Evaluation of the Cyber Security Risk Models (CSRM) in Cloud Computing

[1]Hossein Anisi
[1]School of Computer Science and Electronic Engineering, University of Essex, UK.
[1]anisihossein@hotmail.com

ArticleInfo
Journal of Machine and Computing (http://anapub.co.ke/journals/jmc/jmc.html)
Doi: https://doi.org/10.53759/7669/jmc202202017
Received 30 January 2022; Revised form 25 March 2022; Accepted 18 May 2022.
Available online 05 July 2022.

Abstract – Many devices in the Internet of Things (IoT) ecosystem may be susceptible to cyberattacks due to their diverse nature and lack of standardization. Resource-constrained IoT devices include sensor nodes, smart gadgets, and wearable devices. An organization's RAP (Risk Assessment Process) integrates the evaluation of hazards that are linked to all its resources, as well as the evaluation and prioritization of these risks. It is crucial to begin the risk management process with an accurate and thorough risk assessment. The Cyber Security Risk Models (CSRMs) in Cloud Computing are examined in this research. To understand the uniqueness of IoT systems and why present risk assessment methodologies for IoT are ineffective, it is necessary to understand the current state of risk assessment for IoT. There are constraints to periodic evaluations IoT due to device interoperability. Continuous testing of IoT solutions is thus essential.

Keywords – Internet of Things (IoT), Cyber Security Risk Models (CSRM), Risk Assessment Process (RAP), Confidentiality, Integrity, Availability (CIA).

I. INTRODUCTION

Smart cities, smart energy grids, smart vehicles, and smartphones are some of the examples of 'objects', which have now become networked and intelligent. IEEE presents a definition of an Internet of Things (IoT) object or system as a collection of entities (which integrates data resources, people and cyber-physical devices), which have the capacity to transmit data and interact with the physical ecosystem by actuating, processing data and sensing data. By 2025, IDC (International Data Corporation) projected that approximately 41 billion IoT devices will be used. It is probable that the significant architectures listed in the directive of EU on networking and data system security could be powered by IoT. Smart urban environments, for instance, are incorporating IoT device sensors, and data analytics to streamline resource utility and enhance the performance of system infrastructure. Presently, there are thousands of patients in America with web-linked pacemakers. As such, IoT plays a significant role in not only digitization of communities but in enhancing the health of the community.

IoT-based infrastructures [1] may be vulnerable to attacks and malfunctions if proper security measures are not in place. On the other hand, IoT users' right to secrecy is paramount. People's everyday lives, both at work and at home, are increasingly reliant on Internet-connected "things." There is a risk that sensitive personal information will be exposed online. In the Internet of Things, addressing privacy concerns is just as critical as addressing security concerns. The IoT's heterogeneous computer networks and resource-constrained machines that could afford lightweight security and privacy solutions have proved to be weak connections for IoT networks. It is also conceivable that IoT solution suppliers miss security and privacy issues because they're too complicated, pressed for time to market, or just don't know any better. Securing non-security experts could benefit from the use of security patterns as a solution to the problem at hand.

Knowledge and expertise that may be transferred to the software engineering industry can be found in these well-known approaches. In the past, patterns' answers have been demonstrated to be trustworthy. In addition, the advantages and disadvantages of a design are often described in depth. The establishment of a remedy centred on the pattern could act as a better starting point for IoT system design process. When it comes to designing secure systems, patterns and architectures are not enough, but they may play a key role in the development process. According to Zheng et al. [2], security knowledge and competency patterns are universal and time-tested. Patterns like these may be a great assistance to designers when it comes to systems security and privacy since they help implement solid solutions like safe authentication process, secure storage and processing, secure connectivity between devices, and secure connection to the server. Books and catalogues on security patterns may help users apply security knowledge and expertise to their problems.

The IoT age [3], on the other hand, presents new security concerns that current techniques and methodologies are unable to handle. The least understood of the P2C, C2C, and P2P attack types is the cross-domain cyber-to-physical (C2P) assault. The complexity and variety of IoT systems, as well as their greater attack surfaces, make them more vulnerable to security breaches. The cloud layer, edge/fog layer, and IoT field and devices (smart, connected gadgets) are all common components

of modern IoT systems. There was an increase in attack surface area as a result of the explosion in connection. Because of the restricted data transport and storage capabilities of IoT field devices, they are often used in dynamic (physical) execution contexts with dynamic actuation. In other words, the Internet of Things (IoT) is characterised by unpredictability.

This paper critically reviews the IoT technology in Section II while a security analysis is done in Section III. In Section III, a definition of IoT risks; security and privacy concerns; IoT vulnerabilities and attacks; cyber risks in the IoT domain; and IoT risks and applicable theories, has been provided. Section IV presents an evaluation of the cyber risk models. Lastly, Section V concludes the paper.

II. IOT TECHNOLOGY

IoT Architecture

Various IoT architectures [4] have been described in the literature, each with a distinct number of layers. IoT World Forum Conceptual Framework is used in our taxonomies of the IoT infrastructure. The many layers that normally make up an IoT system may be finely granularized using this design. To provide just one recent example, this architecture has been used by all but one of the H2020 large scale experiments for Internet of Things in the European Union. The seven tiers are as provided in **Fig. 1**.

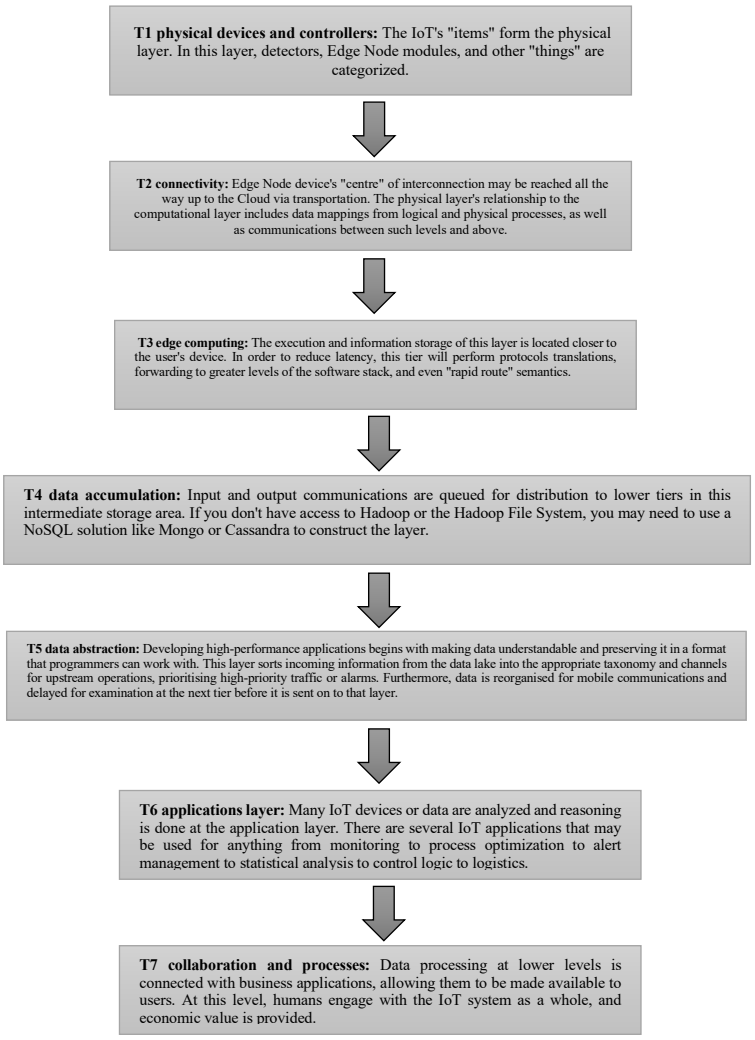

Fig 1. Seven tiers of the IoT system

Perception (T1), network (T2) and application (T3) are only three levels of a simplified IoT architecture that is widely used in the literature (groups T4, T5, T6, and T7). We indicate how this contribution fits into the IoT's international forum Metamodel as well as the three-layer IoT infrastructure.

Since its conception in 1999, the Internet of Things (IoT) boom has had a profound influence on every sector. Initially, the goal was to interconnect any non-Internet-linked item to the Web to make it sentient. Gartner predicts that by 2020, there will be more than 25.1 billion IoT sensors in operation [5]. Based on wireless sensor nodes, the IoT is constructed. To put it another way, field gadgets are being integrated into the World wide web through the IoT surge. An automated framework for wireless router-based communication amongst dispersed gadgets has already been established as part of the IoT. B2B

and B2C are two of the most prevalent ways in which humans connect with the Internet, and this trend is expcected to continue in the future

A solitary gadget may now communicate with both people and the Internet thanks to the advent of the Internet of Things (IoT). The ability to transfer data between any standalone system, the World wide web, and humans is what distinguishes IoT technology. Automated and user-initiated activities both work well for controlling this flow of information. As an instance, a faucet may be set to irrigate a plant using a meteorological predicting software, such as Rainfall Prediction. Increasing the danger of cyber-attacks on IoT devices because they are open to the Internet is a good thing. Risk experts have discovered a new class of dangers associated with the Internet of Things (IoT) because of the technology's singularity and extreme complexity. The IoT cybersecurity risk specialists need to understand and manage the risks associated with IoT devices. Section III presents a security analysis for IoT models.

III. SECURITY ANALYSIS

Definition of IoT risk

The probability of a bad thing happening, together with the magnitude of the consequences, is what we mean when we talk about cyber risk. There are several factors that contribute to risk, such as the likelihood of an attack and its effect on an organisation. Information technology (IT) risk [6] is defined by ISO standards and IEC as the possibility for a risk to leverage asset defects and harm an organization's systems. An event's possibility and effect are taken into account while assessing it. In terms of information security, there are three things to watch out for: assets, threats, and weaknesses in the system. For testing purposes, the OWASP's (Open Web Application Security Project's) certification guidelines define threat as the chance times the impact.

Threats and vulnerabilities may be seen in a number of ways when attempting to define risk. Using a scale from 0 to 10, NIST's CVSS (Common Vulnerability Scoring System) [7] measures cyber risk in terms of vulnerabilities intricacy. In this study, we look at how two distinct sets of practitioners specialists and ontology creators—conceive of cyber dangers. As far as both parties are concerned, an attacker's ability to leverage a vulnerability is critical. Interconnected machines that can communicate with each other without the need for human-to-human or human-to-computer contact make up the Internet of Things (IoT) by definition. In such a system, we predict a wide range of cyber threats, which we term IoT risks. Next, we'll take a look at several kinds of IoT system dangers.

Security and Privacy Concerns

CIA (Confidentiality, Integrity, Availability), security, privacy, confidentiality and transparency issues that we examine in the primary research we review. IoT networks and endpoints must address these problems. If such information is accessible in the main research, we additionally categorise security procedures like authentication and authorisation. Patterns and architectures that support and guard against these privacy- and security-related issues are what we're interested in learning about. The following **Table 1** shows the concerns and their explanations.

Table 1. Security and privacy concerns in IoT Systems

Concern	Definition
Confidentiality	Confidentiality ensures that data is not made accessible or revealed to anybody or anything that is not permitted by the owner.
Integrity	To keep data up-to-date, accurate, and full, and to do so consistently throughout its lifespan.
Authentication	It is possible to verify a person's identification using the system or gadget.
Authorization	It is possible for the system to identify what resources and activities the identifiable and authorized users have access to.
Privacy	When it comes to obtaining and storing personal information in compliance with the GDPR, HIPAA, and GLBA, the data is gathered legitimately in line with this legislation.
Accountability	Logging is a common method of tracking back to a specific user the activities they have taken on the system.
Availability	Data or a service may be accessed at any time.

IoT vulnerabilities and attacks

Cyber-attacks resulting in revenue shortfall and data leakage are becoming more common on IoT devices recently. The following are some of the most common causes of IoT vulnerabilities: (a) insecure software or firmware; (b) physical security; (c) Ineffective security configurations; and (d) complex architectures.

By way of the Open Web Application Security Project (OWASP) [8], a complete list of the top 10 IoT architectural vulnerabilities has been released. One of the most often exploited weaknesses in IoT devices is the lack of physical protection. Weak, easy to guess, or default configuration passwords may be used to obtain access to installed systems. Internet of Things (IoT) devices that use unsecured network services will have their confidentiality, integrity, and availability (CIA) jeopardized. If the device's firmware has not been certified, or if the anti-rollback features have not been implemented,

attacks are conceivable. Recent Internet-of-things (IoT) hacks have had devastating results. A recent assault on a Ukrainian power infrastructure resulted in a nationwide blackout. It goes without saying that safeguarding Internet of Things (IoT) systems against attack is an essential step towards reducing risk. IoT system security requires a wide range of complicated technology-related challenges to be addressed. Authentication, access control, and trust management mechanisms discussed in current IoT security research literature, as well as IoT threat modelling, are among the risk mitigation strategies recommended.

According to IoT infrastructure and application ecosystems, IoT threats are categorised. The security of all three levels of the IoT, the application, network, and hardware, is compromised. The application layer is vulnerable to attacks such as SQL injection and misconfiguration. Sybil, replays, preferential transmission, and synchronicity in particular are all examples of physical layer assaults. Even if encryption is used, attacks such as buzzing and Man-in-the-Middle attacks have the greatest influence on the hardware level, which affects the MAC and PHY layers of the mainstream press connectivity control system. Identification, monitoring, and profiling are just a few of the seven types of privacy issues that have been impacted by new technology. Studying IoT hazards and mitigation is necessary since the threat environment is always changing.

There are several security problems in today's IoT systems that need a close look at risk assessment frameworks, risk vectors, and risk rankings. IoT and its associated cyber threats are the topic of this article. One of the most important aspects of our investigation into cybersecurity risk assessment methodologies is the Internet of Medical Things (IoMT) (IoMT). IoT devices' security risk may be estimated computationally, which is one of this study's goals. On the basis of this study's evaluation of the literature and analysis, a scientific approach for calculating the cyber risk associated with Internet of Things (IoT) systems was developed. IoMT devices' risk effect and probability were assessed based on these standards. A discussion of risk estimation formulas will conclude this essay. Based on these methods, IoMT gadgets are given a risk rating and a riskiness (higher, moderate, lower). People's lives are directly impacted and improved by the patient monitoring and life-saving gadgets developed by IoMT. In this paper, the Dempster-Shafer theorem and cyberspace probabilistic reasoning are used to analyse cybercrime concerns.

Cyber threat in the IoT realm

IoT threats affect a wide range of industries, including banking, supply chain, and healthcare. In the United States, healthcare organisations are the most often targeted by cyberattacks, outnumbering both businesses and financial firms. The IoT risk management approach has particular problems due to insider attacks. Utilizing a smart device camera, an insider, for instance, may secretly capture and transmit IP or sensitive company information with a 3rd party individual. To get entry to a company's network, insiders may employ malware-affected connected devices such as memory sticks or USB drives. Internet of Things (IoT) hazards arise whenever adversaries in the system take advantage of weaknesses in IoT systems (or their surroundings). Using IoT devices to manage nuclear power facilities and data centres, for example, might be hazardous. Examples of various forms of IoT risks have been defined in **Table 2** below.

Table 2. Various forms of IoT risks

Type of IoT risk	Definition
Ethical risks	This alludes to the unintended consequences of immoral use of IoT technology. Software created and deployed by the vehicle manufacturing business Volkswagen was used to evade diesel emissions testing. Because to the Clean Air Act, the company's image and financial losses have been severely damaged.
Privacy and security risks	Vulnerabilities may be exploited to take control of assets with the intention of inflicting damage. Many popular websites like Reddit, CNN, Netflix, Twiter tand others were damaged by the Mirai (IoT specialist malware) Botnet's DDoS assault on DYN in October 2016 [9]. Data control loss, whether temporary or permanent, is a serious concern for any company, and it falls within the umbrella of the IoT privacy issue. In May 2014, a security breach at eBay resulted in the hacking of customer details, notably passwords.
Technical risks	This is caused to bad design, testing, etc. in the software or hardware. Chip-level security issues have been discovered in personal microchips manufactured in the last 20 years. An Intel 86 microcontroller architectural vulnerabilities, known as Meltdown, allows an unauthenticated rogue method to access all of the system's memory even if it is not permitted to do so. IoT security and privacy are put at risk as a result of poor design.

If a risk occurs and has a negative effect on or destroys an IoT assets, it is an IoT hazard that is present. One illustration of this is spoofing attempts on corporation devices such as computers and cellphones, which infect several Embedded technologies and disrupt a production plant's supply chain. Readers will benefit from reading the next section, which discusses several IoT risk hypotheses.

IoT Risks – Applicable Theories

Incorporating IoT into existing scientific beliefs about cybersecurity risk is a simple matter. The percentage of trust may well be evaluated by integrating data from many sources. When used as a formalized framework, it may be considered as a way to express ambiguous information. Dempster-Shafer Religion as a System of Belief Modeling uncertainty in risk assessment is done using functions. As a result, it determines whether or not there are any dangers to the security of an information system and, if so, what can be done about it. The belief functionality paradigm may be used to integrate the influence of risk variables and hazard countermeasures. Risk control methods' influence on ISS (information systems security) may be simply assessed using this tool. This strategy breaks down the total data security risk into its subdimensions. Threats and controls are assessed independently for each sub-component when assessing risk for that sub-component. As a result, the whole risk may be calculated employing the calculus of confidence functions.

Many IoT risk evaluation theories exist. Quantitative risk analysis in a variety of disciplines, including data security, is often performed using game-theoretic computers. In a Nash equilibrium, no member of a system can benefits from an unequal discrepancy in the network since everyone else's tactics remain the same. “Assault” and “Defend” are two distinct situations in which one must make a decision between one's own defence and the other's. Achievement or failure of the attack is reflected in the corresponding outcome S. As a result, both players' fates are tied to the outcome of their individual attacks. ARA uses a game-theoretic method, in which the likelihood of S is estimated and limits are put in place on how (d, a). Employing a decision tree structure, players' Evolutionarily stable requirements are analysed at node S In the next step, dynamic programming is being used to examine each player's tree structure in order to determine the parameters which must be met in order for the game to reach its equilibria. For quantitative approach, [10] gives a fair overview of some game-theoretic computer approaches. In-depth discussion is given to such topics as Neumann's two binary pure stabilization and Nash equilibria using purified or intervening medium. Game-theoretic configurations employed in risk appraisal, especially in the context of digital infrastructures and data security, may be modelled computationally.

As a means of quantifying digital security threats, the Cyber Security Game (CSG) is used to establish the best utilisation of safety approaches for any specific systems and at any defined venture level. A mission effect framework is used to record the effects of cyber events and then combined with the possibility that an attack would be successful to get the risk score. Type-2 fuzzy concept and failure mode and effect analysis (FMEA) are used in a risk mitigation method that incorporates both techniques. As a complicated research approach, FMEA is designed to identify possible failure modes, situations or problems influencing the system's dependability, ease of maintenance and safety. Accessibility to data and structures, communications and security architecture, information assurance, and the enhancement of safe data systems are all examined in this technique. This approach provides information on the fundamental viewpoints and failures of programs that result in software vulnerabilities.

IV. CYBER RISK MODELS

Risk Assessment Process (RAP) Models

RAP is the process of identifying all of an organization's assets as well as estimating and prioritising the risks associated with them. Because it serves as a prelude to risk mitigation, risk evaluation is an essential phase in the whole risk assessment process. At the risk assessment stage, factors such as attack probability and impact are taken into account. Risk assessment recommendations are provided by the NIST (National Institute of Standards and Technology). Assuming the risk is low enough (risk appetite), you may accept the risk, mitigate it, transfer it, or avoid it entirely by taking the impacted item out of the equation. Various forms of IoT risk evaluation techniques will be summarised in this part, as well as the vulnerabilities of such devices.

Many devices in the Internet of Things (IoT) ecosystem may be exposed to cyber-attacks because of their heterogeneity. The Internet of Things (IoT) makes use of resource-constrained devices including sensor network, smart gadgets, and wearables. These devices are susceptible to the following flaws: Device and its associated systems can be subverted if the computer networks on the IoT devices are not protected enough; (b) CIA (confidentiality, integrity, and availability) triad is subverted; (c) lack of system software verification onto console could amount to CIA triad contraventions and the failures for compliances; (d) usage of OS modules and platforms that have not been encrypted from hazardous distribution chains could authorize devices to be disrupted; and (e) and (f) IoT device flaws are exploited by a small string of attacks like Hajime, BrickerBot, IoT Reaper,or Mirai. The McAfee Wireless Assessment Report 2019 points out the growing number of IoT devices in homes, which might be a target for hackers [11]. IoT devices, such as smart buzzers and surveillance cameras, may be hijacked due to a flaw in a component named ilnkP2P, which is utilised in P2P communication.

To get certificates, hackers take advantage of flaws in online and mobile apps, both of which are often found on IoT devices. In order to interpret and observe the video stream, create alerts, remove spare videos from distributed memories, and accessibility to account data, these issues could be exploited. XSS risks in software devices, file path crawling in cloud servers, unsigned product upgrades, and devices that disregard the validity of the server certificate are all potential sources of vulnerability. Web application firewalls that protect workstations from HTTP traffic should be utilised by IoT providers. DDoS assaults fueled by botnets have recently targeted thousands of IoT devices, sending malicious traffic to legitimate websites in an effort to degrade their functionality. Risk evaluation models often include a formal risk assessment approach for IoT devices because of the significant dangers they pose.

RAP frameworks like as NIST, OCTAVE and , ISO/IEC are widely used nowadays. The distinctive elements of each risk assessment approach are apparent. The structure of the methodology and the technique used to quantify risk are two crucial variables that must be taken into consideration. For the purpose of evaluating IoT risk assessment, we'll look at a few current risk assessment frameworks, their unique methodologies, and whether or not they're appropriate. There are both quantitative and qualitative methods for assessing a firm's cyber risk. The NIST methodology is well-documented and offers direction on risk evaluation and administration execution, but it lacks a model against which it may be compared. According to NIST, there is no methodology for assessing the effect of the Internet of Things (IoT) on society. Companies may use the NIST framework to prepare for catastrophe and recovery. For IoT risk assessment, nevertheless, NIST has additional concerns. Documentation of the risks and obstacles associated with IoT devices is provided in the NIST IR 8228 report.

Eight phases are proposed in Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [12]. As an example, these phases may be: (1) creating a framework for assessing risk; (2) creating asset profiles; (3) pinpointing potential risk regions; (4) pinpointing potential threats; (5) pinpointing potential mitigation strategies; and finally, (eight) pinpointing potential solutions. Some systems blend qualitative and quantitative methodologies. An IoT risk assessment methodology has been developed by GSMA using OCTAVE as the primary risk evaluation platform. Because of its organised approach, the GSMA is well-suited to the supply chain. Standardisation of cyber risk is a goal of ISO (International Guidelines Organization), which contains standards for cyber risk. Complementary approaches like NIST and ISO may be used in conjunction with the primary risk assessment procedure. System recovery may be made easier with tools like Threat Assessment & Remediation Analysis (TARA), but it falls short whenever it comes to the control of negative effects of the cyber hazards. This article is mostly concerned with NIST, ISO, TARA, and OCTAVE. The next part presents a critical evaluation of these IoT threat models, depending on several aspects.

Before looking into the IoT threat framework, it is fundamental to comprehend the peculiarity of the IoT system and the rationale behind risks assessment methodologies for IoT are inadequate. There are constraints to periodic evaluations in the IoT due to the interconnections of IoT objects. Constant evaluation of IoT systems [13] is required. IoT devices that are linked to the Internet run the potential of introducing new dangers and vulnerabilities. When it comes to conventional methods to risk assessment, assets are considered values of businesses. However, with the Internet of Things (IoT), devices themselves might serve as the foundation for assaults. When evaluating the procedures by which IoT items are bound (interconnection, which allow devices to effectively pair and function, failure may also occur in IoT systems.

In light of the above, an IoT-specific version of the classic cyber risk assessment procedure is required. IoT deployment differs from typical IT deployments because of its networking approach. In the Internet of Things, a variety of connection types and devices may be used, some of which do not accommodate the CIA triangulation. Automated software patches or upgrades and data encryption are two common precautions. An increase in attack surface is possible because IoT devices are so versatile and interoperable. Upgrades to hardware, protocols, and applications all expand the attack vector, necessitating further security measures. A thorough risk assessment procedure for IoT is recommended in light of these issues. The following section compares the advantages and disadvantages of the majority of the most extensively used IoT threat assessment models now in use.

There were a number of CSRMs explored before, including OCTAVE, NIST, and ISO. In the IoT context, particular attention must be given in evaluating risk since the concept of IoT introduces complex threat on assets and devices. IoT risk strategies don't exist at this point in time. However, current risk assessment models may be tweaked to meet the threats of the Internet of Things (IoT). IoT cyber risk may now be measured using new concepts introduced by [14] in their model for standardising impact assessment methodologies. To help firms integrate IoT devices with services, they conducted an empirical examination of several risk assessment approaches. In order to standardise IoT risk impact evaluation, this strategy used a goal-oriented approach. There has been a new introduction of an IoT MicroMort framework for estimating IoT risk, which could also test and evaluate IoT-connected gadgets. This method can even estimate the danger of IoT in the future. The dynamic and distinctive nature of the Internet of Things (IoT) necessitates new risk assessment approaches. It has also been suggested to use an IoT privacy accreditation technique to evaluate security solutions automatically. The COBIT5 risk management approach is used to map IoT-related hazards, and an IoT risks framework is recommended with interlinked procedures, events, functions and obligations. CURF (Core Unified Risk Framework) evaluates and measures the completeness of current methodologies. IoT-specific risk vectors are evaluated in all of the aforementioned frameworks to reduce and manage the dangers that IoT devices bring into being.

NIST Model

New standards, guidelines, and tools have been developed by the NIST Cybersecurity for IoT initiative in order to enhance the security of IoT devices and the environments in which they exist. By engaging with partners from across government, business, international organisations, and academia, this initiative aims to build trust and facilitate global development. (a) distinct assessments could be developed based on device category and operation, (b) sector best practises can result to prerequisites and evaluation techniques that are best for the business, (c) can create evaluations to facilitate the versatility required to fulfil consumer demands, (d) capitalise distinct comparability evaluation perspectives (such as attestation of third parties and individual-based) with respect to the hazards linked to the types of IoT devices. It's important to NIST to safeguard devices, data, and personal privacy when it comes to IoT risk assessment. As a risk management paradigm, NIST is well-suited to crisis and recovery preparedness in the IoT sector.

OCTAVE Model

OCTAVE's asset containers cover both virtual and real security, making it a good fit for home automation risk assessments. OCTAVE makes it easier to identify numerous security flaws in IoT-based smart homes, displays the hazards to house occupants, and provides mitigation strategies. OCTAVE puts into consideration four stages as shown in **Fig 2**.

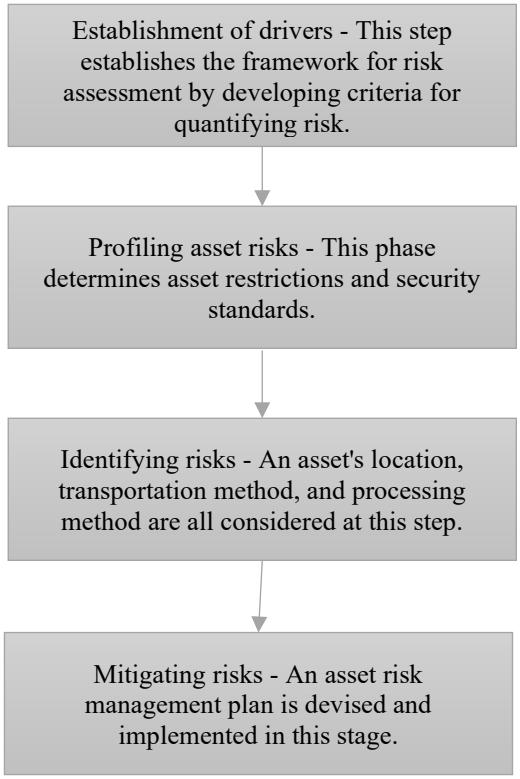

Fig 2. Stages of OCTAVE

To classify recovery impact sections as shown in **Fig. 2**, OCTAVE use a standardised questionnaire, however the risk is not quantified.

TARA Model

For the most critical exposures, TARA provides a prediction framework for TARA. TARA has three key benefits. It reduces the number of possible assaults to a tolerable number. Effective risk and control assessment and communication are made easier thanks to this tool. It may improve results, reduce the overall work required for risk analysis, and assist in making more informed choices. In response to the requirement to analyse the threats and vulnerabilities of a rapidly developing threat ecosystem, Intel(R) designed it for a large, highly valuable, and diversified ecosystem. Neither the quantification of risks nor the promotion of protection against vulnerabilities are part of TARA. TARA is often used in conjunction with the NIST paradigm, and NIST's IoT concerns are also relevant here.

ISO Model

Because of its emphasis on voluntary conformity and standardisation that is based on agreement, ISO is a strong advocate for both compliance and standardisation. The worldwide experience is mirrored in ISO because the measurements are produced by those who require them via an agreement process. Since experts from all around the globe contribute to the development of ISO standards, the organisation represents a wealth of global knowledge and experience. ISO cyber risk analysis has the best opportunity of becoming a global standards reference. There are 161 countries represented and 778 subcommittees in the International Organization for Standardization (ISO) [15]. This makes it difficult to coordinate and integrate specific standards. According to ISO/IEC 27001's definition of confidentiality and availability of data, this standard establishes a risk assessment framework, designates the establishers of IoT risks, and evaluates the threat based on a specific criterion. In order to minimise risks and maximise benefits for Internet of Things (IoT) application domains, ISO/IEC 30141 provides the reference structure. IoT security as well as privacy guidelines are provided by ISO/IEC 27030.

CSRM in industrial and financial sectors

Cyber-Physical Systems (CPS) and SCADA systems represent the two typical types of industrial IoT technologies. To better understand CSRM in the financial and industrial sectors, we've included the following subheadings:

CSRM in SCADA and CPS systems

There are similarities between SCADA and IoT, but the vital purposes of both technologies are to improve the efficiency and control of a particular item or process. As a result, it is critical that we talk about SCADA and CPS risk evaluation systems. An ICS risk model was constructed using the CORAS conceptual model that is UML-oriented threat design approach for SCADA and ICS initiatives. Privacy best practices and the risks assessment of industrial models and SCADA that could be a type of SCADA, are considered. Generally, 24 risks assessment approaches for SCADA systems have been developed or used, and they have all been well evaluated elsewhere. After a thorough examination of ICS risk control systems, a comprehensive framework for stochastic risk assessment has been proposed that takes into account application domain, impact assessment, and tool support. Quantifying risk concerns and recommending encryption and program modifications for vital infrastructures may both help with decision-making.

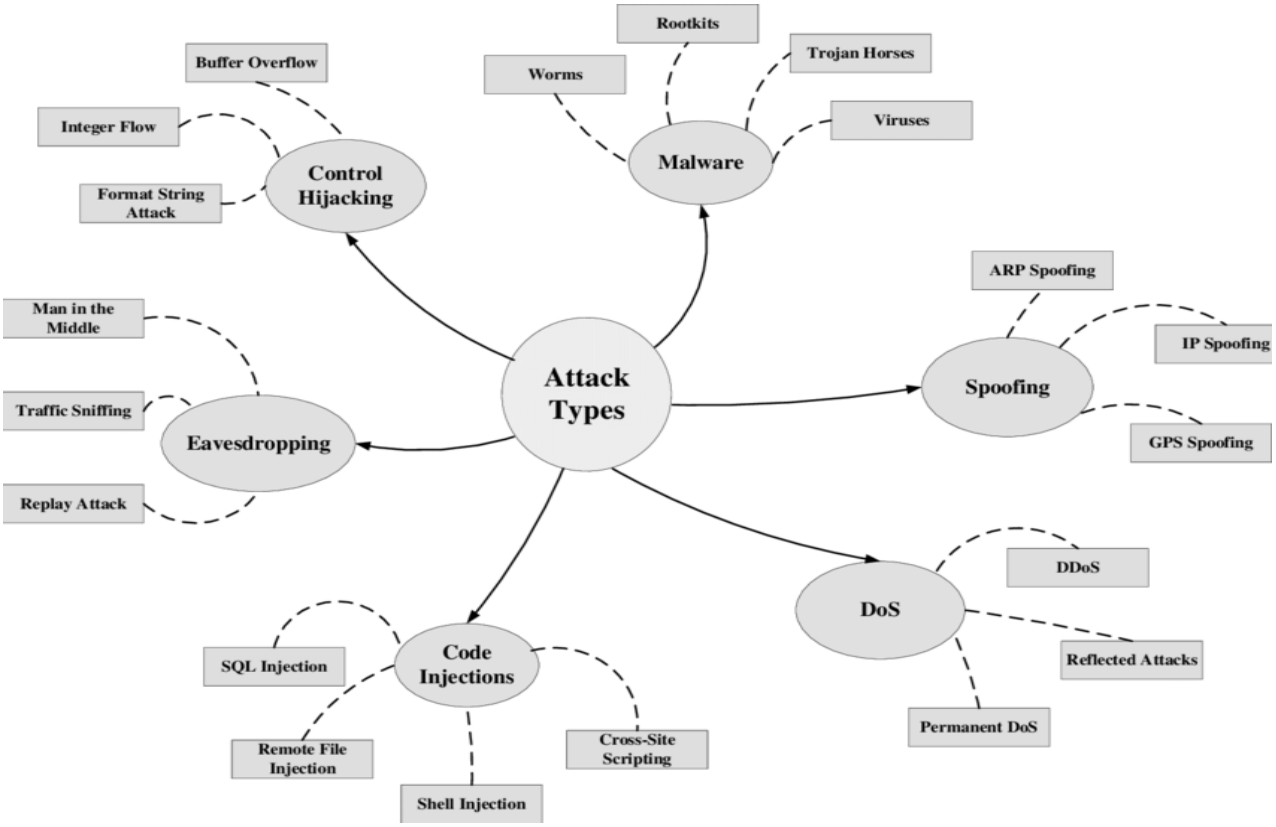

Fig 3. Cyber-attacks on the CPS infrastructure

Attacks on a CPS system's security put the infrastructure shown in **Fig. 3** at risk, reducing its performance and preventing it from providing essential services. CPS, like other systems, must be protected against such threats. Risk management is particularly difficult in the CPS because of the system's intrinsic complexity. A risk management approach for CPS has been presented in order to identify essential CPS assets and analyse their risks. Using easy-to-use platforms, comprehensive information databases, established risk evaluation designs, data joining capabilities, and proven risk investigation diagnostics technologies, the RiskWatch tool gives evaluations of risk and susceptibility. The NIST, NERC, and the American Gas Association have all been mentioned as sources of information on best practises, security devices, and other advances in the industry. SCADA and DCS deployments are constantly being updated to enhance stochastic risk analysis to predict risk (exposure or projected loss). CPS security measures may be simply extended to IoT systems, as well.

CSRM in financial systems

The Internet of Things (IoT) is expected to have a significant impact on the financial and banking sectors in the 21st century. When it comes to the financial sector, the Internet of Things (IoT) has an enormous impact because of the massive data transfer, aggregation, and breakdown of information that it manages. With the rapid advancements in IoT, the financial and banking industries now have the ability to assist their customers in achieving their business objectives and desired results. The financial industry relies heavily on biometric and location sensors for quality control and follow-up. The Internet of Things (IoT) has made it easier for banks to dispatch and concentrate on administration. Identifying what to ship and when to ship it will be made easier for the financial firm with the assistance of this tool.

Customized showcasing is now feasible for the bank because to IoT innovation, which allows it to monitor all client activities and provide services according on their preferences. Using IoT, you can be certain that your financial transactions will be safe and secure throughout the whole transaction process. The Internet of Things (IoT) may help clients save money by assessing their current financial situation and then recommending solutions that meet their specific needs. This will provide a positive customer experience, which will lead to a long-term banking relationship. For the financial and banking business, IoT advances have made it possible for them to uncover any administrative mistake and bring it to the bank's attention so that it can address the issue A bank's historical actions and customer behaviour may be tracked via IoT innovation. Using mobile apps and computerised sensors, IoTs initiatives in the fields of banking and finance gather data. Various financial institutions have mobile application for banking, which provide different silos for data that allow the banking and financial sector to precisely analyse customer behaviour and needs at an enormous scale.

Giving credit and debit card customers satisfying and easy administrations is one of IoT's most important benefits in the banking sector. banks may analyse certain regions and decide whether to increase or decrease the number of ATMs based on ATM usage volumes. In addition, banks may use IoT data to expedite request advantages to customers by providing booths and upgrading administrative services. Banks will be able to better understand their clients' business demands, their supply chain, and acquire insights into their customers thanks to IoT data. Every day, more financial institutions are being targeted by cybercriminals for extortion. Aside from stealing cash and data, hackers want to disrupt operations, ruin infrastructures, and compromise data-rich Financial Services Institutions (FSIs). It is clear that the banking sector's vulnerabilities must be examined and controlled.

NIST is one of the few frameworks now in use by banks for risk assessment. A framework for evaluating finance industry risk systematically has been developed. Using this paradigm, stability risk may be assessed. In addition to highlighting some of the issues financial institutions encounter when trying to evaluate cyber risk, this study examines many of the most popular methods for doing so. This technology also provides recommendations and perspectives on how financial institutions should estimate cyber risk. By putting a monetary value on cybersecurity risk, the RiskLens technology platform makes it easier to manage. RiskLens is based on FAIR, a widely accepted paradigm for quantifying cyber risk. Founded on software as a service, RiskLens evaluates, prioritises, and evaluates security expenditures in the cloud.

Cyber Security Risks Frameworks in Medical systems

The medical sector is one of the most fundamental infrastructural realms, and privacy breaches are on the rise owing to phishing attempts, misconfigured systems, ransomware, spyware assaults, and personnel and third-party vendor mistakes. Therefore, it is critical to detect and address any potential dangers. Many biological equipment (cardiac defibrillators, transdermal insulin pumps) is used in the healthcare industry, and this equipment pose extra privacy hazards. Today, because of widespread World wide web and network use to monitor medical equipment both in real-time and at a fixed location, there is an increasing danger of possible cybersecurity risks. It is difficult to protect devices and electronic health records (EHRs) against these attacks. Owing to IoT pharmaceutical products, medical systems require risk models to identify and manage these hazards. There are other concerns associated with remote telehealth and robot-assisted procedures that need accuracy, precision, and secrecy.

An evaluation of a medical equipment by a doctor may be included into a cyber risk score system. When it comes to medical devices, it is important to examine a doctor's worst-case scenario. Using the Stride threat classification methodology (created by Microsoft(R)), risk ratings for these devices are calculated. The approach of measuring medical device cyber risk has been improved thanks to this score system. The system's primary goals are to be simple to use, cost-effective, and provide outcomes that are visually pleasing. It's important to keep track of any negative events that may occur, and this may be done by using a healthcare risk evaluation framework. This system uses static fault trees and the Bayesian inferences to evaluate the functionality of clinical tools and equipment. Simulation approaches such as Petri net and Monte Carlo are advised for usage in the event of a hemodialysate infection. For the first time, it has been recommended that healthcare IoTs be specified, designed, and implemented according to a formal framework. A standardisation and interoperability approach are helped by this procedure.

It has been suggested that an Artificial Immune System may be used to examine the risks associated with the Internet of Things (IOT). To simulate immunity principles and attack detectors, this system applies set theory to the data. IoT security risks may be quantified in order to provide a reliable and accurate risk assessment procedure. The need for a security model structure that can identify the risks pertaining to healthcare technology and EHR data has grown as the digital age has brought about a major shift in modern medical systems. This ideal infrastructure must also be able to prioritise risks and take required steps to mitigate hazards. HITRUST (Health Information Trust Alliance) ranks in second with 26.4 percent of the healthcare security standards, as per the 2018 HIMSS Cybersecurity Study. It was recommended by [16] that healthcare organisations adopt the Security strategy as a condition of participation. Using NIST recommendations, critical infrastructures may better manage their cyber risk. Standards are set out by ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). HIPAA/ISO/NIST frameworks, Payment Card Industry (PCI), and COBIT standard can all be retrieved in one bundle. NIST CSFs five functions have been broken down into the identification of the risk to recovery, and Symantec(R) has studied how these operations need to be changed for health sectors.

The NIST framework must be tweaked a little in order to comply with healthcare standards and regulations. NIST's Protect function, which focuses on security and employee awareness and training, should be restructured. The Discover

function's essential components, including anomaly detection, should be continually monitored in order to detect a healthcare breach in time. As a result, it's critical for healthcare institutions to develop new technology that may help them better identify when, when, and how breaches occur. Ultimately, the NIST framework's five primary functional areas—Identify, Detect, Protect, Respond, and Recover—are to be carefully researched and updated to meet the medical sector's specific demands. An ideal objective for the future is to extend the five categories to IoT systems so that continuous evaluation may be provided.

V. CONCLUSION

If proper security measures are not in place, IoT-based infrastructures may be vulnerable to attacks and malfunctions. However, the privacy of Internet of Things (IoT) users is of paramount importance. Everyday life is increasingly dependent on Internet-connected "things," both at work and at home. Sensitive information about an individual's private life could be made public through the internet. Issues of privacy are just as significant as confidentiality and protection in the IoT. In the IoT, heterogeneous computer networks and resource-constrained machines that could only afford lightweight privacy and security solutions have established weak interconnections for IoT network. Security analysis and risk models used in real-world scenarios have been reviewed in this paper. CPS systems are vulnerable to attacks, which reduce their performance and make it impossible to provide essential services. Such threats to other systems, including CPS, must be addressed. Because of the CPS's inherent complexity, risk management is particularly challenging. A risk management approach for CPS has been presented to identify essential CPS assets and analyse their risks.

References

[1]. M. H. Amini, J. Mohammadi, and S. Kar, “Promises of fully distributed optimization for IoT-based smart city infrastructures,” in Advances in Intelligent Systems and Computing, Cham: Springer International Publishing, 2020, pp. 15–35.

[2]. W. Zheng, J. Cheng, X. Wu, R. Sun, X. Wang, and X. Sun, “Domain knowledge-based security bug reports prediction,” Knowl. Based Syst., vol. 241, no. 108293, p. 108293, 2022.

[3]. S. M. H. Anik, X. Gao, N. Meng, P. R. Agee, and A. P. McCoy, “A cost-effective, scalable, and portable IoT data infrastructure for indoor environment sensing,” J. Build. Eng., vol. 49, no. 104027, p. 104027, 2022.

[4]. T. Rajmohan, P. H. Nguyen, and N. Ferry, “A decade of research on patterns and architectures for IoT security,” Cybersecurity, vol. 5, no. 1, 2022.

[5]. Gartner.com. [Online]. Doi: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf. [Accessed: 05-Mar-2022].

[6]. C. Wheelus and X. Zhu, “IoT network security: Threats, risks, and a data-driven defense framework,” IoT, vol. 1, no. 2, pp. 259–285, 2020.

[7]. F. Basya, M. Hardjanto, and I. Permana Putra, “SHA512 and MD5 algorithm vulnerability testing using Common Vulnerability Scoring System (CVSS),” bit-cs, vol. 3, no. 1, pp. 1–4, 2022.

[8]. S. Goswami, N. Krishnan, M. Verma, S. Saurabh Swarnkar and P. Mahajan, "Reducing Attack Surface of a Web Application by Open Web Application Security Project Compliance", *Defence Science Journal*, vol. 62, no. 5, pp. 324-330, 2012. Doi: 10.14429/dsj.62.1291.

[9]. S. Ramanauskaitė, N. Goranin, A. Čenys and J. Juknius, "Modelling influence of Botnet features on effectiveness of DDoS attacks", *Security and Communication Networks*, vol. 8, no. 12, pp. 2090-2101, 2014. Doi: 10.1002/sec.1156.

[10]. S. Bonvicini, S. Ganapini, G. Spadoni and V. Cozzani, "The Description of Population Vulnerability in Quantitative Risk Analysis", *Risk Analysis*, vol. 32, no. 9, pp. 1576-1594, 2012. Doi: 10.1111/j.1539-6924.2011.01766.x.

[11]. "McAfee Labs Threats Report: December 2018", *Computer Fraud & Security*, vol. 2019, no. 1, pp. 4-4, 2019. Doi: 10.1016/s1361-3723(19)30004-1.

[12]. R. Borum, "Operationally relevant research and practice in terrorism threat assessments.", *Journal of Threat Assessment and Management*, vol. 2, no. 3-4, pp. 192-194, 2015. Doi: 10.1037/tam0000046.

[13]. Z. Qian and Y. Wang, "Internet of Things-oriented Wireless Sensor Networks Review", *Journal of Electronics & Information Technology*, vol. 35, no. 1, pp. 215-227, 2014. Doi: 10.3724/sp.j.1146.2012.00876.

[14]. I. Lee, "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management", *Future Internet*, vol. 12, no. 9, p. 157, 2020. Doi: 10.3390/fi12090157.

[15]. G. Krigsvoll, M. Fumo and R. Morbiducci, "National and International Standardization (International Organization for Standardization and European Committee for Standardization) Relevant for Sustainability in Construction", *Sustainability*, vol. 2, no. 12, pp. 3777-3791, 2010. Doi: 10.3390/su2123777.

[16]. "Healthcare organisations struggle to maintain security", *Network Security*, vol. 2015, no. 10, pp. 1-2, 2015. Doi: 10.1016/s1353-4858(15)30084-2.