DOI 10.12694/scpe.v18i4.1329
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 18, Number 4, pp. 277–290. http://www.scpe.org © 2017 SCPE

CAPABILITY MATURITY MODEL AND METRICS FRAMEWORK FOR CYBER CLOUD SECURITY

NGOC T. LE, DOAN B. HOANG*

Abstract. Cyber space is affecting all areas of our life. Cloud computing is the cutting-edge technology of this cyber space and has established itself as one of the most important resources sharing technologies for future on-demand services and infrastructures that support Internet of Things (IOTs), big data platforms and software-defined systems/services. More than ever, security is vital for cloud environment. There exist several cloud security models and standards dealing with emerging cloud security threats. However, these models are mostly reactive rather than proactive and they do not provide adequate measures to assess the overall security status of a cloud system. Out of existing models, capability maturity models, which have been used by many organizations, offer a realistic approach to address these problems using management by security domains and security assessment on maturity levels. The aim of the paper is twofold: first, it provides a review of capability maturity models and security metrics; second, it proposes a cloud security capability maturity model (CSCMM) that extends existing cyber security models with a security metric framework.

Key words: Cyber security; Cloud security model; Capability Maturity Model; Security Maturity Model; Security metrics framework.

AMS subject classifications. 68M14, 68N30

1. Introduction. In order to protect a cloud cyber space from numerous security threats, many security models and standards have been developed. Each model focuses on a particular security angle such as risk, asset, identification, physical components, network, data, and application. Few security models consider the security of a system as a whole. It is known that a single minor vulnerability can bring down the whole system and there are myriads of these vulnerabilities. Moreover, these models are inadequate because their security assessment processes are mainly about compliances and they lack meaningful and relevant quantitative security metrics.

In recent years, several security maturity models have been proposed for overall security management. These draw on the theoretical framework of the capability maturity model. In 1989, Humphrey recommended a capability maturity model for software quality assessing [1]. This basic model has been adapted for cyber security for a number of reasons. First, security models based on capability maturity model have been applied with reasonable successes for many fields such as IT, business. Second, maturity models provide a complete management process for cyber security. Third, they can be extended to cover many security aspects or domains. Recently, maturity models have been applied in securing many important traditional cyber spaces such as e-government, e-commerce, education, health, particular in critical national infrastructures such as electricity, water supply, petrol, and transportation [2]. However, few focus on cloud computing security.

Despite having the abovementioned benefits, maturity models have revealed many drawbacks. One of which is that when organizations use maturity models, they look at each maturity level as a target and build their goal to reach the next level up. The problem is that a maturity level is often determined arbitrarily and subjectively. Another issue is that security metrics mainly depend on qualitative measurements, suitable for checking compliance rather than inspiring security action.

To overcome the weaknesses and to take advantages of maturity models, we propose a capability maturity based model for cloud security, the Cloud Security Capability Maturity Model (CSCMM) with a new metrics framework that allows not only managers to assess the security state of the cloud system for decision making process but also security practitioners to identify security gaps and to implement security responses systematically and quantitatively.

The paper has several contributions:

- The paper provides a discussion on cyber security models and standards, capability maturity models, and the need for quantitative security metrics in modelling cyber security holistically to enable the

*Virtual Infrastructure and Cyber Security lab (VICS), Faculty of Engineering and IT, University of Technology Sydney (NgocThuy.Le@student.uts.edu.au, Doan.Hoang@uts.edu.au). Questions, comments, or corrections to this document may be directed to those email address.

assessment of the overall security of a complex entity.

- The paper proposes Cloud Security Capability Maturity Model (CSCMM) that embraces new cloud security domains and renders a quantitative assessment of the overall security with the system of security maturity levels. By doing so, we expand, enrich the capability maturity model theory and apply it to cloud security.
- The paper introduces a security metric framework that underpins the assessment of security maturity level. This framework supports the roadmap to create new security quantitative metrics based on the requirements of cloud stakeholders. Furthermore, it integrates previous qualitative security metrics to assess maturity level of the cloud system.

The remainder of this paper is organized as follows. Section 2 revises knowledge about cyber security, cloud security models, cyber security maturity models, and security metrics. Section 3 proposes CSCMM including its structure and implementation process. Section 4 introduces the security metrics framework that is developed to support the CSCMM model. Section 5 discusses the importance of the quantitative security metrics in security assessment process of the CSCMM model and discusses several advanced security metrics that can be applied for the model. Section 6 concludes the paper with future research.

2. Review of cyber space and security, cloud security models, security maturity models, and security metrics.

2.1. Cyber space and cyber security. The definition of cyber space has changed considerably since Wiener defined cybernetics in 1948 as control and communication in the animal and the machine [3]. Over the last few decades, academic organizations focused on the tangible elements in the cyber space when they paid more attention to the infrastructure components of IT systems, and on intangible elements such as the data or the applications within these systems. Recently, the cyber space has grown to include social networks, clouds, Internet of Things (IOTs), smart cities, smart grids, and other software-defined systems [4]. In order to provide a common understanding of the space and its security, we suggest a unified definition of the cyber space as the space that embraces all three key elements: real and virtual entities, interconnecting infrastructure, and interaction among entities. Interaction as it is fundamental to security; without interaction among entities, including human beings, the question on security may not make sense.

The definition of cyber security has evolved greatly over the past decades. The fundamental concept of security is defined as the quality or state of being secure - being free from danger [5]. Similarly, cyber security can be thought of as a system of processes that protect the resources of a cyber space. However, definitions of cyber security vary with different organizations, some using the term cyber security but others using the terms information security or IT security [6]. We highlight several definitions of cyber security for discussion and clarification. According to Gasser and Morrie [7], computer security, also known as cyber security or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. International Telecommunication Union (ITU) [8] defines cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users assets. From these definitions, it is apparent that information security emphasizes the confidentiality, integrity and availability of information whereas computer security focuses on the availability, integrity, and correct operation of systems. Furthermore, cyber space is expanding to include virtualized infrastructures, service networks, social networks, and internet of things, hence a more embracing definition is needed: cyber security can be considered as a collection of systems, tools, processes, practices, concepts and strategies that are used to prevent and protect the cyber space from unintended interaction and unauthorized access and to preserve the confidentiality, integrity, availability, authenticity, accountability (CIAAA) and other properties of the space and its resources.

This definition clarifies the scope of cyber security in three aspects. Firstly, the term cyber security is used to focus attention on security of the cyber space rather than the security in a narrower sense. Secondly, prevention, not just protection is an integral part of the definition. It makes sense to look at security in a wider context where prevention and protection are interrelated. Preventing some vulnerability from being exploited can be considered as protecting the space and on the other hand, knowing how to protect the cyber space implies to some extent the knowledge of how security breaches occur and how they can be prevented. Thirdly, with rapid emergence of many modern technologies, such as virtualized infrastructures (cloud, software defined networks, network functions virtualization), internet of things, social networks, service networks and other new and emerging technologies, additional considerations, including adaptability, resiliency or safety should be included in the definition.

2.2. Cloud security models and standards. Cloud is a particular cyber space. Based on virtualization and shared IT resources, cloud computing is seen as a technological evolution of cyber space. It plays an important role in the world IT development and it will continue to evolve extensively over the next decades [9]. However, clouds, as cyber infrastructures, with three service models (IaaS, PaaS, and SaaS), four deployment cloud types (Private, Public, Hybrid, and Community) are facing challenging security issues.

Identified cloud security aspects include governance and compliance, virtualization, identity management [10][11][12], and various threats aspects [13][14]. Cloud Security Alliance (CSA) published the security report namely 'The Treacherous Twelve Cloud Computing Top Threats in 2016' providing organizations with the awareness of cloud security issues in making educated risk-management decisions [15].

To combat cloud security problems, researchers, businesses, and organizations have been making efforts to mitigate cloud security risk and tackle security threats by development cloud security standards and models. In 2014, the European Union Agency for Network and Information Security (ENISA) [16] released the report Cloud standards and security to provide an overview of standards relevant for cloud computing security. CSA introduced and developed security guidance for critical areas of focus in cloud computing through 3 versions including Version 1.0 [17], Version 2.1 [18] (2009), and Version 3.0 [19] (2011). The latest version (Version 3.0) was tailored for meeting the security demand changes. The aim of this guidance was to introduce better standards for organizations to manage cyber security for cloud by implementation security domains. The guidance approached cloud architecture with cloud service model (SaaS, PaaS, and IaaS) and four deployment models (Public, Private, Community, and Hybrid Cloud) with derivative variations that address specific requirements. The guidance focuses on thirteen different domains which are divided into two general categories: governance and operations. The governance domains focus on broad and strategic issues as well as policies within a cloud computing environment, while the operational domains focus on more tactical security concerns and implementation within the architecture.

This guidance is relevant to cloud computing, its service models and its deployment models. Regarding cloud security management, the guidance focuses on cloud-specific issues: interoperability and portability, data security, and virtualization. Dividing the implementation domains into two groups with strategic and tactical categories is another salient point of the guidance. This approach allows cloud consumers and providers to bring financial and human resources into security consideration. Furthermore, the guidance can be mapped to existing security models such as Cloud Control Matrix [20]. Despite these benefits, however, the guidance has a number of drawbacks. The guidance lacks assessment guide for each domain. It does not consider security metrics for security practices. Therefore, organizations find it difficult to determine the security level of a domain.

In addition, there are many standards concerning cloud security. The ISO/IEC (A joint technical committee of the International Organization for Standardization - ISO and the International Electrotechnical Commission - IEC) 27017 Standard illustrates the information security elements of cloud computing. It assists with the implementation of cloud-specific information security controls, supplementing the guidance in ISO 27000 series standards, including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management. The National Institute of Standards and Technology NIST released the following standards on cloud computing: NIST SP 500-291, Cloud Computing Standards Roadmap, NIST SP 800-146, Cloud Computing Synopsis and Recommendations, NIST SP 800-144, Guidelines on Security & Privacy in Public Cloud Computing, NIST SP 500-292, Cloud Computing Reference Architecture and NIST SP 500-293, US Cloud Computing Technology Roadmap.

2.3. Cyber Security Maturity Model. A fundamental question that has to be asked concerning a cyber space or a system is whether the cyber space or the system is secure or at least to what level it is secure. For example, is a cyber space secure when a huge number of bugs, viruses, spams and malwares have been found and fixed? Or is a cyber space secure when substantial investment in a firewall system and an IDPS (intrusion detection and prevention system) has been made? It is difficult to claim that a cyber space is safe and secure based on the numbers of vulnerabilities found and fixed as there may be a number of bugs still undetected.

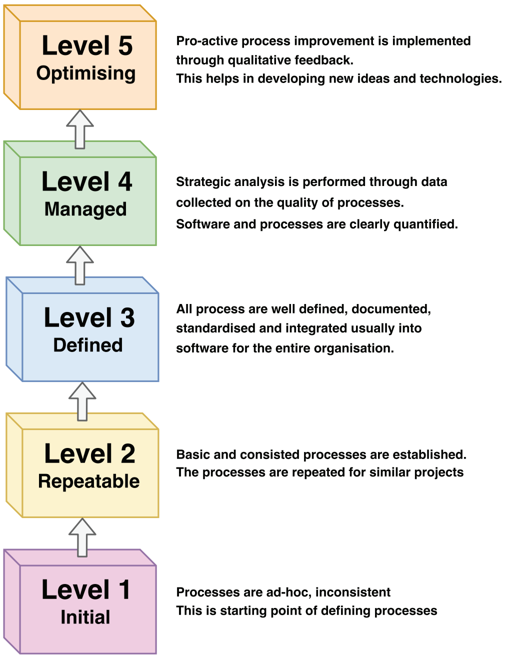

Level 5
Optimising
Pro-active process improvement is implemented through qualitative feedback.
This helps in developing new ideas and technologies.
Level 4
Managed
Strategic analysis is performed through data collected on the quality of processes.
Software and processes are clearly quantified.
Level 3
Defined
All process are well defined, documented, standardised and integrated usually into software for the entire organisation.
Level 2
Repeatable
Basic and consisted processes are established.
The processes are repeated for similar projects
Level 1
Initial
Processes are ad-hoc, inconsistent
This is starting point of defining processes

FIG. 2.1. *Capabilities maturity model process levels*

This implies that vulnerability is only one of the many aspects of security. Yet, many of the current security models deal with security problems in an ad hoc manner; a specific security measure is put into action simply to treat the issue at hand without regard to or understanding its impact on the whole cyber space. These models handle security from a bottom-up perspective and are case specific. They provide no assurance of the overall level of security of the protected entity.

What is needed is to view and study cyber security holistically from a top-down perspective to produce a security model that allows us to make an assessment of the overall security level of the entity requiring protection. Furthermore, the model should allow us to identify the entity's weaknesses and the appropriate measures to deal with them. Measures may include an investment in resources, and the enforcement of practices. Among those proposed models, the cyber-security maturity model provides organizations to some extent a roadmap for measuring, assessing, and enhancing cyber security. Relative to other models, it provides managers with sound footing for making an informed security assessment of their organization.

As mentioned above, Maturity Models are based on the Capability Maturity Model (CMM). Humphrey [1] recommended the CMM to assess quality of software and to help software organizations improve the maturity of their software processes by evolving from ad hoc, chaotic processes to mature, disciplined software processes. The fundamental ideas of CMM are as follows: (1) the model is divided into 5 levels from initial to optimizing level, from simple to complex, from low to high requirement; (2) each level has a set of maturity requirements. It means that to achieve a specific maturity level, the standard requirements of quality and technology need to be implemented by specified sets of practices; (3) to reach a higher maturity level, the software must satisfy all lower levels (Figure 2.1). Eventually, maturity models show the level of perfection or completeness of certain capabilities. They define maturity levels which measure the completeness of the analyzed objects via different sets of (multi-dimensional) criteria.

The structure of the cyber security maturity model can be described in terms of its functions, key components, and types of maturity model [21]. There are three main functions of a maturity model: a means of assessing and benchmarking performance; a roadmap for model-based improvement; and a means to identify gaps and develop improvement plans. The key components include: maturity levels which are the security measurement scales or transitional states, security domains which are logical groups of practices and processes, attributes which are core contents of the model arranged by domains and levels, diagnostic methods for assessment, measurement, gap identification, benchmarking, and improvement roadmaps to guide improvement efforts such as Plan-Do-Check-Act or Observe-Orient-Decide-Act. The three types of maturity models are progression, capability, and hybrid. While the progression model describes levels as higher states of achievement similar to the progression of human mobility being from crawl, walk, jog to run, the capability model shows levels as the extent to which a particular set of practices has been institutionalized. The hybrid model is the combination of the best features of progression and capability maturity models where maturity levels express both achievement and capability. Most recent cyber security maturity models are hybrid models which describe maturity security levels over distinguished domains of a system (such as a cloud) in an integrated framework.

In our previous paper [22], we compared twelve security maturity models in order to investigate their strengths and weaknesses. It was demonstrated that cyber security maturity models help managers to manage more effectively the security of their organizations [23][24]. They allow better security risk management, produce cost saving, promotes self-improvement, and support good security procedures and processes. More importantly, they encourage all stakeholders to take steps along a secure mature path as mapped out by the maturity model, rather than activate security controls blindly without regard to the security of the overall organization. Despite all these benefits, maturity models only provide a bare minimum compliance model rather than an aspired cyber security model that can deal with emerging cyber environment, its demanding usage, as well as its sophisticated attacks. Therefore, three specific issues from security maturity models should be addressed. First, identifying the maturity levels of cyber security of each domain is arbitrary and subjective as a result of checking for compliances; a security model should be more than compliance. Second, most cyber security maturity models draw on international cyber security standards such as ISO27000 series or NIST. Security practices in these standards are mainly measured by qualitative metrics/processes; quantitative metrics should be essential for any security assessment. Third, the model should be flexible for addressing specific dimension of a cyber space or extensible for dealing with emerging cyber spaces.

2.4. Cyber security metrics.

Metrics and measures. To assess the level of a security state, metrics or measurements have been used. The usage these two terms, however, has different meanings and implications. Metrics imply tools to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. A measure is a concrete, objective attribute, such as the percentage of systems within an organization that are fully patched, the length of time between the release of a patch and its installation on a system, or the level of access to a system that a vulnerability in the system could provide. Measures are quantifiable, observable, and objective data supporting metrics [25]. According to the Information Assurance Technology Analysis Center (IATAC), a measurement is the act or the process of measuring, where the value of a quantitative variable in comparison to a (standard) unit of measurement is determined. A measure is a variable to which a value is assigned as a result of the measurement. A metric is a system of related measuring enabling quantification of some characteristic of a system, component or process. A metric is composed of two or more measures [26].

Importance of security metrics. Lord Kelvin [27] stated that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind. Therefore, metrics are needed to assess the security of the cyber space. In terms of software quality assessment, Humphrey [28] insisted that quality management is impossible without quality measures and quality data. As long as software people try to improve quality without measuring and managing quality, they will make little or no progress. Trapero et al. [29] indicated the importance of quantitative security metrics.

However, it is difficult to measure the cyber security state for 3 reasons: vulnerabilities are hard to measure by anyone, even the owner of the system; the set of weakness (vulnerabilities) known to the observer is not known by the owner of the system and thus is not measured by the owner; no system owner can know the totality of his adversaries. Despite having several difficulties in security measuring, cyber security metrics can support organizations in (1) verifying that their security controls are in compliance with a policy, process, or procedure, (2) identifying their security strengths and weaknesses; and (3) identifying security trends, both within and outside the organizations control [30].

Security metrics categories. Security metrics can be categorized by what and how they are measured. What are measured may include process, performance, outcomes, quality, trends, conformance to standard, and probabilities. How these things are measured may be categorized by the methods such as: maturity; multidimensional scorecards; value; benchmarking; modeling; and statistical analysis [31]. In terms of management/organizational perspective, there are several security metric categorizations. In [32], the Center for Internet Security (CIS) divided security metrics into three groups which are Management, Operations, or both. Chew et al. [33] grouped security metrics by Implementation, Effectiveness and Efficiency, and Business Impact. Savola [34] differentiated metrics into Management, Operational, and Technical. These categorizations may overlap as well as interrelate. However, these taxonomies tend to simplify complex socio-technical or practice-theory relationships [35].

Security metrics requirement. In a metrics system, several requirements of a good security metric are considered carefully and have been proposed by organizations and researchers. Jaquith [30] asserts that security metrics requirements should include consistently measured, cheap to gather, expressed as a cardinal number or percentage and using at least one unit of measure, and contextually specific. According to Wesner [36], security metrics should be SMART (Specific, Measurable, Actionable, Relevant, and Timely). Brotby [37] proposes PRAGMATIC (Predictive, Relevant, Actionable, Genuine, Meaningful, Accurate, Timely, Independent, Cheap). Herrmann [38] considers that a good security metric is one that possesses Accurate, Precise, Valid, and Correct characteristics.

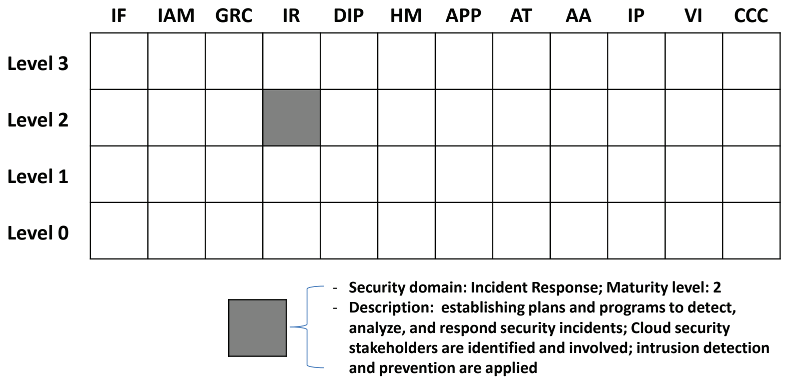
Security metrics program. Once the security metrics have been decided by an organization for its system, a security metrics program has to be established to provide the organization with a map to manage, control, or improve the system security domains [39]. Several methods to build up a security metrics program are deployed. First, Payne [40] proposed Seven Steps model to establish security metrics including: defining the metrics program goal(s) and objectives; deciding metrics to generate; developing strategies for generating the metrics; establishing benchmarks and targets; determining metrics are reported; creating an action plan and act on it; and establishing a formal program review/refinement cycle. NIST also considered the metrics development and selection cycle via seven steps from identify stakeholders and interest to business mission impact [41].

Chew et al. [33] proposed five key components of making a metrics program plan: program initiation; development of information security metrics; analysis of information security metrics; reporting information security metrics; maintaining an information security metrics program. Campbell and Blades [42] listed five steps in a security metrics program: identifying the business drivers and objectives for the security metrics program; determining who your metrics are intended to inform and influence; identifying the types and locations of data essential for actionable security metrics; establishing relevant metrics; and establishing internal controls to ensure integrity of data and data assessments and to protect confidentiality.

3. Cloud security capability maturity model (CSCMM). To solve all above problems from cloud models and cyber security maturity models, we developed a Cloud Security Capability Maturity Mode (CSCMM) with two dimensions including domain and maturity level (Figure 3.1). The first dimension presents twelve cloud security domains. Each domain is a set of cyber security practices. The practices within each domain are the achievement objectives specific for cloud security domain. The second dimension shows four maturity levels which apply seperately to each domain. The maturity levels indicate a progression of maturity.

The model is built from a combination of existing cyber security standards, frameworks, and innovation. It provides the guidance to support the organizations implement and enhance their cyber security capabilities on cloud system. The model can be tailored for appropriate goals of different cloud service model (IPSaaS) and deployments (Public, Private, and Hybrid Cloud).

3.1. CSCMM domains. There is not a complete cloud security standard because cloud technology is evolving much faster than standards [43]. Therefore, creating a set of security domains just based on the current security standards is not adequate to take into account emerging issues and attack surfaces. For CSCMM, we choose a systematic review approach on existing cloud security models and standards, traditional security maturity models as well as trends in emerging technologies. Systematic review methodology is a means of evaluating and interpreting available research relevant to a particular research question, topic area, or phenomenon of interest [44]. As a result, we investigated fourteen security models including five traditional and nine cloud security models. We found twelve in twenty one security domains with the highest number of appearances in fourteen models (Figure 3.2). In which, eight security domains are from traditional maturity models and



- Security domain: Incident Response; Maturity level: 2
- Description: establishing plans and programs to detect, analyze, and respond security incidents; Cloud security stakeholders are identified and involved; intrusion detection and prevention are applied

Fig. 3.1. *CSCMM Model Architecture*

standards including infrastructure and facilities security; identity and access management; governance, risk, and compliance; incident response and threat management; data and information protection; human resources management; security awareness and training; audit and accountability. There are four cloud specific security domains such as cloud connections and communication; operabability and portability; virtualization; and application secuirty. Based on different perspective of security domains categories from ISO (strategic, tactical, and operational), CSA (governance, operational), IBM (Process, Technical, and Operational), and Karola (Technical, Social), we settle for these twelve security domains as they cover comprehensive aspects of cyber security and accommodate emerging security issues.

The main contents of these 12 domains are summarized below:

1. Infrastructure and facilities security (IF): The security of an IT system also depends on the security of its physical infrastructure and facilities. In the case of cloud computing, this extends to the infrastructure and facilities of the cloud service provider. The customer must get assurance from the provider that appropriate security controls are in place. ISO 27007 can be used to ensure protection against external and environmental threats like fire, floods, earthquakes, civil unrest or other potential threats that could disrupt cloud services; control of personnel working in secure areas; equipment security controls; and supporting utilities such as electricity supply, gas supply, telecommunications.

2. Identities and Access Management (IAM): This domain ensures authentication, authorization, and administration of identities. The main concerns of this domain are related to identity verification, granting a correct level of access to cloud resources, policy managements, and role-based access controls. The purpose of IAM is to prevent unauthorized access to physical and virtual resources as this can threaten the confidentiality, availability, integrity, and other properties of users services and data. These domains can be applied by standards or technologies such as LDAP (Lightweight directory Access Protocol) to provide access to directory servers and SAML 2.0 (Security Authorization Mark-up Language) for exchange of authentication and authorization data between security domains.

3. Governance, Risk, and Compliance management (GRC): This domain focuses on establishing, operating, and maintaining cyber security risk management programs that identify, analyse, and mitigate cyber security risk to the organization. This means governance and compliance policies and procedures are established to protect stakeholders property. This covers implementations of compliance following regulatory requirements between stakeholders. Compliance management is to maintain and provide compliance. It relates to execution of internal security policies, and different compliance requirements such as regulatory, legislative.

4. Incident response (IR): This domain concentrates on incident detection, response, notification, and remediation. The major concerns in incident response are related to establishing and maintaining plans, procedures, and technologies to detect, analyse, and respond to cyber security incidents and events. The incident response lifecycle as expressed in the National Institute of Standards and Technology Computer Security Incident Handling Guide (NIST 800-61) should be used in this domain.

5. Data and Information protection (DIP): Data protection is one of the critical security challenges in cloud

computing. Control of data and compensating controls can be used to tackle the loss of physical control when moving data to the cloud. The concern of information management is who has onus for data confidentiality, integrity, and availability. Therefore, security controls as expressed in ISO 27002 including asset management, access control and cryptography can be applied. Other technologies such as HTTPS for regular connections from cloud services over the internet, VPN using IPSec or SSL for connections also can be used for implementing this domain. Moreover, encryption keys should be used by KMIP (the Key Management Interoperability Protocol) that supports a standardized way to manage encryption keys.

6. Human resource management (HM): People are often described as the weakest entity in any security system. This domain focuses on human resource process, from pre-employment, during employment, and through termination, to ensure that policies and procedures are in place to address security issues. The three areas of human resources security concerned are prior to employment; during employment; termination and change of employment. Human Resources Security in ISO 27002:2013 (Information Security Management) can be used for this domain.

7. Cloud application security (APP): This domain focuses on determining the application software on which type of cloud platform (SaaS, PaaS, or IaaS) for securing. The Open Web Application Security Project (OWASP) or Secure Software Development Life Cycle (SSDLC) can support cloud service entities to secure application running on cloud systems. In terms of technologies and techniques in cloud application security, firewall can be used to control access. VPNs can be considered to limit access to application to users for these domains.

8. Security awareness and training (AT): This domain aims to create a culture of security and ensure the ongoing suitability and competence of all personnel. Consistent training throughout the entire process ensures that employees and contractors are fully aware of their roles and responsibilities and understand the criticality of their actions in protecting and securing both information and facilities.

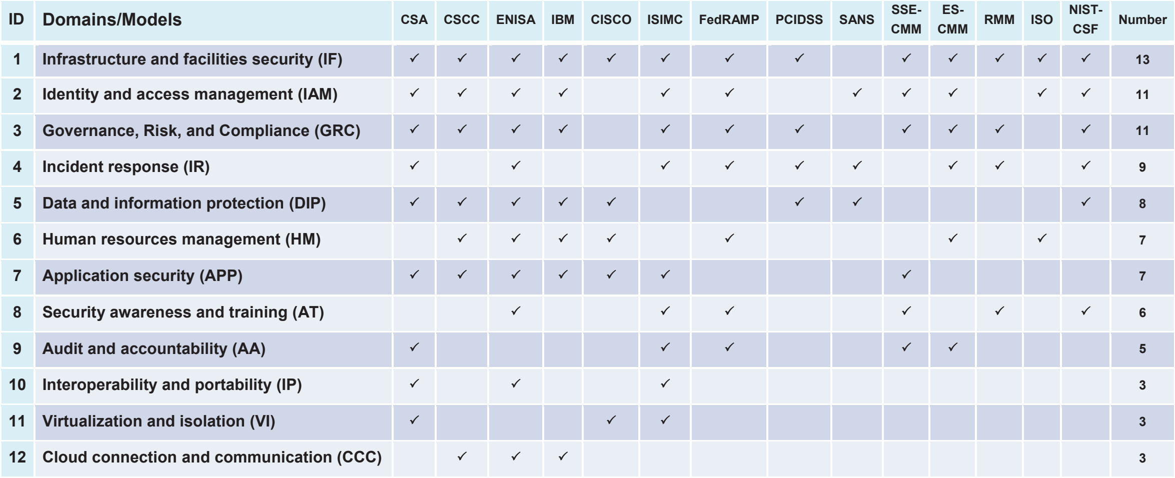
9. Audit and Accountability (AA): This domain aims to provide information about roles, responsibilities, and compliance regarding auditing. It addresses auditing of security controls including checking for proper server maintenance and controls to make sure that it is properly done and security policies are being enforced. The policy may set the level and detail of auditing and specify types of events to be audited. The major procedures of this domain are auditable events; content of audit records, audit processing and monitoring; audit reduction and report generation; protection of audit information; and audit retention.

10. Interoperability and portability (IP): This domain is one of the special domains in cloud computing. It is the ability to move data/services from one provider to another, or bring it entirely back in-house. To ensure this domain, we can use open virtualization formats to provide interoperability, while virtualization can help to remove concerns about physical hardware, distinct differences exist between common hypervisors. It deals with different technologies virtual machine images are captured and ported to new cloud providers such as Distributed Management Task Force (DMTF) and Open Virtualization format (OVF).

11. Virtualization and isolation (VI): This domain focuses on the security issues related to system/hardware virtualization, rather than a more general survey of all forms of virtualization. This domain is associated with multi-tenancy, VM isolation, VM co-resident, hypervisor vulnerabilities, and other virtualized artefacts. Isolation is the technique used to protect each entity within the cloud infrastructure component of a system from unwanted interferences. Isolation is used to identify virtual and physical boundaries, partition containers, processes or logical functional entities, and isolate policy-based security violations.

12. Cloud connection and communication security (CCC): A cloud service provider must allow legitimate network traffic and block malicious network traffic. However, unlike many other organizations, a cloud service provider may not necessarily know what network traffic its customers plan to send and receive. Nevertheless, customers should expect certain external network perimeter safety measures from their cloud providers. For this domain, ISO/IEC 2703332 standards can be used to provide detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002.

In these twelve domains, we integrate isolation aspects into virtualization domain to generate new domain namely virtualization and isolation and introduce domain interoperability portability as a new domain. It is clear that virtualization and isolation have been important techniques in cloud security. Virtualization is considered as the cloud enabling technology and hence it is at the centre of cloud security. However, with emerging attacks



ID	Domains/Models	CSA	CSCC	ENISA	IBM	CISCO	ISIMC	FedRAMP	PCIDSS	SANS	SSE-CMM	ES-CMM	RMM	ISO	NIST-CSF	Number
1	Infrastructure and facilities security (IF)	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	13
2	Identity and access management (IAM)	✓	✓	✓	✓		✓	✓		✓	✓	✓		✓	✓	11
3	Governance, Risk, and Compliance (GRC)	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓	11
4	Incident response (IR)	✓		✓			✓	✓	✓	✓		✓	✓		✓	9
5	Data and information protection (DIP)	✓	✓	✓	✓	✓			✓	✓					✓	8
6	Human resources management (HM)		✓	✓	✓	✓		✓				✓		✓		7
7	Application security (APP)	✓	✓	✓	✓	✓	✓				✓					7
8	Security awareness and training (AT)			✓			✓	✓			✓		✓		✓	6
9	Audit and accountability (AA)	✓					✓	✓			✓	✓				5
10	Interoperability and portability (IP)	✓		✓			✓									3
11	Virtualization and isolation (VI)	✓				✓	✓									3
12	Cloud connection and communication (CCC)		✓	✓	✓											3

FIG. 3.2. *The appearance of security domains in security model*

recently on the virtualization layer, this domain has to be taken seriously. Isolation techniques have emerged as a new approach for securing cloud computing. The development of isolation theory with assessing process is necessary.

3.2. Security maturity levels. To investigate the common features of each maturity level in previous security maturity models, we compared ten prominent professional security maturity models (Figure 3.3). As a result of this investigation, we adopt four maturity levels (SMLs) for our CSCMM model. Maturity levels are identified by the following attributes: (1) the SMLs apply independently to each domain. For instance, an organization could be implementing at SML1 in one domain, SML2 in another domain; (2) the maturity level of a domain is determined by the minimum of all security practices implemented in that domain. For example, to gain security maturity level at SML2 in one domain, the organization has to implement all the security practices in SML1 and SML2; (3) SML achievement should align with business objectives and organizations security strategy.

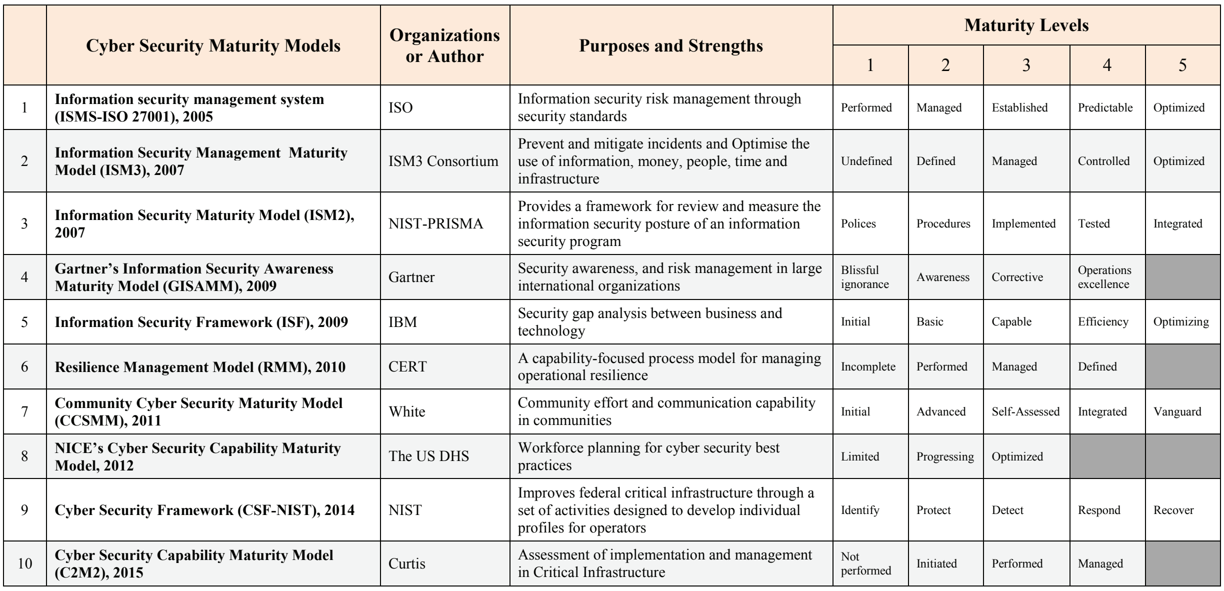
Expressed below are common features that define each maturity level.

- SML0 (Undefined): at this level, organizations are at the starting point with a commitment to establish a security maturity assessment model. They have no plans to check or test security processes.

- SML1 (Initiated): at this level, most organizations focus on basic security practices. Some basic security physical hardware devices or networks need to be implemented on IaaS, basic protection on virtual machine monitor, access control and encryption on PaaS, basic application security and multi-tenancy on SaaS.

- SML2 (Managed): at this level, organizations focus on building and planning Information Security programs and apply cloud security standards. Cloud security stakeholders such as provider, consumer, and third-party are identified and involved. Cloud security activities need to be guided by policies. Some cloud automatic security tools are applied such as intrusion detection and prevention systems. Especially, security metrics system needs to be applied at this level to support security decision making. For IaaS, security mechanisms to protect network and data are applied to achieve selected security standards compliance. For PaaS, it is ensured that the virtual machine monitor needs to be protected by higher security policies. For SaaS, automatic security system for web-based, software, or database need to be implemented.

- SML3 (Optimized): it is defined as the highest maturity level. This is real-time protection level. All the security program support 24/7 staffed operations and fully automated. It is assured that all security policies and procedures are implemented. This is the ideal cloud security status with optimal use of resources from facilities, time to costs and human. This level is called resilience when the organization can detect and tackle with security threats automatically proactively and the time to achieve resilience status is almost zero. All people in the organization have adequate skills and knowledge about security on cloud.



	Cyber Security Maturity Models	Organizations or Author	Purposes and Strengths	Maturity Levels				
				1	2	3	4	5
1	**Information security management system (ISMS-ISO 27001), 2005**	ISO	Information security risk management through security standards	Performed	Managed	Established	Predictable	Optimized
2	**Information Security Management Maturity Model (ISM3), 2007**	ISM3 Consortium	Prevent and mitigate incidents and Optimise the use of information, money, people, time and infrastructure	Undefined	Defined	Managed	Controlled	Optimized
3	**Information Security Maturity Model (ISM2), 2007**	NIST-PRISMA	Provides a framework for review and measure the information security posture of an information security program	Polices	Procedures	Implemented	Tested	Integrated
4	**Gartner's Information Security Awareness Maturity Model (GISAMM), 2009**	Gartner	Security awareness, and risk management in large international organizations	Blissful ignorance	Awareness	Corrective	Operations excellence	
5	**Information Security Framework (ISF), 2009**	IBM	Security gap analysis between business and technology	Initial	Basic	Capable	Efficiency	Optimizing
6	**Resilience Management Model (RMM), 2010**	CERT	A capability-focused process model for managing operational resilience	Incomplete	Performed	Managed	Defined	
7	**Community Cyber Security Maturity Model (CCSMM), 2011**	White	Community effort and communication capability in communities	Initial	Advanced	Self-Assessed	Integrated	Vanguard
8	**NICE's Cyber Security Capability Maturity Model, 2012**	The US DHS	Workforce planning for cyber security best practices	Limited	Progressing	Optimized		
9	**Cyber Security Framework (CSF-NIST), 2014**	NIST	Improves federal critical infrastructure through a set of activities designed to develop individual profiles for operators	Identify	Protect	Detect	Respond	Recover
10	**Cyber Security Capability Maturity Model (C2M2), 2015**	Curtis	Assessment of implementation and management in Critical Infrastructure	Not performed	Initiated	Performed	Managed	

Fig. 3.3. *Discovering Cyber Security Maturity Models*

4. Security metrics framework. To assess the maturity level of CSCMM model in general and a security domain in particular, we propose a security metrics framework with the following steps (Figure 4.1).

Inputs. This first step describes the requirements for the security metrics framework: security practices and activities, goals and objectives, security requirements. A set of security practices for a particular domain or multiple domains is defined and/or selected. This depends on the demand of upper management or the schedule of assessment process of the CSCMM model. These securities then determine what to measure. What-to-measure may be one security activity or several security activities from the selected domains. Stakeholders are identified which include upper managers who decide on information requirements, managers who carry out the directive, practitioners who implement the security metrics, and security metrics consumers. Goals and Objectives define the goals and objectives of security metrics plan or program from the stakeholders viewpoint.

Metric plan. Classification of security activities or practices is also necessary to indicate the type of measurement (governance, management, operational, and technical) and to decide on the metrics plan and the method to measure as security metrics should be SMART [36] or PRAGMATIC [37]. Security metrics components identification identifies the elements or dimensions related to the metrics. These may include real-virtual, infrastructures, and interaction of entities in the (cloud) cyber space, and other factors such as cost, time, threats, and vulnerabilities. Determination of measuring methods is based on the qualitative or quantitative nature of the security practices. Quantitative metrics are usually based on mathematical models and numerical data. The unit of measurement for each component of security metrics program is then derived. Data collection has to be planned to meet the characteristic requirements such as obtainable, cheap to collect, quantitative express, automatically.

Measuring. Relevant and measurable metrics have already determined and selected from previous steps, this step carries out the actual measurement according to the measuring method and the data collection plan. In general, a security metric is a function of its measured components:

$$x = f(x_1, x_2, x_3, \dots, x_n) \tag{4.1}$$

in which, $x_1, x_2, x_3, ..., x_n$ are security metric components and x could be a countable value based on a maturity benchmarking (next step). f is a function of the specification of security metrics identified in the metric plan. If x does not yield a value or it is impossible to implement the measurement one has to go back to the metric plan step redefine the set security components and their impacts.

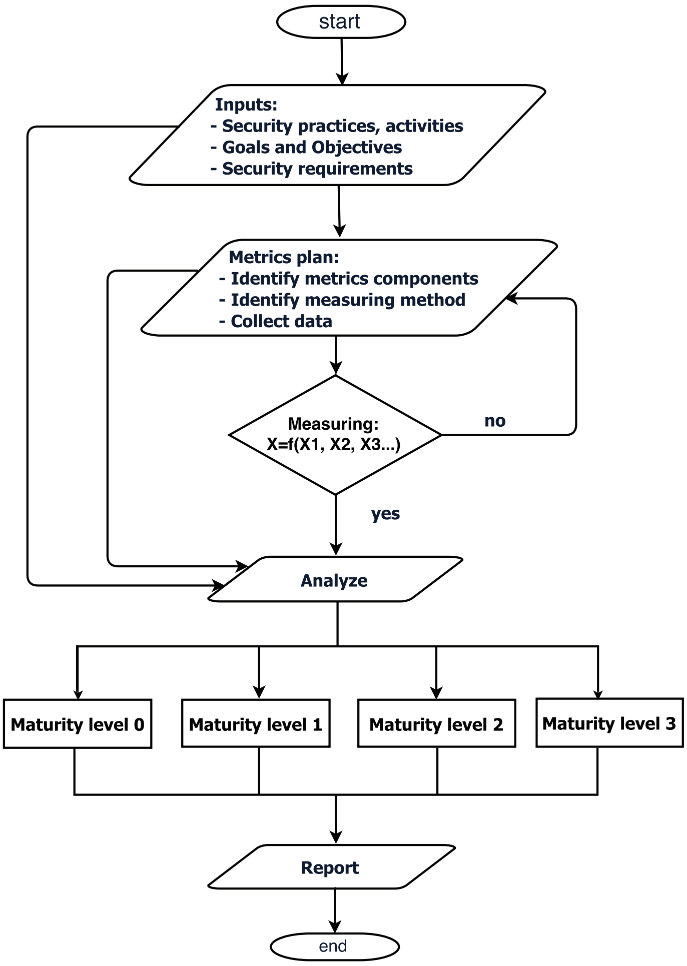


Fig. 4.1. *CSCMM metrics framework diagram*

Analyze. This step consists of several operations such as holistic analysis, interpretation, and consolidation. Holistic analysis means that the analysis takes into account not only the measured metrics but also the elements of the inputs and the metric plan steps of the metrics framework. This is important as some quantitative metrics lose their original meanings when reduced to a pure numerical number. Interpretation of the obtained metrics is to decipher the true security status of the cyber space under protection. Interpretation also provides the reasons and their impact on the measured result. The effectiveness and efficiency of the proposed metrics should be evaluated.

Maturity level determination. Benchmarking is the process of comparing ones own performance and practices against peers within the industry or noted best practice organizations outside the industry. Benchmarks can be used, for example, to determine a minimum essential configuration for workstations, servers, laptops, routers, firewalls, and other network devices or for the holistic system. The method for assigning maturity level depends on the specification of the security metrics. It could be assigned as a percentage range from Level 0 (say, 0-25%) to Level 4 (say, 75-100%); a weighted value; a value interval, or times to security incident response from months (level 0), days (level 1), hour (level 2), to real-time (level 3) [45].

Report. The last step is reporting that shows and informs the ultimate impact and consequences to metrics consumers. All steps of the metrics need to be described. The frequency of reports depends on requirement of the organization and its upper managers. On the one hand, the report provides the assessed security status of the cloud system relates and explain clearly the impact of the security status to the management on the organization business plan and direction. On the other hand, to the security experts and practitioners, the report identifies security weaknesses and suggests action plans for remedy and provides a roadmap for strengthening the security of the system.

5. The selection of advanced security quantitative metrics for CSCMM. With the proposed security metrics framework, the overall security assessment can be balanced and complemented between existing qualitative assessment for senior managers of an organization and quantitative assessment for its security experts. In terms of the qualitative assessment, capability maturity model theory provides senior managers with a sound picture of security compliance of their system in terms of practices but it does not relate well the impact of the security assessment to their business plan and direction. In terms of quantitative assessment, advanced security metrics allow mappings between the outcome of security assessment and costs/benefits to the organization. Furthermore, good quantitative security metrics allow the identification of a specific domain or an individual practice of the model and suggest appropriate security measures for achieving a higher level of maturity.

Among many quantitative security metrics, Mean Failure Cost (MFC) metrics [46] is an excellent candidate metric for CSCMM. MFC is the predictive quantitative metric that quantifies the costs each (among many) stakeholder needs to invest to the mission for better security or the benefits the stakeholder stands to lose due to the lack of security. MFC is considered as an advanced security metrics for a number of reasons. First, it includes the stakeholders, the impact of security properties on stakeholders, and the threats that can affect system. Second, it can embrace traditional metrics such Mean time to failure (MTTF), Mean Time To Explore (MTTE), and Mean Time Between Breaches (MTBB). Third, it meets many essential security metrics requirements such as SMART or PRAGMATIC.

In addition, the assessment process in the CSCMM model can deploy other state-of-art quantitative metrics including check-list based, state-based stochastic, microaggregation technique, fuzzy analytic hierarchy, attack graph based, Dynamic Bayesian Network (DBN) based, formal methods, and tree weighting. Check-list-based metrics propose an advanced security measurement system that reflects the characteristics of each field (critical infrastructure facilities) to achieve effective information security management [47]. State-based stochastic metrics focus on progression of an attack process over time. This applies for 4 types of significant attacks: Buffer Overflow, Man-in-the-middle, SQL injection, and Traffic Sniffing [48]. Microaggregation is the technique to protect cloud data through anonymity in order to prevent exposure of person's identity [49]. Fuzzy analytic hierarchy presents a quantitative framework based on Fuzzy Analytic Hierarchy Process (FAHP) to quantify the security performance of an information system [50]. Attack graphs based provides a method for quantitatively analysing the security of a network using attack graphs that are populated with known vulnerabilities and likelihoods of exploration and then exercised to obtain a metric of the overall security and risk of the network [51]. Dynamic Bayesian Network (DBN) based model is used to capture the dynamic nature of vulnerabilities that change overtime. An attack graph is converted to a DBN by applying conditional probabilities to the nodes, calculated from the Common Vulnerabilities Scoring System [52]. Formal methods are being used for verification of cloud computing systems including verification of security in partitioned cloud, firewall, and big data [53]. Tree weighting proposes an initial framework for estimating the security strength of a system by decomposing the system into its security sensitive components and assigning security scores to each component [54].

One of the quantitative metrics proposed for CSCMM is called the Mean Remediate Time (MRT). The metric quantifies the costs (here, in term of time) each cloud stakeholder has to spend to remediate as a result of a security breach or failure. The metric relates the stakeholders cost vector to the probability of a realized threat vector through three multiplicative matrices: stakeholder, threat class, and threats matrix. To arrive at the quantitative MRT, a new cloud security stakeholder model is introduced to identify cloud security stakeholders and their interrelationships. In addition, a security threat probability distribution proposed based on attack-graph, Common Vulnerability Scoring System (CVSS) and Markov chain theory. Clearly, quantitative metrics are not applicable to all cloud domains as for some domains existing qualitative metrics are more appropriate for security compliance. However, the essence of a quantitative metric is that it allows the security assessors to ascertain the security level of each domain and of the overall cloud so that senior management of the organization can make appropriate decisions in terms of sound security investment, meaningful system upgrade accordance to their business plan. The quantitative metric must also allow security practitioners or security managers to identify the security weaknesses of the system and provide the roadmap for security implementation.

6. Conclusion. This paper reviewed and revised a number of security concepts and models including cloud security models, security capability maturity models, and security metrics. The security capability maturity models are of particular interest as they systematically cover all important aspects of a cyber-infrastructure. The paper proposed a Cloud Security Capability Maturity Model that includes cloud-specific security domains and provides quantitative assessment of the overall security of the cloud under consideration. To support the measuring of security maturity level, a security metrics framework was introduced. This framework includes relevant quantitative metrics for measurable assessment. It presents a balance assessment of the overall security of an organisation/system qualitatively and quantitatively. For senior managers, CSCMM offers a meaningful security assessment of the security status of their infrastructure for making decision concerning business plan and direction. For security experts or practitioners, CSCMM with its quantitative metrics enables proactive measures and responsive actions. The paper also suggested future research with advanced metrics that involve various stakeholders, components of cloud security systems.

REFERENCES

[1] Humphrey, *Cmm*, IEEE, 1 (1989).

[2] P. D. Curtis and N. Mehravari, *Evaluating and improving cybersecurity capabilities of the energy critical infrastructure*, in Technologies for Homeland Security (HST), 2015 IEEE International Symposium on, pp. 1–6.

[3] N. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, vol. 25, MIT press, 1961.

[4] S. Cirani, M. Picone, and L. Veltri, *A session initiation protocol for the internet of things*, Scalable Computing: Practice and Experience, 14 (2014), pp. 249–263.

[5] M. Whitman and H. Mattord, *Management of information security*, Cengage Learning, 2013.

[6] R. Von Solms and J. Van Niekerk, *From information security to cyber security*, computers & security, 38 (2013), pp. 97–102.

[7] M. Gasser, *Building a secure computer system*, Van Nostrand Reinhold Company New York, NY, 1988.

[8] D. Craigen, N. Diakun-Thibault, and R. Purse, *Defining cybersecurity*, Technology Innovation Management Review, 4 (2014).

[9] M. C. Lacity, *Advanced outsourcing practice: Rethinking ito, bpo and cloud services*, Palgrave Macmillan, 2012.

[10] A. Behl and K. Behl, *An analysis of cloud computing security issues*, in Information and Communication Technologies (WICT), 2012 World Congress on, pp. 109–114.

[11] D. Catteddu, *Cloud Computing: benefits, risks and recommendations for information security*, Springer, 2010, pp. 17–17.

[12] C. S. C. Coucil, *Security for cloud computing ten steps to ensure success version 2.0*, report, March, 2015.

[13] W. R. Claycomb and A. Nicoll, *Insider threats to cloud computing: Directions for new research challenges*, in 2012 IEEE 36th Annual Computer Software and Applications Conference, pp. 387–394.

[14] S. Farhan Bashir and S. Haider, *Security threats in cloud computing*, in Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, pp. 214–219.

[15] C. S. ALLIANCE, *The treacherous twelve - cloud computing top threats in 2016*, 2016.

[16] ENISA, *Security standards for cloud usage*, report, August 2014.

[17] J. Archer and A. Boehm, *Security guidance for critical areas of focus in cloud computing*, Cloud Security Alliance, 2 (2009), pp. 1–76.

[18] G. Brunette and R. Mogull, *Security guidance for critical areas of focus in cloud computing v2. 1*, Cloud Security Alliance, (2009), pp. 1–76.

[19] C. Alliance, *Security guidance for critical areas of focus in cloud computing v3. 0*, Cloud Security Alliance, (2011).

[20] B. Swain, P. Agcaoili, M. Pohlman, and K. Boyle, *Cloud controls matrix*, 2010.

[21] J. Allen and N. Mehravari, *How to be a better consumer of security maturity models*, report, Citeseer, 2014.

[22] N. T. Le and D. B. Hoang, *Can maturity models support cyber security?*, in 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), pp. 1–7.

[23] M. Siponen and R. Willison, *Information security management standards: Problems and solutions*, Information & Management, 46 (2009), pp. 267–270.

[24] B. Stevanovi, *Maturity models in information security*, International Journal of Information, 1 (2011).

[25] P. E. Black, K. Scarfone, and M. Souppaya, *Cyber security metrics and measures*, Wiley Handbook of Science and Technology for Homeland Security, (2008).

[26] B. Bates, K. M. Goertzel, and T. Winograd, *Measuring Cyber Security and Information Assurance: A State-of-the Art Report*, Information Assurance Technology Analysis Center, 2009.

[27] W. Thomson, *Lord kelvin: Electrical units of measurement. popular lectures and addresses*, 1889.

[28] W. S. Humphrey, *A discipline for software engineering*, Addison-Wesley Longman Publishing Co., Inc., 1995.

[29] R. Trapero, L. Jesus, and S. Neeraj, *Quantifiably Trusting the Cloud: Putting Metrics to Work*, IEEE Security & Privacy, 3 (2016), pp. 73–77.

[30] A. Jaquith, *Security metrics*, Pearson Education, 2007.

[31] W. K. Brotby, *Information security management metrics*, A definitive guide to effective security monitoring and, (2009).

[32] C. f. I. Security, *The cis security metrics*, 2010.

[33] E. Chew, M. Swanson, K. Stine, N. Bartol, A. Brown, and W. Robinson, *Performance measurement guide for information security*, 2008.

[34] R. Savola, *Towards a security metrics taxonomy for the information and communication technology industry*, in Software Engineering Advances, 2007. ICSEA 2007. International Conference on, IEEE, pp. 60–60.

[35] S. Kowalski, R. Barabanov, and L. Yngstrm, *Information security metrics: Research directions*, (2011).

[36] J. P. Ravenel, *Effective operational security metrics*, Information Systems Security, 15 (2006), pp. 10–17.

[37] W. K. Brotby and G. Hinson, *Pragmatic security metrics: applying metametrics to information security*, CRC Press, 2013.

[38] D. S. Herrmann, *Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI*, CRC Press, 2007.

[39] S. E. Schimkowitsch, *Key Components of an Information Security Metrics Program Plan*, thesis, 2009.

[40] S. C. Payne, *A guide to security metrics*, SANS Security Essentials GSEC Practical Assignment Version, 1 (2010).

[41] W. Jansen, *Directions in security metrics research*, Diane Publishing, 2010.

[42] G. Campbell and M. Blades, *Building a metrics program that matters*, Journal of healthcare protection management: publication of the International Association for Hospital Security, 30 (2014), p. 116.

[43] B. Duncan and M. Whittington, *Compliance with standards, assurance and audit: does this equal security?*, in Proceedings of the 7th International Conference on Security of Information and Networks, ACM, p. 77.

[44] B. Kitchenham, *Procedures for performing systematic reviews*, Keele, UK, Keele University, 33 (2004), pp. 1–26.

[45] R. Lentz, *Security intelligence maturity model*, 2015.

[46] M. Jouini, A. B. Aissa, L. B. A. Rabai and A. Mili, *Towards quantitative measures of Information Security: A Cloud Computing case study*, International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1 (2012), pp. 248-262

[47] Y. You, I. Cho, and K. Lee, *An advanced approach to security measurement system*, The Journal of Supercomputing, 72 (2016), pp. 3443–3454.

[48] J. Almasizadeh and M. A. Azgomi, *A stochastic model of attack process for the evaluation of security metrics*, Computer Networks, 57 (2013), pp. 2159–2180.

[49] S. Tonni, M. Rahman, S. Parvin, and A. Gawanmeh, *Securing Big Data Efficiently through Microaggregation Technique*, in Distributed Computing Systems Workshops (ICDCSW), 2017 IEEE 37th International Conference, pp. 125–130.

[50] S. Thalia, A. Tuteja, and M. Dutta, *Towards quantification of information system security*, Springer, 2011, pp. 225–231.

[51] S. Noel, S. Jajodia, L. Wang, and A. Singhal, *Measuring security risk of networks using attack graphs*, International Journal of Next-Generation Computing, 1 (2010), pp. 135–147.

[52] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, *Measuring network security using dynamic bayesian network*, in Proceedings of the 4th ACM workshop on Quality of protection, ACM, pp. 23–30.

[53] A. Gawanmeh, and A. Ahmad, *Challenges in formal methods for testing and verification of cloud computing systems*, Scalable Computing: Practice and Experience, 3 (2015), pp. 321–332.

[54] C. Wang and W. A. Wulf, *Towards a framework for security measurement*, in 20th National Information Systems Security Conference, Baltimore, MD, pp. 522–533.

Edited by: Amjad Gawanmeh
Received: May 2, 2017
Accepted: Oct 28, 2017