EURASIP Journal on Information Security

RESEARCH Open Access

IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process

Kamalanathan Kandasamy[1*], Sethuraman Srinivas[2], Krishnashree Achuthan[1] and Venkat P. Rangan[3]

Abstract

Security vulnerabilities of the modern Internet of Things (IoT) systems are unique, mainly due to the complexity and heterogeneity of the technology and data. The risks born out of these IoT systems cannot easily fit into an existing risk framework. There are many cybersecurity risk assessment approaches and frameworks that are under deployment in many governmental and commercial organizations. Extending these existing frameworks to IoT systems alone will not address the new risks that have arisen in the IoT ecosystem. This study has included a review of existing popular cyber risk assessment methodologies and their suitability to IoT systems. National Institute of Standards and Technology, Operationally Critical Threat, Asset, and Vulnerability Evaluation, Threat Assessment & Remediation Analysis, and International Standards Organization are the four main frameworks critically analyzed in this research study. IoT risks are presented and reviewed in terms of the IoT risk category and impacted industries. IoT systems in financial technology and healthcare are dealt with in detail, given their high-risk exposure. Risk vectors for IoT and the Internet of Medical Things (IoMT) are discussed in this study. A unique risk ranking method to rank and quantify IoT risk is introduced in this study. This ranking method initiates a risk assessment approach exclusively for IoT systems by quantifying IoT risk vectors, leading to effective risk mitigation strategies and techniques. A unique computational approach to calculate the cyber risk for IoT systems with IoT-specific impact factors has been designed and explained in the context of IoMT systems.

Keywords: Risk assessment, Internet of Medical Things, Risk vectors, Cybersecurity risk assessment frameworks, Risk rank

1 Introduction

1.1 IoT technology

IoT revolution of this millennium is the next wave of technology that has impacted, and empowered every industry, since its initial formation in the year 1999 [1]. The IoT vision started with a simple goal of connecting any standalone device to the Internet and thereby convert it to be a smart device. As per a recent Gartner prediction, the count of IoT devices is expected to hit 25 billion devices in 2020, and 65% of companies would adopt IoT devices [2]. Wireless sensor network (WSN) is the very foundation of IoT communication. IoT wave is elevating the Internet to its next level by introducing full integration with field-level devices [3]. The IoT has already created an intelligent platform to collaborate on distributed things through wireless and wired networks. So far, human interaction with the Internet through business-to-business (B2B) and business-to-commerce (B2C) is a common phenomenon. With the arrival of IoT, any standalone device has the potential to interact with not only humans but also with the Internet [4]. The unique aspect that identifies IoT technology is the enablement of data transfer between any standalone device, the Internet, and humans. This communication can be

* Correspondence: kamalanathan@am.amrita.edu
[1]Amrita Center for Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri Campus, Clappana Post, Kollam, Kerala 690525, India
Full list of author information is available at the end of the article

easily managed through both automated and user-initiated actions. For example, a water sprinkler can be controlled to supply only the needed amount of water to a garden if it is directed by a weather forecasting application. Any device that is exposed to the Internet is subject to cyber-attacks and IoT devices are no exception, thereby increasing the risks associated with them. Due to the uniqueness and high-level complexity of IoT technology, a new category of risks is identified by risk experts [4]. Understanding the risks born out of IoT devices and managing them become an imminent need of the IoT security risk professionals.

1.2 IoT vulnerabilities and attacks

IoT devices, in recent times, are increasingly subject to cyber attacks leading to revenue loss and data loss. Common IoT vulnerabilities arise due to the following factors: (a) complex architecture, (b) inappropriate security configuration, (c) physical security, and (d) insecure firmware or software [5]. A comprehensive list of top 10 vulnerabilities for the IoT architecture is introduced by the Open Web Application Security Project (OWASP) [6]. Physical security is one of the main vulnerabilities that has been repeatedly exploited in IoT devices. Unauthorized access to deployed systems is gained through weak, guessable, or hardcoded passwords [7]. Confidentiality, integrity, and availability (CIA) will be compromised if the IoT devices have insecure network services. Attacks are possible if either the firmware on the device is not validated or if the anti-rollback mechanisms are not in place. IoT attacks have recently caused disastrous consequences. A Ukrainian power grid was recently attacked, leading to knockout of electricity [8]. Needless to say, the protection of IoT systems from attacks is a necessary step leading to risk reduction. Securing IoT systems involve solving many complex technology-related issues. A recent IoT security research literature discusses the existing authentication, access control methods, and trust management techniques [9] and recommends that IoT threat modeling could be used for the IoT risk mitigation process.

IoT attacks are classified based on IoT architecture and application scenarios [10]. All three IoT layers, namely application, network, and hardware layers, have security issues. Injection and buffer overflows are a few of the attacks in the application layer. The physical layer can have Sybil, replay attacks, selective forwarding, and synchronization attacks in general. Jamming and MiTM (Man in The Middle) attacks are the dangerous ones in the hardware layer [11] affecting the physical layer (PHY) and media access control (MAC) layer communication protocols even though encryption mechanisms are in place. The impact of the evolving features on the seven categories of privacy threats including identification, tracking, and profiling are summarized in [12]. The constantly expanding IoT threat landscape warrants a study of IoT risks and its mitigation.

Given the security vulnerabilities in modern IoT systems, it is important to holistically analyze cyber risk assessment frameworks, risk vectors, and risk ranking. In this manuscript, we discuss cyber risks related to IoT environment and IoT systems. We present a critical analysis of cybersecurity risk assessment frameworks, their challenges, and perspectives for the future, with emphasis on industrial and healthcare sectors, particularly the Internet of Medical Things (IoMT). Developing a computational approach for computing cyber risk for IoT systems is one of the goals of this research. Based on the literature review and analysis, a scientific approach to computing the cyber risk for IoT systems was designed as a part of this research, taking into consideration the IoT-specific impact factors. These factors were applied to compute the risk impact and likelihood of IoMT devices. The risk computing approach and formula are discussed in the later section of this research work. The formulas calculate the risk score and assess the risk level (high, medium, low) of IoMT devices. IoMT devices directly impact and benefit human life, by providing health monitoring tools and life-saving devices. The foundational aspects of cybersecurity risks are examined in this research through the lens of applicable theories including Dempster-Shafer theory and cybersecurity game theory.

2 Cyber risks in the IoT domain

2.1 Definition of IoT risk

The cyber risk (sometimes called Information Technology (IT) risk) is defined as the combined likelihood of an undesirable event and its impact level. Risk is described by the US NIST (National Institute of Standards and Technology) as a function of the probability of a given threat source's exercising any potential vulnerability and the resulting impact of that adverse event on the organization. The International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) defines IT risk as the potential for a threat to exploit asset vulnerabilities and damage the organization. It is evaluated in respect of a combination of the likelihood of an event occurring and its impact. Asset, threat, and vulnerability are three key components of the information security risk. The Open-Web Application Security Project (OWASP) testing guide computes risk as equal to the likelihood multiplied by impact where specific numbers for likelihood and impact are assigned. There are different definitions for risk considering threats and vulnerabilities. A vulnerability-centric definition of cyber risk is found in NIST's Common Vulnerability Scoring System (CVSS) which computes risk severity with scores ranging from 0

to 10.Conceptualization of cyber risks is investigated as reflected in expressions of two groups of professionals: cybersecurity experts and creators of ontologies pertaining to cybersecurity [13]. The concept of vulnerability, along with its exploitation by an attacker, is given importance by both groups. The very definition of the Internet of Things (IoT) refers to the system of interrelated computing devices, mechanical and digital machines with the ability to transfer data over a network without any human-to-human or human-to-computer interaction [14]. Quite obviously, we expect several types of cyber risks in such a system and we call them IoT risks. Different types of such risks in an IoT system are discussed in the next subsection.

2.2 Types of IoT risks

Many domains including finance, supply chain, and healthcare are impacted by IoT attacks. The healthcare sector is the largest target of cybersecurity attacks in the USA, compared to industrial and financial institutions [15]. There are insider threats that cause unique challenges in the case of the IoT risk assessment process [16]. For example, the insider can discreetly take a picture or video of sensitive organizational information or IP using a smart device camera and then deliberately share it with a third party. An insider can also connect to the network of organizations (by flash drive, Bluetooth, or Wi-Fi) using a malware-infected smart device. If the vulnerabilities in IoT devices (or the IoT environment) are exploited by threats in the system, it leads to IoT risks. As an example, the use of IoT devices to automate their controls can compromise nuclear power plants and information centers. Examples of different types of IoT risks are explained below [17] with Fig. 1.

a) Ethical IoT risk: This refers to the unforeseen adverse effects of unethical actions using IoT devices. Volkswagen, an automotive manufacturing company, developed and installed software to cheat diesel emissions tests. This violated the USA's Clean Air Act, compromised organization and industry standards, and resulted in massive reputational and financial losses [18].
b) Security and privacy IoT risk: This refers to the exploitation of vulnerabilities in the system to gain access to assets with intent to causing harm. In October 2016, the Mirai (IoT specialized malware) Botnet launched a DDoS attack on DYN which led to parts of the internet going down and affected Twitter, Netflix, CNN, Reddit, and many others [19]. This category includes the privacy IoT risk also which refers to the temporary or permanent loss of data control that is detrimental to the organization. eBay data breach that happened in the month of May 2014 caused its customer records, including passwords to be hacked "(https://www.businessinsider.in/Cyber-Thieves-Took-Data-On-145-Million-eBay-Customers-By-Hacking-3-Corporate-Employees/articleshow/35630666.cms)".
c) Technical IoT risk: This is due to hardware or software failure because of poor design, evaluation, etc. It was recently found that personal computer chips created over the most recent 20 years contain chip-level security flaws. Meltdown is an Intel ×86 microprocessor hardware vulnerability that enables

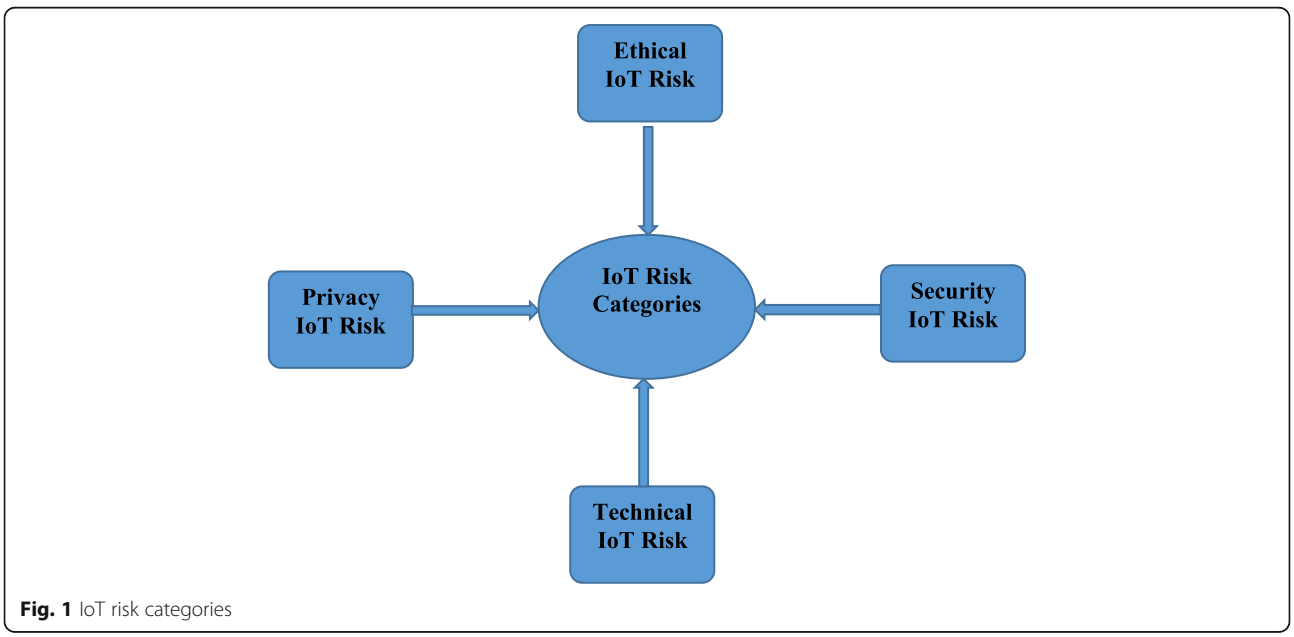

Fig. 1 IoT risk categories

a rogue method to read all memory although it is not authorized to do so "(https://www.kaspersky.com.au/blog/35c3-spectre-meltdown-2019/21886/)". Poor design issues lead to privacy and security IoT risks.

An IoT risk is the likelihood of a threat occurring and resulting in an adverse effect on or damage to an IoT asset. An IoT-based example of this is the probability of a phishing attack occurring on a connected corporate device like a company laptop or a smartphone, which then causes several IoT sensors to be infected with malware and consequently the disruption of a manufacturing plant's production line. We discuss IoT risk theories in the next subsection for the benefit of the reader.

2.3 IoT risks—applicable theories

Scientific theories that support the concept and evolution of cybersecurity risk can be easily extended to the IoT domain. A belief function is a mathematical function of the degree of belief by combining evidence from different sources [20]. It can be considered as the formal framework for representing and reasoning with uncertain information. Dempster-Shafer Theory of Belief Functions is used to model uncertainties in the risk assessment process [21]. It defines risk as the probability of information system security failures, and it assesses whether threats and control measures are present or not. The impact of risk factors and the countermeasures of the risk can be incorporated using the belief function framework. The impact of risk control measures on information systems security (ISS) for multiple threats can be performed easily using this function. The overall information security risk is decomposed into its sub-components in this method. Risks are evaluated for each sub-component by evaluating the impact of threats and controls on sub-components separately. Aggregation of all the risks is performed using the calculus of belief functions which determines the overall risk.

IoT risk assessment theories are delineated in Fig. 2. Indeed, game-theoretic computing is used for quantitative risk assessment in different fields, including information security [22]. Nash equilibrium is a steady condition of a framework, including the cooperation of various members where no member can pick up from an uneven difference in the system if the other's strategies stay unaltered. In a Defend–Attack circumstance, a successive choice game is exhibited where the safeguard picks a protection d, and the aggressor picks an assault a. For this situation, the parallel result S speaks to the achievement or disappointment of the assault. Consequently, the repercussions for the two players depend upon the accomplishment of one's strike. The game-theoretic strategy to adversarial risk analysis (ARA) needs figuring likelihood over S, restrictive on (d, a). A decision tree is used to process players' Nash equilibrium condition at node S. Thereafter, the decision tree for each player is solved using linear programming to determine the equations that must be satisfied at Nash equilibrium. The reader is referred to an excellent review by Sahinoglu et al. [22] on certain game-theoretic computing methods and applications for quantitative risk assessment. Specific game-theoretic methods including Neumann's two-way zero-sum pure equilibrium with optimal mixed strategy solutions and Nash equilibria with pure and mixed strategies are dealt with in detail.

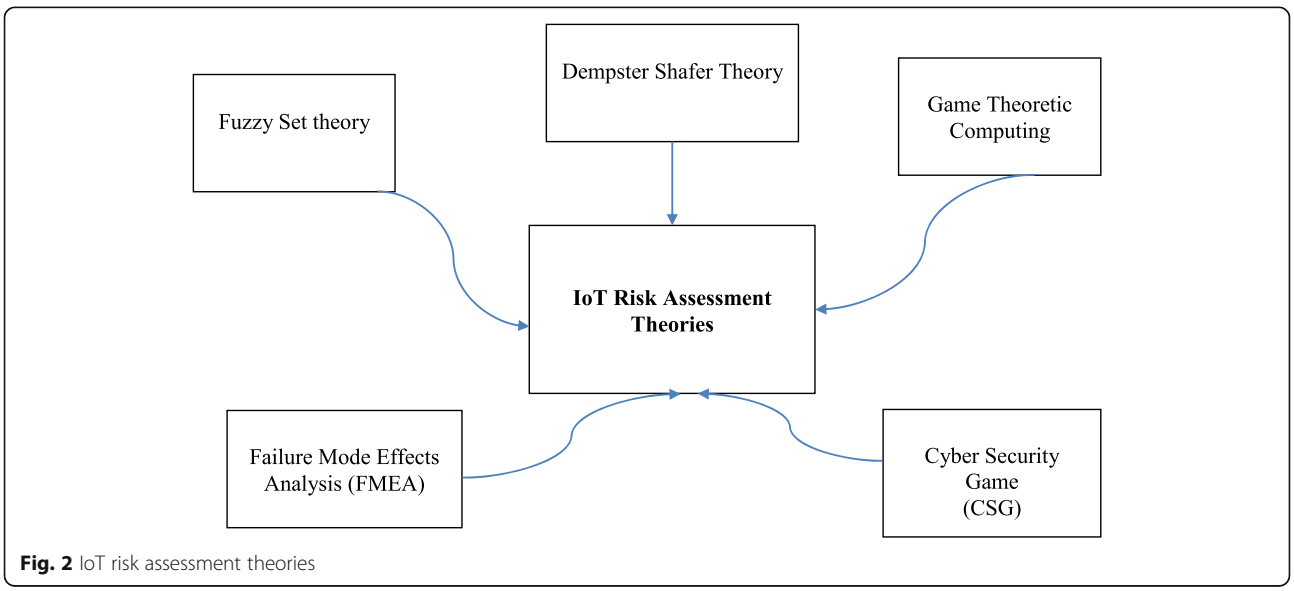

Fig. 2 IoT risk assessment theories

Computational models are given to include the quintessence of game-theoretic arrangements used in a risk evaluation, particularly in reference to digital frameworks and information security.

Cyber Security Game (CSG) [23] is a method to distinguish digital security hazards quantitatively and use this measurement to decide the ideal use of safety techniques for any specified systems for any predetermined venture level. The risk score is dictated by using a mission impact model to register the results of cyber incidents and joining that with the likelihood that assaults will succeed. A multidimensional methodology that incorporates both FMEA (Failure Mode and Effects Analysis) and fuzzy set theory is utilized for the risk management process [24]. FMEA is a complex designing investigation technique used to distinguish potential failure modes, circumstances, and problem areas affecting the system's hardware and software reliability, maintainability, and safety. This methodology examines five elements of data security: access to data and frameworks, communication security, infrastructure, security management, and secure data systems' improvement. Information with respect to the basic perspectives and failures of projects that produce vulnerabilities in their systems is given by this method.

3 Cyber risk frameworks

Risk assessment process (RAP) involves the identification of risks pertaining to all the assets in an organization including risk estimation and prioritization. Risk assessment is the core portion of the risk management process since it forms a foundation step towards risk treatment. Attack likelihood and impact of the attack are some of the features that are considered in the risk assessment process. There are guidelines on how to conduct the risk assessment process by NIST [25]. Risk treatment includes (a) accepting the risk if it is under harmless level (risk appetite), (b) mitigating risk by applying security measures, (c) transferring risk, or (d) avoiding risk by removing the affected asset itself. This section will summarize the vulnerabilities of IoT devices and different types of IoT risk assessment processes.

3.1 Vulnerabilities of IoT devices

The IoT environment deals with a lot of heterogeneous devices, and these devices might be vulnerable to cyber attacks. Sensor nodes, smart devices, and wearable devices that are used in the IoT domain are resource-constrained devices. The following vulnerabilities are possible with these devices: (a) CIA (confidentiality, integrity, and availability) triad is compromised if the network services are not secure enough on the IoT devices; (b) device and its related components are compromised if the web, API, and cloud are not secured; (c) lack of firmware validation on a device can lead to CIA triad violation and non-compliance; (d) use of insecure OS platforms and the use of components from a compromised supply chain could allow the device to be compromised; and (e) lack of hardening of devices (hardening is the process of securing a system by reducing its surface of vulnerability) lead to vulnerabilities. Few attacks such as Hajime, IoT Reaper, BrickerBot, or Mirai [26] exploit the vulnerabilities of IoT devices. The McAfee Mobile Threat Report 2019 [27] highlights the increasing proliferation of IoT devices leading to possible points of attack at homes. Due to the vulnerability of a component called ilnkP2P used in the P2P communication of the IoT devices, attackers can hijack devices like smart doorbells and security cameras. Attackers use vulnerabilities in web, and versatile applications utilized by certain IoT gadgets to secure certifications. These vulnerabilities would be utilized to understand and see the video feed, set cautions, expel spared video cuts from distributed storage, and read account data. Possible vulnerabilities could be due to (a) possibilities of cross-site scripting (XSS) attacks in Web applications, (b) possibilities of file directory traversal in cloud server, (c) unsigned device updates, and (d) device that ignores server certificate validity. Indeed, a Web application firewall that can protect servers from HTTP traffic at the application layer should be used by IoT suppliers. Recently, tremendous botnet-powered distributed denial-of-service (DDoS) attacks have exploited vulnerabilities of a few thousands of IoT gadgets utilizing them to send bad traffic to valid websites. Vulnerabilities drastically increase the risks born due to IoT devices, thereby mandating the need for a structured risk assessment process that is usually part of risk assessment frameworks.

3.2 IoT and RAP frameworks

There are a few popular RAP frameworks like NIST, ISO/IEC, and OCTAVE [28] that are currently in use. Each risk assessment methodology has its unique aspects. Two critical aspects that are pertinent to the measurement of risk are (a) nature of the approach and (b) the methodology adopted to measure the risk. Herein, we seek to investigate a few existing RAP frameworks, the specific methodology adopted by each RAP and their suitability to assessing IoT risks. There are qualitative and quantitative approaches to measure the cyber risks of an organization. The National Institute of Standards and Technology (NIST) [29] framework is well documented and provides guidance on risk assessment and management implementation [30], but it does not have a model to refer to. NIST does not contain an IoT impact assessment model, and it assesses risks qualitatively. Organizations can very well choose the NIST framework for disaster and recovery planning. However, NIST has special considerations for IoT risk

management. NIST IR 8228 [31] documents the potential challenges with IoT devices and risk considerations in achieving device and data security. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is another qualitative risk assessment framework that proposes eight steps [32]. These steps include (1) setting up criteria for measuring risk, (2) developing asset profiles, (3) identifying asset containers, (4) identifying concerned areas, (5) identifying threat schemes, (6) recognizing risks, (7) examining risks, and (8) mitigating risk. Qualitative and quantitative methods are combined in a few systems. GSMA company has come up with a framework for the IoT risk assessment process "(https://www.gsma.com/iot/iot-security-assessment/)" employing OCTAVE as the base risk assessment platform. GSMA is based on a structured approach that can fit into the supply chain model. ISO (International Standards Organization) includes cyber risk standards, and it promotes the standardization of cyber risk [33]. Few methods could be considered as complementary methods along with a main risk assessment process like NIST, and ISO. Threat Assessment & Remediation Analysis (TARA) is one such example that facilitates system recovery but fails in addressing the cyber risk impact level [34]. We focus mainly on NIST, OCTAVE, ISO, and TARA in this article. A critical analysis of these IoT risk frameworks based on different factors is presented in the next section.

4 Critical analysis of IoT risk frameworks

Before analyzing the IoT risk frameworks, it is important to know the uniqueness of IoT systems and the reasons for the inadequacy of current risk assessment approaches for IoT [35]. IoT systems can undergo drastic changes in a short period due to the interoperability of IoT devices, and hence, periodic assessments have their limitations in IoT systems. IoT systems have to be continuously assessed. Interconnected assets with the Internet can bring in new risks and device compromise in the IoT environment. Assets are treated as values of organizations in traditional risk assessment approaches, but IoT devices themselves can be the basis for attacks in the case of the IoT environment. In IoT systems, failure can also happen when the assessment is done for the processes through which devices are bound i.e., the connections that allow these devices to couple and operate. Hence, the traditional cyber risk assessment process has to be customized for IoT systems keeping the above points in view. Due to its connectivity model, IoT deployment is different from traditional IT. The IoT environment deals with various connectivity models and devices which may not support the CIA triad. Common safeguards include technologies such as data encryption, authentication, and access controls, and automated software patching or updates. Though IoT devices are flexible and interoperable, they increase the attack surface. Device firmware updates, protocol updates, and the applications again lead to increased attack surface that needs to be secured. Based on these considerations, it is advisable that the IoT risk assessment process should be designed to be very comprehensive. Most of the widely used IoT risk assessment frameworks are compared for their strengths and weaknesses in the next subsection.

4.1 IoT CSRF analysis

Several CSRFs (Cyber Security Risk Frameworks) were discussed in the previous section, including OCTAVE, NIST, and ISO. Needless to add, special care needs to be taken for assessing risk in the IoT environment as the notion of IoT brings in complex risk on assets/devices. There are no standard IoT risk frameworks that are currently available. But the existing risk assessment frameworks can be slightly modified to handle the IoT risks. To standardize the impact assessment approaches, Radanliev et al. [36] have built a model to identify and capture IoT cyber risk from the derived risk vectors that offer new design principles for assessing cyber risk. They also performed an empirical analysis of different risk assessment methods to define a target state for companies integrating IoT devices with services [37]. This method used a goal-oriented approach for standardizing IoT risk impact assessment. A new IoT MicroMort model for calculating IoT risk has been introduced [38] which can test and validate IoT-connected devices. This system can even calculate future forecasts for IoT risk. New methodologies to assess risk considering the dynamics and uniqueness of IoT have been described elsewhere [35]. An IoT security certification methodology for assessing security solutions in an automated way has also been proposed [39]. Here, IoT-related risks are mapped with COBIT5 risk management process, and an IoT risk framework is proposed with the associate effective processes, roles, operations, and risk areas [40]. A Core Unified Risk Framework (CURF) [41] compares different existing methods and provides a measure of completeness. In all the above frameworks, the risk vectors specific for IoT systems are considered to mitigate and manage the risks materialized by IoT devices.

4.2 NIST considerations for IoT

NIST's Cybersecurity for IoT program [31] has created and connected norms, rules, and related tools to improve the security of associated gadgets and the conditions where they are. By working together with partners crosswise over government, industry, universal bodies, and academia, this program intends to develop trust and empowers advancement on a worldwide scale. NIST suggests possible approaches to IoT conformity

assessments such as (a) different assessments can be created based on device type and function, (b) industry can lead to best practices for creating requirements and assessment approaches, (c) can design assessments to enable the flexibility needed to meet market demand, (d) leverage different conformity assessment approaches (e.g., self-attestation, third party attestation) based on the risk associated with device type or environment, and (e) focus on IoT device capabilities, not the use. NIST has three goals concerning IoT risk management—to protect device security, data security, and privacy of individuals. NIST is a widely used framework for risk management, and it is highly suited for disaster and recovery planning in domains involving IoT systems.

4.3 OCTAVE for IoT

OCTAVE is appropriate for the risk assessment of smart homes as it has an asset container to cover cyber and physical security [42]. OCTAVE helps to find out various security vulnerabilities of IoT-based smart homes, presents the risks on home inhabitants, and proposes approaches to mitigate the identified risks. OCTAVE considers four phases as follows:

1) Establish drivers phase: This phase develops criteria for measuring risk which is the foundation for risk assessment
2) Profile assets phase: This phase establishes limits for assets and identifies security requirements
3) Identify threats phase: This phase identifies security threats from the assets where the information asset is stored, transported, or processed
4) Risk mitigation phase: This phase determines and executes a risk mitigation strategy for the identified assets.

OCTAVE uses a standardized questionnaire for categorizing recovery impact portions and does not quantify the risk.

4.4 TARA for IoT

TARA is a predictive framework for the most crucial exposures. There are three main advantages of TARA. It breaks down prospective attacks to a manageable list of probable attacks. It improves the quality of risk and control evaluations and communicates risks and recommendations to the organization. It can enhance outcomes, decrease the general effort of risk analysis, and help to make better decisions. It was developed for a big, highly precious, and diverse environment within Intel$^{(R)}$ in response to a need to assess the security risks of a very complicated, quickly evolving threat landscape. TARA does not quantify the impact of risks and does not promote the defense against vulnerability. In most of the cases, TARA is used along with the NIST framework and the IoT considerations of NIST are applicable here also.

4.5 ISO for IoT

ISO promotes compliance and standardization and is based on voluntary compliance and consensus-based standardization. Indeed, the international experience gets reflected in ISO since the measures are created by the individuals that need them through an agreement procedure. ISO reflects an abundance of global experience and learning since the specialists from all over the world help in building up the required ISO standards. The biggest chance for ISO cyber risk assessment is the potential to grow into a worldwide standardization reference. Since ISO contains individuals from 161 nations and 778 specialized boards and subcommittees, this poses a great challenge in the coordination and integration of specific standards. ISO/IEC 27001 standard establishes and maintains information security risk criteria, recognizes risks related to the loss of security and availability for information, identifies the owners of those risks, and analyses information security risks according to certain criteria. ISO/IEC 30141 gives the reference architecture needed to reduce the risks and maximize the benefits for IoT applications. Also, ISO/IEC 27030 gives the guidelines for security and privacy for IoT systems.

Table 1 summarizes the focus areas, strengths, weakness, and other attributes for each of these CSRF. It also gives details on the approach of assessment, industries where they are used, and the published standards.

From Table 1, it can be inferred that all four CSRF's cover the CIA principles. In consonance with a critical analysis of the CSRFs, it is also important to venture into the risk assessment process followed in the industries, finance, and healthcare sectors. In the next section, we elucidate the CSRFs that are currently being used in these sectors for IoT.

4.6 CSRF in industrial and financial sectors

Supervisory Control Received and Data Acquisition (SCADA) systems and Cyber-Physical Systems (CPS) are the main examples of industrial systems using IoT. In the following subsections, we delineate CSRF in such industrial and financial sectors.

4.7 CSRF in SCADA and CPS systems

SCADA and IoT are both about sensors and data acquisition, but the common goal of both systems is the optimization of use and better control over the devices or a process. Hence, it is essential to discuss the risk assessment systems in SCADA and CPS systems. Security best practices and risk assessment of Industrial Control Systems (ICS) and SCADA, which is a type of ICS are

Table 1 Comparison of CSRF

Name of CSRF	Owner	IoT focus areas	Strengths	Weakness	Industries used/ applied	IoT risk assessment approach	CIA coverage (Y/N)	IoT published standards
NIST	NIST	Standards, Technology, Partnerships, Publications, Market Intelligence, and government adoption	More valuable framework in managing cyber risks and excellent for disaster and recovery planning	Framework is documented but this is not an automated tool. No quantification of risk.	Manufacturing, insurance, healthcare, financial, government, and security/risk consultancy firms	Compliance (standards and guidelines with documentation)	Y	Yes
OCTAVE	Octave Allegro	Information assets of the organization	Standardized questionnaire is addressed to explore and classify recovery impact areas	No quantification method for calculating recovery	Smart homes, aimed for companies with limited resources	Qualitative method	Y	No
TARA	Intel	Threat susceptibility Analysis and Risk Remediation Analysis	Predictive framework for most crucial exposures	No quantification of risk impact	Manufacturing, insurance, healthcare, financial	Qualitative method	N	Yes
ISO	ISO with 164 national standard bodies	Global standardization of risk assessment	Promotes standardization of cyber risk and follows international experience and knowledge	International standardization on requires a level of compulsory compliance	Small business or corporate, government or private	Compliance (Standards and guidelines with documentation)	Y	Yes

taken into consideration [43], and a risk model has been developed for ICS using the CORAS framework tool [44] which is a UML (Unified Modelling Language)-based risk modeling language. Around 24 risk assessment methods developed or applied for SCADA systems are reviewed excellently elsewhere [45]. A detailed survey of the ICS risk management systems [46] has considered application domain, impact measurement, and tool support, and finally, a general probabilistic risk analysis framework has been presented. Decision support is provided by quantifying risk factors [47] and encryption and modification of the operation software for critical infrastructures are also recommended. Cybersecurity attacks in a CPS system lead to various risks affecting the infrastructure, degrading the performance and making the critical services unavailable. As in other systems, it is important to protect CPS from such risks. Of note, due to the inherent complexity of the CPS system, risk management is very challenging. To identify the critical CPS assets and assess their vulnerabilities, a risk management framework for CPS has been reported [48]. RiskWatch tool provides risk/vulnerability assessments and utilizes easy-to-use interfaces, complete information databases, predefined risk examination layouts, information connecting capacities, and demonstrated risk investigation diagnostic systems [49]. Pointers to set of rules, best practices, security devices, innovations of governmental agencies (NIST) and industrial associations like North American Electric Reliability Corporation (NERC), or American Gas Association (AGA) have been described [46]. Probabilistic risk assessment to estimate the risk (exposure or expected loss) for SCADA and DCS installations are being improved by constant updates. Furthermore, all the security controls in CPS systems may be easily extended to the IoT systems.

4.8 CSRF in financial systems

In the global economy of the 21st century, it appears highly likely indeed that the IoT domain will change how banking and financial sectors operate. Since the financial business manages enormous data transfer, assembling and breaking down of information, IoT systems have a huge impact on it which is beneficial to both the financial administrations and the client. Rapid innovations in IoT have given an impetus to the banking and money industry enabling them to help their clients in their pursuit of business goals and outcomes. Biometric and positional sensors play a vital role in the financial business to follow-up with quality control. With the IoT innovation, banks can dispatch better and remain focused on administration. It will help the financial business to comprehend what item to dispatch and furthermore help to choose the opportune time for dispatching the item. IoT innovation has made customized showcasing workable for the bank to monitor all customer exercises and offer services according to their preferences. The IoT innovation guarantees that the entire financial experience ought to be protected and secure. IoT can assist in saving money with understanding the customers' present financial condition and offer solutions to the customer as per requirements. This will guarantee a good customer experience leading to a healthy banking

relationship with their client. IoT innovations have also made it workable for the banking and monetary industry to identify any administration flaw and carry it to the notice of the bank to deal with the issue. With IoT innovation, a bank can likewise follow the past activities and client behavior. IoT innovation in the banking and finance industry gathers information through portable applications and computerized sensors. Indeed, almost every bank has mobile applications for banking that give silos of information at a humongous scale, which helps the banking and monetary industry to accurately dissect client conduct and requirements.

One of the most significant advantages of IoT in the financial segment is giving fulfilling, simple administrations to both credit and debit card clients. Banks can dissect the use of ATM stands in explicit territories and increment/decline the establishment of ATMs relying upon use volumes. Banks can also utilize IoT information in expediting request benefits to clients by giving booths and by improving administration services. The client information accessible through IoT will help banks recognize their clients' business needs, their value chain—like providers, retailers, distributors—and furthermore gain client insights. Cyber attacks on the financial institutions are increasing day by day. Stealing money/data, disrupting operations, destroying infrastructure, and compromising data-rich financial services institutions (FSIs) are some of the goals of cybercriminals. It is quite evident that the risks presented by financial sectors have to be assessed and managed. There are few risk assessment frameworks used currently by banks including NIST. A framework that assesses risk quantitatively for financial sectors has been elaborated [50]. This is based on the VaR type framework to assess stability risk. Some challenges that financial institutions face in measuring cyber risk are highlighted and several leading cyber-risk management methodologies have also been assessed [51]. Recommendations and insights into how financial institutions can quantify cyber risk are also provided by this system. The RiskLens software platform [52] helps to manage cybersecurity risk by quantifying it in financial terms. RiskLens is built on FAIR [53], which is a world standard cyber risk quantification model. RiskLens is based on software as a service solution type, and it assesses, prioritizes, and justifies security investments.

4.9 Cyber Security Risk Frameworks in healthcare systems

The healthcare sector is one of the 16 critical infrastructure sectors, and data breaches are increasing every day in healthcare due to phishing attacks, misconfigured databases, ransomware attacks, malware attacks, and errors caused by employees and third-party vendors. Hence, it is important to identify such risks and treat them. Unlike the other sectors, healthcare sectors use many biomedical devices (for example, cardiac pacemakers, continuous subcutaneous insulin pumps), and these devices cause additional risks to patient privacy. Currently, thanks to the ubiquitous application of the Internet and networks in real-time and static monitoring of medical devices, there is a proportional rise in the risk of potential cybersecurity threats. These cybersecurity threats impact the effectiveness of the device and electronic health records (EHR) security. Therefore, healthcare systems need risk frameworks that can assess such risks due to IoT medical devices and mitigate them. Further, remote telemedicine and robot-assisted surgeries need precision, accuracy, and privacy and pose different risks to patient privacy and safety.

4.10 CSRF for healthcare and medical IoT devices

A cyber risk scoring system has been proposed [54], which takes a doctor's assessment of a medical device into account. A doctor's worst-case assessment of the potential of a medical device to impact a patient is considered here. A STRIDE model (developed by Microsoft$^{(R)}$ to classify threats [55]) is used to generate risk scores for these devices. This scoring system improves the method of assessing cyber risk for medical devices. Ease of use, low cost, and intuitively appealing results are the three key objectives of this system. In case of any adverse events, we would want to capture the impact factors and this is accomplished by a medical risk assessment model [56]. Risk scenarios are shown using a static fault tree, and this system introduces Bayesian inference to investigate the operations of medical devices. Haemodialysis infection is used as an example case, and simulation methods like Monte Carlo simulation and Petri net are recommended. Interestingly, a structured framework has been proposed [57] to describe, design, and implement healthcare IoTs. This process helps in standardization and interoperability. An IoT risk assessment method by an Artificial Immune System has been reported [58]. Using set theory, this system derives the simulation of immune principles and the attack detectors. Quantifying risk assessment of IoT security enables an accurate and credible risk assessment process. With the digital age ushering in a revolution in medical healthcare practices, a cybersecurity risk framework that can identify the risks involved with the medical devices and EHR data has become a necessity. This ideal framework should also be able to prioritize the risks and take necessary actions for mitigation of risks. According to the 2018 HIMSS Cybersecurity Survey "(https://www.himss.org/sites/hde/files/d7/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf)", the most used (57.9%) security framework in healthcare is NIST, and Health Information Trust Alliance (HITRUST) comes next with 26.4%. Herman et al. [59] suggested considering the NIST

cybersecurity framework as a mandatory aspect for healthcare sectors. NIST guidelines [60] improve the cyber risk management process for critical infrastructures. HITRUST [61] CSRF is based on ISO standards and the International Electrotechnical Commission (IEC) standards. This has the package containing HIPAA, ISO, NIST risk management framework, COBIT, and Payment Card Industry (PCI) Data Security Standard. Symantec(R) has broken down the NIST CSFs five functions from identifying the risk until the recovery process and analyzed how these functions need to be modified for health sectors. To meet healthcare requirements and regulations, the NIST framework needs to undergo a few modifications. PROTECT function of NIST which deals with security along with awareness and training to employees' needs to be modified. To identify a healthcare breach in time, the core components of the DETECT function which includes anomaly detection should be continuously monitored. It is important for healthcare organizations to come up with technologies to understand when and how the breaching occurs and how to mitigate the risk. Ultimately, the five core functional areas of the NIST framework—Identify, Protect, Detect, Respond, and Recover are to be thoroughly studied and modified according to the needs of the healthcare sector. Extending the five areas to IoT systems to provide continuous assessment is an ideal goal for the future.

4.11 IoMT risk domain

It is critical to understand the extraction of the cyber risk vectors for the IoMT, especially medical devices. Aman et al. [62] have aligned risk management system models relating to security services with the standard HIPAA requirements and gauged existing risk management approaches for IoT-driven eHealth. The Internet of Medical Things (IoMT) is a combination of medical devices and applications that are connected to healthcare information technology systems using a wireless network or online computer network. For example, IoMT connects patients with doctors and allows the transfer of medical data over a secure network. Thus, unnecessary hospital visits are reduced. Patient monitoring is one of the main applications of IoMT in hospitals. Several hospital types of equipment like magnetic resonance imaging (MRI), functional MRI (fMRI), computed tomography (CT), and positron emission tomography (PET) scanners are monitored remotely by the device manufacturers, and this is very helpful for them to detect and correct issues with the devices in real time even before the issue reaches them or gets magnified in severity. Several companies also use IoMT for performance upgrades of their products and for remote diagnostics. Biosensors are one of the main components of IoMT and detect characteristics of blood, respiration, and tissues. Non-bio/physical medical sensors measure body temperature, motion, the electrical activity of the heart and muscles, and other patient characteristics.

IoMT has privacy and security issues in all layers like IoT. The perception layer of IoMT has to acquire data (e.g., heart rate, temperature) from sensors and transfer to the network layer. There are four different medical things (MTs) possible in the perception layer:

a) Wearable devices: Smartwatches, temperature and pressure sensors, heart monitoring and muscle activity sensors, and glucose and biochemical sensors
b) Implantable devices: Swallowable camera capsule for visualization of the gastrointestinal tract, embedded cardiac pacemakers, and implantable cardioverter-defibrillators (ICD)
c) Ambient devices: Motion sensors, door sensors, vibration sensors, etc.
d) Stationary devices: Imaging devices like CT scan and surgical devices

Possible attacks in each of the IoMT layers are given below [63]:

- IoMT perception layer: Device tampering, tag cloning, and sensor tracking.
- IoMT network layer: Eavesdropping, replay, MiTM, rogue access, and DoS.
- IoMT middleware layer: Cross-site request forgery, session hijacking, and cross-site scripting (XSS).
- IoMT application layer: SQL injection, account hijacking, ransomware, and brute force.
- IoMT business layer: Information disclosure, information deception, disruption due to DoS, and unauthorized access of the system due to sinkhole attack

IoMT risk r of a medical device d can be calculated as $r(d) = \Sigma\, p\,(d) \times k\,(d)$ where p represents the impact of successful attack of device d and k represents the likelihood of an attack of device d.

4.12 Applications of IoMT devices

Remote patient monitoring (RPM) helps in monitoring patients' heart activities and glucose level, and the doctors can be automatically alerted when needed. There are wearable smart devices that can monitor a user's physiological parameters such as heart rate, oxygen saturation (pulse oximeter), electrocardiogram (ECG) patterns, blood glucose levels, the electrical activity of cardiac pacemaker in the event of a cardiac event, etc., in real-time and transmit these data to the consulting physician. Thus, healthcare providers, insurers, doctors,

and patients all greatly benefit from IoMT due to improved quality of patient care. Not surprisingly, a cardiologist can monitor a patient's heart activity using smartphones and patients can view their own data using online patient portals. An in-home glucose monitor and an emergency room heart monitor are some other applications of IoMT. IoMT helps insurers to view patient data more quickly and make the processing of claims faster and accurate. However, there are ample opportunities for many kinds of attacks in IoMT. IoMT devices are subject to a lot of cyber attacks and need risk management processes to help in the mitigation efforts [64]. Some of the popular IoMT devices are elucidated below to help appreciate this application better:

Smart glucose monitor: Diabetes patients wear this to keep tabs on their blood sugar levels. This wearable medical gadget is connected to a remote system and with cell phones so it can perform a continuous evaluation of blood glucose levels.

Pacemaker: It is a little gadget that is set in the chest or mid-region to help control aberrant heart rhythms. This gadget uses low-intensity electrical stimuli to prime the heart to function at a normal rate.

Insulin pumps: These are little, automated gadgets that sense blood sugar levels of the wearer and mimic the manner in which the human pancreas works by injecting little portions of short-acting insulin ceaselessly through microneedles.

4.13 IoMT attacks

There are heavy challenges in implementing IoMT devices including the high infrastructure cost, security concerns, load with the existing network, and lack of standardization. Bluetooth Low Energy (BLE) is a wireless personal area network technology aimed at novel applications in healthcare, home entertainment, and security. BLE has risks including Man in the Middle (MitM) attacks, replay attacks, and network communication decryption. Encryption is not carried out by many devices in the BLE link layer [65]. Though encryption is done, there are chances for some BLE devices to be affected by Man in the Middle (MitM) attacks. Network traffic is intercepted by the attacker through impersonation [66]. Denial of service (DoS) attacks are also possible. Food and Drug Administration (FDA) recommends following certain measures such that the proper safeguards are applied by device manufacturers "(https://www.fda.gov/medical-devices/digital-health/cybersecurity)". Blockchain technology offers the only framework robust enough to meet IoMT security challenges. One of the most life-threatening situations is when one of the IoMT gadgets controlling drugs shuts down due to a patch-related reboot in the middle of a surgical procedure. Unfortunately, this can have catastrophic consequences for the life of the patient on the operating table. Banerjee et al. [67] list security techniques using blockchain technology. FDA provides recommendations to mitigate and manage cybersecurity threats. A playbook [68] by MITRE Corporation(R) covers preparedness and response for medical device cybersecurity issues. Patients in general appear to be unaware of the dangers of cyber attacks, and they consider the security of their implanted medical devices (IMDs) as a secondary aspect [69] perhaps due to lack of adequate awareness. It remains to be seen whether patients and clinicians will acknowledge the need for specialized security safeguards even if they are created and provided [70]; hence, more work needs to be done to enhance awareness of potential cybersecurity risks in the medical device arena.

4.14 Risk vectors for IoMT

A unique taxonomy toolset has been proposed [71] to handle the vulnerabilities of medical devices. This has an effort gap analysis matrix to find out the gaps of efforts in applications. This toolset helps to better understand what effort has been made by different associated parties to tackle the medical device vulnerability problem and also helps the associated parties determine which areas need further attention. Sixteen risk factors are extracted by Yoneda et al. [72] using the risk breakdown method for the embedded medical devices. These risk factors come under three categories viz., intentional, unintentional, and external risks between the devices. For the purpose of risk prediction, a framework called PRIME has been developed [73] which incorporates discrete prior medical knowledge into the predictive models using the posterior regularization technique. With a log-linear model, PRIME can automatically learn the importance of different prior knowledge. For risk prediction, two deep learning models viz., convolutional neural network (CNN) and long short-term memory network (LSTM), are used.

4.15 IoT risk assessment considerations

It is indeed evident that it is not possible to build a perfect risk assessment system for IoT devices unless the risk vectors or risk attributes are identified. Apart from the original risk vectors from the traditional systems, special IoT vectors also need to be considered for an IoT risk assessment system.

4.16 IoT risk assessment summary

There are four types of IoT risk vector classes that have been identified: cloud-related, real time-oriented, autonomous, and recovery-related. Table 2 summarizes below the list of IoT risk vectors for each of these classes that are used for risk assessment for any IoT system [36].

NIST has come up with three main goals for IoT risk assessment: (a) device protection, (b) data protection, and (c) user privacy. They are delineated with their subcategories in Table 3 below for the benefit of the reader [31].

4.17 Risk assessment scale and ranking

The first step in risk assessment is to identify the threats for an IoT asset under consideration followed by the determination of the inherent risk and its impact. Risk impact has ratings like high, medium, and low. As an example, a "high" impact rating means that the impact could be substantial. Medium implies that the impact would be damaging, but recoverable, and/or is inconvenient. Low represents that the impact would be minimal or non-existent. The next step is to determine the likelihood of the given exploit taking into account the control environment that your organization has in place. Examples of likelihood ratings are as follows:

- High—the threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
- Medium—the threat source is motivated and capable, but controls are in place that may impede the successful exercise of the vulnerability.
- Low—the threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

The risk ranking can be calculated as risk ranking (rr) = impact (if exploited) × likelihood (of the exploit).

Some examples of risk rankings are as follows:

- Severe—a significant and urgent threat to the organization exists and risk reduction remediation should be immediate.
- Elevated—a viable threat to the organization exists, and risk reduction remediation should be completed in a reasonable period of time.
- Low—threats are normal and generally acceptable, but may still have some impact on the organization. Implementing additional security enhancements may provide further defense against potential or currently unforeseen threats.

Calculation of risk rank is done based on quantitative weightage (this refers to the impact of risk) and the risk score (this refers to the likelihood of risk) as explained above.

Table 4 depicts how the ranking can be done for each risk. If the risk rank is very high, then the risk has a severe impact. There are five levels shown for IoT risks based on the rank calculation. There are risks with rank ≤ 10 and these risks come under a very low level since they are not worthy to be considered. Low and moderate risks need to be considered. High and very high risks need better treatment as their impacts are high.

Table 5 depicts the ranking of risk for some of the IoT vectors. These unit vectors belong to the "device protection" category as per the NIST IoT document [31]. As discussed already, the other two categories are data protection and individual privacy. Device protection has four risk mitigation areas including asset management, vulnerability management, access management, and incident detection.

- *Asset management*: For maintaining an accurate inventory of all IoT devices and their relevant characteristics which helps to use this information for cybersecurity and privacy risk management purposes.
- Vulnerability management: For identifying and eliminating known vulnerabilities in IoT device

Table 2 IoT risk vectors

S. no	Cloud-related	Real-time	Autonomous	Recovery
1	Cloud-computing platforms	Operational models in real time	Automated environments	Economic impact
2	Cloud technology skills	Customized products	Robotics and autonomous systems	Impact assessment
3	Cloud data centers	A platform for real time information	Robotics and artificial intelligence	SWOT (Strength, Weakness, Opportunities, Threat) analysis
4	Cloud software	Digital real time and interoperable records	Robotics in IoT	Financial and fiscal state control
5	Cloud monitoring	Cyber-physical systems	Artificial intelligence and control systems	N/A
6	Integration in cloud computing	N/A	N/A	N/A
7	Cloud security networks	N/A	N/A	N/A

Table 3 IoT risk assessment categories of NIST

S. no	Device protection	Data protection	User privacy
1	Asset management	Strong encryption capability of IoT device	Disassociated data management
2	Vulnerability management	Sanitation of sensitive data	Informed decision making
3	Access management	Provide secure back-up	Processing permissions management
4	Incident detection	Verify the identification of other computing devices	Information flow management

software and firmware to reduce the likelihood and ease of exploitation and compromise.

- Access management: For preventing unauthorized and improper physical and logical access to IoT devices by people, processes, and other computing devices.
- Device security incident detection: For monitoring and analyzing IoT device activity for signs of incidents involving device security.

Identifying asset vulnerabilities is one of the primary steps in the risk assessment process. IoT devices are the main assets considered here. Sample IoT vectors and their risk ranking calculations are furnished in Table 5 for each of the abovementioned risk mitigation areas under the "device protection" category. The ideal next step is the identification of threats and the impacts and likelihood of risks. The goal is to prevent an IoT device from attacks, like distributed denial of service (DDoS) attacks, and eavesdropping on network traffic or compromising other devices on the same network segment. Like this example, ranking can be calculated for risk in any category including data security and privacy.

Table 5 shows the rank details of each unit vector and the implication of risk rank. For example, when the IoT device does not support the use of strong credentials, weightage 95 is given to this IoT vector along with 0.9 as a risk score which calculates the risk rank as 85. This rank comes under high priority since the chances of unauthorized access and tampering through credential misuse are more. Next section deals with the IoT risk computational model with the practical application of IoMT risk categorization. A novel method for computing IoT risk and its application to the IoMT domain is presented in the next section.

4.18 IoT risk computation: a novel method and its application

In this novel approach, the goal is to compute the cyber risk for IoT systems considering the IoT specific factors and apply this method to IoMT devices to ascertain their risk level. The risk for any given device d is computed as follows:

$$r(d) = w(d) \times s(d)$$

where w represents the potential risk impact due to vulnerabilities/attacks and s represents the likelihood of the risk.

To calculate the risk impact, the following parameters are considered.

a) Type of the network: An unsecured network provides no security and exposes all open traffic, and hence, the risk impact would be maximum. Insecure network services running on the IoT systems, that are also exposed to the Internet, compromise the confidentiality, integrity, or availability of information or allow unauthorized remote control as covered by OWASP [6].
b) Protocol type: IoT requires lightweight protocols such as 6LoWPAN and IEEE 802.15.4. There are communication protocols like MQTT, DSS, TCP, UDP, and connectivity protocols like Wifi, Zigbee, Bluetooth, and RFID. Each protocol is subjected to attacks [74].
c) Count of heterogenous systems involved: If there are more intermediate systems involved, the impact of the risk would be huge. Critical IoT infrastructure systems with more number of

Table 4 Risk rank calculation

Qualitative level	Quantitative weightage (W)	Risk score(S)	Rank = $W \times S$ (shown examples)	Risk rank range	Description
Very high	96–100	1.0	97 × 1.0=97	81–100	Risk is of very high concern; severe impact
High	80–95	0.8	90 × 0.8=72	51–80	Risk is of high concern
Medium	31–79	0.5	50 × 0.5=25	21–50	Risk is of moderate concern
Low	11–30	0.2	25 × 0.2=5	5–20	Risk is of low concern
Very low	0–10	0.1	10 × 0.1=1	0–4	Risk is not of concern

Table 5 Risk rank calculation for IoT device protection

IoT risk vector	Quantitative weightage (W)	Risk score(S)	Rank = $W \times S$	Description/implication
IoT device does not have a unique built-in identifier	75	0.8	60 (medium)	Remote access and vulnerability management are affected
IoT device's external dependencies are not revealed by the manufacturer	60	0.7	42 (medium)	Managing the risk of external software and services are not possible
Patches or upgrades for the IoT device are not released by the manufacturer	50	0.6	30 (low)	Known vulnerabilities cannot be removed
IoT device is not capable of having its software patched or upgraded	60	0.6	36 (medium)	Known vulnerabilities cannot be removed
No vulnerability scanner that can run on or against the IoT device	60	0.6	36 (medium)	Cannot automatically identify known vulnerabilities
The IoT device does not support the concealment of displayed password characters	80	0.7	56 (medium)	Increases the likelihood of credential theft
The IoT device does not support strong credentials cryptographic tokens or multifactor authentication)	95	0.9	85 (high)	Tampering through credential misuse is possible
The IoT device does not support enterprise user authentication system	90	0.8	72 (medium)	Each user needs more credentials
The IoT device is not able to log its operational and security events	70	0.6	42 (medium)	Probability of detection of malicious activities are very less

heterogenous devices tend to increase the cyber attacks, mainly the network-related attacks [75]

d) Device security: An unsecured device is prone to a lot of attacks. For example, the number of IoT devices that can be affected is limited to IP-based cameras for Persirai and DVRs, routers, and CCTV cameras for Mirai. The MicroMort values are calculated with the total number of IoT devices from the Garner report [76].
e) CIA type: If an attack affects confidentiality, integrity, and availability, then this will create a huge risk impact. If there is going to be a replay attack (confidentiality and integrity are affected) and DoS attack (affects availability), then the impact of the risk is high and this could happen in the network layer of the implantable devices [77].

Table 6 shows the weights for each of the above risk impact parameters.

Based on the above discussion, the risk impact w of device d can be derived as below.

$$w(d) = [nwt(d) + prt(d) + het(d) + des(d) + cia(d)]/5$$

To calculate the likelihood of the risk, the following parameters are considered (Table 7).

a. Count of past attacks for the device (pat): If there is a history of past attacks, then it is more likely that the device gets attacked again.
b. IoT layer that undergoes lots of attacks (lyr): As discussed earlier, all layers of IoT undergo the cyber attacks and whichever layer undergoes more attacks gets more weight. It is observed that the network layer of IoT/IoMT undergoes a number of attacks [77].
c. Type of sector using IoT (scr): IoT is used widely in industries, financial sectors, and healthcare sectors.

Table 6 Risk impact parameters with weights

S. no	Risk impact parameter (RIP)	RIP types	Weights (*W*)
1	Type of network (nwt)	Unsecured network	10
		Network with minimum security	5
		Completely secured network	2
2	Protocol prone to attacks (prt)	Prone to more attacks	10
		Prone to fewer attacks	5
		Not prone to attacks	2
3	Count of heterogeneous systems involved (het)	More heterogeneous systems involved	10
		Few heterogeneous systems involved	5
		No heterogeneous systems involved	2
4	Device security (des)	Completely unsecured device	10
		Partially secured device	5
		Totally secured device	2
5	CIA type affected (cia)	CIA—all there are affected	10
		Only CI or IA or CA is affected	5
		Either C or I or A get affected	2

Table 7 Risk likelihood parameters with weights

S. no	Risk likelihood parameter (RLP)	RLP types	Weights (W)
1	Past attacks on the device (pat)	Device underwent lots of past attacks	10
		Device underwent few past attacks	5
		Device underwent no attacks in the past	2
2	IoT layer with more attacks (lyr)	Network layer	10
		Application layer	5
		Physical layer	2
3	Sector (scr)	Healthcare	8
		Financial	7
		Others	5
4	Device risk factor (drf)	Pacemaker, insulin pump	9
		Remote heart monitor	8
		Blood sugar monitor	6
		Medical sensors	4

It is important to identify which sector is impacted more due to IoT attacks. A survey finds that 82% of healthcare industries have undergone IoT-focused cyber attacks, and 230 out of 700 of the survey respondents belong to the healthcare sector "(https://www.fiercehealthcare.com/tech/82-healthcare-organizations-have-experienced-iot-focused-cyber-attack-survey-finds)".

d. Device risk factor (for IoMT only): There are a number of IoMT devices used in the healthcare sector, but we categorize them according to the fatal risk they can create to patients. For example, pacemaker and insulin pumps can cause death to patients if they are controlled remotely by attackers.

Based on the above discussion, the likelihood of risk can be derived as below.

$$S(d) = [pat(d) + lyr(d) + scr(d) + drf(d)]/4$$

The abovementioned formulae for computing impact and likelihood are applied in Table 8 for IoMT devices. This table shows the risk score calculation based on the risk impact and risk likelihood parameters as discussed above. For example, when the pacemaker undergoes side-channel attack, we calculate the impact of the attack and its likelihood with the formulae explained above and derive the risk score to be 72, which represents a higher risk level when compared to the tampering attack of the blood sugar monitor which comes under the medium risk level. Accordingly, the risks can be treated/mitigated.

In the above scenario, when the pacemaker is not secured (des = 10) along with a few heterogeneous systems (het = 5), it undergoes side-channel attacks due to unsecured network (nwt = 10) and the protocols susceptible to attacks (prt = 10). Hence, the risk impact is calculated as 8, as per the formula discussed above. Control of the pacemaker remotely by attackers can be fatal, and hence, it is classified under the high-risk factor (drf = 10) in the healthcare sector (scr = 8). A side-channel attack is a network attack (lyr = 10), and we assume that the pacemaker has undergone such attacks in the past (pat = 10). Finally, the risk score is calculated as 72 which represents a high-risk level. In the same way, tampering of blood sugar monitor leads to the risk impact factor of 6 and the risk likelihood factor of 6, and hence, the risk score is 36 which represents a medium risk level. As discussed in Table 4, the risk score range of 21–50 falls in medium risk level and the risk score range of 51–80 falls in high-risk level.

5 Conclusion

This work provides comprehensive coverage of the IoT risk domain through the lens of risk frameworks, applicable theories, industries, risk vectors, and a novel risk score computational model. A critical analysis of the cyber-security risk assessment frameworks suitable for IoT systems is presented. Applications of IoT risk assessment frameworks in the area of finance and healthcare are discussed, with the aim of presenting the maturity of the IoT risk domain. Four risk frameworks are discussed in detail, viz., NIST, OCTAVE, TARA, and ISO. IoT risk considerations of these frameworks are explained along with their strengths and weakness, and focus areas. A solid treatment of the IoMT risk domain is included with the intention of bringing to the fore critical risk issues connected with the IoMT domain. A summary of the IoT risk assessment is presented along with a risk scoring system, suitable for the IoT domain to highlight the quantitative approach. Risk rank for IoT risk vector categorizes the risks into low, medium, or high categories. This study has initially focussed on the broader IoT domain and finally narrowed down to IoMT

Table 8 IoMT real incident risk classification

IoMT device	Attack	Nwt	prt	het	des	cia	*Risk impact*	pat	lyr	scr	*drf*	*Risk likelihood*	*Risk score*	*Risk level*
Pacemaker	Side channel	10	10	5	10	5	***8***	10	10	8	*9*	***9***	***72***	***High***
Blood sugar monitor	Tampering	5	5	10	5	5	***6***	5	5	8	*6*	***6***	***36***	***Medium***

risk analysis. The highpoint of this work is the introduction of a novel IoT risk computational model, that computes risk impact and risk likelihood, leading to risk score. An application of this model to IoMT devices is presented to convince the reader about the need for a unique approach to IoT risk computation. This work has the potential to trigger more investigations in the area of IoT and IoMT risks.

Abbreviations

AGA: American Gas Association; ARA: Adversarial Risk Analysis; BLE: Bluetooth Low Energy; CCTV: Closed-circuit television; CIA: Confidentiality, Integrity, and Availability; CNN: Convolutional neural network; COBIT5: Control Objectives for Information & related Technology; CPS: Cyberphysical systems; CSG: Cyber Security Game; CSRF: Cyber Security Risk Framework; CT: Computed tomography; CURF: Core Unified Risk Framework; DDoS: Distributed denial-of-service; DSS: Digital signature services; DVR: Digital video recorder; ECG: Electrocardiogram; EHR: Electronic health records; FAIR: Factor Analysis of Information Risk; FDA: Food and Drug Administration; FMEA: Failure Mode and Effects Analysis; HITRUST: Health Information Trust Alliance; HTTP: Hyper Text Transfer Protocol; ICD: Implantable cardioverter-defibrillators; ICS: Industrial Control Systems; IMD: Implanted medical devices; IoMT: Internet of Medical Things; IoT: Internet of Things; ISO: International Standards Organization; LSTM: Long short-term memory; MAC: Media access control; MQTT: Message Queuing Telemetry Transport; MRI: Magnetic resonance imaging; MT: Medical things; NERC: North American Electric Reliability Corporation; NIST: National Institute of Standards and Technology; OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation; PCI: Payment Card Industry; PET: Positron emission tomography; PHY: Physical; RAP: Risk assessment process; RFID: Radio frequency identification; RIP: Risk impact parameter; RLP: Risk likelihood parameter; SCADA: Supervisory Control Received and Data Acquisition; TARA: Threat Assessment & Remediation Analysis; TCP: Transmission Control Protocol; UDP: User Diagram Protocol; UML: Unified Modeling Language; XSS: Cross-site scripting

Acknowledgements

The authors would like to express our immense gratitude to our beloved Chancellor Sri. Mata Amritanandamayi Devi (AMMA) for providing motivation and inspiration for this manuscript.

Authors' contributions

KK and SS conceived of the manuscript. KK wrote the manuscript. SS revised the manuscript. KA and VR edited the manuscript. The authors read and approved the final manuscript.

Authors' information

Kamalanathan Kandasamy is a PhD student and research associate at the Amrita Center for Cyber Security Systems and Networks at Amrita Vishwa Vidyapeetham. He has 7 years of experience in the information technology industry and more than 10 years of work experience in various cybersecurity projects including the areas of cloud security, database security, and cyber governance at Amrita University. His research areas of interests include cyber risk assessment and management, medical device security, and cyber threat intelligence.

Sethuraman Srinivas: Dr. Sethuraman Srinivas (Sethu) has 25+ years of experience in the information technology industry with a current focus on the cybersecurity domain. He is a seasoned information technology executive with a special focus on information security governance, metrics, and program management. Currently, he is an advisor to many firms in the San Francisco Bay area in the area of information security. He was recently part of IBM's managed security services for 7 years where he specialized as a strategy consultant in the area of security intelligence and operations. He managed medium to large cybersecurity programs in the area of cybersecurity governance, security analytics, big data, intrusion detection and prevention systems, risks, and security metrics. Sethu started his IT career in Wipro's R&D and was a software developer for 10 years, and other roles held by him were configuration manager, software development manager, oracle retail specialist, and advisory IT architect, for Computer Sciences Corporation (CSC). Sethu holds a Ph.D., in information technology, with specialization in information assurance. Sethu has a Master's in Computer Application, and a Bachelor's in Applied Sciences. Sethu has published cybersecurity academic papers in peer-reviewed journals (IEEE and ACM), and his research interests are in the area of security analytics, cybersecurity GRC, privacy databases, risk frameworks, big data, and governance automation. Sethu is an adjunct faculty with Amrita University for the past 7 years, in the school of engineering, with a focus on the Cybersecurity domain. He regularly handles classes in the area of application security, database security, and cybersecurity governance.

Krishnashree Achuthan: Dr. Krishnashree is an ardent researcher with multi-disciplinary interests and holds a PhD degree from Clarkson University, NY, USA. Her areas of interest in Cybersecurity and Governance, Mathematical Modeling of Systems, Cybersecurity Policy, IoT Security, Public Safety, Innovation, and Educational Technologies & Entrepreneurship. She also leads research teams focused on the enhancement of laboratory education through virtual laboratories. She holds 33 US patents and has published over 50 publications in Journals and Conferences. She has played an active role in several strategic initiatives for Govt. of India and served as the Principal Investigator.

Venkat P. Rangan: Dr. Venkat Rangan founded and directed the Multimedia Laboratory and the Internet and Wireless Networks (Wi-Fi) Research at the University of California at San Diego, where he served as a Professor of Computer Science and Engineering for 16 years. He is currently the Vice Chancellor of Amrita Vishwa Vidyapeetham. He has over 85 publications in international (mainly the IEEE and the ACM) journals and conferences and also holds 22 US patents. He is the fellow of the ACM (1998). He is the youngest to achieve this international distinction. He received the NSF National Young Investigator Award (1993), the NCR Research Innovation Award (1991), and the President of India Gold Medal (1984). In 2000, Internet World featured him on its cover page and named him as one of the top 25 Stars of Internet Technologies. In 2012, Silicon India ranked him as one of the 50 Indians Who Redefined Entrepreneurship in the Last 65 Years of Independence. He is an internationally recognized pioneer of research in multimedia systems and Internet E-Commerce. In 1993, he founded the first International Conference on Multimedia: ACM Multimedia 93, for which he was the Program Chairman. This is now the premier world-wide conference on multimedia. He also founded the first International Journal on Multimedia: ACM/Springer-Verlag Multimedia Systems, which is now the premier journal on multimedia.

Funding

Not applicable.

Availability of data and materials

Materials used in the manuscript may be requested from the corresponding author.

Competing interests

The authors declare that they have no competing interests and that there is no conflict of interest regarding the publication of this manuscript.

Author details

[1]Amrita Center for Cyber Security Systems and Networks, Amrita Vishwa Vidyapeetham, Amritapuri Campus, Clappana Post, Kollam, Kerala 690525, India. [2]IBM Security, San Francisco, CA, USA. [3]Amrita Vishwa Vidyapeetham, Amrita nagar post, Ettimadai Campus, Coimbatore, Tamilnadu 641105, India.

Received: 3 September 2019 Accepted: 13 May 2020
Published online: 26 May 2020

References

1. S. Li, L. Da Xu, S. Zhao, The Internet of Things: a survey. Inf. Syst. Front. **17**(2), 243–259 (2015)
2. Mark Hung, Gartner insights on how to lead in a connected world, 2017. https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf
3. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions. Future Generation Computer Systems **29**(7), 1645–1660 (2013)
4. Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). A middleware for the internet of things. arXiv preprint arXiv:1604.04823.

5. Minhaj Ahmad Khan, Khaled Salah, IoT Security: review, blockchain solutions, and open challenges, future generation computer systems, Nov 2017, doi: 10.1016/j.future.2017.11.022
6. OWASP, Top IoT vulnerabilities, 2016. URL https://www.owasp.org/index.php/Top_IoT_Vulnerabilities
7. Xingbin Jiang et al, An experimental analysis of security vulnerabilities in industrial IoT devices, ACM Transactions on Internet technology, 2020.
8. J. McCarthy, O. Alexander, S. Edwards, D. Faatz, C. Peloquin, S. Symington, A. Thibault, J. Wiltberger, K. Viani, Situational awareness for electric utilities, NIST SP 1800–7 practice guide. NIST Special Publication **1800-7**, 1–241 (2017)
9. Mardianabinti Mohamad Noor and Wan Haslina Hassan, Current research on Internet of Things (IoT) security: a survey, Elsevier, Computer Networks 2019.
10. K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, Y. Jin, Internet-of-Things security and vulnerabilities: taxonomy, challenges, and practice. Journal of Hardware and Systems Security **2**, 97–110 (2018)
11. Panagiotis I., Radoglou Grammatikis et al, Securing the Internet of Things: challenges, threats and solutions, Elsevier, Internet of Things Journal, 2019, doi.org/10.1016/j.iot.2018.11.003
12. Jan Henrik Ziegeldorf et al, Privacy in the Internet of Things: threats and challenges, security and communication networks 7.12 (2014): 2728-2742, https://doi.org/10.1002/sec.795
13. Alessandro Oltramari and Alexander Kott, Towards a reconceptualisation of cyber risk: an empirical and ontological study, Journal of Information Warfare, volume 17, issue 1, Winter 2018
14. Olakunle Elija et al, An overview of Internet of Things (IoT) and data analytics in agriculture: benefits and challenges, IEEE Internet of things Journal, 2018. DOI: https://doi.org/10.1109/JIOT.2018.2844296
15. Marwedel, P. & Engel, M. Cyber-physical systems: opportunities, challenges and (some) solutions. in 1–30 (Springer International Publishing, 2016). doi: 10.1007/978-3-319-26869-9_1
16. Nurse J.R.C., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S., 2015. Smart insiders: exploring the threat from insiders using the Internet-of-Things, Proc. 2015 Workshop Secure Internet of Things (SIoT), pp. 5–14
17. Petar Radanliev et al, Cyber risk in IoT systems, 2019, DOI: 10.20944/preprints201903.0104.v1, https://www.researchgate.net/publication/331867864_Cyber_Risk_in_IoT_Systems
18. A. Zhou, *Analysis of the Volkswagen Scandal Possible Solutions for Recovery* (School of Global Policy and Strategy, UC at San Diego, 2016)
19. Manos Antonakakis et al, Understanding the MiraiBotnet, Proceedings of 26th USENIX Security Symposium, 2017
20. Glenn Shafer and Rajendra Srivastava, The Bayesian and Belief-Function formalisms; a general perspective for auditing, A Journal of Practice and Theory, 1990.
21. R. Srivastava, An information systems security risk assessment model under Dempster-Shafer Theory of belief functions. Journal of Management Information Systems **22**(4), 109–142 (2006)
22. Mehmet Sahinoglu, Luis Cueva-Parra and David Ang, Game-theoretic computing in risk analysis, 2012 Wiley Periodicals, Inc.
23. Scott Musman et al, A game theoretic approach to cyber security risk management, Journal of DefenseModeling and Simulation: Applications, Methodology, Technology, 2018, Vol 15(2).
24. Maisa Mendonca Silva et al, A multidimensional approach to information security risk management using FMEA and fuzzy theory, International Journal of Information Management, 2014.
25. National Institute of Standards and Technology (NIST). 2012. Guide for conducting risk assessments SP-800-30—revision 1.
26. C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, ddos in the iot: Mirai and other botnets. IEEE Computer **50**, 80–84 (2017)
27. McAfee Mobile Threat Report, https://www.mcafee.com/enterprise/en-us/.../reports/rp-mobile-threat-report-2019.pdf
28. ENISA. 2016. Risk management resources and approaches, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management [Accessed online 14 April 2017]
29. NIST, C. Cybersecurity framework NIST. https://www.nist.gov
30. M. Barrett, J. Marron, V. Yan Pillitteri, J. Boyens, G. Witte, L. Feldman, *Draft NISTIR 8170, The cybersecurity framework: implementation guidance for federal agencies* (2017)
31. Katie Boeckl et al, NISTIR 8228, Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks, June 2019
32. R.A. Caralli, J.F. Stevens, L.R. Young, W.R. Wilson, *Introducing OCTAVEAllegro: improving the information security risk assessment process* (2007)
33. ISO. ISO - International Organization for Standardization. (2017). https://www.iso.org/home.html.
34. Wynn, J., Whitmore, G., Upton, L., Spriggs, D., McKinnon, R., McInnes, R., Clausen, J. Threat Assessment & Remediation Analysis (TARA) Methodology Description Version 1.0. (2011).
35. Jason R. C. Nurse et al, Security risk assessment in Internet of Things systems, University of Oxford, 2018
36. Petar Radanliev, David C. De Roure et al, Standardisation of cyber risk impact assessment for the Internet of Things, Oxford e-Research Center, University of Oxford, 2018
37. Petar Radanliev, David Charles De Roure et al, Cyber risk management for the Internet of Things, Oxford e-Research Center, University of Oxford, 2019, doi:10.20944/preprints201904.0133.v1
38. Petar Radanliev, David Charles De Roure et al, Future developments in cyber risk assessment for the internet of things, Elsevier, Computers in Industry 2018.
39. Sara N. Matheu-Garcia, José L. Hernández-Ramos, Antonio F. Skarmeta, Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices, GianmarcoBaldini Computer Standards & Interfaces, 2018, DOI : https://doi.org/10.1016/j.csi.2018.08.003
40. Faride Latifi et al, A COBIT5 Framework for IoT risk management, International Journal of Computer Applications (0975–8887), Volume 170–No.8, July 2017
41. Gaute Wangen, ChristofferHallstensen, and Einar Snekkenes. A framework for estimating information security risk assessment method completeness - Core Unified Risk Framework, 2017, Springer International Journal of Information Security.
42. B. Ali et al., Cyber and physical security vulnerability assessment for IoT-based smart homes. Journal of Sensors **18**, 817 (2018). https://doi.org/10.3390/s18030817
43. Guillermo A. Francia, III, David Thornton, and Joshua Dawson, Security best practices and risk assessment of SCADA and Industrial Control Systems, 2012.
44. F. Den Braber et al., *The CORAS model-based method for security risk analysis* (SINTEF, Oslo, 2006)
45. Yulia Cherdantsev et al, A review of cyber security risk assessment methods for SCADA systems, computers & security 56 (2016) 1–27, Elsevier.
46. Patricia A. S. Ralston et al, Cyber security risk assessment for SCADA and DCS networks, Elsevier ISA Transactions, Volume 46, Issue 4, October 2007, Pages 583-594
47. M. Elisabeth Paté-Cornell et al, Cyber risk management for critical infrastructure: a risk analysis model and three case studies, DOI: https://doi.org/10.1111/risa.12844
48. Halima Ibrahim Kure et al., An integrated cyber security risk management approach for a cyber-physical system, Appl. Sci. 2018, 8, 898; doi:10.3390/app8060898
49. How to do a complete automated risk assessment: a methodology review. Riskwatch White Paper, http://www.riskwatch.com/news/whitepapers/How to do a complete automated risk assessment_10-02RW.pdf; 2002
50. Antoine Bouveret, Cyber risk for the financial sector: a framework for quantitative assessment, 2018 International Monetary Fund.
51. Larry Santucci, Quantifying cyber risk in the financial services industry, Federal Reserve Bank of Philadelphia Consumer Finance Institute, 2018
52. RiskLens. Risk analytics platform | FAIR Platform Management. (2017). Available at: https://www.risklens.com/platform
53. FAIR. What is a cyber value-at-risk model? (2017). Available at: http://www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model
54. Ian Stine, Mason Rice, Stephen Dunlap, John Pecarina, A cyber risk scoring system for medical devices, International Journal of Critical Infrastructure Protection, Dec 2019.Elsevier.
55. Introduction to Microsoft Software Development Lifecycle (SDL) Threat Modeling, University of California, Berkeley, 2015 California(people.eecs.berkeley.edu/~daw/teaching/cs261f12/hws/Introduction_to_Threat_Modeling.pdf), 2015
56. Li Mei, Liu Zixian, Li Xiaopeng, Liu Yiliu, Dynamic risk assessment in healthcare based on Bayesian approach, Reliability Engineering and System Safety (2019), doi: https://doi.org/10.1016/j.ress.2019.04.040
57. Phillip Laplante, Mohamad Kassab, Nancy Laplante, Jeffrey M. Voas, Building caring healthcare systems in the Internet of Things, IEEE Systems Journal 2017,

58. Caiming Liu, Yan Zhang et al., Research on dynamical security risk assessment for the Internet of Things inspired by immunology, 8th International Conference on Natural Computation (ICNC 2012)
59. Andy Herman, Mandatory cybersecurity risk management framework in healthcare sector, Research Note, ASA Institute for Risk &Innovation, Seattle, 2016
60. NIST Framework for improving critical infrastructure cybersecurity – version 1.1, published April 2018
61. Introduction to the HITRUST Common Security Framework, HITRUST Alliance, LLC., 2014
62. Waqas Aman et al, An empirical research on InfoSec Risk Management in IoT-based eHealth, MOBILITY 2013.
63. S. Darwis et al., Towards composable threat assessment for medical IoT (MIoT), The fourth International Workshop on Privacy and Security in HealthCare 2017 (PSCare17). Procedia Computer Science **113**, 627–632 (2017)
64. Faisal Alsubaei, Abdullah Abuhussein, Vivek Shandilya, Sajjan Shiva, IoMT-SAF: Internet of Medical Things Security Assessment Framework, Internet of Things (2019), doi: https://doi.org/10.1016/j.iot.2019.100123
65. "GATTack.io." https://gattack.io/.
66. T. Melamed, *An active man-in-the-middle attack on bluetooth smart devices* (WIT Press, 2018). https://doi.org/10.2495/SAFE-V8-N2-200-211
67. M Banerjee et al, A blockchain future for internet of things security, Digital Communications and Networks, Volume 4, Issue 3, August 2018, Pages 149-160
68. MITRE: Medical device cybersecurity regional incident preparedness and response playbook 2018. https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and
69. R. Altawy et al., Security tradeoffs in cyber physical systems: a case study survey on implantable medical devices, EEE, 2016. DOI: Digital Object Identifier. https://doi.org/10.1109/ACCESS.2016.2521727
70. Tamara Denning et al, Patients, pacemakers, and implantable defibrillators: human values and security for wireless implantable medical devices, CHI '10 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM 2010
71. J. Holdsworth et al., *Medical device vulnerability mitigation effort gap analysis taxonomy* (Elsevier, Smart Health, 2017)
72. Shoichi Yoneda et al, Risk assessment for embedded medical devices, 2018 IEEE 7th Global Conference on Consumer Electronics (GCCE 2018)
73. Risk prediction on electronic health records with prior medical knowledge, Fenglong Ma et al, KDD '18, August 19–23, 2018, London, United Kingdom
74. Akram Abdul-ghani Hezam et al, ,A comprehensive IoT attacks survey based on a building-blocked reference mode, International Journal of Advanced Computer Science and Applications · April 2018, DOI: 10.14569/IJACSA.2018.090349
75. Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, S. Shieh, IoT security: ongoing challenges and research opportunities, in: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, 2014, pp. 230–234. https://doi.org/10.1109/SOCA.2014.58.
76. K. Savage, IoT devices are hacking your data & stealing your privacy - infographic, 2017.
77. S. Shiva et al, Security and privacy in the Internet of Medical Things: taxonomy and risk assessment, 2017, DOI: https://doi.org/10.1109/LCN.Workshops.2017.72

Publisher's Note