs, enhance efficiency, and boost public awareness of health concerns. Information systems, particularly for the healthcare Industry 5.0, are designed, developed, implemented, and administered as a component of health information technology [12].

Security is a critical concern for all businesses; the security of business operations is the key to an enterprise's success. A security estimate is essential for evaluating performance and the level of protection. Unnecessary threats exploit hardware and software bugs or vulnerabilities jeopardize availability, integrity, confidentiality, and non-repudiation. Breaches and disruptions may also expose other security components such as authentication, privacy, and encryption. Risk assessment involves numerous phases, including identifying, quantifying, and prioritizing information security threats, which vary depending on risk management approaches. Some risk management models have been identified in the literature and are listed below:

- Information security risk assessment;
- Fuzzy comprehensive evaluation method;
- Analytic hierarchy process;
- Bayesian network;
- Decision-making trial and evaluation laboratory method

Major findings from the literature survey can be summarized as follows:

- Precision healthcare, intelligence-based infrastructure and artificial-enabled medical equipment enhance human accuracy in the healthcare business and enable patients to receive highly effective, individualized treatment methods. Industry 5.0 journeys in the healthcare industry are just getting started. Computer-generated care, isolated patient intensive care, and AI-integrated medical devices are just the beginning [13,14].
- A feasibility study is a way to determine if a health service is possible, whether it is an expansion of an already-running business or a new project. This study is a crucial step in the process of strategic planning. The hacker may access private patient information. Additionally, the attacker may change patient data mistakenly or intentionally, which could negatively impact the patient's health [15].
- Quantification is an unavoidable feature of our current technological environment. The GPSs, satellites, computers, and networks that enable us to live are all connected via a sophisticated technical infrastructure. Healthcare is not achieved d by completing a different set of activities within the margins of a known space (the clinic or the ambulant) but rather as a dataset combined into an organization that treats and manages all features of life (health, law, relaxation, work, and social relations) [16].
- Industry 5.0 is the culmination of the best possible integration of big data, AI, the IoT, cloud computing, COBOTS, innovation, and creativity. Industry 5.0 is predicted to generate higher-value employment with greater latitude for design thinking and innovation. It aids in raising labor productivity and provides more scope for customer customization [17,18].
- Human–machine interactions are essential to the success of the industrial revolution because it makes personalized services possible and moves us towards a more advanced awareness of Industry 5.0. Industry 5.0 is being implemented more extensively to accommodate highly personal requirements and build a virtual environment with cutting-edge computers and information technologies [19–22].
- From the literature review, a COVID-19 case study is being used to compare the healthcare system to Industry 5.0. In the case of highly contagious diseases such as COVID-19, risk assessment was valuable for devices designed for automated operations. It was helpful in tracking infected patients and providing life support, such as through online counseling and revealing the availability of beds, drugs, vaccines, and other amenities. Personalized patient body screening, online reporting of medical tests, online data collection, and secure storage and tracking are highly advanced concepts related to the healthcare industry with optimized security requirements and security solutions. Creating more cognitive technology to provide better instruction for automated technology is highly required [23–25].
- Industry 5.0, which is capable of rejuvenating human creativity and craftsmanship in production while embracing automation and robotic collaboration to assist employees, is likely to upend this. Applying a human-centric approach as a key aspect of Industry 5.0 focuses on healthcare security with reduced threats and security risk, advocating a security-by-design approach in Industry 5.0 [26,27].

It is evident from the literature survey that healthcare security risk assessments concerning Industry 5.0 are still in their infancy. A considerable effort is being made in relation to threat analysis and security risk estimation for healthcare systems that can proactively address the potential threats and mitigate security risk for better allocation of resources for security measures based on Industry 5.0.

From the aforementioned references, it is evident that security measures for various threats and security risks for the interconnected systems in Industry 5.0 that specifically focus on healthcare are key factors for the successful delivery of a secure system. Therefore, there is an urgent need to develop a mechanism for security risk estimates correlated with healthcare Industry 5.0. To meet this requirement, the study identifies various threats and security risks and develops a framework for security risk assessment based on Industry 5.0.

3. Why Industry 5.0?

Industry 1.0 started in the early 1700s when steam and machines were used for the first time. During this time, machinery in the spinning industry caused output to increase by a factor of eight. Steam was a vital part of this revolution, which led to more production and better efficiency in many businesses. During this time, steam power replaced human physical effort in the spinning industry. In the nineteenth century, electricity was utilized as a leading power source in industry. This was the beginning of the era of Industry 2.0. One of its advantages is the ease of using electricity over steam and water. This feature enabled the power supply to be used in several applications. Throughout this time period, management tools, in addition to the arrival of electricity, improved the performance and efficiency of enterprises. The major collaborative components that enabled the 20th Century's Industry 3.0 were the semiconductor industry, digital circuits, programmable integrated circuits, communications, wireless communications, renewable energy, and automation. The most significant downside of Industry 3.0 was that automated solutions could fail under various conditions.

Industry 4.0 emerged in the twenty-first century, focusing on all industries through the application of intelligent systems. ML (Machine Learning) is positively helping the fourth industrial revolution. Some of the revolution's successes are fully automated systems and AI systems that work in unexpected places. One of the problems with Industry 4.0 is that it needs to have fully expert systems for industries. Another problem is that all the data in the cloud could be hacked. Industry 4.0 makes use of mathematical concepts such as optimization and network theory. Michael Rada coined the phrase "Industry 5.0". The use of collaborative robots to assist in risk management is one of the most essential features of Industry 5.0. Robots are designed to recognize, comprehend and perceive the human operator along with the job's objectives and expectations. Figure 2 depicts the industrial evolution journey from Industry 1.0 to 5.0.

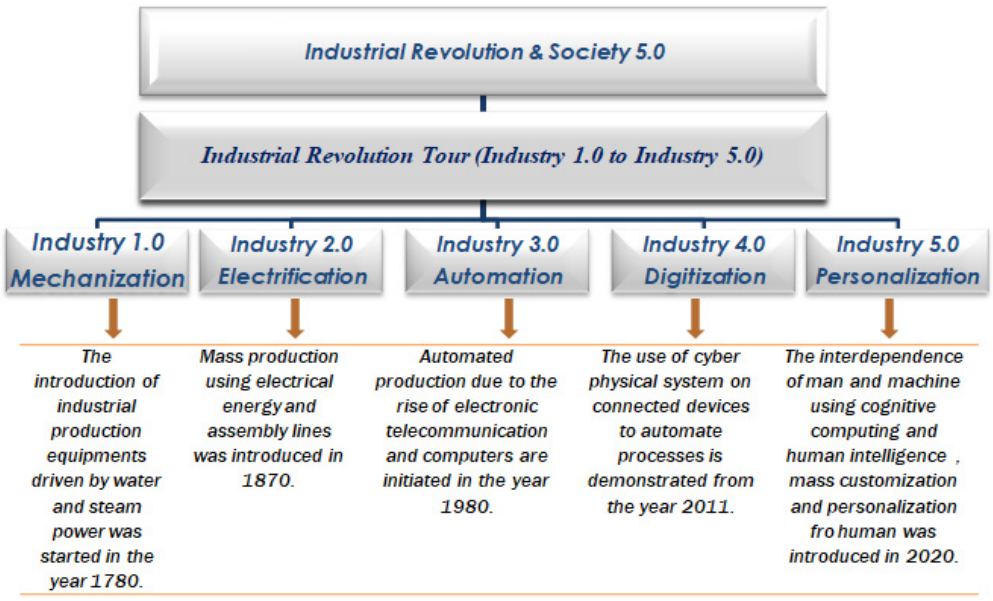


Figure 2. Industrial evolution [28].

Need of Migration from Industry 4.0 to Industry 5.0

Industry 4.0 mostly worked on customizing things and did not offer individualization or personalization services. There was a gap in Industry 4.0 for personalization, and one more major shortcoming of Industry 4.0 is believed to be full automation with complete dependency on machines. According to the survey or data, full automation is harmful to human life. Aljazeera, 2020, reports more than 400 crashes have been caused by self-driving

vehicles due to a lack of human control. Due to full automation, crashes and the death rate increase daily [29].

The US's new Advanced Driver Assistance System (ADAS) report says that from July 2021 to May 2022, there were 367 accidents. According to the Tesla report, 80,000 vehicles with self-driving assistant program cars with a trial control over speed reported 273 crashes on 15 June 2020. If these incidents increase, there will be more possibilities for collisions, and the death rate will increase. Therefore, Industry 5.0 has been prioritized over Industry 4.0 due to humans' involvement in providing more support and possibilities to reduce mechanical disasters through human and software-enabled intelligent observations to provide optimal control [30].

The level of collaboration between machines and humans is dynamic and highly correlated with machine intelligence in the workforce and a substantial proportion of manufacturing processes. The goal of Industry 5.0 is to create value that goes beyond financial gains. The purpose of Industry 5.0 is to raise society's standard of living, not just for those who work in the industrial sector [31].

4. Industry 5.0 for Healthcare Systems

As per the European Union (EU), Industry 5.0 promotes the vision of industries beyond their efficiency and productivity. The major objective is to improve the industrial sector's purpose and value in society. Industry 5.0 is a notion that goes beyond the definition of "industry". The well-being of workers is placed at the center to respect the world's manufacturing boundaries through new technology to create jobs, growth, and revenues.

Industry 5.0 represents many more applications than Industry 4.0. When assessing the strategic implications of Industry 5.0, it is necessary to have an extensive and universal view that applies to all industries. The European Commission recognized resilience, sustainability, and a human-centric approach as the three essential components of Industry 5.0. All three have a big influence on company strategy. Society 5.0 is a significant revolution that began in Japan and could potentially change society. It is concerned with putting the human being at the center of technological and innovative modification for the benefit of mankind. The main purpose of Society 5.0 is to improve people's quality of life by exploiting the possibilities of Industry 4.0 [32].

Industry 5.0 may improve production quality by transferring repetitive, boring tasks to robots, machines, and roles that require critical thinking. Because intellectual practitioners engage with technology, Industry 5.0 encourages more skilled enterprises than Industry 4.0. The main motive of Industry 5.0 is personalization and individualization, especially in the healthcare sector, because Industry 5.0 completely fulfills the individuals' requirements. That is why the fifth industrial revolution is more important than previous revolutions. The primary objective of Industry 5.0 in the healthcare industry is to further enhance human life security in pandemic scenarios and everyday life. Mass personalization with a human touch is an essential component of the healthcare industry for the current environment, with a paradigm shift from mass customization to personalization. Digital transformation will substantially improve quality, safety, and waste reduction. In this context, Figure 3 below illustrates the industrial revolution targeting healthcare operations from Industry 1.0 to Industry 5.0. Industry 5.0's system architecture in the healthcare sector uses 5th-generation connectivity as the backbone for connecting healthcare devices. The Internet of Things (IoT) provides data so that artificial intelligence can be used to support digital interests. This impacts patients' well-being and quality of life and the convenience and welfare of individuals in communities worldwide. The role of artificial intelligence in Healthcare Industry 5.0 helps to encompass systematic illness prediction, digital diagnosis, robotic surgery, patient surveillance in virtual mode, and AI therapy to facilitate society. It offers effective data processing and analysis for medical data and provides support through online courses for treating social anxiety sufferers and many more [33].

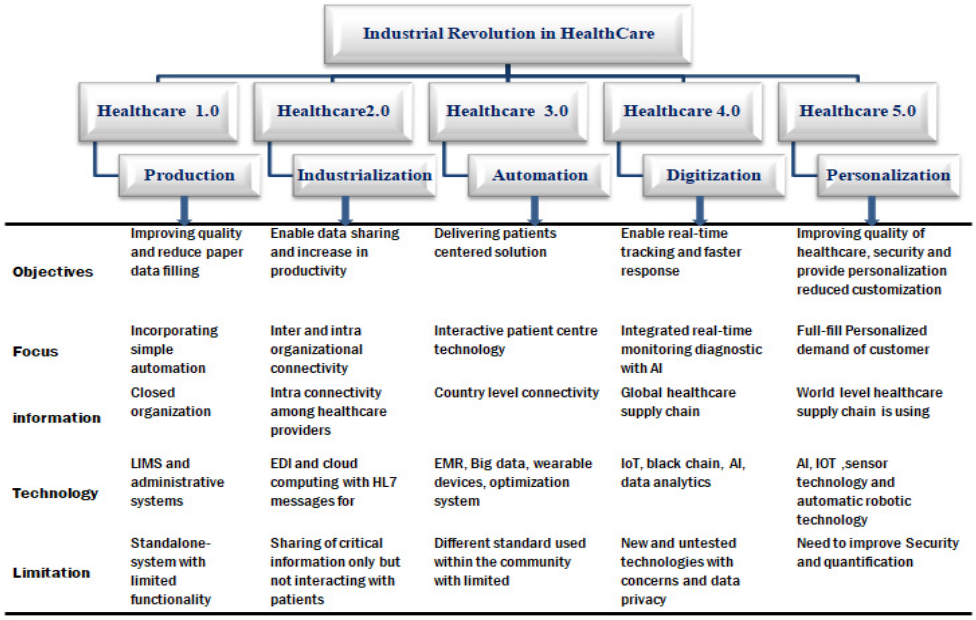


Figure 3. Evolution of industrial revolution in healthcare.

The healthcare industry is one of the leading reasons for increased market share. Because of sedentary lifestyles and a significant expansion of the senior population, the prevalence of lifestyle illnesses has risen in tandem with age-related disorders. This has increased the healthcare industry's need for 3-D clinical imaging devices.

Furthermore, technical advancements, along with increasing awareness of the benefits of this generation, such as the accurate visible portrayal of inner organs, less injury to surrounding tissues, and accuracy of data offered by various clinical imaging systems, have propelled market expansion. Governments worldwide are also pushing the market with increasing healthcare budgetary allocations and research and development (R & D) initiatives. The major driving technologies related to Industry 5.0 are shown in Figure 4. The comparative chart between Industry 4.0 and Industry 5.0 based on security analysis from the healthcare perspective is displayed in Table 1.

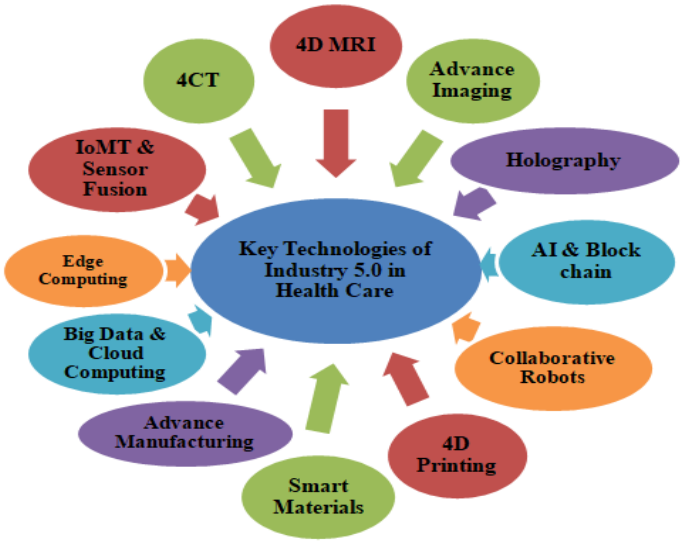


Figure 4. Major driving technologies of industry 5.0 in healthcare.

Table 1. Comparative chart based on security analysis for healthcare.

S. No	Security Analysis for Healthcare	Industry 4.0	Industry 5.0
1	Focused on smart manufacturing systems, mass production, working, and smart supply chain	√	X
2	Focused on the sustainability, human centric, environmental responsibility, and social benefits	X	√
3	Working on real-time monitoring and integrated chain	√	
4	Focusing on utilization of ethical technology for human value	X	√
5	Human reliability, human–computer interaction, and repetitive environments	√	
6	Utilization of Automation Technology	X	√
7	Automation, information	√	
8	Digital transformation	X	√

4.1. Data Breaches in Healthcare Industry

Data breaches are one of the most critical concerns in the current scenario. A "data breach" refers to confidential or protected data accessed by an unauthorized user or third party with malicious intent. Data breaches directly impact the user's confidence and relationship with their associations; moreover, the associations' status, characteristics, and fair price are all affected. Every year, thousands of people are affected by data breach incidents due to an organization's data being transferred over the internet, and confidential business data are stored on servers that may connect tolocal networks in ways that are not secure from attackers. As a result, most cybercriminals targeting the corporate sector or government agencies have more accurate information or financial information related to their credentials.

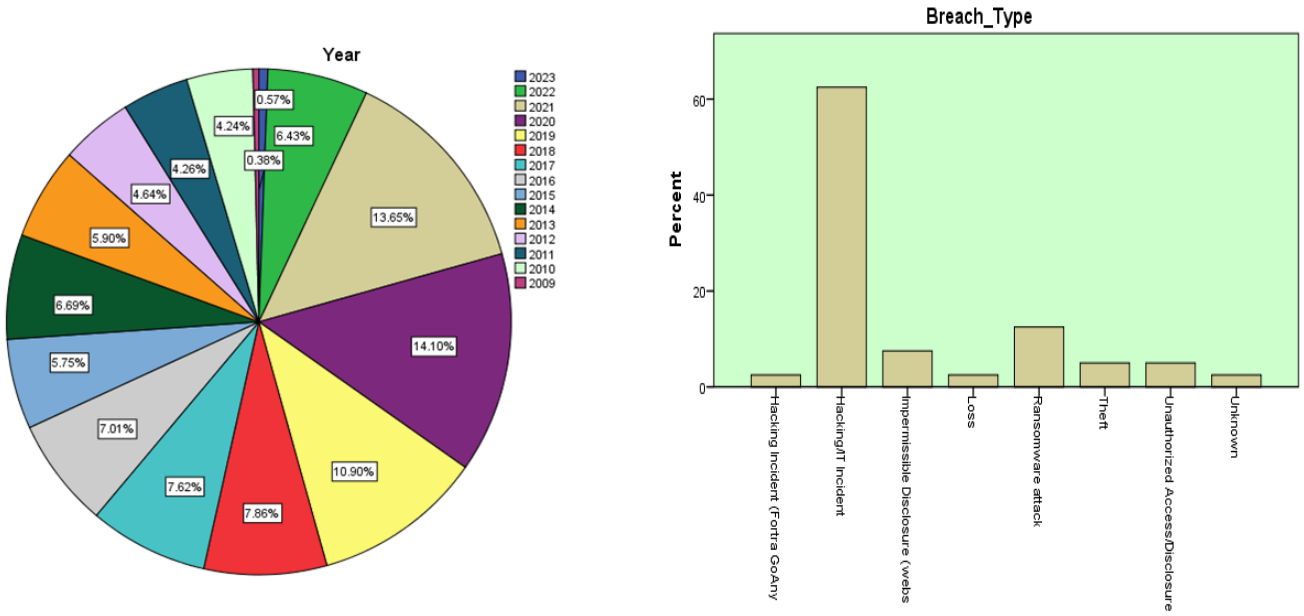
In recent years, there has been an increase in the number of events involving data breaches in the healthcare industry. Unauthorized access to customer data is particularly common in the healthcare industry. According to the HIPAA Journal, between 2009 and 2020, 3705 breaches involving 500 or more healthcare records were reported to the HHS Office for Civil Rights. In 2015, one of the most significant healthcare data breaches in history exposed the personal information of nearly 78.8 million people, according to Anthem, Inc., Indianapolis, IN, USA. The information stolen from the users included names, social security numbers, home addresses, and dates of birth. The healthcare industry was the source of most of 2015′s data breaches [34].

Based on HIPAA data breach complaints, an analysis found that the most common types of data breaches involve hacking, illegal internal access, theft or loss, and the wrong way of getting rid of redundant data. Bit Glass looked at HHS data on hospital breaches and found that more than 500 data breaches were reported in 2020. In 67.3% of all cases, hacking and IT incidents were the most significant risk.

Theft or loss, as well as unlawful disclosure, are other significant factors. There were over 55% more accidents overall in 2020 than in 2019. An unofficial or unauthorized user gained access to the health data of approximately 3.3 million people in one of the primary healthcare data breaches reported in 2020. In 2021, Trinity Healthcare faced one more incident in which the health-related data of 586,689 patients were unguarded; likewise, 1,290,670 people were affected by the data breaches that occurred involving MEDNAX Services. Another major incident involved an attack on the Inova Health Organization that exposed the personal information of 1,045,270 people. Northern Light Health, Dental Care Alliance, Health Share of Oregon, Elkhart Emergency Physicians, Inova Health System, Florida Orthopaedic Institute, and Luxottica of America are a few more examples of data security breaches in 2020.

4.2. Breaches of Healthcare Data by Year

The HHS Office of Civil Rights reported 4419 data breach reports between 2009 and 2021 based on healthcare services that affected more than 500 records. In total, 314,063,186 healthcare records have been reported due to breaches, and most of them were compromised due to being lost, stolen, shared without permission or exposed. It was found in 2018 that one documented healthcare data breach is responsible for affecting 500 or more records. The rate has increased in only four years. Five hundred or more daily records were compromised in the 1.95 healthcare data breaches reported in 2021. The affected cases of healthcare data breaches with their types on daily occurrences from 2021 to 2023 are depicted in Figure 5a,b.



(**a**) (**b**)

Figure 5. (**a**) Records of data breaches in healthcare (**b**) types of data breaches in healthcare [35,36].

4.3. Exposure of Healthcare Records by Year

It has been observed that the records are generally increasing year over year and experienced a sharp increase in 2015. The reported records of data breaches due to leaked, stolen or improperly shared in the year 2015 are more than 1113.27 million. Figure 6 reports the records of healthcare data breaches related to 2015 and other significant data breaches related to healthcare insurance companies that are also serious.

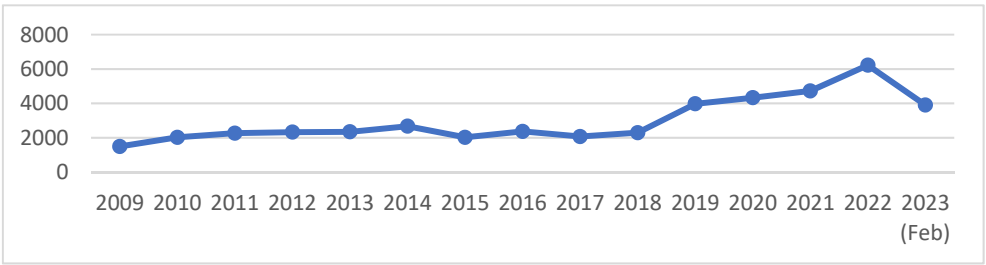


Figure 6. Average size of healthcare data breaches [36].

4.4. Top 10 Healthcare Data Breaches Reported by Office for Civil Rights (OCR)

The most significant healthcare data breach reported in year 2022, HHS, reported more than 590 healthcare organization data breaches that may have affected up to 48 million people. Five hundred ninety entities informed the HHS Office of healthcare data breaches

in December 2022. Furthermore, 48.6 million people were affected by data breaches in 2022 compared to 2021, when 40 million data breaches were recorded, as shown in Table 2. Healthcare information security has confirmed a list of the most significant data breaches reported to the OCR [37].

Table 2. Healthcare data breaches reported by Office for Civil Rights (OCR).

S. No	Year Wise	Number of Incidents	Company Name	Cases Reported by	Case Regarding	Security Threats	Reported to
1	2022	48.6 million	HHS	590 Healthcare organizations	Healthcare information breach	Hacking/IT incident	OCR
2	2022	423,624	One Touch Point (OTP)	35 different healthcare organization	Patient metadata	By third mailing party	OCR
3	March 2022	360,000	TTUHSC	Numerous organizations have reported	ECL	Google meta data	OCR
4	Oct. 2022	3 million	AAH	Arora healthcare organization	Company used tracking pixels from Google	Metadata	OCR
5	2022	2,000,000	Shield Healthcare Group	Massachusetts-based healthcare organization disclosed to HHS	Patient personal data	Unauthorized access	HHS
6	2021	1,918,941	PCF	Professional Finance Company	Metadata	Hacking/IT incident	OCR
7	2021	1,608,549	Baptist Medical Centre	Baptist Health System.	Patient Metadata	Unauthorized access/disclosure	OCR
8	2022	1,500,000	CHN	Community Health Network	Metadata	Using third-party tracking technology	OCR
9	2021	10,362,296	Novant Health	Novant Health Organization	EHR	Unauthorized access	OCR

5. Healthcare Related Threats, Security Risk and Symmetrical Solutions

This section examines the healthcare threats and security risks associated with the various stages of the healthcare security process. Thereafter, the section underlines the symmetrical solutions related to security risk assessment for the healthcare system. Furthermore, mathematical modeling to estimate the most prioritized values for deeper impact analysis has also been undertaken. The contemporary study related to healthcare security based on Industry 5.0 is accountable for enabling advanced technological support and the development of innovative practices for risk estimation and analysis.

5.1. Healthcare Security Risk

Industry 5.0 in healthcare needs high-quality, custom-made implants that can be changed and last long. The goal of Industry 5.0 is to resolve problems like too much production, needing more transparency, and choosing the wrong tools. This revolution will influence product dependability, product lifetime, profit, efficiency, service and business models, information security, the environment, machine and human safety, and IT security. In fact, a pandemic like COVID-19 requires various customization concerns that directly and indirectly influence society. These challenges have prompted answers within Industry 5.0 to different healthcare hurdles through advanced assistance and suitable analysis using ICT-enabled supports and tools. The following issues and their practical solutions are as follows:

- Tracking of COVID-19;
- Transparency in treatment;

- Tracking of crowded places;
- Performing automated treatment;
- Intelligent use of medicinal apparatus;
- Process and execution of digital treatment;
- Hospital management;
- Personalized and inspired treatment;
- Identification of high-risk patients.

It is known that workdays in the healthcare industry are very hectic, highly regulated, and sometimes understaffed. This challenging environment has possibilities for minimal error space. The adverse impact may harm the organization's reputation, operational activities, and profits. Security risk assessment mechanisms are capable of identifying, analyzing, and estimating critical security measures in applications. They are also helpful for risk containment by controlling bugs and vulnerabilities within the applications and at the design level. After the successful implementation of a security risk assessment mechanism, an organization can comprehensively understand the application portfolio from an attacker's perspective. The patient's well-being is of the utmost significance in healthcare, which is increasingly dependent on medical systems and technology. Security threats involved in healthcare procedures are depicted in Figure 7.

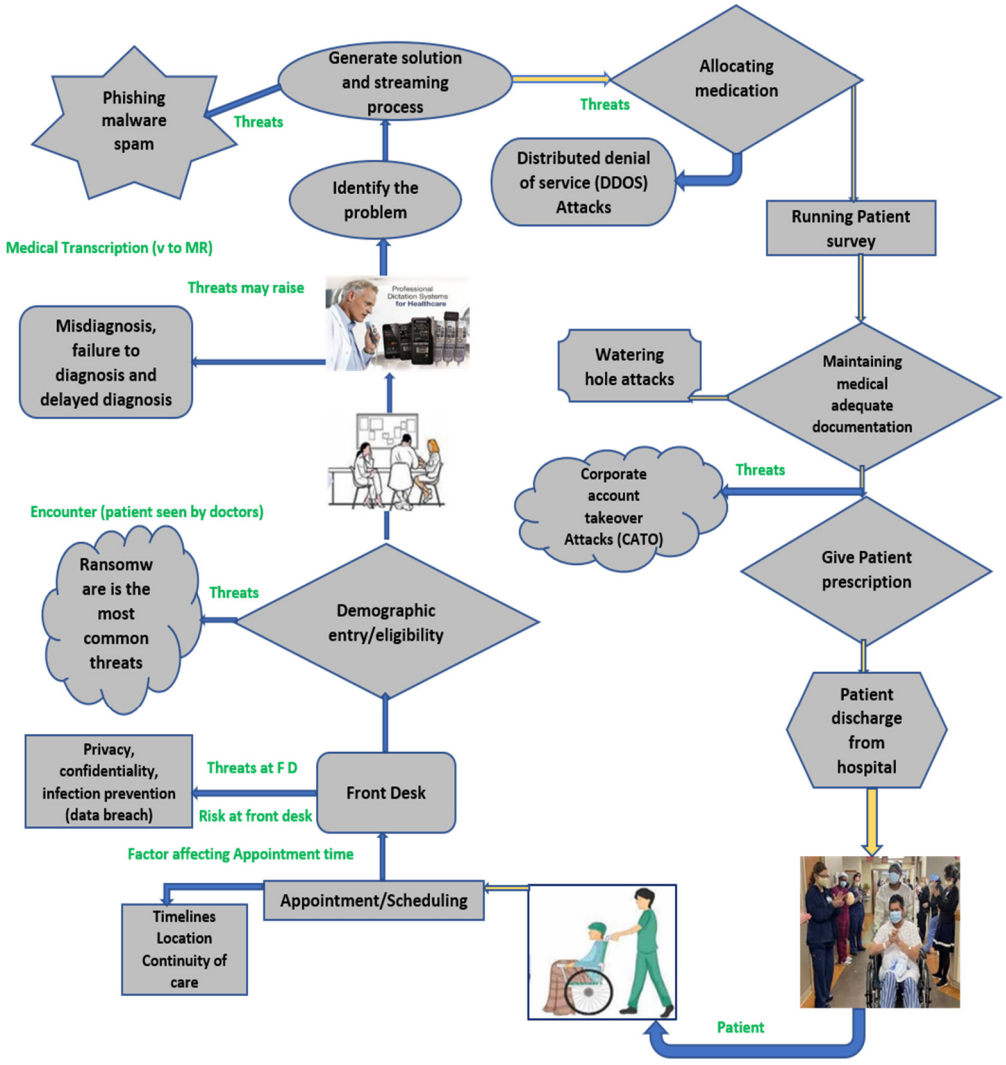


Figure 7. Security threats involved in healthcare procedures.

Treating patient through proper advanced tools with an integrated digital environment and supportive care may have greater possibilities in terms of healing diseases. Cyber-

attacks on the systems or devices that use the protected health information (PHI), or personal identification information (PII) of patients or other related data may compromise patient safety and privacy. Using ransomware, the applicability may be compromised or unable to access medical devices and medical records. It steals information from the encrypted files and leads attackers to mistakenly or intentionally change the patient's data, severely endangering the patient's health. In this way, the attackers achieve control over the devices or system and get full access to Personal Identification Information (PII), Protected Health Information (PHI), and other data to compromise patient safety and privacy. Losing access to medical devices and records can encrypt and capture files like a ransomware attack. The other common risks to healthcare sectors are as follows, which need to be addressed concerning Industry 5.0:

- Corporate compliance, laws, rules, and standards;
- Eligibility requirements for Medicare;
- Confidentiality and privacy (data breach) identification;
- Anomaly detection on medical records;
- Personnel, qualifications, and staffing;
- Patient's rights;
- Managing medications;
- Controlling and preventing rate of infections;
- Reporting abuses;
- Environmental safety and protection.

Security Threats in the Healthcare Sector: The top five healthcare security threats for 2021 include ransomware, botnets, cloud misconfigurations, web application attacks, and phishing. Due to the COVID-19 epidemic, stakeholders rushed to enable the remote delivery of healthcare services. It may lead to cyber-attacks targeting the healthcare industry and increased cyber incidents. According to security firms and researchers monitoring the sector, healthcare providers are increasingly the target of ransomware, online application attacks, phishing scams, and other threats [38].

The Growing Ransomware Threats: Since the start of the worldwide COVID-19 outbreak, ransomware has emerged as one of the most significant cyber risks to the healthcare industry. Attackers have found that hospitals and clinics providing essential, life-saving services can be more easily blackmailed than ransomware victims in almost any industry. Several healthcare institutions are increasingly vulnerable to attacks due to new digital tools and services. Between January 2020 and February 2021, 293 publicly reported healthcare data breaches were the subject of analysis. In roughly 55% of breaches where a root cause was discovered, ransomware were found to be the main culprit.

Cloud Flaws and Configuration Errors: 53% of the 790 healthcare IT researchers surveyed by Infolox said that their organization had been the victim of a data breaches related to the cloud in the past year. In March, it said two cloud servers had been broken into and used to steal protected health information from about 50,000 people in the Medicare and Medicaid programs. In August of last year, private information about more than 3.1 million patients was found in an unprotected cloud database that was thought to belong to a company that makes software for managing patients.

Web Application Attacks: Web application attacks aimed at healthcare workers have drastically increased lately due to COVID-19-related activity. In December 2020, web application attacks on hospitals and other healthcare targets increased by 51%, according to security vendor researchers. The attacks continued a pattern that Imperva claims will last until 2020. In 2020, the business community estimated that healthcare organizations would be the target of an astounding 187 million monthly attacks. Healthcare organizations saw 498 attacks per month on average last year, a 10% rise from 2019. The most frequent types of attacks were:

- Cross-site scripting;
- SQL injection;
- Assaults involving protocol manipulation;

- Remote code execution or remote file inclusion.

Botnets: Malicious bots, which aim to steal data from websites, disseminate spam, or download harmful software, are also significant challenges in the healthcare industry. According to Ray, the healthcare sector has a particular issue due to bot traffic. Bots might be responsible for content scraping, account creation, account takeover, and other types of fraud from a security standpoint. There have been countless instances where fraudsters have stuffed credentials into bots and cracked passwords to access accounts [39].

Phishing: The healthcare sector is seriously at risk from phishing attacks, just like businesses in almost every industry. A recent study by Palo Alto Network's Unit 42 team of researchers found that between December 2020 and February 2021, the number of phishing attempts involving or aimed at pharmacies and hospitals rose by 189%. In fact, vaccination-related phishing attempts surged by 530% within the same time period. In a poll of 168 healthcare cyber security specialists conducted by the Healthcare Information and Management Systems Society (HIMSS) last year, 57% of participants reported phishing attacks in their organizations. In contrast, 20% claimed other social engineering assaults had occurred [40].

Prior to that, it is essential to recognize the healthcare sector's difficulties from various angles. The list given below has some challenges healthcare service providers face in their current situation [12,31].

- Utilizing cutting-edge medical technology;
- Cyber security;
- Changes in healthcare regulation and services;
- Issues regarding payment and invoice processing;
- Drug price optimization issues;
- Issues for integrated healthcare services;
- Lacking of healthcare staffs;
- Global business upheaval;
- Drug outbreak.

Since the data include private information about the user's health, finances, and personal life, hackers often go after the healthcare industry. It also has personal information that can be used to pose as the user and blackmail or hurt the client in other ways. Additionally, private medical information about diseases that can kill or spread through sexual contact can make the user or patient feel bad. The main problems facing businesses in terms of data breaches include the following:

- Possibility of harming reputation;
- Identity crisis issues;
- Consumer loss issues;
- Issues of trust failure.

According to a research organization, Ponemon, working on data privacy, data protection and information security policies, the average cost of healthcare data breaches was USD 429 in 2019 and USD 499 in 2020. As data collection expands, future expenses will rise. Similarly, it takes healthcare organizations 236 days to recover from breaches and approximately 96 days to identify them, the most prolonged recovery period compared to other industries. It is also necessary to note that the personnel of the affected firms deal with heavy workloads, unfavorable criticism, emotions, and angry customers.

5.2. Symmetrical Solutions

Symmetrical solutions are responsible for generating a roadmap through the proper analysis of contemporary research in the proposed area. The main focus is to find the appropriate solutions based on similar conditions. This step is responsible for enlightening authors to fill their research gap through these best practices. The best practices suitable for these solutions are as follows:

An article entitled "The Panorama between the COVID-19 Pandemic and Artificial Intelligence (AI): Can it be the Catalyst for Society 5.0?" focuses on artificial intelligence and developing robotics technology to treat COVID-19-infected patients. Quick information on illness dynamics provision understanding the patterns of disease onset offers practical advice for decisions and interventions in prevention and care. Super-intelligent, human-centered "Society 5.0" is a notion of society. It offers a remedy for upcoming technological developments as well as the rising use of robotics, (IoT), and big data analytics with an AI focus [41].

A research article explored the collaboration between human intelligence and cognitive computing in the published paper "Value-Oriented and Ethical Technology Engineering in Industry 5.0: A Human-Centric Perspective for the Design of the Future" in June 2020. It is directly related to providing computerization as a supplementary improvement to human bodily, sensory, and intellectual abilities by placing people at the center. I5.0 is fundamentally restructuring human responsibilities in terms of manufacturing so that workers can profit. This article focuses on value-sensitive design in the industry 5.0 era and presents a conceptual study with technical and empirical observations [42].

An IoT-based cyber risk mitigation plan was introduced by Nicole M. Thomasian and Eli Y. Adashi to ensure patient safety by validating robustness of medical Internet of Things technologies. A regulatory framework designed for IoT Device Cyber Security Capability Core Baseline Principles by the National Institute of Standards and Technology is responsible for addressing cyber security issues in IoMT, including malfunctioning devices, enhancing physical security and breach detection [43].

A research article in *Risk Management and Healthcare Policy* published by Dove Press entitled "Security risk assessment of healthcare web application through adaptive neuro-fuzzy inference system: a design perspective" evaluated the assessment of security risks using soft computing techniques to enhance the healthcare security of web applications to a great extent. The applied mechanism is fruitful in terms of avoiding security risk factors in healthcare web applications to enhance data security and provide a roadmap to developers and security experts for higher security risk factor identification and impact analysis [44].

Symmetrical solutions represent a development pathway to protect healthcare systems from various threats to the application. The most prioritized agenda is to identify security risks, develop preventive steps and provide suggestive measures to mitigate them for greater security. It provides direction for the development of a perspective framework for healthcare security risk assessments with respect to Industry 5.0.

6. Development of Security Risk Assessment Framework for Healthcare Industry 5.0 ($SRVF^{HI5.0}$)

The results from the literature review represent a roadmap, highlighting technological advancements with greater emphasis on the integration of healthcare systems with Industry 5.0. It discovers security risks associated with healthcare processes, including issues related to data privacy and security, data protection measures, personalized healthcare and enhanced collaboration and healthcare regulatory compliance challenges while allowing for the effective integration of healthcare systems with Industry 5.0. This roadmap resulted in the practical development of a perspective framework for risk assessment in healthcare industry 5.0. This will lead to a focus on the systemization of issues, which requires a deeper realization of developing strategies related to security risk evaluation in healthcare Industry 5.0 [45].

This kind of framework is not available for the assessment of security risk in the case of Industry 5.0 as per the healthcare system. In the absence of any standardized framework, the author has made a unique effort to develop a perspective framework to correlate healthcare security risks with Industry 5.0, which can be used by practitioners working in the area of healthcare security.

It discovers healthcare issues related to data privacy and security, data protection measures, personalized healthcare, and enhanced collaboration and healthcare regulatory

compliance challenges while effectively integrating healthcare systems with Industry 5.0. The proposed framework will help to address these issues at the earliest possible time. The information received from this stage will provide a strong basis for the factorization of attributes related to healthcare security and Industry 5.0.

The framework: A reliable security risk assessment for healthcare issues is highly desirable from an Industry 5.0 perspective. A literature review reveals that more significant, precise, and prominent needs to be published in this domain to sufficiently correlate healthcare issues with Industry 5.0 safety risks. The techniques provided are either theoretical or best practices. Therefore, in the absence of any framework or model for security risk assessment, developing a methodology for risk assessment of healthcare issues concerning Industry 5.0 is worthwhile. The proposed framework encompasses the following steps, as discussed in detail in Figure 8.

- **Identification and Conceptualization:** The primary phase of any problem-solving activity is directly related to conceptualization, which identifies the significant problems, optimized solutions and the process for implementation. It is also responsible for recognizing the significant healthcare security issues with Industry 5.0. It will help to uncover the most appropriate components and attributes through a retrospective review of the available best practices, consolidated rules, and architectures to develop their technological aspects;
- **Security issues based on healthcare:** The primary responsibility of this phase is to investigate various components of healthcare. Recognition of security-related problems based on healthcare services is a crucial phase activity. Some of the prominent security issues related to healthcare and industry 5.0 have been reviewed in the literature, and a commonly accepted set is mentioned here. The common security issues related to healthcare are data breaches, ransomware attacks, phishing, insider threats, regulatory compliances, data encryption and physical security.
- **Security issues based on Industry 5.0:** The steps recognize security-related issues based on Industry 5.0. This phase is responsible for discovering security issues associated with industrial IoT components, which are directly involved in facilitating services related to personalization. Security issues based on Industry 5.0 are also identified in the initial stage of research, including data privacy, unauthorized access and data collection, data theft, operation disruption, insecure communication channel, cyber security, resilience, standards and human factors. Addressing these issues early means that a more meaningful attempt can be made to discover security issues involved with the rapid growth of applications based on Industry 5.0.
- **Factor Identification:** Factor identification is one of the most important activities for developing a roadmap to derive a commonly accepted set of security risk factors encompassing healthcare with Industry 5.0. An effort will be undertaken to determine connected factors that may be essential for security risk assessment.
- **Correlative Analysis:** This step refers to examining the nature of the dependence of security-related issues based on healthcare and Industry 5.0, finding correlations among them, and establishing connections between them following their anticipated influence and importance;
- **Security Risk Assessment:** With security risk assessment, safety mechanisms and security technologies can be analyzed and evaluated. Assessing security risk will help trade off security goals and costs;
- **Validation:** The fundamental purpose of validation is to ensure that the established models and metrics accurately measure what they are designed to measure. The validation process involves various processes to ensure the proper product is being built. The metrics' values are valid measurements to investigate in the context of an empirical investigation;
- **Suggestive Measures:** As a result of the developed model, a generic guideline in the form of a developer's manual could be made for making an effective assessment mechanism for a safe healthcare environment based on Industry 5.0. It is highly

desirable to provide some suggestive measures to the development teams to revisit the model to achieve the security indexes with justified evaluation and description;

- **Review and Revision:** Review and revision is an informal phase, positioned at the end, with free entry to all other related phases and recommendations for adequate exposures and return for a more comprehensive assessment based on the preceding phases. It will provide a free assistance mechanism through informal review and revisions at any stage of the perspective framework [46].

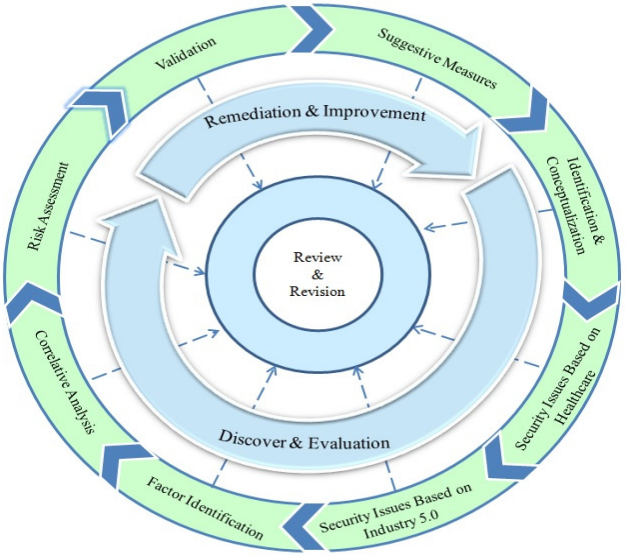


Figure 8. Security risk assessment framework for healthcare Industry 5.0.

Challenges for Industry 5.0: Industry 5.0 will make sure that the creation and use of innovations in the workplace significantly move forward the crucial goals of sustainability and climate neutrality, resilience and the well-being of people and society as a whole, and the resilience of value networks. Industry 5.0 wants to put people's requirements and wants at the center of the manufacturing procedure instead of just focusing on how technology can make money. Technology should not violate or interfere with a worker's rights and should help make the process fit each worker's needs. This is related to the need for sustainable business practices. Utilizing natural resources wisely, recycling them, and reducing waste and pollution are all goals of Industry 5.0. The fifth industrial revolution has the power to start a new socio-economic era that can bridge between the "top" and the "bottom", opening up countless chances for society.

7. Validation of Security Risk Assessment Framework for Healthcare Industry 5.0 ($SRVF^{HI5.0}$)

In order to achieve the desired security level, it is important to validate the proposed framework to establish the effectiveness and objectivity of evolutions for security criteria. Validation is helpful for determining the optimized security levels and provides support for designing feasible security evaluation criteria and tools for future research. In the absence of any concrete evolution criteria in the initial stage, the authors developed a methodology to validate the perspective framework with the help of statistical analysis to confirm the framework's effectiveness and its objectivity with respect to its given phases. The focus of this study is to ensure the validity of the risk assessment framework through the use of the following questions. The primary question is about the importance and need of theoretical validation of the risk assessment framework and what is the relevance of this theoretical validation to the course of study. In the absence of any standardized mechanism for benchmarking, statistical analysis is helpful in validating the proposed framework to attain objectivity and effectiveness. The primary step is to observe each essential security activity through its relative importance to ensure the effective, sustainable

evolution criteria. These criteria should be framed in such a manner as to form a tool or opinionnaire targeting all activities related to each phase. On the basis of the prepared opinionnaire, the researchers performed statistical validation through an expert survey and statistically validated the course of the study by performing exploratory factor analysis and reliability analysis. Furthermore, the results of statistical analysis will provide a strong basis for the acceptance of the proposed risk assessment framework based on healthcare Industry 5.0 for implementation and future analysis and research. A step-wise procedure is adopted for the theoretical validation of the proposed framework for security risk assessments based on Healthcare Industry 5.0 ($SRVF^{HI5.0}$). It is responsible for statistical analysis to validate the measure of the suitability of different criteria, the reliability of the tool and factor analysis. To fulfill this purpose, a step-wise procedure is adopted for theoretical validation of the proposed framework, as shown in Figure 9.

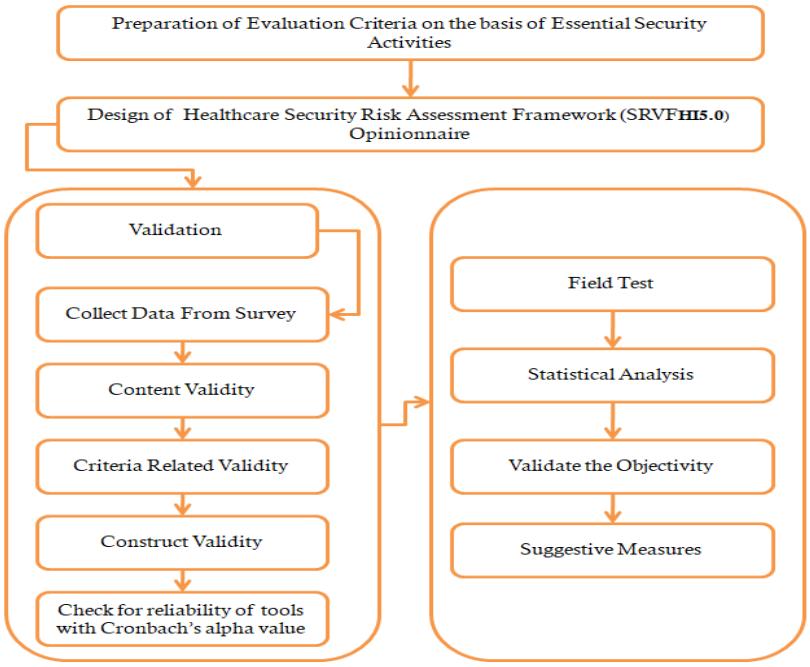


Figure 9. Step-wise procedure to validate the security risk assessment framework [47,48].

In this research, the collected security evolution controls are illustrated in Table 3. This survey has a total of 29 evolution controls for the assessment of the proposed framework for security risk assessment based on healthcare Industry 5.0. This research work carries with it an expert assessment survey to verify the suggested approach and its effectiveness for future research in terms of empirical analysis. This study was conducted in an online mode, and the questions included in the survey regarding the various controls were administrated appropriately for effective evolution. The results from the survey were analyzed properly against the statistical analysis tool using SPSS 20.0 for the suitability of the evolution controls using an opinionnaire, the reliability of the opinionnaire and the conformation of statistical relevance. This opinionnaire validation procedure is validated through content validation and exploratory factor analysis, and the reliability of the opinionnaire is determined using validated controls. Theoretical variables were evaluated through the use of factor analysis, which disclosed a general direction in terms of the reliability, convergence validity, and discriminate validity of different controls. Exploratory factor analysis is responsible for corroborating the validity of security evolution criteria for all the related phases and the derived values from the factor analysis. Cronbach's alpha coefficient was used to assess the dependability of each influencing element at the multi-control scale. Cronbach's alpha is frequently used to validate reliability and provides a more conservative value than other assessment factors. Lastly, the cross-tab analysis confirms the objectivity of the

proposed security risk assessment framework based on healthcare Industry 5.0 ($SRVF^{HI5.0}$) for implementation and future analysis and research.

Table 3. Stage-wise items and CVR value (essential and not essential). * Item added in Draft II; ** Item added in Draft III.

Stage I	Stage II	Stage III	ITEMS	CVR_{E+NE}(Draft–I)	CVR_{E+NE} (Draft–II)	CVR_{E} (Draft–III)
1	1	1	Is it highly productive to identify requirements and systematic conceptualization as building blocks for the development of proposed framework on the basis of existing/theoretical work?	0.3	1.0	1.0
		2 **	Does the primary phase of problem-solving activities directly related to conceptualization to identify the significant problem?	0.4	-	-
2	2	3	Whether the ongoing step is responsible for delivering the adequate and appropriate knowledge, qualified to represent perspective of all risk.	0.2	0.5	1.0
3	3	4	Is this step in the proposed framework important?	0.4	1.0	0.8
4	4	5	Role of recognizing security issues based on healthcare system is a more progressive step for determining various security issues.	0.3	0.8	0.8
5	5	6	Whether this thread will ensure to fetch all relevant security threats and risk related to healthcare system through proper research and analysis.	0.4	0.8	1.0
	6 *	7	Is the recognition of security-related problems based on healthcare services the only crucial phase activity?	0.3	−0.1	-
6	7	8	Is it the mandatory step to ensure daily risk management related to healthcare issues?	0.3	0.5	1.0
7	8	9	Is the relation of this step to the proposed framework important?/is this step relevant to the proposed framework?	0.2	1.0	0.8
8	9	10	Role of recognizing security issues based on Industry 5.0 is the more progressive step to determine various security issues.	0.3	0.8	0.7
	10 *	11	Does the recognition of security-related problems based on healthcare Industry 5.0 is the only crucial phase activity?	0.1	−0.3	-
9	11	12	Whether this thread will ensure the discovery of all relevant security threats and risk related to Industry 5.0 through proper research and analysis facilitating services related to personalization.	0.5	0.4	0.8
10	12	13	Is it the mandatory step to ensure daily risk management related to Industry 5.0 issues?	0.0	0.8	0.8
		14 **	Will this step determine the connected factors that may be essential for security risk assessment?	0.3	-	-
11	13	15	Is the relation of this step to the proposed framework important?	0.2	1.0	0.7
12	14	16	Is this step the most vital part in discovering unknown/known factors for healthcare security based on Industry 5.0?	0.2	0.4	0.8
13	15	17	Are the discovered factors responsible for risk assessment based on above scenario?	−0.4	0.8	0.7
14	16	18	Is the relation of this factorization of attributes to proposed framework important?	0.4	1.0	0.7
15	17	19	Does establishing correlation among healthcare security factors with Industry 5.0 an acceptable technique for analysis on the basis of anticipated influence and importance?	0.0	0.8	0.8

Table 3. *Cont.*

Stage I	Stage II	Stage III	ITEMS	CVR_{E+NE}(Draft–I)	CVR_{E+NE} (Draft–II)	CVR_{E} (Draft–III)
16	18	20	Is the relation of this step to proposed framework important?	0.4	0.8	0.7
17	19	21	Does the security risk assessment have an immediate impact on security goals and costs?	0.3	−0.2	-
		22 **	Should the safety mechanisms, and security technologies be analyzed to trade off security and budget?	0.0		-
18	20	23	Does the quantitative/qualitative security risk assessment proficient to establish impact analysis?	0.0	0.7	0.7
19	21	24	Does impact analysis rating have profound significance for security evaluation and performance analysis?	0.2	0.6	0.8
20	22	25	Is this step responsible for enlightening the researchers to fill their research gap through these best practices?	0.2	−0.6	-
		26 **	Does it provide a pathway to protect healthcare system from various threats in the application?	0.2		-
21	23	27	Does establishment of risk evaluation and risk acceptability criteria help to trade off security goals and cost?	0.3	0.8	0.8
22	24	28	Is the relation of this step to proposed framework important?	0.0	0.8	0.8
23	25	29	Does the identification of security risk offer significant reason as the one of the best preventive steps?	0.2	−0.1	-
24	26	30	Is this step helpful for ensuring that the established models and metrics accurately measure what they are designed to measure?	−0.1	0.4	1.0
25	27	31	How important is the relation of this step to the proposed framework.	0.3	0.8	0.8
		32 **	Could the generic guideline in the form of a developer's manual be made for making an effective assessment mechanism?	0.2		-
26	28	33	Does generic guidelines developed from the above process an effective assessment mechanism for a safe healthcare environment based on Industry 5.0?	0.3	0.8	1.0
27	29	34	Is the relation of this step to proposed framework important?	0.1	0.4	0.8
28	30	35	Is it highly desirable to provide some suggestive measures to the development teams to revisit the model?		0.2	-
29	31	36	Is this step required for recommendations of adequate exposures and return for a more comprehensive assessment based on the preceding phases?		1.0	0.7
		37 **	Is it mandatory to revisit to verify its adherence to the set forth objectives to cater to the security needs?		-	0.0
30	32	38 **	Is it fruitful to develop any benchmarking to plan for review?		−0.1	-
31	33	39	Is it helpful for free assistance mechanism through informal review and revisions at any stage of the perspective framework?		1.0	0.8
32	34	40	Is the relation of this step to proposed framework important?		0.8	0.8
33	35	41	Is this integrated framework suitable for healthcare security?		0.4	0.8
34	36	42	Does the phase of framework accomplish the security risk assessment?		0.4	1.0
			Average CVR Value	0.26	0.60	0.89

7.1. Methodology

This section describes the steps that were used to ensure the validity and reliability of the security risk assessment framework, which is based on the healthcare Industry 5.0 opinionnaire utilized for the study. The approaches applied are discussed below [48–52]:

7.1.1. Domain Identification and Item Generation

The most significant aspect of developing sound measures is directly dependent on the generation of items. From the successful review of literature based on a theoretical assessment of the security evaluation framework, authors have recognized the most prominent domain or theme in which assessment can be carried out for healthcare security with respect to Industry 5.0. While administering the security risk assessment framework ($SRVF^{HI5.0}$) opinionnaire, 40 items were initially pooled from various reviews and categorized into ten main themes: P1 (identification and conceptualization), P2 (security issues based on healthcare), P3 (security issues based on Industry 5.0), P4 (factor identification), P5 (correlative analysis), P6 (security risk assessment), P7 (validation), P8 (suggestive measures), P9 (review and revision). P10 is the computed variable for overall observation. Furthermore, the intense observation of each theme is classified to generate items and verified as per their relevance from Table 3 (stage 1). For this study, 20 experts were drawn from numerous research domains, including security, healthcare security analysis and IoT. Out of 42, 29 items were identified at the last stage for assessing opinions about the healthcare security risk assessment framework ($SRVF^{HI5.0}$) opinionnaire through expert opinions.

7.1.2. Content Validation

To determine valid items, this study used Lawshe's [53] content validity ratio (CVR). Only 20 experts were chosen to provide opinions regarding the appropriateness of the 42 items identified for assessing opinions about the healthcare security risk assessment framework ($SRVF^{HI5.0}$) opinionnaire. Subject experts were asked to provide the rating of the items on a two-point scale (1 = Essential; 2 = Not Essential). The survey was conducted online, and an opinionnaire was utilized to collect data. Experts were also briefed on the research's basis. To evaluate the content validity, CVR was calculated according to Lawshe's instructions.

The security risk assessment framework ($SRVF^{HI5.0}$) was further revised by accumulating additional descriptive items. After analyzing the opinionnaire at the first stage, it had 34 items. Further, the revised opinionnaire was distributed to the 15 experts, which resulted in two additional items. Another round of analysis was conducted with revised opinionnaire, as the CVR_{E+NE} values were less. In the final stage, another additional 6 items were added. The average value of CVR_E for all the items was estimated and 13 items (itemno.2, 7, 11, 14, 21, 22, 25, 26, 29, 32, 35, 37, 38) was deleted due to their low CVR_E value. As a result, a final legitimate opinionnaire containing 29 items has been generated for the subsequent stage of the test.

7.1.3. Items Administration at Development Stage

The opinionnaire with 29 items was distributed online as a security risk assessment framework ($SRVF^{HI5.0}$), which was conducted, all over the country. The opinionnaire was sent as an online survey to around 113 experts in the field. The distribution of the 29-item questionnaire to a total sample size of 270 was deemed appropriate, as well as a large number of respondents would mitigate subject variance for scale development. Only 113 (41.9%) working responses were obtained. However, the obtained responses were considered a study limitation at this stage of the study. The analysis of the return responses shows an elevated degree of satisfaction with this opinionnaire.

7.2. Analysis and Results

The steps which were performed for the analysis and results are mentioned below:

Validation of the Items

In order to determine the validity of the SRVF$^{HI5.0}$ opinionnaire, the content validity ratio (CVR) was determined in three steps, as shown in Table 3. The findings and analyses were further addressed [49]:

Stage First: A total of 16 experts answered out of a total of 20. In contrast, just 15 replies were determined to be exhaustive. Based on the data (shown as Draught I), CVR was computed to be 0.26, which was significantly lower than the crucial value of 0.49 at ($p < 0.05$) level for 15 experts mentioned in Table 3.

Stage Second: The analysis and discussion of Draft-I highlight some of the items that received low scores. Two additional items were added to Draft-II and submitted for expert review. The CVR of the opinionnaire was determined to be 0.60, which was significantly higher than the crucial value of 0.49 at ($p < 0.05$) level for 15 experts at 0.05 level.

Stage Third: 6 more items were added because of the low CVR in the previous drafts. Out of all 42 items, many items (2, 7, 11, 14, 21, 22, 25, 26, 29, 32, 35, 37, 38) were deleted due to the low CVR value. At this stage, only 12 experts responded, and with their responses, the calculated average value of CVR is 0.89 for 29 items, which is much more than the critical value for 12 experts. This was then considered to be acceptable for further statistical study and trials.

7.3. Analyzing Exploratory Factor Analysis and Reliability of the Opinionnaire

Again, the opinionnaire for 29 items was tested for reliability using two methods, including yielding 'Cronbach's alpha' of 0.899 and 'Guttman Split-Half Coefficient' of 0.665, indicating that the items in the opinionnaire are interrelated and measure the same attribute, i.e., opinion toward the healthcare security risk assessment framework (SRVF$^{HI5.0}$).

Prior to performing factor analysis, we performed the 'Kaiser-Meyer-Olkin (KMO)' of sampling adequacy. It was advised that KMO values less than 0.7 be considered meritorious, and Table 4 reveals that the data utilized in the study had a KMO value of 0.709. This ensures that the sample size is insufficient yet adequate for factor analysis. Furthermore, Bartlett's test of Sphericity is significant ($p < 0.000$), showing that there are some correlations between the variables. Tables 5 and 6 are responsible for delivering the information regarding the distribution of samples with respect to job profile and work experience in percentage.

Table 4. Test report based on KMO and Bartlett's test.

'Kaiser-Meyer-Olkin Measure of Sampling Adequacy'		0.709
'Bartlett's Test of Sphericity'	'Approx. Chi-Square'	3510.472
	'Df'	210
	'Significance'	0.000

Table 5. Indicating the distribution of sample across job profile.

Job Profile	N	Percent
Academics	69	61.1
Research and Industry Expert	44	38.9
Total	113	100

Table 6. Indicating the distribution of sample across working experience.

Working Experience	N	Percent
Less than 05 Years	25	22.1
More than 05 Years	32	28.3
More than 10 Years	56	49.6
Total	113	100

7.3.1. Item Analysis

Cronbach's Alpha was deployed to assess the degree of internal consistency among all sets of items. The Cronbach Alpha for the opinionnaire was 0.899. As stated by Victor and Swamy (2011) [52], only items with "r" values greater than 0.3 were chosen. As seen in Table 7, all 29 items had values greater than 0.3. The final scale scores ranged from 29 to 145 in ascending order.

Table 7. Showing the communalities of 29 items.

Communalities			
Items Code	**Items**	**Initial**	**Extraction**
P1_a	Is it highly productive to identify requirements and systematic conceptualization	1.000	0.881
P1_b	This step is responsible for delivering adequate and appropriate knowledge about risk	1.000	0.806
P1_c	Is the relation of this step to the proposed framework important?	1.000	0.896
P2_a	The role of recognizing security issues based on healthcare system is the more progressive step for security issues.	1.000	0.906
P2_b	This thread will ensure the fetching of all relevant security threats and risk related to healthcare system.	1.000	0.904
P2_c	Is it the mandatory step to ensure daily risk management related to healthcare issues?	1.000	0.910
P2_d	Is the relation of this step to the proposed framework important?	1.000	0.751
P3_a	Role of recognizing security issues based on Industry 5.0 is a more progressive step	1.000	0.881
P3_b	This thread will ensure to discover all relevant security threats and risk related to Industry 5.0.	1.000	0.925
P3_c	Is it the mandatory step to ensure daily risk management related to Industry 5.0 issues?	1.000	0.875
P3_d	Is the relation of this step to proposed framework important?	1.000	0.961
P4_a	The vital part of discovering unknown/known factors for healthcare security based on Industry 5.0?	1.000	0.921
P4_b	Are the discovered factors responsible for risk assessment based on above scenario?	1.000	0.897
P4_c	Is the relation of this factorization of attributes to proposed framework important?	1.000	0.936
P5_a	Establishing correlation among healthcare security factors with Industry 5.0	1.000	0.947
P5_b	Is the relation of this step to the proposed framework important?	1.000	0.886
P6_a	Does the quantitative/qualitative security risk assessment proficient for establishing impact analysis?	1.000	0.943
P6_b	Does impact analysis rating have profound significance for security evaluation	1.000	0.912
P6_c	Does establishment of risk evaluation and risk acceptability criteria help to trade off security goals?	1.000	0.941
P6_d	Is the relation of this step to proposed framework important?	1.000	0.836
P7_a	Is this step helpful for ensuring that the established models and metrics are accurately measured?	1.000	0.711
P7_b	How important is the relation of this step to the proposed framework?	1.000	0.491
P8_a	Do generic guidelines developed from above process make for an effective assessment mechanism for Industry 5.0?	1.000	0.961
P8_b	Is the relation of this step to proposed framework important?	1.000	0.900

Table 7. *Cont.*

Communalities			
Items Code	**Items**	**Initial**	**Extraction**
P9_a	Is this step required for recommendations of adequate exposures?	1.000	0.697
P9_b	Is it helpful for free assistance mechanism through informal review and revisions?	1.000	0.565
P9_c	Is the relation of this step to the proposed framework important?	1.000	0.525
P10_a	Is this integrated framework suitable for healthcare security?	1.000	0.941
P10_b	Does the phase of framework accomplish the security risk assessment?	1.000	0.888

7.3.2. Final Form of the Tool

The final form of the tool/opinionnaire, having 10 components with 29 items finalized for final observation with their initial and extraction values, is shown in Table 7.

7.3.3. Scoring

The final opinionnaire consisted of demographic variables like job profile and work experience in the first part and 29 questions of the close-ended type to check the opinions regarding the healthcare security risk assessment framework ($SRVF^{HI5.0}$) opinionnaire surveyed by the experts in the following part. The items were measured in the 5-point Likert Scale, with the ratings indicating the different levels of opinion.

1—Very Low
2—Low
3—Moderate
4—High
5—Very High.

7.3.4. Interpretation

This study covers the initial level of validation of the proposed framework theoretically based on expert opinion to check the appropriateness of the activities related to all phases of the proposed work. The content validity ratio (CVR) is utilized to determine validity in three steps according to Lawshe's instructions to prove the working of the opinionnaire. Furthermore, based on the percentage values obtained from the opinionnaire through cross-tab analysis using SPSS 20.0 software, we can affirm the suitability of the framework.

Job_Profile is recoded as a result variable, and a summary of the result for overall performance is evaluated and is shown in Figure 10a–c. In addition, the degree of commonality of the opinionnaire in 29 items is shown in Table 7. The overall performance is evaluated in a two-fold manner under two categories. The first category is about Job_Profile, which is sub divided into academics and research and industry experts and another category is their Work_Experience. With this tool, we again surveyed 215 people to get an opinion about the overall performance using random sampling techniques through online mode. The results indicate that 92.6% have a positive opinion of the performance acceptability observation. In this study, 30.7% strongly agreed and 61.9% expressed their positive opinion on the overall performance of framework for future analysis and research. The collected responses from multiple experts validated the opinionnaires' questions based on the statistical analysis and have significant acceptance for future study direction.

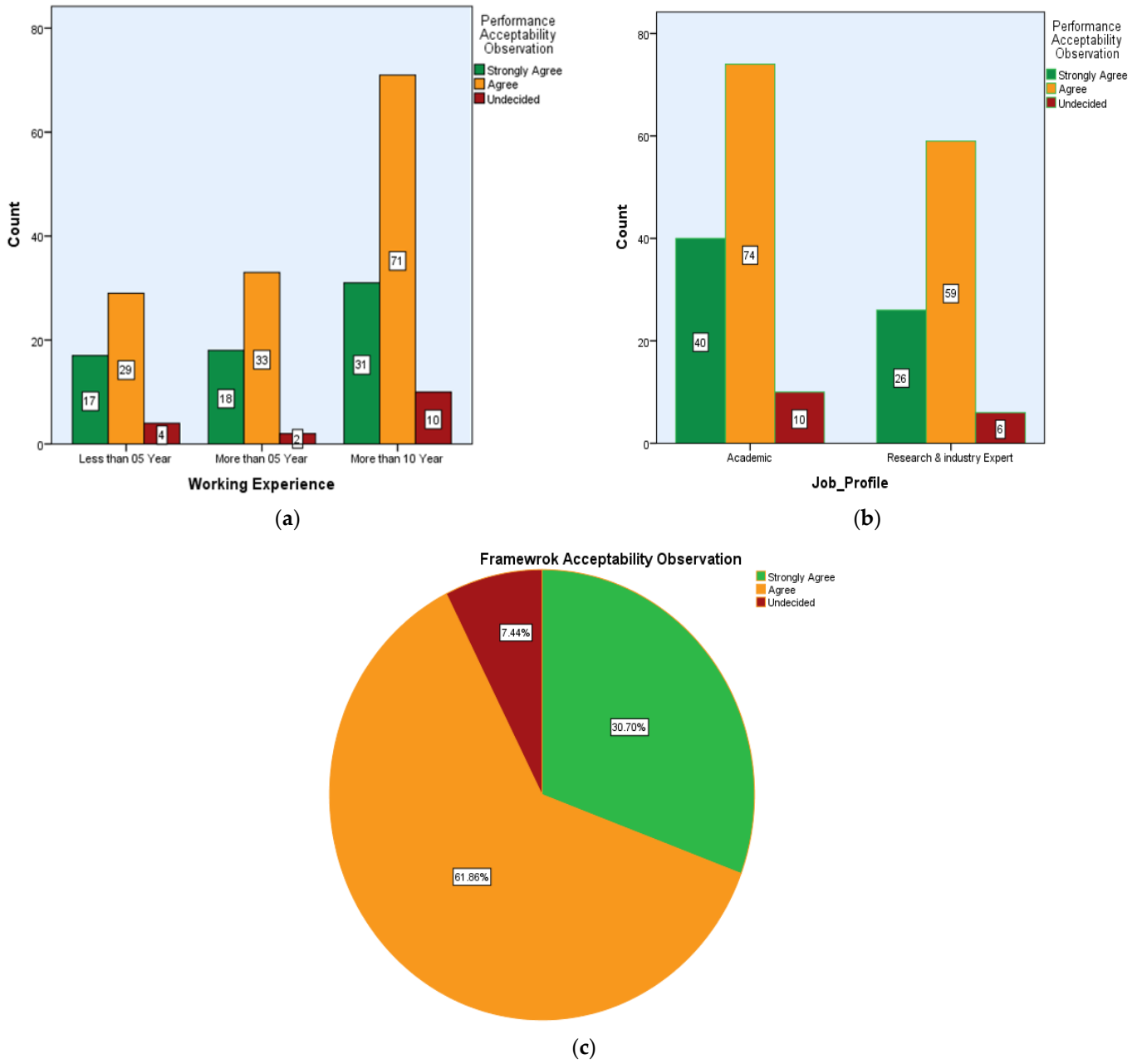


Figure 10. (**a**–**c**): Summary of overall performance.

8. Summary and Conclusions

This work undertook an in-depth study of several research articles to illustrate the role of Industry 5.0 in the healthcare system. It expresses the role of industry evolution in the context of the healthcare system and emphasizes the importance of transformation from Industry 4.0 to Industry 5.0 for higher societal acceptance of healthcare services. The data collected for healthcare security breaches serves as the foundation for the realization of developing a perspective framework in the absence of any standard available method connected to security threats and security risk evaluation for Industry 5.0.

The article provides recommendations and establishes the next step to make Industry 5.0 more human-centric while being secure and sustainable at the same time. New idea generation is motivated by social, technical and environmental requirements. The significance of this research increases further by recognizing various healthcare security risks and threats during the proposed healthcare procedures based on Industry 5.0. Critical analysis based on a symmetrical solution provides a roadmap for correlating healthcare

systems through an Industry 5.0 perspective. This article sought to reveal the gaps in security risk assessment for the healthcare-related issues correlated with the components of Industry 5.0. The statistical analysis was performed to validate the suitability of different criteria, the reliability of the tool, and factor analysis. The results of the statistical analysis confirm the validity of objectivity and provide an adequate basis for the acceptance of the proposed security risk assessment framework based on healthcare Industry 5.0 ($SRVF^{HI5.0}$) for implementation as well as future analysis and research. The proposed framework is a novel concept to build suggestive measures for impact analysis and strengthen security indexing for higher acceptability.

Author Contributions: All authors contributed equally to this manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number: IFP22UQU4260426DSR203.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used in this study are available upon request from the corresponding author.

Acknowledgments: The authors extend their appreciation to the Deanship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number: IFP22UQU4260426DSR203. The authors would like to acknowledge Samson R. Victor from the Department of Education, Indira Gandhi National Tribal University, Madhya Pradesh, for his technical assistance with statistical analysis.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. He, Y.; Aliyu, A.; Evans, M.; Luo, C.; Park, W. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *J. Med. Internet Res.* **2021**, *23*, e21747. [CrossRef] [PubMed]
2. System, H.; Almalawi, A.; Khan, A.I.; Alsolami, F.; Abushark, Y.B. Managing Security of Healthcare Data for a Modern. *Sensors* **2023**, *23*, 3612.
3. Alves, J.; Lima, T.M.; Gaspar, P.D. Is Industry 5.0 a Human-Centred Approach? A Systematic Review. *Processes* **2023**, *11*, 193. [CrossRef]
4. Traore, T.; Shanks, S.; Haider, N.; Ahmed, K.; Jain, V.; Rüegg, S.R.; Razavi, A.; Kock, R.; Erondu, N.; Rahman-Shepherd, A.; et al. How prepared is the world? Identifying weaknesses in existing assessment frameworks for global health security through a One Health approach. *Lancet* **2023**, *401*, 673–687. [CrossRef] [PubMed]
5. Ahmad, M.; Nadeem, M.; Seh, A.H.; Khan, R.A. Cyber Security Quantification of Healthcare Medical Devices through Soft Cyber Security Quantification of Healthcare Medical Devices through Soft computing technique. *Int. J. Adv. Technol. Eng. Sci.* **2021**, *9*, 21–27.
6. Radanliev, P.; De Roure, D.; Nicolescu, R.; Huth, M.; Santos, O. Artificial Intelligence and the Internet of Things in Industry 4.0. *CCF Trans. Pervasive Comput. Interact.* **2021**, *3*, 329–338. [CrossRef]
7. Alojaiman, B. Technological Modernizations in the Industry 5.0 Era: A Descriptive Analysis and Future Research Directions. *Processes* **2023**, *11*, 1318. [CrossRef]
8. Attaallah, A.; Al-Sulbi, K.; Alasiry, A.; Marzougui, M.; Ansar, S.A.; Agrawal, A.; Ansari, T.J.; Khan, R.A. Fuzzy-Based Unified Decision-Making Technique to Evaluate Security Risks: A Healthcare Perspective. *Mathematics* **2023**, *11*, 2554. [CrossRef]
9. Kaur, J.; Khan, A.I.; Abushark, Y.B.; Alam, M.; Khan, S.A.; Agrawal, A.; Kumar, R.; Khan, R.A. Security risk assessment of healthcare web application through adaptive neuro-fuzzy inference system: A design perspective. *Risk Manag. Healthc. Policy* **2020**, *13*, 355–371. [CrossRef]
10. Almulihi, A.H.; Alassery, F.; Khan, A.I.; Shukla, S.; Gupta, B.K.; Kumar, R. Analyzing the Implications of Healthcare Data Breaches through Computational Technique. *Intell. Autom. Soft Comput.* **2022**, *32*, 1763–1779. [CrossRef]
11. 5 Biggest Healthcare Security Threats for 2021 | CSO Online. Available online: https://www.csoonline.com/article/3262187/biggest-healthcare-security-threats.html (accessed on 24 January 2023).
12. Ávila-Gutiérrez, M.J.; de Miranda, S.S.-F.; Aguayo-González, F. Occupational Safety and Health 5.0—A Model for Multilevel Strategic Deployment Aligned with the Sustainable Development Goals of Agenda 2030. *Sustainability* **2022**, *14*, 6741. [CrossRef]

13. Islam, M.S.; Hasan, M.M.; Wang, X.; Germack, H.D.; Noor-E-alam, M. A systematic review on healthcare analytics: Application and theoretical perspective of data mining. *Healthcare* **2018**, *6*, 54. [CrossRef] [PubMed]
14. Yin, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13. [CrossRef]
15. Javaid, M.; Haleem, A. Critical components of industry 5.0 towards a successful adoption in the field of manufacturing. *J. Ind. Integr. Manag.* **2020**, *5*, 327–348. [CrossRef]
16. Bajic, B.; Suzic, N.; Moraca, S.; Stefanović, M.; Jovicic, M.; Rikalovic, A. Edge Computing Data Optimization for Smart Quality Management: Industry 5.0 Perspective. *Sustainability* **2023**, *15*, 6032. [CrossRef]
17. Espina-Romero, L.; Guerrero-Alcedo, J.; Avila, N.G.; Sánchez, J.G.N.; Hurtado, H.G.; Li, A.Q. Industry 5.0: Tracking Scientific Activity on the Most Influential Industries, Associated Topics, and Future Research Agenda. *Sustainability* **2023**, *15*, 5554. [CrossRef]
18. Skobelev, P.O.; Borovik, S.Y. On the Way from Industry 4.0 To Industry 5.0: From Digital Manufacturing to Digital Society. *Industry 4.0* **2017**, *2*, 307–311.
19. Longo, F.; Padovano, A.; Umbrello, S. Value-oriented and ethical technology engineering in industry 5.0: A human-centric perspective for the design of the factory of the future. *Appl. Sci.* **2020**, *10*, 4182. [CrossRef]
20. Haleem, A.; Javaid, M. Industry 5.0 and its expected applications in medical field. *Curr. Med. Res. Pract.* **2019**, *9*, 167–169. [CrossRef]
21. Zhang, Q.; Chen, Y.; Lin, W.; Chen, Y. Optimizing Medical Enterprise's Operations Industry 5.0. *Discret. Dyn. Nat. Soc.* **2021**, *2021*, 9298166. [CrossRef]
22. Pereira, A.G.; Santos, F.C.; Lima, T.M. Industry 4.0 and Society 5.0: Opportunities and Threats. *Int. J. Recent Technol. Eng.* **2020**, *8*, 3305–3308. [CrossRef]
23. Islam, A.; Islam, M.; Uzir, M.U.H.; Wahab, S.A.; Latiff, A.S.A. The panorama between COVID-19 pandemic and Artificial Intelligence (AI): Can it be the catalyst for Society 5.0? *Int. J. Sci. Res. Manag.* **2020**, *8*, 2011–2025. [CrossRef]
24. Lepore, D.; Micozzi, A.; Spigarelli, F. Industry 4.0 accelerating sustainable manufacturing in the COVID-19 era: Assessing the readiness and responsiveness of italian regions. *Sustainability* **2021**, *13*, 2670. [CrossRef]
25. Raje, S.; Reddy, N.; Jerbi, H.; Randhawa, P.; Tsaramirsis, G.; Shrivas, N.V.; Pavlopoulou, A.; Stojmenović, M.; Piromalis, D. Applications of Healthcare Robots in Combating the COVID-19 Pandemic. *Appl. Bionics Biomech.* **2021**, *2021*, 7099510. [CrossRef] [PubMed]
26. Rojas, C.N.; Peñafiel, G.A.A.; Buitrago, D.F.L.; Romero, C.A.T. Society 5.0: A Japanese concept for a superintelligent society. *Sustainability* **2021**, *13*, 6567. [CrossRef]
27. O'brien, R.; Bair, E.F.; Venkataramani, A.S. Death by Robots? Automation and Working-Age Mortality in the United States. *Demography* **2022**, *59*, 607–628. [CrossRef]
28. Adel, A. Future of industry 5.0 in society: Human-centric solutions, challenges and prospective research areas. *J. Cloud Compup.* **2022**, *11*, 40. [CrossRef]
29. Report: Nearly 400 Crashes by 'Self-Driving' Cars in the US | Automotive Industry News | Al Jazeera. Available online: https://www.aljazeera.com/economy/2022/6/15/report-nearly-400-crashes-by-self-driving-cars-in-the-us (accessed on 20 August 2023).
30. Teslas Running Autopilot Involved in 273 Crashes Reported since Last Year—The Washington Post. Available online: https://www.washingtonpost.com/technology/2022/06/15/tesla-autopilot-crashes/ (accessed on 20 August 2023).
31. Javaid, M.; Haleem, A.; Vaishya, R.; Bahl, S.; Suman, R.; Vaish, A. Industry 4.0 technologies and their applications in fighting COVID-19 pandemic. *Diabetes Metab. Syndr. Clin. Res. Rev.* **2020**, *14*, 419–422. [CrossRef]
32. Rehman, A.; Abbas, S.; Khan, M.A.; Ghazal, T.M.; Adnan, K.M.; Mosavi, A. A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. *Comput. Biol. Med.* **2022**, *150*, 106019. [CrossRef]
33. Khalil, R.A.; Saeed, N.; Fard, Y.M.; Al-Naffouri, T.Y.; Alouini, M.-S. Deep Learning in Industrial Internet of Things: Potentials, Challenges, and Emerging Applications. *arXiv* **2020**, arXiv:2008.06701.
34. Barata, J.; Kayser, I. Industry 5.0—Past, Present, and Near Future. *Procedia Comput. Sci.* **2023**, *219*, 778–788. [CrossRef]
35. The Top Healthcare Data Breach Statistics of 2023 | Persona. Available online: https://withpersona.com/blog/top-healthcare-data-breach-statistics-2023 (accessed on 13 August 2023).
36. Available online: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (accessed on 24 July 2023).
37. Raghupathi, W.; Raghupathi, V.; Saharia, A. Analyzing Health Data Breaches: A Visual Analytics Approach. *AppliedMath* **2023**, *3*, 175–199. [CrossRef]
38. Khan, S.A.; Khan, R.A. Security assessment framework: A complexity perspective. *Comput. Fraud Secur.* **2014**, *2014*, 13–17. [CrossRef]
39. Khan, S.A.; Kumar, R.; Khan, R.A. *Software Security: Concepts and Practices*; CRC Press: Chapman & Hall, FL, USA, 2023.
40. Alvarez-aros, E.L.; Bernal-torres, C.A. Technological competitiveness and emerging technologies in industry 4.0 and industry 5.0. *An. Acad. Bras. Ciênc.* **2021**, *93*, e20191290. [CrossRef]
41. Ksibi, S.; Jaidi, F.; Bouhoula, A. A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach. *Mob. Netw. Appl.* **2022**, *28*, 107–127. [CrossRef]
42. Eich, A.; Klichowicz, A.; Bocklisch, F. How automation level influences moral decisions of humans collaborating with industrial robots in different scenarios. *Front. Psychol.* **2023**, *14*, 1107306. [CrossRef]

43. Thomasian, N.M.; Adashi, E.Y. Cybersecurity in the Internet of Medical Things. *Health Policy Technol.* **2021**, *10*, 100549. [CrossRef]
44. Akundi, A.; Euresti, D.; Luna, S.; Ankobiah, W.; Lopes, A.; Edinbarough, I. State of Industry 5.0—Analysis and Identification of Current Research Trends. *Appl. Syst. Innov.* **2022**, *5*, 27. [CrossRef]
45. Seh, A.H.; Ahmad, M.; Nadeem, M.; Pandey, A.K.; Agrawal, A.; Kumar, R.; Khan, R.A. Usable-Security Assessment of Healthcare Software System Through Fuzzy ANP-TOPSIS Method. *Int. J. Syst. Dyn. Appl. (IJSDA)* **2021**, *10*, 1–24. [CrossRef]
46. Agrawal, A.; Alenezi, M.; Khan, S.A.; Kumar, R.; Khan, R.A. Multi-level Fuzzy system for usable-security assessment. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 657–665. [CrossRef]
47. Kim, J.; Lee, C.; Chang, H. The Development of a Security Evaluation Model Focused on Information Leakage Protection for Sustainable Growth. *Sustainability* **2020**, *12*, 10639. [CrossRef]
48. Robert, F. *Devellis, Scale Development: Theory and Applications*, 3rd ed.; SAGE Publications Inc.: New York, NY, USA, 2011.
49. Ayre, C.; Scally, A. Critical Values for Lawshe's Content Validity Ratio. *Meas. Eval. Couns. Dev.* **2014**, *47*, 79–86. [CrossRef]
50. Mishra, S.; Sharma, M.; Sharma, R.C.; Singh, A.; Thakur, A. Development of a Scale to Measure Faculty Attitude Towards Open Educational Resources. *Open Prax.* **2016**, *8*, 55. [CrossRef]
51. Victor, S.R.; Srinivasan, V. Development of A Scale to Identify Teaching Practices Among Pre- University Teachers. *J. Educ. Lit.* **2015**, *3*, 13–18.
52. Samson, R.V.; Swamy, S. *Development of an Attitude Scale to Measure Computer Application of Secondary School Teachers*; All India Association for Educational Research (AIAER): Pondicherry, India, 2011.
53. Lawshe, C.H. A Quantitative Approach to Content Validity. *Pers. Psychol.* **1975**, *28*, 563–575. [CrossRef]