ISSN: 0067-2904

Methodologies, Requirements, and Challenges of Cybersecurity Frameworks: A Review

Alaa Dhahi Khaleefah, Haider M. Al-Mashhadi
Department of Computer Information Systems, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq

Received: 28/10/2022 Accepted: 18/2/2023 Published: 30/1/2024

Abstract

As a result of the emergence of new business paradigms and the development of the digital economy, the interaction between operations, services, things, and software across numerous fields and communities may now be processed through value chain networks. Despite the integration of all data networks, computing models, and distributed software that provides a broader cloud computing solution, the security solution is missing or inadequate, and more work is required to strengthen security requirements such as mutual entity trustworthiness, access controls, identity management, and data protection, all aspects of detecting and preventing attacks or threats. In order to combat cybersecurity threats, various international organizations, academic universities, institutions, and organizations have been working hard to establish cybersecurity frameworks (CSFs). This paper describes CSFs from the perspectives of standard organizations such as ISO CSF and NIST CSF, as well as several proposed frameworks from researchers, and briefly discusses their characteristics and features. The common ideas described in this study could be helpful for creating a CSF model in general.

Keywords: Cloud computing, Cybersecurity framework, ISO-CSF, NIST-CSF.

منهجيات، متطلبات وتحديات أطر الأمن السيبراني: مراجعة

علاء ضاحي خليفه, حيدر محمد عبدالنبي
قسم نظم المعلومات, كلية علوم الحاسوب وتكنلوجيا المعلومات, جامعة البصرة, بصرة, العراق

الخلاصة

نتيجة لظهور نماذج أعمال جديدة وتطور الاقتصاد الرقمي ، يمكن الآن معالجة التفاعل بين العمليات والخدمات والأشياء والبرامج من خلال العديد من المجالات والمجتمعات من خلال شبكات سلاسل القيمة. على الرغم من تكامل جميع شبكات البيانات ونماذج الحوسبة والبرامج الموزعة التي تقدم حوسبة سحابية أوسع ، فإن الحل الأمني له تأثير مهم خطير ومفقود أو ضعيف ، وهناك حاجة إلى مزيد من العمل لتعزيز متطلبات الأمان مثل الثقة المتبادلة بين الكيانات ، تعد ضوابط الوصول وإدارة الهوية ، وكذلك حماية البيانات ، كلها جوانب للكشف عن الهجمات أو التهديدات ومنعها. تعمل العديد من المنظمات الدولية والجامعات والمؤسسات الأكاديمية والمنظمات بجد لإنشاء أطر للأمن السيبراني ((CSF) من أجل مكافحة تهديدات الأمن السيبراني بواسطة (CSFs) تصف هذه الورقة عوامل النجاح الحرجة من منظور المنظمات القياسية مثل ISO CSF و NIST

*Email: mashhad01@gmail.com

CSF ، بالإضافة إلى العديد من الأطر المقترحة من الباحثين ، وتناقش بإيجاز خصائصها وميزاتها. يمكن أن تكون الأفكار الشائعة الموضحة في هذه الدراسة مفيدة في إنشاء نموذج CSF بشكل عام.

1. Introduction

The use of cloud computing technology and the Internet of Things (IoT) has sparked interest in combining technological tools and hardware from various domains and places to develop cyber-physical systems (CPSs). Pervasive and grid networking architectures, computer models, and software architectures are already supporting this transition. Regrettably, security paradigms have not progressed as quickly. In fact, the most common paradigm now is the security perimeter, in which devices are deployed to specific fields with only sporadic or no integration. This generates security challenges about the system's overall behavior (authentication and availability), the position of private information (confidentiality), the safeguard of software and vital data (integrity), and, very importantly, the efficiency to respond quickly to any new breaches [1] and [2].

Cybersecurity software and devices always work to develop their detection and defense abilities against any possible threats. They exist in racks that contain cybersecurity servers to serve diverse management zones like IoT nodes, cloud infrastructure, corporations, storage servers, and networks. The cybersecurity software consists of groups of rules and conditions to test the stream of data from different sources; these groups of instructions may be used by many property firms to control the cybersecurity systems in any organization [3].

Furthermore, the complexity of ICT infrastructures expands system vulnerabilities, encouraging the development of novel exploit methods to supplement existing traditional techniques such as distributed denial of service (DDoS) and botnets [4] and [5]. Even if they have been extensively developed and inserted into distributed systems, access control and identity management strategies cannot ensure the authenticity and trustworthiness of the entire series over time, nor can they track the dissemination of sensitive information and confidential material along the value stream [6–19]. Moreover, because the end user is often uninformed of the chain's topology and structure, determining if application providers, security techniques (e.g., encryption, integrity), and confidential strategies are compatible with his certain requirements is challenging. This situation clearly aids attackers, who take advantage of the lack of visibility across different subsystems and the lack of appropriate integrated procedures capable of correlating activities and metrics from many environments. By contrasting various goals and condensing common notions, this work seeks to synthesize the many diverse opinions on CSFs into a succinct picture. This study provides a brief discussion of the traits and attributes of CSFs as well as a manual for designing CSFs in organizations.

2. Related Works

There are many studies that try to discuss cybersecurity frameworks, such as [20–24]. Reviewing the research on decentralized filtration and management is done in the study [21]. approaches using dynamic models in situations involving industrial CPSs. [23] Survey data collection methods for distributed IDSS using data collectors or agents In the work [19], security and privacy concerns in dispersed IoT systems are analyzed. Security- and privacy-related characteristics and challenges are addressed in terms of data collection, aggregation, mining, and analytics at various tiers. [24] surveys several efforts on defenses versus assaults in distributed applications, with an emphasis on expansion ability and processing challenges. To determine most of the appropriate remedies, mathematical frameworks are used. [20] examines accurate estimates for the development of assaults in parallel computing based on

risk-interconnected relationships, sequential work, analytical algorithms, and the identification of assault attributes.

In [25], machine learning (ML) techniques for snooping disclosure are presented. They mostly use profound learning structures or neural nets to retrieve pertinent facts from massive amounts of data [25].

Additionally, several research studies [26, 27] analyze countermeasures in particular contexts. In [26], a method is suggested for determining how reliable information sent between dispersed automobiles in a protected automobile ad-hoc network (VANET) environment is. For manufacturing equipment, a methodology for danger rating is put forth in [27], in which threats are anticipated depending on certain transmission schemes to determine the likelihood of network nodes becoming bargaining partners.

Identity administration and authorization functionality are critical in spreading information security architectures because they validate the legitimacy of any physical or mental structure that is a part of the overall design or validate the authorization to view non-homogeneous assets and services distributed and spread toward various companies. [28-36] constitute the most prominent contributions on the subject.

Verification and authorization operations have consistently been viewed as a major difficulty in uncentralized contexts, as frequently documented in the scientific literature. The majority of newly developed solutions make use of a detached approach that tries to reconcile the separation of identification and authorization functionalities [29]. Realized and OAuth 2.0 are only a couple of the intriguing solutions that have recently been proposed in the research journals for access control in multi-domain systems [31–34]. They provide the option of using a reputable certificate authority to verify clients in a unified environment.

3. Reference Methodologies, Requirements and Challenges

Figure 1: Supply chain in the industries that deals with data through deferent sectors and ICT infrastructures.

Most business processes, such as design, implementation, establishment, purchase, manufacturing, investing, distribution, and after-sales services, now follow a completely digital workflow that spans multiple domains, connects multiple processes, applications, and

equipment, and provides them with appropriate client data and their status, as shown in Figure 1.

Convergence of available computing fields, such as the IoT, Software Defined Networking (SDN), and cloud computing, is intended to achieve this main goal, and everything-as-a-service and service-oriented paradigms were used to apply to CPSs with the help of automaticity and dynamic composition [37, 38]. With software, service-centric models, data sharing, and multitenancy being pushed, this represents a revolution in the way systems are conceptualized, planned, developed, and operated. The main issues are discussed in the sections below.

3.1 Multi-tenancy and Virtualization challenges

Although network grids improve solution and agility, the closer integration of various organizational functions, as well as the requirement to share resources and data, raise privacy and confidentiality concerns that may not be resolved [39].

Interdependence among tenants, or between SPs and their RPs, is made possible in reality by virtualization and multi-tenancy. If a virtual resource, such as a VM or maybe even a Virtual Network Function (VNF), has an influence on different renters associated with identical equipment, appropriate isolation (at the CPU, storage, RAM, and network levels) can mitigate the impact, as long as the overcommitment ratios are not too high. Even if a physical infrastructure attack, such as a DDoS against a service provider's infrastructure, does not result in increased traffic inside tenants' virtual networks, it will most likely affect all tenants.

Although a number of existing cloud security technologies are now available, they are primarily designed to secure infrastructure and are aimed at cloud service providers. Due to encryption and privacy concerns, tenants' resources are restricted. Services and their interfaces are so diverse that implementing universal security policies across many infrastructures and domains is difficult. However, the wide range of solutions and interfaces makes it challenging to set uniform security policies for service chains that span numerous systems and environments.

Service providers frequently employ affinity and anti-affinity policies to determine whether or not various virtualized practical codes of the services’ serial must be connected to a physical resource (affinity policies) [40, 41]. If separate servers, networks, and infrastructures do not go down at the same time, anti-affinity can be employed for high availability and resilience. Affinity protocols decrease the attack domain because no network link is exposed to connection attackers. An effective server or virtual server assault will harm all service elements aggregated under the affinity protocols. In terms of detection, attacks on one service instance will likely affect others in the same affinity group. Affinity policies might thus be utilized as an early warning system to prevent attack transmission throughout numerous services. Unfortunately, there is no standard means for cloud service suppliers or particular renters to quickly share this information with other companies.

3.2 From infrastructure-centric models to service-centric models

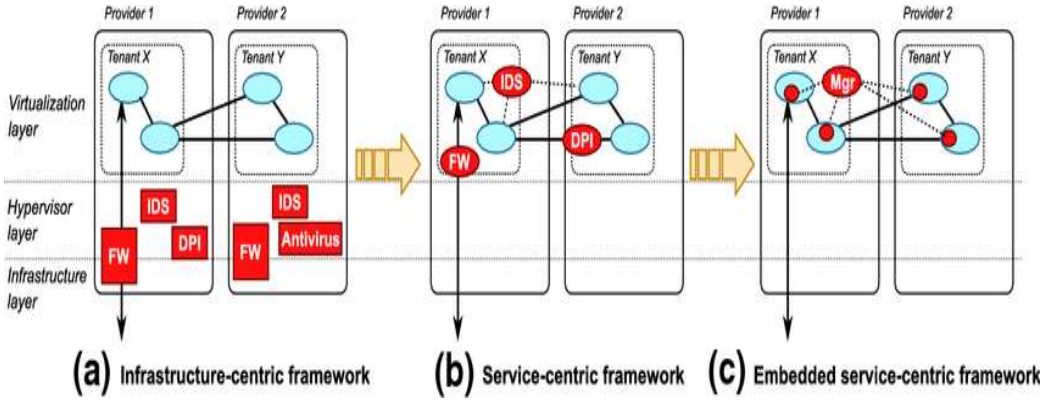

Figure 2: The transformation of cybersecurity architectures from infrastructure-centric models to service-centric models.

As shown in Figure 2a, most cybersecurity equipment has typically been built to secure the hardware infrastructure rather than the applications that are performed on top of it. The introduction of virtual machines and cloud models has accelerated the move from infrastructure-centric to service-centric model structures by creating software and fundamental equipment that are gradually divided (as depicted in Figure 2b). This architecture is widely applied nowadays, with sensors installed in VNFs and VMs that gather incidents, logs, and frames and send them to virtual objects of networking devices connected into programmed graphs for analysis.

There's no need to depend on (or trust) third-party services; each tenant has complete control and responsibility for its own security management. This model's implementation is simple, and it can be simply coupled with software orchestration approaches. However, running the security equipment necessitates more resources. Furthermore, visibility is frequently limited to a few components, making it difficult to correlate events with the entire series.

The goal is to improve performance. The next transition stage is a service-centric structure, which eliminates the requirement for traditional on-premise security hardware, spreads security requirements across each software component, and leads them through a single protection admin that localizes all protection applications, as shown in Figure 2c. A distributed security architecture eliminates the need for numerous and widely dispersed separate and unrelated programs with the lofty goal of inspecting the system while linking events in time and space. Its goal is to move attack and vulnerability detection from endpoints to traditional security stations (either hosted on dedicated hardware or in the cloud). Unlike existing SOC techniques, the goal is to provide the majority of protection services from a single central location while providing the security context gathered by smart local agents. Rather than using static analysis and evaluation equipment, the concept is to continuously outsource surveillance and inspection operations to such agents. As a result, the primary design will be more dynamic and responsive to changing threats, requiring fewer local resources to maintain.

This proposed mechanism also creates additional issues that need to be addressed correctly. The first is reliable and secure data transit through networks, which needs to be protected to prevent clogging of the main communication routes. The second will be how to carry out the bare minimum of operations on diverse and resource-limited end terminals. The ability to evaluate and correlate large amounts of data from various sources while also taking identification, organization, and access control strategies into account is the third limitation. Network components that move data and control instructions must be able to manage identities

and distribute raw surveillance as well as observations among multiple classification techniques [42].

3.3 The Transition to 'as-a-Service' Models

Small businesses, which have traditionally brought innovations and tailored solutions to market, are frequently hampered by the rising complexity and range of communication and information technology. To get past this roadblock, businesses are going more and more towards the as-a-service architecture as a dependable, affordable substitute for full asset creation. The ability to virtualize or share hardware, networks, processes, and applications among various tenants is the fundamental idea. Such resources can be accessed using software APIs without a thorough understanding of their fundamental structure being necessary. Even the most complicated service meshes can be efficiently built using APIs. The most common examples of this straightforward description, which has led to a flood of commercial services, are infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), software-as-a-service (SaaS), network-as-a-service (NaaS), and data-as-a-service (DaaS). Additionally, one of the newest implementations in the "as-a-service" groups is the Internet of Things (IoTaaS), also known as "things-as-a-service" (TaaS), which lacks a widespread understanding in the industry. New corporate positions and interactions reflect this change. In reality, Resource Providers (RPs) are the owners of valuable digital goods and grant Service Providers (SPs) non-exclusive, segmented access to them.

Applications, infrastructure, and information are dynamically assembled by end users into new value networks and business concepts. Cloud providers are those who incorporate storage and computation services and infrastructure into virtualization services using IaaS, PaaS, or FaaS models (i.e., those who supply plain VMs, memory, and so forth); infrastructure providers are those who own real estate infrastructure and provide services (data centers, inter-location links, IoT facilities, and so on). Infrastructure developers are software programmers who improve system capabilities and publish them in public or private portals. Software selection, cloud storage, IoT device connectivity, or data brokering They can use software orchestration technologies to successfully automate conventional deployment and management tasks in specific domains (e.g., cloud and NFV), allowing them to deploy technological devices, setup them, and govern life-cycle events.

3.4 Distributed Cybersecurity Frameworks: Challenges and Benefits

The accessibility of software-defined architectures allows for exceptional agility in constructing, updating, and destroying even complex service topologies; however, due to their high dynamicity, allocation of resources becomes a hurdle in these systems. Based on the number of renters, equipment, and processes included in the series, the locations and volume of services may actually change frequently. As the number of instances of such resources and the range of services in a chain rise, more resources are needed. Hardware (CPU, memory, storage) as well as network resources (data routing between instances and/or functions) are both required to run the services (throughput, link capacity, bandwidths).

The distribution of resources is affected by the deployment of extra security services. A distributed cyber-security architecture, in general, necessitates collaboration in the selection, instantiation, and placement of security functions, as well as in the distribution of obtained data, metrics, and activities. This must ensure that the discovery requirements are met while also adhering to the service's overall resource constraints and allocation rules [43, 44].

The requirement to analyze network packet traces is one of the key issues with present IDS/IPS systems. This is possible when the protection equipment is installed with the host itself as the one it is protecting, but it becomes problematic when it is installed remotely. The problem is caused mostly by the usage of stupid local devices, which are unable to collect the discrete sets of data necessary for the activate to detect specific threats because these properties change often. The introduction of customizable solutions for internet probing will essentially eliminate the issue in this regard. Finding the ideal balance when comparing the degree of detail in the data gathering and sending with the pace at which capital is allocated will be the challenge. Real advancements in inspection and monitoring procedures will also be possible with this technology. To improve overall effectiveness, one could use the principles of attraction. Some detection activities can only be completed in a single instance when two or maybe more service instances are grouped together and they're likely to face the same physical reality (like CPU, memory, and network activity delay).

3.5 Tools for Management and Orchestration Integration

Rapid, efficient reaction and management activities, in addition to the gathering of information and parameters for analytics and identification, are extremely difficult concerns for any distributed system. People's capacity to notice issues and develop remedies is key to the effectiveness of today's response. In order to trigger a faster and more consistent reaction, new cyber-security frameworks are anticipated to rely extensively on software orchestration tools. Integration with the strong monitoring entity regarding Network Function Virtualization (NFV) enables, among other things, the removal of a corrupted VNF, the isolation of a segment under assault, and the routing of traffic via scrub units or cloud-based services [45].

The service coordinator may or may not include the weather protection system. Most likely, corporate and commercial endeavors will dominate in determining it. In fact, the skills required to run a SOC differ significantly from those required to manage NFV and cloud providers. Small firms are likely to rely on outsourced security services, but larger businesses might benefit more from integrated solutions. Decoupling security operations and service management will undoubtedly call for access control using technologies to prevent adding fresh vulnerabilities to the system [46].

4. Standard Security Frameworks

When it comes to security, using cloud technology is similar to any other classic IT infrastructure. Because of the aggregation of digital assets, cloud computing, like any modern technology, poses major hazards to enterprises and makes them more attractive assault targets. Analyses of the cloud services' current security impact a few years ago were naturally focused on information security or data security. People-to-people contact, programs, and services available online have been the subject of recent research. Data protection, sometimes known as "cyberspace protection," essentially does that [47].

Data protection, information system security, and cyber security are all terms that are frequently used interchangeably. While there are numerous parallels between these phrases, we believe there is one significant difference. Before long, problems concerning the distinction between data and information security may arise. Both terms refer to the same level of protection because information is really just data that is evaluated and given meaning by a system. Data protection is the primary objective of standard information security, which focuses on the data's availability, confidentiality, and integrity (CIA). Authenticity, authorization, auditability, cryptography, non-repudiation, and traceability are factors that affect information security [48].

With information as a crucial element, the term "cybersecurity" can be used to describe the interactions and links between both the internet and the real world. [43].

The material on interconnected networks created by information technology and the electronic world formed by such networks is how cyberspace is defined [49, 50].
Cybersecurity, depending on the International Telecommunication Union (ITU), is a collection of instruments, regulations, standards, and security principles, directives, risk management strategies, events, and assurances, as well as technology that can be used to protect organizations, businesses, and users' assets online. The entire transported and/or stored data in the cyber environment is owned by organizations and consumers, as are the computers that are online, users, facilities, apps, services, and telecommunications networks [51, 52].

Dealing with security concerns is the most difficult component of properly integrating cloud computing technologies. As a result, actions must be taken to address cloud computing security risks while also reaping the benefits of this technology.

To date, businesses have implemented a range of measures to address cloud computing, cybersecurity, and safety requirements. How valuable are the NIST CSF and ISO/IEC standards, for instance, to the cybersecurity as well as cloud computing standard landscapes?

4.1 27,001, 27,017, and 27,032 from ISO and the NIST cybersecurity framework

Figure 3: Organizations of Cybersecurity Frameworks.

ISMS (Information Security Management System) Security standards can be created and maintained as guidelines or frameworks [53]. In addition, over the past 15 years, additional laws and regulations have been passed that include requirements for information security [54]. There are many organizations that describe the cybersecurity frameworks and standards as shown in Figure 3.

a. International Organization of Standardization ISO

In 1947, the non-governmental International Organization of Standardization (ISO) was founded. The International Telecommunication Union (ITU) and the International Electrotechnical Commission (IEC) promote it. Specialized groups, who are participants in ISO or IEC, were set up mostly by organizations to address certain technical activity sectors and support the development of international standards [55]. One of ISO's most important standards is ISO/IEC 27,000, ISMS. Those are specifications for information security [56]. The 27000 family of standards establishes the requirements and principles for a networked ISMS.

•ISO/IEC 27,000, a standard defining an overview with terminology.

•Standards (ISO/IEC 27,001, ISO/IEC 27,006, and ISO/IEC 27,009) that specify requirements.

•Standards outlining broad recommendations (ISO/IEC 27,002, ISO/IEC 27,003, ISO/IEC 27,004, ISO/IEC 27,005, ISO/IEC 27,007) ISO/IEC TR 27,008, ISO/IEC TR 27,013, ISO/IEC TR 27,016, and ISO/IEC 27,021) are the standards.

•Standards outlining industry-specific regulations (ISO/IEC 27,010, ISO/IEC 27,011, ISO/IEC 27,017, ISO/IEC 27,018, ISO/IEC 27,01).

Table 1 lists the most important standards in this study, along with their title, status, and most current edition.

Table 1: The ISO 27 K family of standards

Standard	Title	Status	Last version
ISO 27,000	Information technology, Security techniques, Information security management systems, Overview and vocabulary	Published 2009	The fifth edition in 2018
ISO 27,001	Information technology, Security techniques, Information security management systems, Requirements	Published 2005	Second edition in 2013
ISO 27,002	Information technology, Security techniques, Code of practice for Information security controls	Published 2007	Second edition in 2013
ISO 27,017/ ITU-T X.1631	Code of practice for information security controls based on ISO/IEC 27,002 for cloud services	Published 2015	_
ISO 27,032	Information technology, Security techniques, Guidelines for cybersecurity	Published 2012	_

A framework called ISO/IEC 27,001 [56] addresses ISMS requirements for organizations of all sizes, types, and industries (including retailing, defense, banking, education, healthcare, and government), as well as for businesses of all dimensions (from tiny corporations to giant corporations) (including businesses, governments, and non-profit organizations). An ISMS is a group of policies, practices, instructions, and related activities and resources that a corporation provides to keep its systems safe, in accordance with ISO/IEC 27,000:2018 [57]. The focus of this standard is on the conditions for designing, constructing, installing, operating, monitoring, as well as upgrading such a system. The ISO 27K family of specifications, as well as other IT specifications, consider the plan-do-check-act (PDCA) paradigm as a continuous improvement process paradigm, as illustrated in Figure 4 [53]. We characterize the different information resources and the security requirements that go along with them during the planning stage, then we identify and assess cybersecurity threats before developing controls and processes to lower these risks. The implementation of these safeguards and restrictions will follow. Finally, in

order to make adjustments and improvements for future development, the ISMS performance must always be analyzed and assessed on a frequent and ongoing basis. ISO/IEC 27,001, which aims to control and decrease an organization's risk of data breaches to an acceptable level, is the cornerstone for information security risk management. Additionally, Annex A lists the controls where the security controller is chosen, and ISO/IEC 27,002 offers instructions and recommendations for putting these controls into practice**.** [58]**.**

Figure 4: Sequence of PDCA in ISO 27,000 [36]

Figure 5 depicts the ISO/IEC 27,001 implementation clauses.

Figure 5 : the ISO/IEC 27,001 implementation clauses.

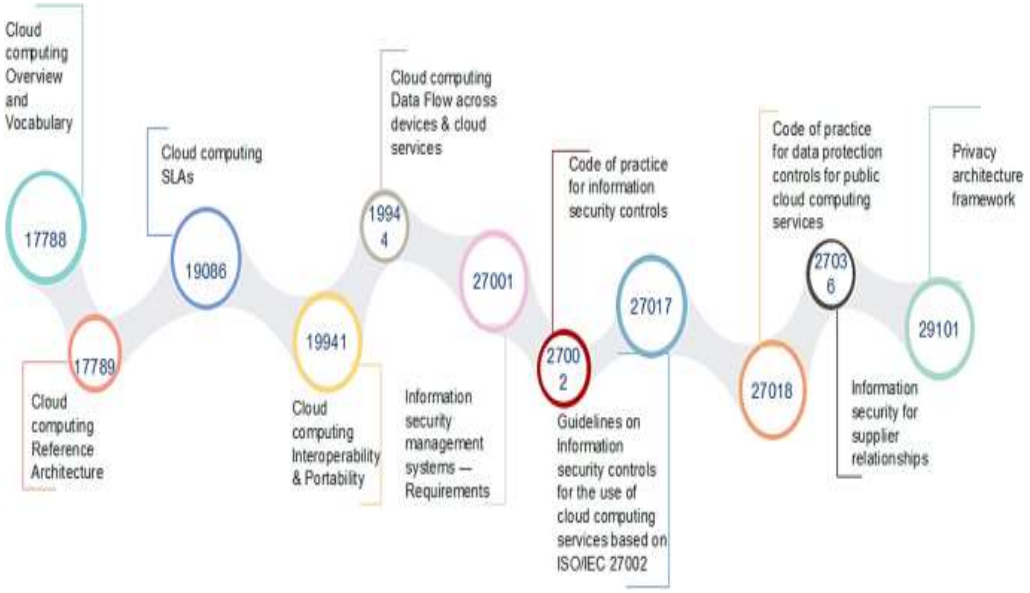

Figure 6: ISO Cloud Computing standards.

In late 2015 and early 2018, the recommendation was made public [57]. It was created in collaboration with the ITU-T by the Joint Technical Committee ISO/IEC JTC1. Technically, it establishes security measures for cloud service consumers (CSCs) and cloud service suppliers (CSPs) according to ISO/IEC 27,002:2013. It has the support of ISO/IEC JTC 1/SC 27, ITU-T Q8/SG17, national guidelines organizations, and the Security Cloud Alliance, in addition. It references ISO/IEC 27,000, 27,002, ISO/IEC 17,788 (Cloud Services and Terminology), and ISO/IEC 17,789 (Cloud Computing—Document Structure) (see Figure 6). Additionally, organizations that offer cloud-based services and wish to completely cover all aspects of cloud security must look into ISO 27,017.

This standard suggests seven more controls in addition to the 37 controls included in ISO/IEC 27,002 as well as instructs them. The following crucial issues are covered by these new regulations:

- Responsibility in data protection are integrated. Or divided through the customer and the supplier in a Cloud Computing environment.
- When the contract/agreement is ended, the cloud service customer's assets are deleted and removed.
- Virtual computing segregation and protection for customers.
- Hardening and configuring virtual machines to match the organization's needs.
- The client's capacity to keep an eye on cloud computing services
- Administrative procedures pertaining to the computing environment
- Alignment of virtual and physical network security management.

4.2 NIST-CSF

NIST would be an independent agency that continues to work closely to create and use standards, measurements, and technologies for business. In 1901, it was established. The National Institute of Standards and Technology (NIST) has developed a cybersecurity framework to assist businesses in managing cyber-security concerns. To assist businesses in directing their cybersecurity activities and incorporating cybersecurity risks within risk management procedures, this method places a strong emphasis on business drivers. The Cybersecurity Enhancing Act of 2014 made changes to the original version, which was created in accordance with Executive Order 13,636. The framework provides risk management

principles and best practices to small and large businesses alike, regardless of focus, sector, or nation [59] [60] [61].
to increase the vital infrastructure's dependability and security. Depending on the objectives and requirements of the firm, these practices are applied in a wide variety of ways. The framework's objectives include figuring out their current cybersecurity posture, articulating their desired cybersecurity state, prioritizing improvement options, gauging how well they're doing at getting there, and distributing cybersecurity risk to several stakeholders. NIST CSF can also serve as a springboard for developing a cybersecurity program or as support for and justification of the company's cybersecurity risk management. The system model is made up of five concurrent as well as continuous operations (recognize, guard, detect, respond, and restore), classifications and defining subclasses of wanted results for every activity, and instructive citations to every subclass provided by the core, implementation tiers, and profile of an existing framework. The Framework Core is made up of concurrent and continuously running functions such as Identify, Protect, Discover, Respond, and Recover, as well as classes and subclasses that specify expected results for each function.

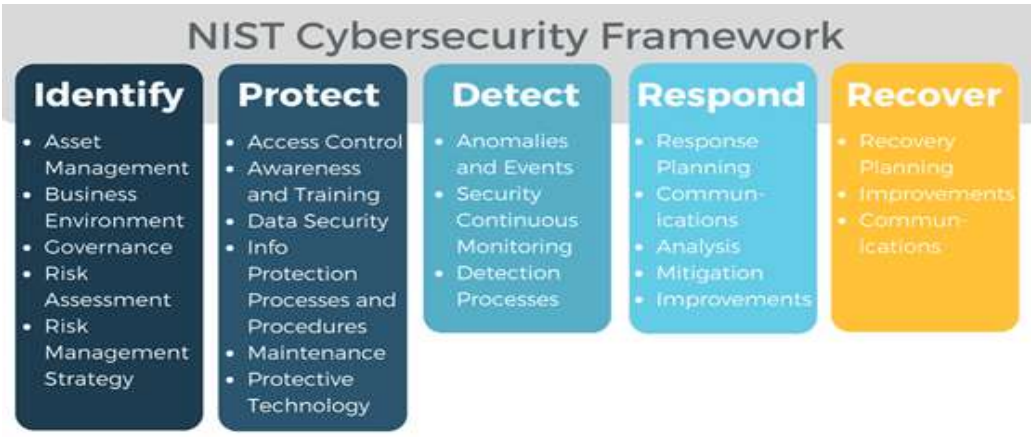

Figure 7: NIST cybersecurity framework's steps

Tiers of framework implementation can be used by businesses to guide their risk management decisions about cybersecurity. The four phases are repeatable, flexible, and largely risk-informed. The paper claims that they highlight the rigor and complexity of cybersecurity risk control rather than indicating maturity levels [62]. Advancement to higher tiers is influenced by a number of variables, including the formalization, approval, establishment, adaptation, or the organization's performance in improving current risk analysis practices; the level of company culture and risk awareness related to cybersecurity; how this is approached and tried to communicate; and information sharing practices with outside parties. The architecture profile is created by combining the framework's kernel and layer selections with indications of organizational needs, resource availability, and risk tolerance. It is employable to characterize both the desired target condition (the target profile) and consequently the present level of cybersecurity activities. In order to achieve cybersecurity objectives and achieve the target profile, the organization uses the gaps between the two profiles as seen by the comparison to plan activities and chart a route. As a result, Figure 7 depicts the NIST CSF phases.

4.3 The ISO standards and the NIST CSF cybersecurity framework for cloud computing.

Customers who require unlimited, pooled, instantly provided, and released computational capacity (resources) that can be monitored and controlled without needing to spend on infrastructure or physical resources may find cloud computing to be a simple and cost-effective platform. Although cloud computing has various benefits, it is susceptible to security and

privacy concerns. Security professionals examined the distinctions between information security and cybersecurity during this investigation. According to a study, cybersecurity is the protection of digital and electronic information in the cyber environment, which consists of networked computing devices, people, infrastructure, applications, services, and communications technologies. As a result, we examined how to handle cloud computing, cybersecurity, and data security risks utilizing ISO standards and procedures. These regulations should take into account security elements like identification, privacy, secrecy, integrity, durability, physical security, and cloud security [63].

Then after, a framework proposal which solves the three issues raised is essential.
The capacity to design and apply the new security standards for business/enterprise clouds is a critical component to consider within this framework. A nice place to start could be with recent frameworks. [64, 65] that take care of business cloud security and make sure all implementation and service delivery comply with all technical requirements.

Organizations need a thorough roadmap to create effective cybersecurity planning, and the first step should be to identify the extent to which the organization's baseline principles and controls are understood and implemented. The problem is that neither the NIST CSF nor ISO standards offer a framework for figuring out the maturity level of a company. A maturity model, to start, might be described as a standard based on a variety of criteria with the aim of evaluating lower levels of maturity or stages in order to evaluate the sufficiency of the things being examined [66]. Because the NIST CSF lacks a model It keeps track of the framework’s progress and allows for some implementation freedom. However, including the implementation tiers and the framework profile, two significant frameworks, could help academics define maturity models [57]. These two tools, however, are not meant to be used as maturity assessment tools; rather, they are merely conceptual tools that help in understanding the company's cybersecurity risk management approach [62].

A methodology for determining an organization's mental maturity must be created, and it must take cloud-specific security domains into account. Several studies of various types have been conducted on this subject [52] [63] [67] [68]. The authors of [67] recommend an ISMM for information security that has 23 evaluated areas and 5 levels (performed, managed, established, predictable, and optimized). The NIST CSF categories are part of the compliance evaluation process they have developed. In order to examine an organization's dependency on ICT, Bahuguna et al. [52] created five levels of maturity and related these to four more levels. Moreover, a Cybersecurity Resilience Maturity Measurement (CRMM) approach for evaluating cybersecurity resilience maturity has been developed [63]. They've divided the risk and resilience intersections into four stages (initializing, defining, managing, and optimizing). The Cloud Security Capability Maturity Model (CSCMM) is made up of twelve domains of cloud security, where each is made up of a set of cybersecurity practices, as well as four levels of development (nonspecific, initiated, managed, and optimized).

It's also a security metric framework and a combination of multiple cybersecurity methodologies. Six steps make up the security metrics framework: first, describing the security processes and activities, as well as the purposes, goals, and security prerequisites; second, categorizing the identified security activities or procedures, as well as the metrics strategy and measurement technique. Finally, they use mathematical models and numerical data to calculate security metrics, as well as numerical simulations and mathematics data. They begin by analyzing the measured metrics, input elements, and metric plan steps. Fifth, they benchmark

the outputs of the preceding steps to determine maturity levels. Finally, they inform metrics users of the effects of the security state on the organization's business plan [63] [69] [70].

5. Modern Cybersecurity Frameworks

Many literary works, some of which are briefly reviewed in this section, attest to the need to fulfill the demanding needs addressed in Sect. 2. [71, 81] Discuss security in multi-domain, multi-tenancy systems that are dispersed.
[71] [73] [77] [78] [79] examine the current situation of distributed cyber-security systems. Using dynamic models, the survey [73] evaluates the literature on distributed filtering and control techniques in industrial CPS environments. [78] Data collection options for distributed IDSS employing data collectors or agents are examined. The options are unlimited when it comes to information collection, consolidation, mining, and analytics. In the paper [75], security and privacy concerns in dispersed IoT systems are examined, with an emphasis on security as well as privacy-related characteristics and problems at different phases. With a focus on scalability and computing effort constraints, [79] explores recent work into cyberattack countermeasures within distributed systems. To decide which countermeasures to employ, theoretical models are used in [71]. Threat correlation, action sequences, statistical models, and the extraction of attack attributes are all addressed as techniques for anticipating the progression of attacks on distributed systems.

Using machine learning algorithms to identify intrusions is presented in [81]. To take out relevant features from massive amounts of information, they primarily utilize neural networks and deep learning structures. There are more studies [72] [74] [75] [76] that examine security frameworks in specific circumstances in more detail. A method for determining the veracity of messages sent between dispersed cars is provided in [50] inside a secured Vehicle Ad-hoc Network (VANET) environment, calculating the possibility for compromised nodes in the network using specific propagation models. The authors propose a risk assessment approach for industrial systems in [74]. Identity and access management and user access capabilities are essential in distributed cybersecurity frameworks because they confirm the legitimacy of both the material and logical things included in the construction as well as the authorization to access dissimilar services and infrastructure dispersed and deployed across various organizations. [7-10, 12-16] provide the most illustrative pieces on this subject.

Services for authentication and authorization have been around for a while as a significant difficulty in decentralized scenarios, according to academic research. The number of new solutions used a decoupled strategy, which separates the authorization and authentication processes in an effort to combine them [8]. Recently, numerous novel approaches to identity management across systems have been put forth in the academic literature, including OpenID Connect and OAuth 2.0. [10] [13] [14] They demonstrate how to verify clients in an integrated structure using a trusted identity provider.

Controlling access based on attributes is a practical attempt at fine-grained authorization developed by the National Institute of Standards and Technology (NIST) (ABAC) [6]. According to this theory, access to resources is managed by taking into account user-specific identity-related attributes, and the user is given accessibility only after ownership of identity-related attributes that adhere to the access policy has been verified. Identity-Based Access Control (IBAC) and Role-Based Access Control are two additional methods for resource protection (RBAC) [7]. If a user's identity is listed on a certain access control list, they are permitted access to a resource or service in IBAC. The roles and privileges of users determine access rights in RBAC. Alternative strategies [9] [12] [15] [16] Using cryptographic techniques,

build on the ABAC logic to solve the access control problem. The Modern Security Frameworks are based on the requirements that are defined in the Standard Security Framework, but in most situations, the Modern Security Frameworks concentrate on specific requirements, not all of them, because they are suggested for certain situations and requirements, like integrity only, confidentiality only, or detection of attacks, and in special cases, they concentrate on detecting, protecting, and recovering the system from any threats. Some modern approaches try to deal with all aspects of standard requirements.

6. Conclusion

Among the most difficult elements of implementing the cloud computing concept is ensuring security and privacy. Furthermore, the heightened cybersecurity threats and the convergence of digital assets make the targets of attacks more appealing. Cybersecurity management, on the other hand, has never been more critical than it is now. To strengthen the security of critical infrastructure, mitigate this risk associated with cloud computing, and create, keep, or improve the organization's information security program, establish, develop, or maintain information security management. In this study, we looked into the rules and principles that govern cybersecurity and information security in the cloud. Based on the findings of our research, we recommend the establishment of the NIST CSF subcategories and the merging of the security criteria of ISO 27,001, ISO 27,017, and ISO 27,032. For cloud organizations desiring to manage cybersecurity efforts. Therefore, the frameworks serve as a helpful manual for organizations looking to set up an appropriate technique for cybersecurity inside the cloud computing system or to add to and maintain their current risk management mechanisms and cybersecurity programs. This is because they adjust these controls, combine these methods, and specify maturity levels.

References

[1] S. Scott-Hayward, S. Natarajan and S. Sezer, "A Servey of Security in Software Defiend Networks," *IEEE Communication Serveys & Tutorial*, vol. 18, no. 1, pp. 623-654, 2016.

[2] N. Schnepf, R. Badonnel, A. Lahmadi and S. Merz, "Automated Verfication of Security Chains in Software-Defiend Networks with Synaptic," *in IEEE Conference on Network Softwarization (NetSoft), Bologna, Italia*, 2017.

[3] S. Hares, D. Hares, M. Zarny, C. Jacquenet, R. Kumar and J. Jeong, "Interface to Network Security Functions (I2NSF): Problem Statement and Use Cases," *Internet Engineering Task Force (IETF)* , Saline, 2017.

[4] G. PEK, L. BUTTYAN and B. BENCSATH, "A Survey of Security Issues in Hardware Virtualization," *ACM Computing Surveys*, vol. 45, no. 3, pp. 40:2 - 40:34, 2013.

[5] R. Rapuzzi and M. Repetto, "Building Situational Awareness for Network Threats in Fog/Edge Computing: Emerging Paradigms Beyond the Security Perimeter Model," *Future Generation Computer Systems*, vol. 85, pp. 235-249, 2018.

[6] A. Alomari, S. K. Subramaniam, N. Samian, R. Latip and Z. Zukarnain, "Resource Management in SDN-Based Cloud and SDN-Based Fog Computing: Taxonomy Study," *Symmetry*, vol. 734, no. 13, pp. 1-30, 2021.

[7] I. Indu, R. Anand and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574-588, 2018.

[8] B. Lang, J. Wang and Y. Liu, "Achieving Flexible and Self-contained Data Protection in Cloud Computing," *JOURNAL OF IEEE ACCESS*, vol. 5, pp. 1510 - 1523, 2017.

[9] R. Li, C. Shen, H. He, Z. Xu and C.-Z. Xu, "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing," *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 344–357, 2018.

[10] L. Lynch, "Inside the Identity Management Game," *IEEE Internet Computing*, vol. 15, no. 5, pp. 78–82, 2011.

[11] D. Ramesh and R. Priya, "Multi-Authority Scheme based CP-ABE with Attribute Revocation for Cloud Data Storage," *in IEEE*, 2016.

[12] S. Sciancalepore, G. Piro, D. Caldarola, G. Boggia and G. Bianchi, "On the design of a decentralized and multi-authority access control scheme in federated and cloud-assisted Cyber-Physical Systems," **IEEE Internet of Things Journal**, vol. 5, no. 6, pp. 5190 - 5204, 2018.

[13] M. Shehab and S. Marouf, "Recommendation Models for Open Authorization," *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*, vol. 9, no. 4, pp. 582-594, 2012.

[14] A. Vapen, N. Carlsson, A. Mahanti and N. Shahmehri, "A Look at the Third-Party Identity Management Landscape," *IEEE*, vol. 20, no. 2, pp. 18-20, 2016.

[15] J. Wei, W. Liu and X. Hu, "Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage," *IEEE SYSTEMS JOURNAL*, vol. 12, no. 2, pp. 1731 - 1742, IEEE SYSTEMS JOURNAL.

[16] K. Xue, W. Chen, W. Li, J. Hong and H. Peili, "Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2018, 2062 - 2074.

[17] K. Yang, X. Jia, K. Ren and B. Zhang, "Combining data owner-side and cloud-side access control for encrypted cloud storage," *in Proceedings IEEE INFOCOM, Turin*, 2013.

[18] K. Yang, Z. Liu, X. Jia and X. S. Shen, "Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach," *IEEE Transactions on Multimedia*, vol. 18, no. 5, pp. 940 - 950, 2016.

[19] Y. Zhu, D. Huang, C.-J. Hu and X. Wang, "From RBAC to ABAC: Constructing Flexible Data Access Control for Cloud Storage Services," *IEEE*, vol. 8, no. 4, pp. 601 - 616, 2015.

[20] M. Abdlhamed, K. Kifayat, Q. Shi and W. Hurst, "Intrusion prediction systems," *in Springer, New York*, 2-017.

[21] D. Ding, Q.-L. Han, Z. Wang and X. Ge, "A Survey on Model-Based Distributed Control and Filtering for Industrial Cyber-Physical Systems," *IEEE*, vol. 15, no. 5, pp. 2483 - 2499, 2019.

[22] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "*IEEE Internet of Things Journal*," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125 - 1142, 2017.

[23] H. Lin, Z. Yan, Y. Chen and L. Zhang, "A Survey on Network Security-Related Data Collection Technologies," *IEEE* , vol. 6, pp. 18345 - 18365, 2018.

[24] P. Nespoli, D. Papamartzivanos, F. G. Mármol and G. Kambourakis, "Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks," *IEEE Communications Surveys & Tutorials* , vol. 20, no. 2, pp. 1361 - 1396, 2018.

[25] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandra and S. Venkatraman, "Robust Intelligent Malware Detection Using Deep Learning," *IEEE* , vol. 7, pp. 46717 - 46738, 2019.

[26] F. Ahmad, V. N. L. Franqueira and A. Adnane, "TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks," *IEEE* , vol. 6, pp. 28643 - 28660, 2018.

[27] K. Huang, C. Zhou, Y.-C. Tian, S. Yang and Y. Qin, "Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems," *IEEE*, vol. 65, no. 10, pp. 8153 - 8162, 2018.

[28] I. Indu, P. R. Anand and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. Pages 574-588, 2018.

[29] B. Lang, J. Wang and Y. Liu, "Achieving flexible and self-contained data protection in cloud computing," *IEEE*, vol. 5, pp. 1510 - 1523, 2017.

[30] R. LI, C. Shen, H. He, X. Gu, Z. Xu and C.-Z. Xu, "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing," *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 344 - 357, 2018.

[31] L. Lynch, "Inside the identity management game," *IEEE Internet Computing*, vol. 15, pp. 78-82, 2011.

[32] S. Sciancalepore, G. Piro, D. Caldarola, G. Boggia and G. Bianchi, "On the design of a decentralized and multi-authority access control scheme in federated and cloud-assisted Cyber-Physical Systems," *IEEE Internet of Things Journal* , vol. 5, no. 6, pp. 5190 - 5204, 2018.

[33] M. Shehab and S. Marouf, "Recommendation models for open authorization. IEEE Trans. Dependable Secure Comput," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 583 - 596, 2012.

[34] A. Vapen, N. Carlsson, A. Mahanti and N. Shahmehri, "A look at the third-party identity management landscape," *IEEE Internet Computing*, vol. 20, no. 2, pp. 18-25, 2016.

[35] J. Wei, W. Liu and X. Hu, "Secure and efficient attribute-based access control for multiauthority cloud storage," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1731 - 1742, 2018.

[36] K. Xue, W. Chen, W. Li, J. Hong and P. Hong, "Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Trans. Inf. Forensics Secur," *IEEE Transactions on Information Forensics and Security* , vol. 13, no. 8, pp. 2062 - 2074, 2018.

[37] A. Alomari, S. K. Subramaniam, N. Samian, R. Latip and Z. Zukarnain, "Resource Management in SDN-Based Cloud and SDN-Based Fog Computing: Taxonomy Study," *symmetry*, vol. 13, no. 5, pp. 1-30, 2021.

[38] J. Son, A. V. Dastjerdi, N. R. Calheiros, X. Xiaohui Ji, Y. Yoon and R. Buyya, "CloudSimSDN: Modeling and Simulation of Software-Defined Cloud Data Centers," *in IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Shenzhen*, 2015.

[39] M. Repetto, A. Carrega and R. Rapuzzi, "An architecture to manage security operations for digital service chains," *Future Generation Computer Systems*, vol. 115, pp. 251-266, 2021.

[40] A. A. Khan, M. Khan and W. Ahmed, "Improved scheduling of virtual machines on cloud with multitenancy and resource heterogeneity," *International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, pp. 815–819, 2016.

[41] "Network functions virtualisation (nfv) “terminology for main concepts in nfv'," *ETSI GS NFV 003 V1.4.1, france*, 2018.

[42] M. Repetto, D. Striccoli, G. Piro, A. Carrega, G. Boggia and R. Bolla, "An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains," *Journal of Network and Systems Management*, vol. 29, no. 2, pp. 29-37, 2021.

[43] N. Bouten, R. Mijumbi, J. Serrat, J. Famaey, S. Latré and F. D. Turck, "Semantically Enhanced Mapping Algorithm for Affinity-Constrained Service Function Chain Requests," *IEEE*, vol. 14, no. 2, pp. 317 - 331, 2017.

[44] M. Ghazna, N. Shahriar, S. Kamali, R. Ahmed and R. Boutaba, "Distributed Service Function Chaining," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 35, no. 11, pp. 2479 - 2489, 2017.

[45] "Network Functions Virtualisation (NFV); Management and Orchestration," *ETSI GS NFV-MAN 001 V1.1.1, france*, 2014.

[46] M. Alenezi, K. Almustafa and K. A. Meerja, "Cloud based SDN and NFV architectures for IoT infrastructure," *Egyptian Informatics Journal*, vol. 20, no. 1, pp. 1-10, 2018.

[47] ISO/IEC, "Information technology — Security techniques — Guidelines for cybersecurity," *ISO/IEC 27032, Geneva*, 2012.

[48] H. Hasrouny, A. E. Samhat, C. Bassil and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7-20, 2017.

[49] ENISA, "National Cyber Security Strategy; Canada’s Vision for Security and Prosperity in the Digital Age," *European Union Agency for Cybersecurity, NENISA, Psychicko*, 2018.

[50] R. v. Solms and B. V. Solms, "Cyber Security and Information Security – What goes where?," *emerald insight*, vol. 26, no. 1, pp. 2–9, 2018.

[51] ITU-T, "Series X: Data Networks, Open System Communications and Security, X.1205," *ITU-T*, 2008.

[52] A. Bahuguna, R. K. Bisht and J. Pande, "Roadmap Amid Chaos: Cyber Security Management for Organisations," *in International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru*, 2018.

[53] G. Disterer, "ISO/IEC 27000, 27001 and 27002 for Information Security Management," *Journal of Information Security*, vol. 4, no. 2, pp. 92-100, 2013.

[54] H. Edward, "Information Security Management System Standards," *Datenschutz und Datensicherheit*, vol. 35, no. 1, pp. 7–11, 2011.

[55] ISO/IEC, "International standard ISO/IEC Information technology—Security techniques—Information security management systems—Requirements"," *ISO/IEC. 27001*, 2013.

[56] ISO/IEC, "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services," *ISO/IEC 27017*, 2015.

[57] ISO/IEC, "Information technology — Security techniques — Information security management systems — Overview and vocabulary," *ISO/IEC 27000*, 2018.

[58] ISO/IEC, "Information technology — Security techniques — Code of practice for information security controls," *ISO/IEC 27002*, 2013.

[59] "Framework for Improving Critical Infrastructure Cybersecurity," *National Institute of Standards and Technology*, 2014.

[60] R. Kissel, "Glossary of Key Information Security Terms," *NISTIR 7298*, 2019.

[61] B. Krumay, E. W. N. Bernroider and R. Walser, "Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework," *Secure IT Systems*, vol. 11252, pp. 369–384, 2018.

[62] N. I. o. S. a. Technology, "Framework for Improving Critical Infrastructure Cybersecurity,Version 1.1," *National Institute of Standards and Technology*, 2018.

[63] U. M. Mbanaso, L. Abrahams and O. Z. Apene, "Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework," *The African Journal of Information and Communication*, vol. 23, pp. 1–26, 2019.

[64] V. Chang, Y.-H. Kuo and M. Ramachandran, "Cloud Computing Adoption Framework – a security framework for business clouds," *Future Generation Computer Systems*, vol. 57, pp. 24-41, 2016.

[65] V. Chang, M. Ramachandran, Y. Yao, Y.-H. Kuo and C.-S. Li, "A Resiliency Framework for an Enterprise Cloud," *International Journal of Information Management*, vol. 36, no. 1, pp. 155 - 166, 2016.

[66] R. Wendler, "The maturity of maturity model research: A systematic mapping study,*" Information and Software Technology*, vol. 54, no. 12, pp. 1317-1339, 2012.

[67] S. Almuhammadi and M. Alsaleh, "Information Security Maturitymodel for NIST Cyber SECURITYFRAMEWORK," *Comput Sci Inform Technol*, vol. 51, pp. 51–62, 2017.

[68] N. T. le and D. B. Hoang, "Capability Maturity Model and Metrics Framework for Cyber Cloud Security," *Scalable Computing*, vol. 18, no. 4, pp. 277–290, 2017.

[69] M. Abdel-Basset, M. Mohamed and V. Chang, "NMCDA: a framework for evaluating cloud computing services," *Future Generation Computer Systems*, vol. 86, pp. 12-29, 2018.

[70] N. Tissir, S. E. Kafhali and N. Aboutabit , "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal," *Journal of Reliable Intelligent Environments*, vol. 7, pp. 69–84, 2021.

[71] A. Mohamed, K. Kashif, S. Qi and H. William, "Intrusion prediction systems," *in Intrusion prediction systems, New York, Springer*, 2017, pp. 155 - 174.

[72] F. Ahmad, V. N. L. Franqueira and A. Adnane, "TEAM: a trust evaluation and management framework in context-enabled vehicular ad-hoc networks," *IEEE Access*, vol. 6, pp. 28643–28660, 2018.

[73] D. Ding, Q.-L. Han, Z. Wang, Z. Wang and X. Ge, "A Survey on Model-based Distributed Control and Filtering for Industrial Cyber-Physical Systems," *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, vol. 15, no. 5, pp. 2483–2499, 2019.

[74] K. Huang, C. Zhou, Y.-C. Tian, S. Yang and Y. Qin, "Assessing the Physical Impact of Cyber-Attacks on Industrial Cyber-Physical Systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 8153-8162, 2018.

[75] H. M. Al-Mashhadi and A. A. Khalf, "Hybrid Homomorphic Cryptosystem for Secure Transfer of Color Image on Public Cloud," *IJCSNS International Journal of Computer Science and Network Security*, vol. 18, no. 3, pp. 2018, 2018.

[76] H. M. Al-Mashhadi and M. . H. Alabiech, "Symmetric ECC with Variable Key using Chaotic Map," *International Journal of Computer Science Issues*, vol. 14, no. 6, pp. 24-28, 2017.

[77] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[78] H. Lin, Z. Yan, S. Member, Yu Chen and L. Zhang, "A Survey on Network Security-Related Data Collection Technologies," *IEEE*, vol. 6, pp. 18345 - 18365, 2018.

[79] P. Nespoli, D. Papamartzivanos, F. G. Mármol and G. Kambourakis, "Optimal Countermeasures Selection Against Cyber Attacks: A Comprehensive Survey on Reaction Frameworks," *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, vol. 20, no. 2, pp. 1361-1396, 2018.

[80] V. R, M. Alazab, S. KP, P. Poornachandran, A. AL-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent," *IEEE Access*, vol. 7, pp. 1-27, 2019.

[81] V. R, M. Alazab, S. KP, P. Poornachandran and S. Venkatraman, "Robust intelligent malware detection using deep learning," *IEEE Access*, vol. 7, pp. 46717–46738, 2019.