Future Generation Computer Systems 107 (2020) 620–644

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Cloud computing security taxonomy: From an atomistic to a holistic view

Siyakha N. Mthunzi [a], Elhadj Benkhelifa [a,*], Tomasz Bosakowski [a], Chirine Ghedira Guegan [b], Mahmoud Barhamgi [c]

[a] Cloud Computing Research Lab, School of Computing and Digital Technologies, Staffordshire University, Stoke-on-Trent, Staffordshire, ST4 2DE, UK
[b] Iaelyon School of Management, Université Jean Moulin, Lyon, France
[c] Université Claude Bernard, Lyon 1, France

ARTICLE INFO

Article history:
Received 11 January 2019
Received in revised form 27 June 2019
Accepted 8 November 2019
Available online 6 December 2019

ABSTRACT

Countless discussions around security challenges affecting cloud computing are often large textual accounts, which can be cumbersome to read and prone to misinterpretation. The growing reliance on cloud computing means that not only should we focus on evaluating its security challenges but devote greater attention towards how challenges are viewed and communicated. With many cloud computing implementations in use and a growing evolution of the cloud paradigm (including fog, edge and cloudlets), comprehending, correlating and classifying diverse perspectives to security challenges increasingly becomes critical. Current classifications are only suited for limited use; both as effective tools for research and countermeasures design. The taxonomic approach has been used as a modeling technique towards classifying concepts across many domains. This paper surveys multiple perspectives of cloud security challenges and systematically develops corresponding graphical taxonomy based upon meta-synthesis of important cloud security concepts in literature. The contributions and significance of this work are as follows: (1) a holistic view simplifies visualization for the reader by providing illustrative graphics of existing textual perspectives, highlighting entity relationships among cloud entities/players thereby exposing security areas at every layer of the cloud. (2) a holistic taxonomy that facilitates the design of enforcement or corrective countermeasures based upon the source or origin of a security incident. (3) a holistic taxonomy highlights security boundary and identifies apt areas to implement security countermeasures.

1. Introduction

With rapid growth of "things cyber" and cloud computing being the central driver among a plethora of technologies [1], including a global proliferation of the internet, computing as a resource has become cheaper, readily accessible and yet a global threat domain. Cloud computing much like traditional computing (Grid computing) is designed to allow optimal resources utilization. Due to augmented virtualisation, cloud computing has become the defacto computing platform allowing dynamic, scalable and elastic reconfiguration computing resources according to one's requirements. More so, a pay-per-use computing model now renders computing as a utility, much as electricity, gas, water, etc. giving cloud computing one of its attractive attributes. Cloud service providers (CSP), e.g. Amazon [2] to provide computing platforms, infrastructures, or software as a service, i.e. Platform as a Service (PaaS), Infrastructure as a Service (IaaS) or Software as a Service (SaaS), respectively, according to a negotiated service level agreement (SLA). This sort of service provision is augmented through efficient multitenancy, which arguably presents potential for cost reduction through the sharing of services and resources. In fact, multi-tenancy ensures that cloud resources and services are fully utilized through sharing among co-located (logically or physically) tenants [3]. The capability for services to be scaled horizontally or vertically up or down, and in some cases automatically, ensures efficient utilization of resources [4]. Users can rapidly provision-computing resources without human interaction, while new nodes and physical servers can be added or dropped from the network with limited modifications to the infrastructure set-up and software. Furthermore, cloud capabilities are available over a broad network and accessed through standard mechanisms that promote use in heterogeneous platforms (e.g., mobile phones, laptops, and PDAs) [4,5]. Nonetheless, such co-location poses as a risk and vulnerability in the cloud, which is further complicated by interactions (which are often dynamic, unpredictable, transient

* Correspondence to: School of Computing and Digital Technologies, College Road, Stoke on Trent, ST4 2DE, UK.
E-mail address: e.benkhelifa@staffs.ac.uk (E. Benkhelifa).

https://doi.org/10.1016/j.future.2019.11.013
0167-739X/

and intensive) among different service domains driven by service requirements.

To facilitate seemingly infinite scalability, cloud service providers (CPSs) deploy a global network of data centers. Data centers generally house physical computing infrastructures including servers, routers and networking hardware. Conceptually, one accesses cloud services from a cloud service provider. In some cases, a cloud service provider leases a virtualised computing infrastructure, also known as a virtual network, from an infrastructure provider. An infrastructure provider provides and manages a network infrastructure, also known as the substrate network. Since, CSP provision bespoke services, essentially, they do so over a virtual network which in turn "sits" on atop a substrate network. Arguably, in this present form, this arrangement is meant to provide greater flexibility, manageability and security [6]. However, a well published cloud computing security state-of-the art suggests otherwise, as wide range of prevailing challenges are yet to be addressed. In this case, the activities of the CSP depend on the deployment model, i.e. a 3rd party, a dedicated department in an organization or share between a 3rd party and a dedicated department such as in community or hybrid clouds.

Cloud-computing industry's security fora; including main organizations such as Gartner Research [7], Cloud Security Alliance [8], Verizon Data Breach Investigative Report [9], paint a clear picture that existing security technologies cannot solve most of the current challenges based upon the novelty of cloud environments and its unique characteristics. In academia, much of the rapidly growing research hence focuses on evaluating and classifying these security challenges. Consequently, there is a proliferation of innumerable viewpoints on what constitutes "cloud security challenges". This is clearly demonstrated by an excess of perspective-based taxonomies, for instance, classifications based upon security vulnerabilities in web applications [10], virtualisation point of view [11], service delivery models [12], or the perspective of a service-oriented organization [13], etc. With such invariably perspective-driven classifications, it is conceivable that resultant taxonomies yield similarly invariable results. Logically, one may conclude that an integrally perspective-oriented classification thus results in incomplete representation of the overall cloud security landscape. Now, suppose there are no overlaps among perspectives, it is likely that most challenges will remain entrenched between perspectives and generally unresolved.

Contribution: This paper proposes a holistic taxonomy of cloud security challenges based upon a consolidation of research literature. Our notion of "holistic" is premised on Howard and Longstaff's view of a satisfactory taxonomy; mutually exclusive, exclusive, unambiguous, repeatable, acceptable and useful [14]. This holistic view is broadly encompassing security challenges according to their source or origin characterized as follows: challenges adopted into the cloud, challenges inherent to the cloud and challenges arising from cloud implementations. Notwithstanding the wealth of information in current literature, it is our view that this work is the first of its form available. Central to this contribution, is our holistic premise that security challenges have a source and therefore an origin; adopted by the cloud, inherent to the cloud, or those arising due to cloud implementation. These three distinctions form the root of the proposed taxonomy.

Method: A complimentary mixed method approach (systematic and narrative) is followed with clear aims. The systematic element is valuable to maintain a tightly focused research while providing objective findings. The narrative bias helps in reviewing the broad topic area to meet the targets of the current investigation while facilitating the transferability of research findings for further research [15]. Overall, this mixed approach will ensure a comprehensive research that yields transparent and valid conclusions on the current state-of-the art [16]. The appraisal of literature follows Kitchenham and Charters 'guidelines of performing a systematic literature review; planning, conducting systematic review and documenting [16]. Planning involves developing and validating a review protocol. The "conducting a systematic review" stage pertains to the identification of the relevant research articles, selecting primary studies, assessing the quality of studies and extracting study data. Furthermore, "documentation" relates to the construction of the reviews, including the discussions that arise.

The literature selection scheme followed in surveying cloud security challenges centers around the notion that cloud computing is rapidly evolving in unison with security issues. In addition, the selection criteria takes the view that cloud computing has reached a good level of stability and maturity [17]. Based upon the above assertions, an inclusion criterion thus considers published literature post the world-wide adoption of cloud computing (2010) up-to date. This also includes articles from respected journals, conferences, academia and top ranked scientific organizations. In this respect, impact factor articles from top ranked scientific publications such as, but not limited to, CSA & Gartner, respected journals such as IEEE, Elsevier, ACM, European Journal of Information Systems, meet a level of quality fit for this review. More so, citation data on selected articles from scholarly platforms such as google scholar are presumed to provide not only an indication of material usage, but general acceptability. Due to the seismic proportions of published literature, the review criteria gave preference to relevant articles, i.e. those with breadth and depth with most if not all perspectives of the domains under investigation. The rest of our work is structured as follows: Section 2 is an overview of cloud computing security challenges and taxonomies. Section 3 presents a survey and reconceptualization of cloud security taxonomies in current literature. Section 4 presents the proposed holistic taxonomy to cloud computing security challenges. In addition, this section presents proposed holistic model processes for cloud security countermeasure designs and research. Section 5 presents a summary of this paper's main findings followed by a reference list. Appendix presents graphical re-conceptualized taxonomies mentioned in Section 3 above.

2. Cloud computing security

In the most basic concept, cloud entities embody individuals or organizations that remain in interaction to perform tasks in the cloud [18,19]. Their co-existence and interactions enable the functions of the cloud, albeit also as potential sources of security concern. The responsibility for implementing, operating and management of security is variably viewed from one cloud model to the other. As such, it is important to clarify these responsibilities for both the consumer and CSP. This includes clarity to the consumer regarding any security considerations which may exist outside their control. Without this, it is probable that vulnerabilities are not detected in time and data breaches occur as a result.

The prominence of security concerns in cloud computing is evident in reported data breaches since 2010, some which remain highly ranked in their relevance to cloud security. For instance, a rapidly growing literature indicates that virtual machine vulnerabilities to side-channel attacks expose IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) to breaches.[1] It was hypothesized that at least

[1] https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/.

sixty potential security domains exist within the cloud architecture [20], with arguably more domains sprouting as new implementations introduce new aspects to the cloud. As a prelude to cloud computing, it is important to briefly highlight two fundamental principles that are perhaps at the center of this computing paradigm; underlying concepts and approaches for resource sharing, including tenancy and multi-tenancy, and the concept of virtualization in respect to cloud computing. Tenancy describes users, often existing as disjointed legal entities, sharing a view to common services, application, data and configurations. Thus, multi-tenancy in cloud computing defines a method of sharing an instant of an application among collocated clients, by providing every client an out-and-out, and isolated share of that instant. By leveraging software virtualization, co-located cloud users can share resources such as storage, memory, etc. The challenge, however, is that where genuine and malicious virtual machines (VMs) are co-located, it is possible for the malicious entity to attack VMs through commonly shared resources. [21] argue that it is possible for the malicious entity to covertly implant malicious code into a collocated tenant with no detection. A case in point is the Zeus Botnet exploit which successfully compromised cloud infrastructures.[2] In both scenarios, the legend of multi-tenancy ensured that cloud consumers were oblivious other entities' identity, their security posture or as well as their motivations. Virtualization in the other hand aims to achieve logical abstraction of computing resources from their physical constraints, including compute, network, storage, operating system, etc. [22]. Due to this logical abstraction, resources can be dynamically expanded vertically up or down and horizontally according to requirements.

Cloud computing is replete with challenges, most arguably in existence pre-cloud resurgence [23]. What has clearly changed in the environment, for instance, encryption for data protection and integrity insurance. Considering other cloud-driven technologies such as IoT and cloud converged systems where interconnected objects introduce a host of potential risks, unresolved security challenges could have catastrophic consequences. Current literature clearly questions the effectiveness of traditional security techniques such as intrusion detection systems (IDS) in the modern-day enterprise networks due to virtualization, heterogeneity and their distributed nature. This extends to other causations including a wide threat domain, as well as risks and vulnerabilities existing within the cloud infrastructure. Due to the physical and logical structure of the cloud, such vulnerabilities exist at an elevated level.

While cloud computing facilitates low-cost provisions of computing storage and processing power, adversely, this benefits the hacker community.[3] In the VM model characterized by resource sharing, the ability for malicious activities to fraudulently monitor and retrieve confidential information from CPU, network activity, or storage [24] is of concern. Other security concerns in cloud environments are leveraged by circumventing security systems or exploiting vulnerabilities of application programming interfaces (APIs) in cloud software vendors [25]. Resultantly, server crushes occur because of poorly designed application programming interfaces (APIs) that lack the necessary security measures. Consequently, insecure APIs pose a greater risk by providing execution privileges to unauthorized users [26]. Henning suggests the unique attributes that enable the cloud as equally liable risks to an organization [27].

While scalability, availability, agility and the ability for cloud users to adapt to fluctuations according to business demand gives cloud its attractive features, these attributes provide a breeding ground for malicious activities to scale with relative ease over a wider attack base. Evidence in literature suggests that in co-located tenant environments, it is easy for malicious users to passively observe or send data through exposed side-channels [28, 29]. By monitoring cache usage, adversaries can easily identify a target VM [30] while behavior analysis aids to cross VM information leakage [25]. Nonetheless, new systems designed to mitigate vulnerabilities associated with cache monitoring exist. In fact, [31] suggests datacenter virtualization and middleware sharing to be efficient approaches for a multi-tenant solution, i.e. one application instance for each tenant.

In the foregoing, we brief descriptions of some widely discussed cloud security issues and challenges. For purposes of this paper, we summarize these challenges, as generally covered by Cloud Security Alliance[4] and Gartner Research[5] in Table 1. These also include security issues discussed in existing academic literature. While some sources are discussed in this paper, additional sources have been added to supplement existing literature for the benefit of the interested reader.

3. Existing cloud security taxonomies

A motivation for this paper is the investigation of security classifications in existing literature to determine potential gaps and their possible impacts upon cloud computing security challenges. With possible impact areas established, new solutions for the cloud paradigm can be designed to support all perspectives of the cloud and cloud's functionalities. In this view, it is foremost important therefore, to investigate existing taxonomies and address their challenges. Through a meta-synthesis of various perspectives, this paper re-conceptualizes textual classifications into hierarchical tree-like taxonomies. This is significant as it simplifies visualization for the reader and clearly illustrates entity relationships amongst cloud categories [66]. Thus, in this section, this paper investigates cloud security challenges classifications in academia from a general cloud-wide view. For this purpose, review literatures are carefully chosen from renowned sources including top ranked journals, conferences, scientific organizations. Although these are limited in number, these sources are viewed as archetypal of cloud computing perspectives and thus are enough to constitute a satisfactory security review. In this section, we distinguish:

End-user perspective: As re-conceptualized and illustrated in Fig. 15 (See Appendix), security challenges are classified according to end-user's concerns on issues at the application, virtual and physical levels of the cloud. Objectively, the notion of the end-user is broadened to include the cloud subscriber, software developer and the person or organizations who owns an infrastructure. The authors proposition is a compelling argument for a Trusted Third Party (TTP) as a solution to trust issues in the cloud, at a horizontal level of service. Logically, this is a useful technical proposition towards addressing one of the most prevalent security challenges in the cloud. More so considering the integration of cloud computing with other technologies such as the internet of things (IoT) [67,68]. Nonetheless, their criteria are only limited to local concerns for the end-user and perhaps fail to address the security challenges in other perspectives. One major drawback as a result, is that Zissis and Lekkas's end-user perspective limits their classification to a local tool for this end-user's perspective. By taking a perspective driven approach, this taxonomy does not include challenges in the complete sense of the cloud, i.e. a top-down, bottom-up or left-to-right view excludes other dimensions,

[2] https://aws.amazon.com/security/security-bulletins/zeus-botnet-controller/.

[3] http://www.homelandsecuritynewswire.com/hackers-using-cloud-networks-launch-powerful-attacks.

[4] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[5] http://www.gartner.com/technology/home.jsp.

Table 1
Summary of cloud security challenges.

Challenge	Issue	Reference
Control	Outsourcing, PaaS, SaaS and IaaS. Ease of use by end user's degree of information security & control, i.e. control of data & control over security • Data owner has no full physical control over their data • No control over OSs, network & servers, storage & applications in SaaS • No control over Oss, network & servers in PaaS • Loss of control over networking components in IaaS	[32,33]
Trust	Securely establishing trust between servers & clients, & trusting cloud environments. • Trust between servers & the clients misuse of cloud services • Impose security policies	[5,11,34].
Virtualization	Updating security countermeasures is paramount to preventing data breaches & leaks • Risk to integrity of saved VM images • Malicious insider • Risks to confidential data stored in virtual machines	[35–38]
Malware	Intrusive and hostile software • Sophisticated malware such as Stuxnet & Flame. • Zero-day exploits	[39–42]
Attacks on web services	Prominent attacks & immature coding exploit online vulnerabilities • Injection flaws & cross-site scripting • Signature wrapping attacks • Malware, CSS, and Denial of Service (DoS)	[43–48]
Denial of service	Compromise the availability of services • Semantic & flooding DDoS attacks • FRC attacks falsely use cloud resources: impacts application-layer servers • Exploits are financially detrimental to a cloud consumer • Cause the Operating System (OS) kernel to crash	[32,41,42,49–51]
Weak identity, credential & access management	Insufficient scalability in identity access management systems • Spoofing attacks • DoS attacks • Elevations of privileges • Repudiation	[52]
Data breaches	Unauthorized access/use of confidential/sensitive data. • Vulnerabilities in applications • Malicious insider. • Information disclosure	[21,53,54]
Data loss	Insecure & unnoticed configurations or vulnerabilities result in potential exploits & data loss. • Side-channel attacks expose IaaS, PaaS and SaaS to breaches	[21,53,54]
Insecure interfaces and APIs	Poorly designed APIs in cloud software vendors • Provide execution privileges to unauthorized users	[49,55]
Account & service traffic hijacking	Exploitation of software weaknesses, and personal information • Phishing attack • Service or account hijacking	[49,56]
Malicious insider	Breach of confidentiality by manipulating multi-tenancy • Co-residency attacks • Malicious insider	[49,57,58]
Abuse of cloud resources	Where IaaS providers lose some control • Hackers & spammers take advantage of free limited trials	[49,59,60]
Insufficient due diligence	Choosing and moving functions to cloud environments entails careful consideration	[49,61]
Shared technology vulnerabilities	Vulnerabilities due to intrinsic & prevalent core cloud computing technologies	[59,62]
Privileged user access	Where 3rd parties process data outside the enterprise • Outsourcing means that an enterprise's security controls (physical or logical) are bypassed.	[11,59]
Data location	Location of data & processes where routine maintenance is provided by a cloud vendor, • No information to the cloud consumer about where their data is held, as well as what processes are being performed	[12]
Regulatory compliance	Challenges when dealing with LSAs & other process & regulatory issues • Assurance • Process and regulatory issues	[12,47,59]
Data segregation	Logical storage of data in multi-tenant environments • Cross channel attacks • Malicious insider	[63]
Recovery	Low-cost disaster recovery & data storage solutions	[12,55]
Long term viability	Concerns a cloud consumer's data if a CSP loses their business	[64,65]

which clearly constitute areas of concern, e.g. other cloud entities such as 3rd parties.

Perspective of outsourcing: As re-conceptualized and illustrated in Fig. 16 (See Appendix), this paper illustrates its interpretation of security challenges inspired by Shahzad [32]. A state-of-the-art survey of cloud security issues from [32]'s perspective identifies the outsourcing nature of the cloud as a unique challenge to cloud security. This claim is premised on the view that the cloud

service providers retain control of data. This argument is in line with [33] who suggest outsourcing to embroil risks from 3rd parties through end-to-end interactions. [32] Unlike Ryan [69] includes in their considerations, other unique challenges including multi-tenancy, virtualisation and service level agreements (SLA), economic distributed denial of service attacks (eDDoS) and cloud storage [32]. This is a broad view of security challenges in cloud environments. This thesis shares the common view that security challenges affecting the cloud are either unique to the cloud or traditional. Nonetheless, the contents within this taxonomy are deemed to be too general leaving its application for general use. [32]'s classification does not demonstrate where security issues impact the cloud, which layer of the cloud, at what level, etc.

Architectural, technological, process and regulatory perspective: As re-conceptualized and illustrated in Fig. 17 (See Appendix), [63] state-of-the-art analysis classifies cloud security challenges into two categories; challenges that have architectural and technological aspects and those that are process and regulatory oriented. The authors identify architectural challenges to include multi-tenancy, identity management, insider attacks, virtualisation, cryptography and key management issues. Similarly, they identify process and regulatory issues to include governance and compliance, API security, migration issues, SLA and trust management challenges. It is the view of this researcher that the simplicity of Srinivasan et al.'s classification makes it easier to understand and use. From a broad perspective, this taxonomy incorporates most security challenges commonly discussed in literature and identified in this thesis. However, the omission of traditional security challenges in their assessment and categorization limits the scope of this taxonomy. As is clearly demonstrated in literature, traditional challenges such as the DoS, malware, malicious insider, etc. remain a threat to confidentiality, integrity and privacy in the cloud paradigm.

Traditional and cloud-specific perspective: As re-conceptualized and illustrated in Fig. 18 (See Appendix), a survey by [70] classifies cloud security challenges into traditional and cloud categories. According to the authors, traditional challenges describes those issues common to traditional communication systems such as availability, while cloud challenges described those that are uniquely introduced by the cloud. These include resource location, multi-tenancy, trust, monitoring and logging and cloud standardization [70]. Once again, the simplicity of Rong et al.'s classification makes it easy to understand, but nonetheless with limited usability across the entire cloud system. Remarkably, the authors view virtual machine (VM) security as a traditional challenge whose solutions is available, despite clear evidence in current literature that VM security is indeed a cloud security factor that is absent in traditional systems [37]. This thesis posit challenges in VM security are unique to the cloud due to the operational dependencies between cloud models. This notion is articulated by Ali et al. who distinguish operational dependencies in the virtual layer; Software developers (SaaS) need a platform (PaaS) [55]. One may conclude that since the outsourcing element is a core concept of the cloud, 3rd parties will certainly introduce trust and insurance challenges, which are unique to the cloud.

Uniqueness to cloud and pre-cloud era perspective: As re-conceptualized and illustrated in Fig. 19 (See Appendix), works in [69] classifies security issues from the perspective of their uniqueness to the cloud in contrast to those that have existed in the pre-cloud era. In this regard, their method identifies multi-tenancy issues as traditional, based upon the notion that this concept predates cloud computing and with existing solutions. In fact, they argue this challenges to no longer be a scientific challenge [69]. To substantiate this claim, Ryan identifies operating system (OS) processes isolation and the virtual machine managers (VMM) as mature illustrious mitigations in multitenant environments. In its current form, Ryan's work recognizes threats to cloud resident data as the only cloud-specific challenge, premised in the involvement of third parties such as the cloud provider, its employees and sub-contractors [69]. This is simple classification which is easy to understand. This perspective indeed clearly demonstrates the relationships among cloud entities and the commonalities that exists in respect to data stored on the cloud. Ryan's classification is simple and highlights the need for efforts towards cloud resident data. However, Ryan's perspective is a narrow, and only focusing on cloud computing in respect to cloud stored data. This also demonstrates the non-exhaustiveness of Ryan's taxonomy, as it misses key cloud components and issues around the virtual machine monitor (VMM), trust, control, legal, process and regulatory issues.

Cloud layer perspective: As re-conceptualized and illustrated in Fig. 20 (See Appendix), this is a three-tier taxonomy inspired by [71]. In their work, the authors suggest classifying security issues in cloud environments pursuant to the level they belong. Thus, the authors view challenges from six levels; hardware, VM manager, guest OS, applications, network and governance. At the hardware level, the authors suggest availability, integrity, privacy and accountability as pertinent security issues. Similar security concerns exist at the application level, and all but accountability remain pertinent in network and governance. A guest operating system (OS) can access resources in the VMM by compromising insecure design, thereby compromising the integrity and privacy of that VMM and its tenants [63]. We find this taxonomy useful as it includes some of the core concerns yielded in research. However, we find this taxonomy limited only to general use due to the authors' high-level outlook on security challenges. We believe this taxonomy lacks details to show whether the security challenge exists internally or externally of the cloud. For instance, machines are hardware, and faults exist on the server-side or user-side. From a cloud perspective, faults on the user-side do not necessarily cause the same security concerns as faults on the server-side, so we believe this taxonomy would benefit from further detailing.

Co-residency perspective: As re-conceptualized and illustrated in Fig. 21 (See Appendix), in their work, [58] review prominent attacks in cloud environments, classifying the cloud security domain into four categories; Infrastructure, Data, Communication and External Services Integration. Co-residency attacks breach confidentiality when a malicious insider manipulates multi-tenancy to compromise other tenants on the same physical infrastructure. According to our interpretations, each of the four categories is further divided into security area sub-categories, leading to security issues (e.g. hypervisor & trusted computing base as sub-divisions of infrastructure security, resulting in integrity, confidentiality and availability issues). We find this classification useful as it highlights specific attacks in cloud computing. This classification is also simple and easy to understand. In our opinion, this classification is not exhaustive in its presentation of security challenges. For example, while an insecure trusted computing base is a risk to confidentiality, integrity and availability, it consequentially introduces issues of trust, privacy etc.

Architectural complexities: As re-conceptualized and illustrated in Fig. 22 (See Appendix) based on our interpretation of cloud security challenges according to [33]. According to the authors, identity management, data security and trust & assurance are priority areas for security improvements in cloud environments [33]. The authors argue that cloud security challenges exist due to the architectural complexities. Thus, the authors identify trust

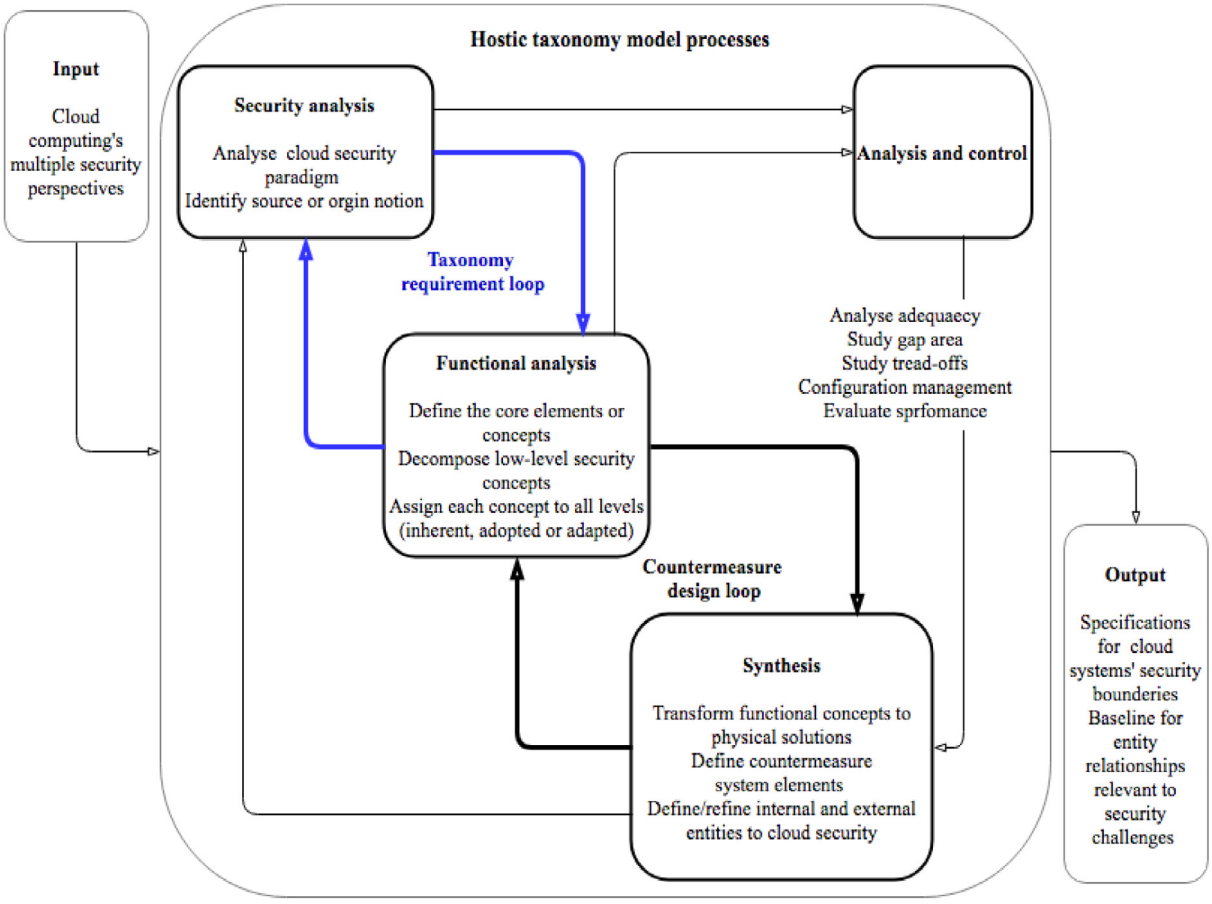


Fig. 1. An illustration of a generic holistic taxonomy development model processes.

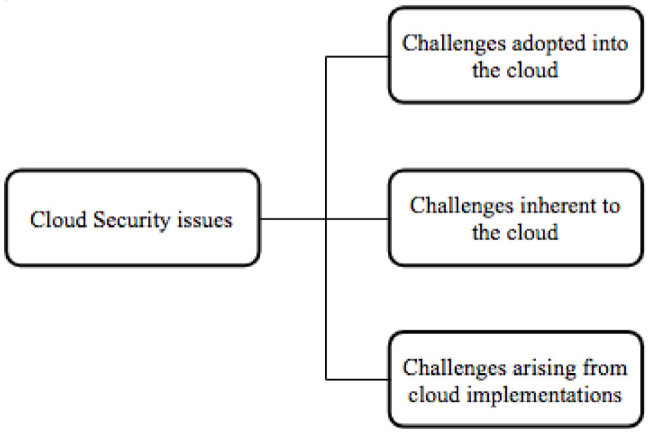


Fig. 2. High-level illustration of the holistic view to cloud computing security challenges.

& assurance, identity management, and data security as priority areas for security improvements in cloud environments. According to the authors, cloud security challenges exist due to the architectural complexities within the cloud environment. In our opinion multi-tenancy in a virtualized environment, control issues related to third parties and architecturally inherent issues such as monitoring, and auditing are equally critical threats to security in cloud computing. We therefore find this taxonomy limited as it does not include some critical security challenges.

Organization's outsourcing cloud components perspective: As re-conceptualized and illustrated in Fig. 23 (See Appendix), this taxonomy represents our understanding of cloud security issues according to [72]. The author's work classifies cloud security issues concerning the outsourcing portions of an organizations as: Trust, Architecture, Software Isolation, Identity Management, Data Protection and Availability. The author postulates that loss of direct control of the security aspects in outsourced environments introduces risks as it gives the cloud service provider "unprecedented levels of trust" to [72]. Likewise, risk management is a challenge in an outsourced environment, as organizations possess limited control to prepare for incidents, setting priorities and contingency plans. We find this classification to be useful, and insightful. For instance, outages as a critical cloud security challenge

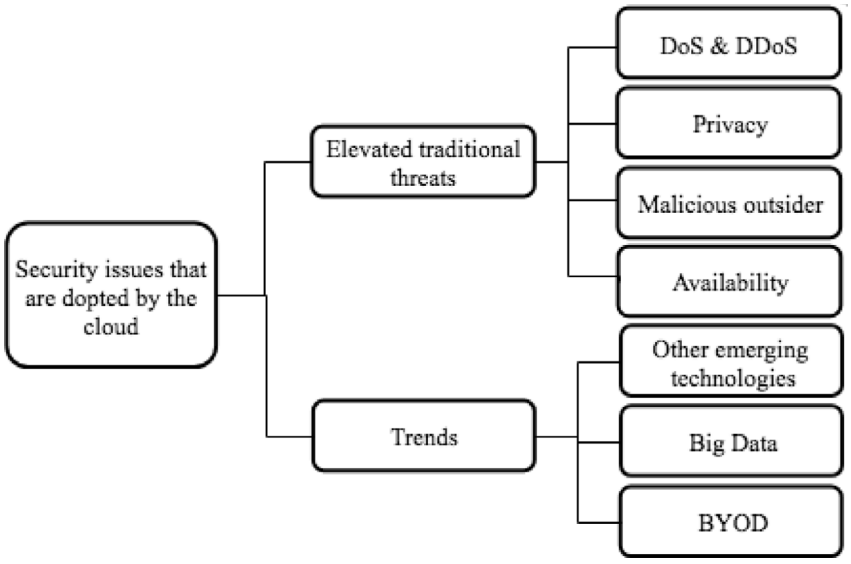


Fig. 3. Taxonomy on unique adopted security issues.

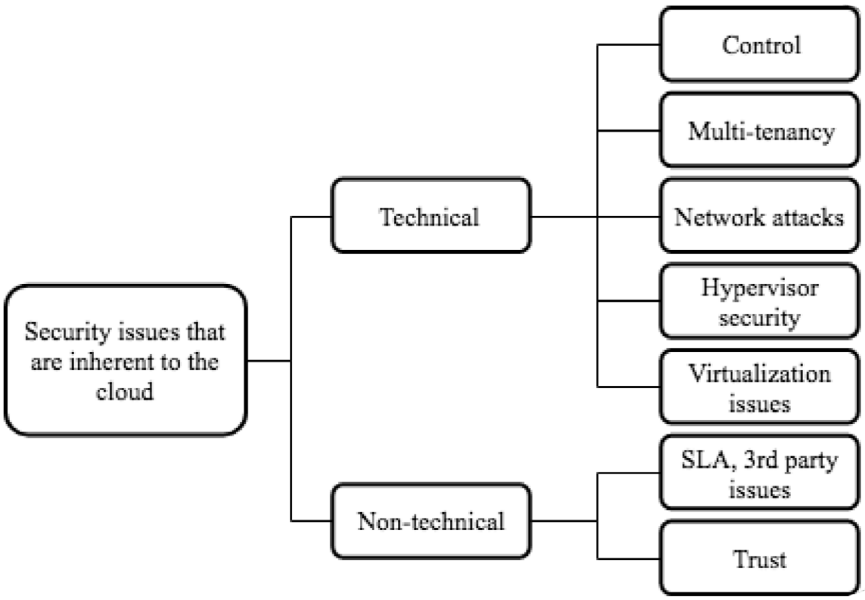


Fig. 4. Taxonomy of security issues inherent to the cloud.

to availability. We also consider architectural challenges including client-side security to be a valuable consideration; cloud interactions begin at the client workstation, through the internet to the cloud. However, we believe that this classification could benefit from illustrating wider coverage. For instance, considering trust issues pertinent to the consumer vs trust issues pertinent to a 3rd party such as a sub-contractor.

Data life-cycle perspective: As re-conceptualized and illustrated in Fig. 24 (See Appendix) this security taxonomy is motivated by [59]. According to the authors, privacy focuses on the complete data lifecycle, from the point when data is generated through to its destruction, while legal issues pertain privacy relate to guidelines in the cloud. The authors define a compliance category relating to governance and control issues. Furthermore, they define the architecture category to include elements such as the network, interfaces and the virtualisation issues (Isolation, hypervisor, data leaks, and VM identification and cross VM attacks) arising due to cloud the architecture and infrastructural implementations. According to the authors, other challenges include decision making, user access and authentication.

Ali's perspective: As re-conceptualized and illustrated in Fig. 25 (See Appendix), this is a taxonomy of cloud security challenges presented in a survey paper by [55]. The authors justify their classification on various grounds; cloud attributes such as resources pooling, underlying technologies such as virtualisation, and the operational dependencies of cloud services on the cloud infrastructure. The authors classify cloud security challenges as: External communicational challenges are mainly based on the dependence on the internet for communication between the cloud provider and customer. Internal challenges, however, are those interactional challenges that arise because of cloud characteristics and technologies, for instance, communication between virtual machines at a network level and another shared communication infrastructure. Architectural challenges are classified as virtualisation challenges linked to a shared virtual environment in

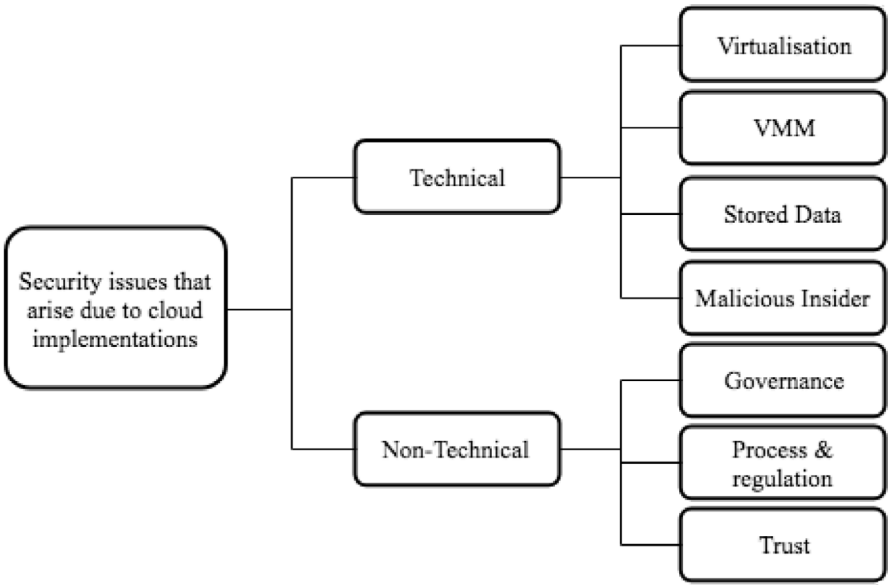


Fig. 5. Taxonomy of unique security issues arising from implementations in the cloud.

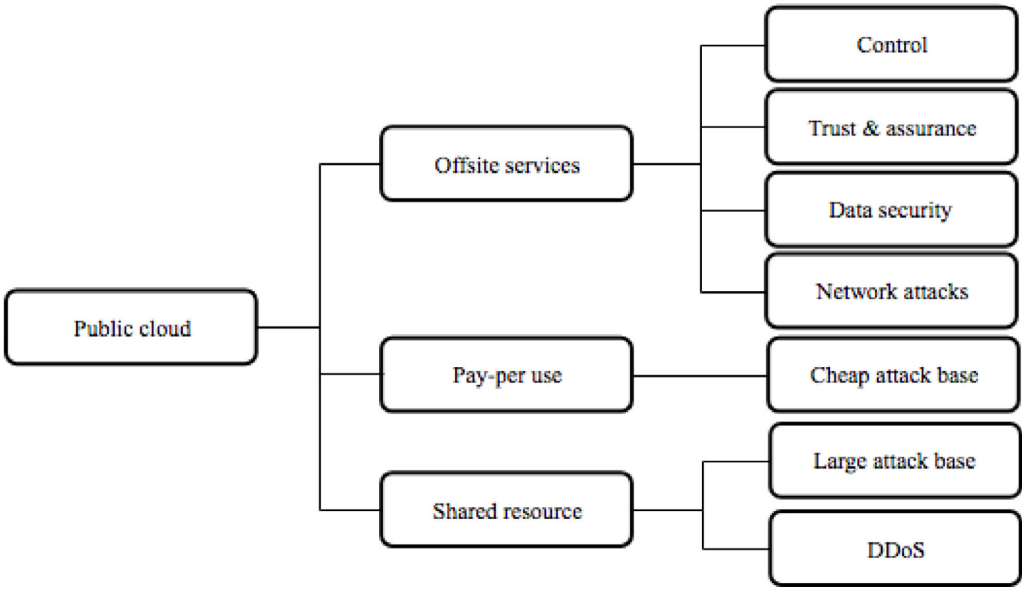


Fig. 6. Taxonomy of unique security issues in public clouds.

multi-tenant setup, for instant, VM isolation. Furthermore, they view data storage issues, insecure APIs and web applications, and Identity management as architectural challenges sub-categories. Contractual and Legal challenges involve agreements: enforcement and insurance, between the Cloud Service provider and consumer; including performance insurance and consequences in times of breach. On the other hand, Legal challenges include issues involving discrepancies in the application of the law due to physical locations and/or jurisdiction.

3.1. Analysis

Clearly, the literature survey shows that existing taxonomies are not generalizable across the cloud security domain. Fig. 12 clearly illustrates this multiplicity of perspectives to cloud security challenges in current literature. To enhance the analysis, the matrix (Table 2) populates earlier taxonomies against relevant areas of the cloud reviewed by authors. This is clearly not an exhaustive list (authors), however, the aim here is to dramatize through visualization and distinguish perspectives that receive greater attention than others in research and perhaps establish overlaps among perspectives. Green shared areas indicate a reviewed area of cloud while red indicate one that has not been reviewed.

The literature reviews above illustrate a multiplicity of perspectives to cloud security challenges in academic research, which perhaps points to the significance placed on specificity when tackling security concerns. Multi-perspectives without doubt collectively highlight security challenges present in cloud computing. In paying attention to specific perspectives, a simplified taxonomy renders that it is easier to identify prominent security challenges for that perspective. For instance, taxonomies (Figs. 16, 18 and 19) are conceptualized as relatively simple, identifying cloud security challenges as specific to the cloud or traditional. Indeed, each containing subcategories for corresponding challenges are relevant for a contiguous main category.

Table 2
A sample of specific topics areas and references covered in articles cloud security challenges (see [73]).

	Sample list of authors											
	[33]	[72]	[5]	[59]	[63]	[70]	[69]	[71]	[32]	[55]	[73]	
Virtual/multi-												
Cloud specific												
Traditional												
Compliance												
Physical												
Application/software												
Network												
Availability/DoS												
Architecture												
Governance												
Process												
Infrastructure												
VM manager												
Data security												
Communication												
External services												
3rd parties												
Technical												
Privacy												
Trust												
Legal & SLA												
IDM & Access												
Data Isolation												
Risk, Management												
Malicious insider												

Arguably, the reader can visualize a broader outlook to security in the cloud to including challenges that are leveraged due to cloud's characteristics. Likewise, the second-tier highlights specific security vulnerabilities. Hence, this paper places emphasis on the simplicity of taxonomies to be a positive attribute towards its usefulness. However, by simple inspection of the matrix above, many gaps exist across multiple perspectives (demonstrated by multiple adjacent red shared areas), implying areas of unexplored security issues. In addition, as has been noted above, while on one hand simplicity is useful to visualize a general outlook, simplicity lacks specific and deeper detail, and hence an inherent deficiency which renders such taxonomies inadequate as tools for developing comprehensive solutions.

On the contrary, other perspectives, for instance Figs. 24 and 26 are considerably extensive, providing detailed categorization; categories, sub-categories, sub–sub-categories, etc. It is the opinion of these researchers that Figs. 24, and 26 closely resemble Howard and Longstaff [14] definition of a satisfactory taxonomy. While complex taxonomies provide greater detail, complexity may perhaps introduce ambiguity. For instance, Fig. 26 would benefit from elucidating which challenges are traditional and which are unique to the cloud at each level of their classification. Clearly, while individual perspective-driven taxonomies denote a simple and yet focused representation of a domain, they fail to communicate distinct challenges. In addition, these taxonomies possess weaknesses inherent with perspective-driven classifications including ambiguity, non-exclusivity, etc. Nonetheless, discrepant perspectives proffer the current paper's holistic assertion; a holistic incorporation of the entire cloud paradigm regardless of perspective shows that cloud security challenges primarily have a source/origin. Whereas the concept of the 'source' forms the basis upon which a comprehensive taxonomy evolves, the comprehensive approach informs the development of a holistic taxonomy for cloud computing security we propose below.

4. A holistic taxonomy of cloud security challenges

Some remarkable methods for classifying concepts have been designed and implemented across many domains. Taxonomic methods are widely applied to help researcher and practitioners alike, investigate, analyze and understand complex concepts and systems. This notion of taxonomies is noted by [74] who allude to taxonomies' importance in discussions and research. In information systems, taxonomies are identified in a review by [75], to provide structure and organization to knowledge enabling researchers to investigate relationships among concepts and draw hypothesis within a domain. Furthermore, the authors note taxonomies' as influential methods towards the design principles of observed phenomenon. This paper takes the philosophical approach to conceptualize cloud computing security knowledge in order to facilitate the design of suitable solutions for the cloud. Hence, the holistic approach is along that of Howard & Longstaff encompassing mutual exclusivity, exhaustivity, unambiguity, repeatability, acceptability and usefulness of a satisfactory taxonomy [14], these are summarized as follows:

- *Mutual exclusivity*: a single subject cannot exist in multiple categories
- *Exhaustivity*: all possible classes are represented in the taxonomy
- *Unambiguity*: the presentation of categories should be consistent and clear in order to provide a complete classification
- *Repeatability*: An element which features more than once should always feature in the same category in all circumstances
- *Acceptability*: To be generally acceptable, the categories should be consistent and intuitive.
- *Usefulness*: Should provide greater insight into the subject topic.

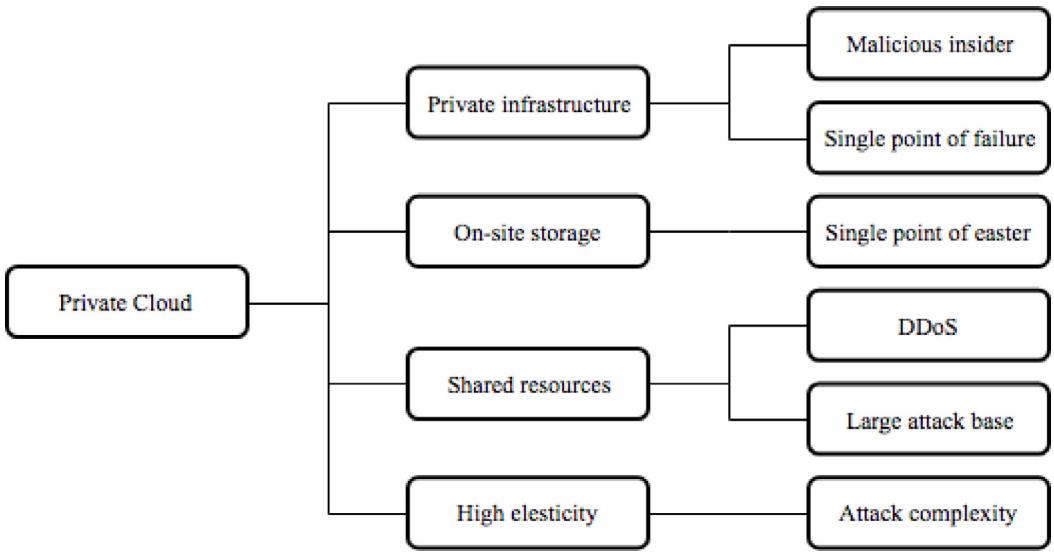


Fig. 7. Taxonomy of unique security issues in private cloud.

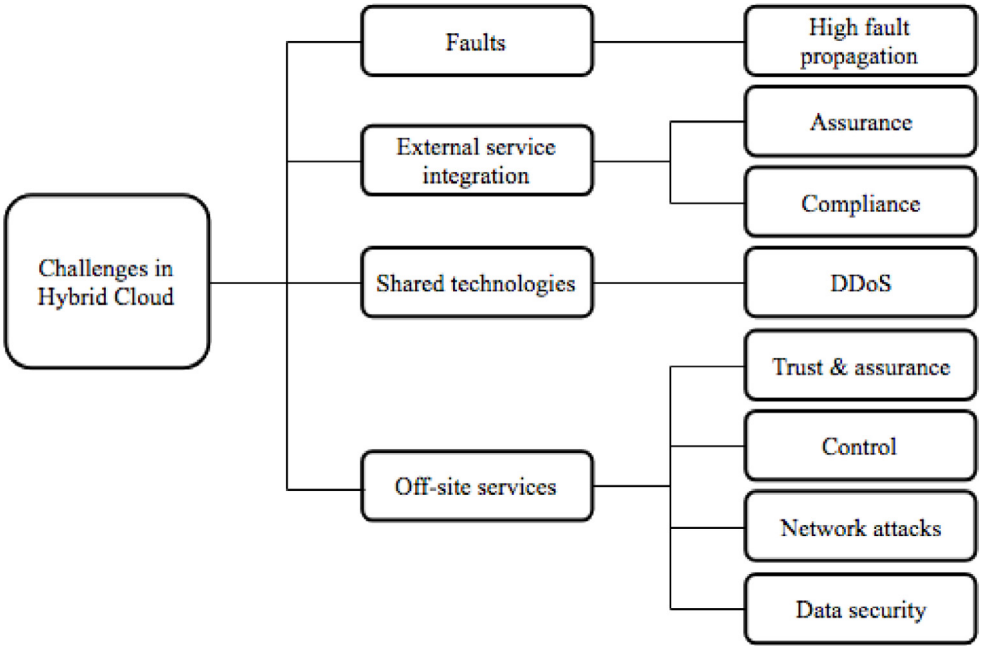


Fig. 8. Taxonomy of unique security issues in hybrid cloud.

In the current paper's efforts towards developing the proposed holistic taxonomy, the high-level model processes illustrated in Fig. 2 are proposed as generic development methods for the cloud systems under the current consideration. For the interested reader, a range of commonly applied taxonomy development methods exist in literature; [75] presents an interesting cross-domain review of us (see Fig. 1).

Briefly, the proposed holistic model processes above foremost constitute an input model. In the current paper, this essentially represents the multiple perspectives within cloud computing's security fora. On the other end, the output are specifications for cloud computing security countermeasures, i.e. security systems baselines, security specifications and configurations. The main model processes comprise the taxonomy requirements loop; models the analysis of the cloud security paradigm and functional analysis; deconstructing, defining and assigning categories to its central concepts. A second loop (design loop) models the continuous processes of functional analysis explained above, and the transformation of functional concepts to physical cloud countermeasures or solutions. In this paper, the design loop facilitates definition and refining of additional security concepts and elements, i.e. sub, sub–sub, sub–sub–sub-categories, etc. An analysis and control model facilitates the evaluation of the analyzed cloud security concepts, and studies gap areas and tradeoffs, both are useful inputs for synthesis model.

4.1. Taxonomy development

As mentioned earlier, the holistic approach adopted in this paper is premised on the view that regardless of the cloud's attributes, characteristics or components, cloud security issues and challenges are broadly defined by their source. Hence in Fig. 2, this paper posits a holistic bird's eye view of cloud security challenges; those adopted by the cloud, issues inherent to the

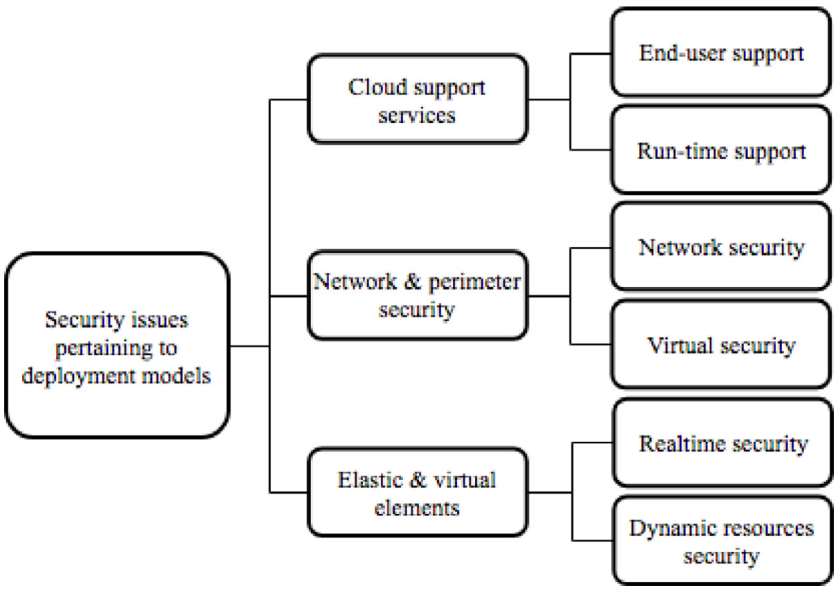


Fig. 9. Taxonomy of security issues unique to cloud deployment models.

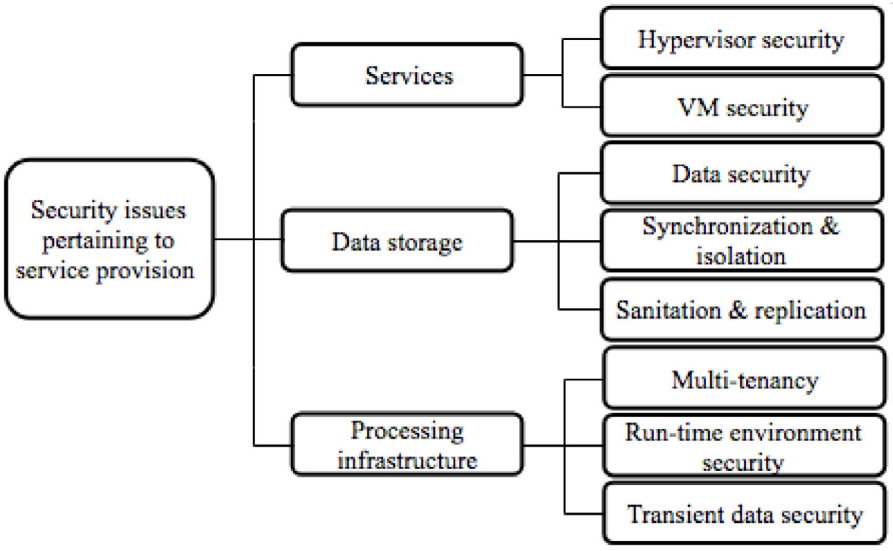


Fig. 10. Taxonomy of security issues unique to cloud service provision.

cloud, and issues arising due to cloud implementations. Examples of each are discussed in turn below.

Issues adopted by the cloud: The argument that some cloud security challenges are not new to information security is shared by several authors including [12,23,76] and [5]. According to Rong et al. traditional challenges commonly refer to augmented and well-known security issues that pose a security challenges for the cloud, mainly due to the physical or logical aspects of the cloud [77]. Such security challenges are non-specific/unique [69] and [32], however they render existing security mechanisms ineffective in cloud environments [27]. For instance, privacy and ultimately the right to privacy is broadly speaking a human right from a legal perspective in the United Kingdom and Europe. Privacy laws, e.g. Privacy and Human Rights Act 1998 in a way guarantees that everyone's right to such privacy.[6] Hence, privacy in the context of personal data is arguably enshrined and enforceable under such Acts. However, when considering privacy in the cloud perspective, it is important to acknowledge the following contexts; Clouds are geo-dislocated, meaning that private data can be held and processed in any location, known or unknown, arguably implying that the enforcement of privacy laws becomes a challenge due to jurisdictional discrepancies. In this context, privacy challenges that existed in the traditional context, whose legal mechanisms for enforcement exist/existed, are leveraged in this new environment (see Fig. 3).

Issues inherent to the cloud: Control mechanisms are well established in the traditional "on-site" model, where data and services are housed within a perimeter to ensure availability. Even where data must leave the premise, for instance, with remote workers, security policies and mechanisms exist to ensure that data remain secure (confidential, integral & available), and accountability for who, where and how data is being held and processed are mature. However, due to the de-parameterized nature of the cloud, and the ambiguity in data location information, traditional policies

6 https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life.

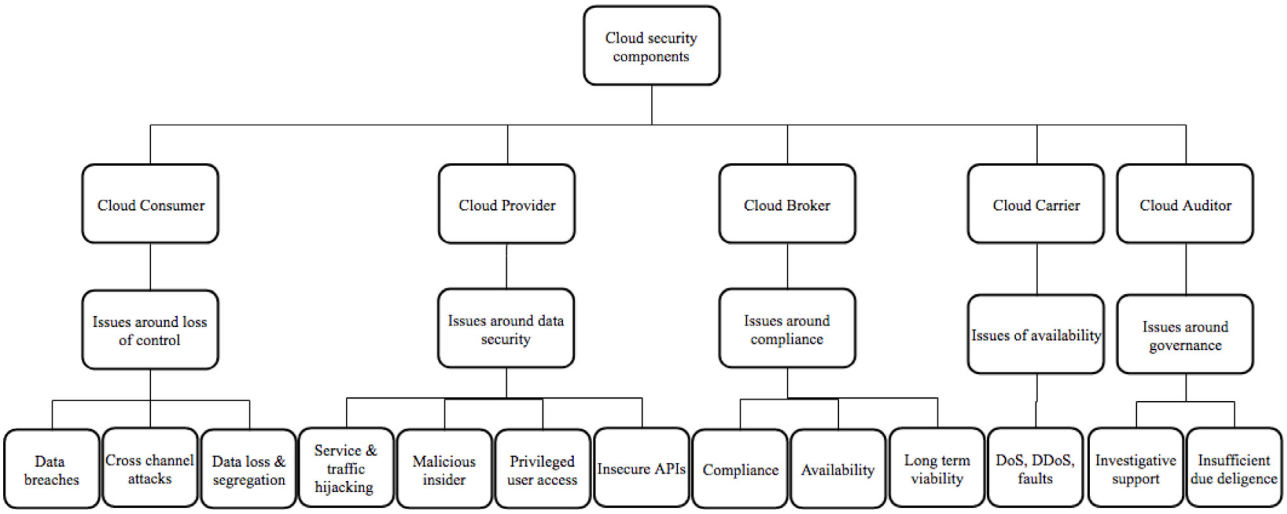


Fig. 11. Taxonomy of security challenges unique to cloud players.

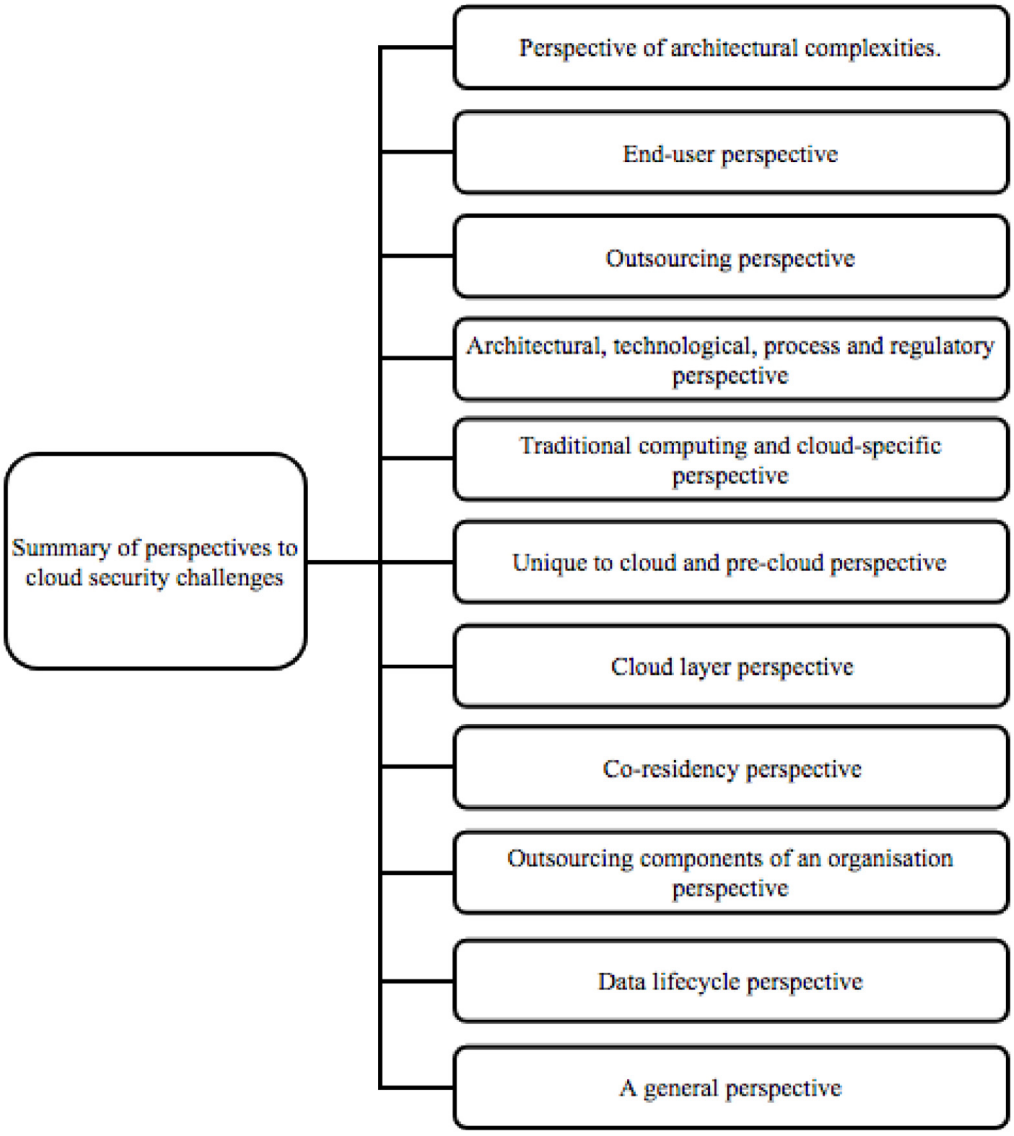


Fig. 12. A taxonomy of example multiple perspectives to cloud security issues.

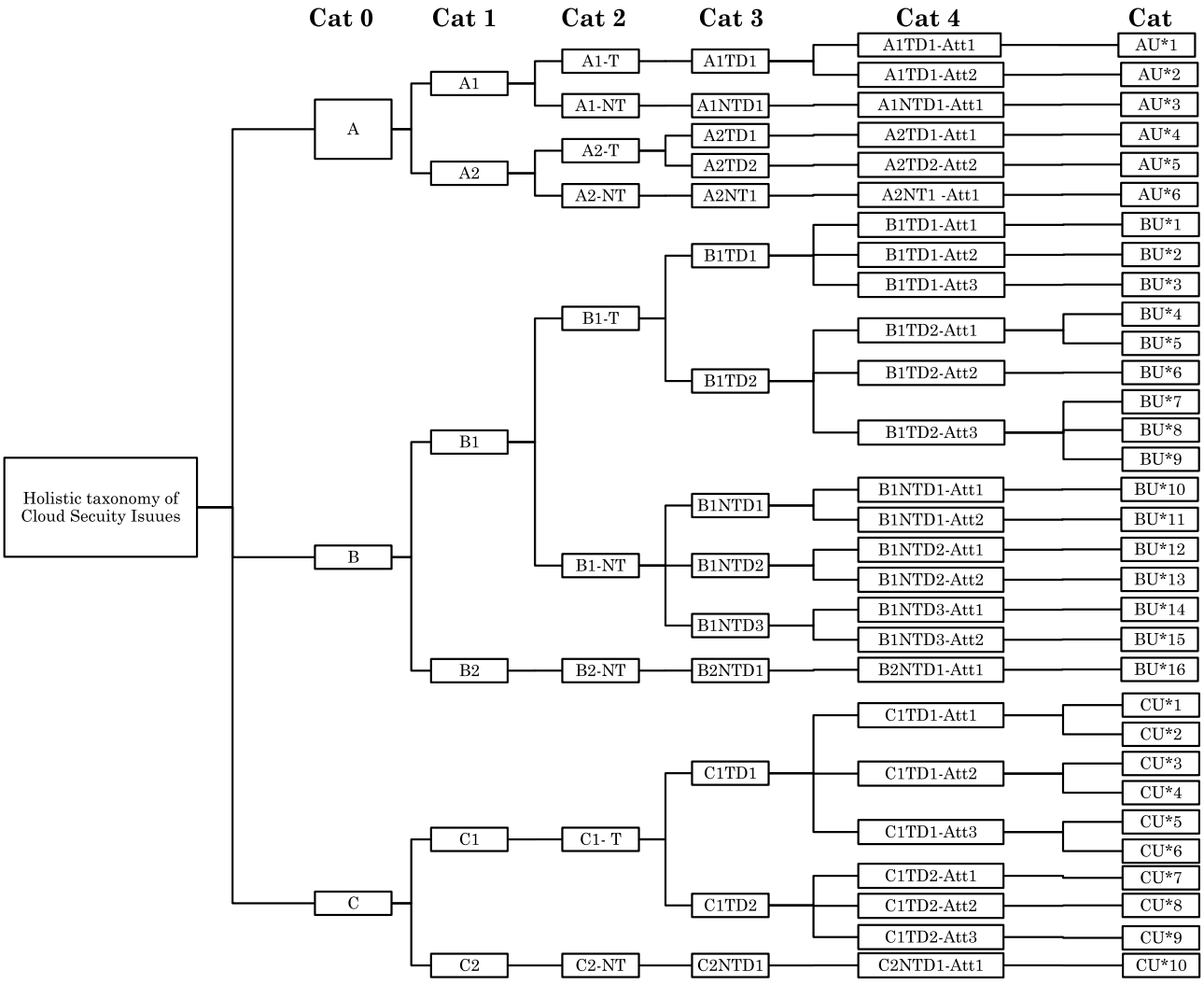


Fig. 13. Our proposed taxonomy for cloud security challenges.

cease to be effective, causing a great deal of discomfort primarily due to the loss of control [12].

Issues arising due to cloud implementations: Big data's compute-intensive business analytics which involves the handling of high velocity, high capacity and high variety data, is an upwards trend. With cloud's rapid resource elasticity, resource pooling, on-demand, transference of risk etc. there is an inevitable convergence of these technologies. From a security point of view, big data analytics is critical as it can improve visualization of the security domain by correlating security relevant data. However, despite these benefits, big data poses a threat to the cloud primarily due to the high volumes of data. As an example, privacy concerns arise where large databases collected through data mining are compromised, e.g. Google's infrastructure collecting and analyzing data for advertising [78]. It is conceivable therefore, that as cloud implementations increase, risk to security including data breaches also increase. Furthermore, it is also conceivable that data security management policies as they exist in the traditional sense, will also be rendered ineffective in the cloud.

While virtualization in the cloud context enables essential cloud features such as location independence, resource pooling, multi-tenancy and rapid elasticity, it inadvertently alleviates traditional security challenges. For instance, cloud customers depend on an internet connection to access cloud resources. In a traditional sense, DoS attacks focus on network entry points with high IP packets [79], in a cloud environment, such as attacks come with a devastating impact. A malicious agent considers what resources they can gain in an attack, how much effort is required to compromise a target and how much access they have to the target [80], as some of the determinants of effecting an attack. The fact that cloud services are offered as a service, where user pay for what they use, it means that malicious agents have an easy access into the cloud infrastructure and act a constant threat in a multi-tenant environment (see Figs. 4 and 5).

Security issues unique to public clouds: Fig. 6 illustrates unique security challenges present in public cloud. In the public cloud scenario, the infrastructure is managed and owned by a 3rd party and located off-site, in which consumers access services through an untrusted base. Public clouds are deemed as financially viable; cheaper model option compared to its alternatives. In addition, as a cloud subset, public clouds benefits from a shared pool of resources. Physical security risks in SaaS are greater in public cloud [12]. Dependence on an internet connection to access off-premise infrastructure introduces risks to network: for instance, attacks associated with the traditional security model such as man-in-the-middle and DoS attacks, threaten the security of data in transit. While traditional security systems such as firewalling, IDS and IPS are well established and mature [59], efforts for developing similarly effective firewalling and filtering systems for public cloud is an ongoing process. Consequently, control,

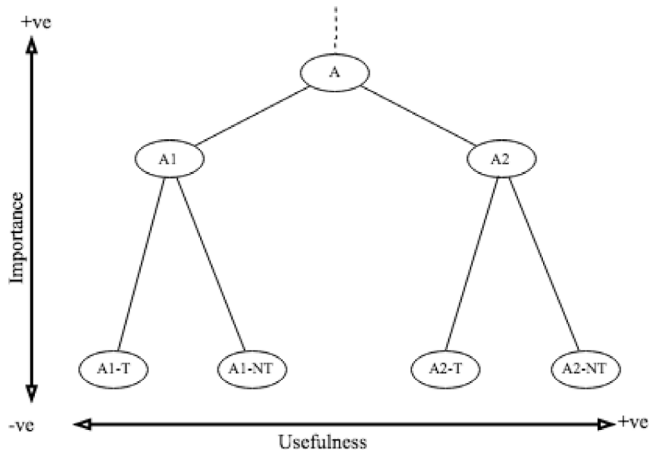


Fig. 14. Usefulness of levels and categories, sub-categories, sub–sub-categories, etc. increases (+vely and −vely) according to a use case scenario.

trust and insurance issues exist as consumers expect their data to remain secure, and providers give assurances of the security of their services.

Security issues unique to private clouds: Fig. 7 illustrates unique security challenges existing in Private clouds. Since private cloud infrastructures are generally managed on-site by the organization and in some cases by a 3rd party/ external organization, the CSP is generally able to specify security configurations, while retaining some level of control. In some cases, issues arise as the private provider relinquishes control over how and if configurations are fully implemented, since this control remains under the infrastructure owner's domain. Consequently, limited control leads to trust and compliance challenges. To mitigate these challenges, consumers access services through a trusted base. The offerings of public cloud versions over a private cloud, while presenting some flexibility and cost benefits, introduces security challenges associated with the public cloud.

Security issues unique to hybrid clouds: Fig. 8 illustrates unique security challenges specific to hybrid clouds, where model infrastructures are managed and owned by both the organization and a 3rd party. In this model, services are located both on-premises and off-premises. The hybrid option is highly dynamic as it benefits from the flexibility and scalability of the public cloud, and the efficiency and security of an on-premise model. Multiple external integrated components yield the hybrid nature of this cloud. However, performance, security and reliability procedures rely on the strength of the integrated services. Integration of services from the private and public options means that multiple platforms are in operation, which results in compliance and insurance issues, particularly when dealing with LSAs and other process & regulatory issues. While heterogeneity aids in evading challenges associated with platform lock-in, the same concept

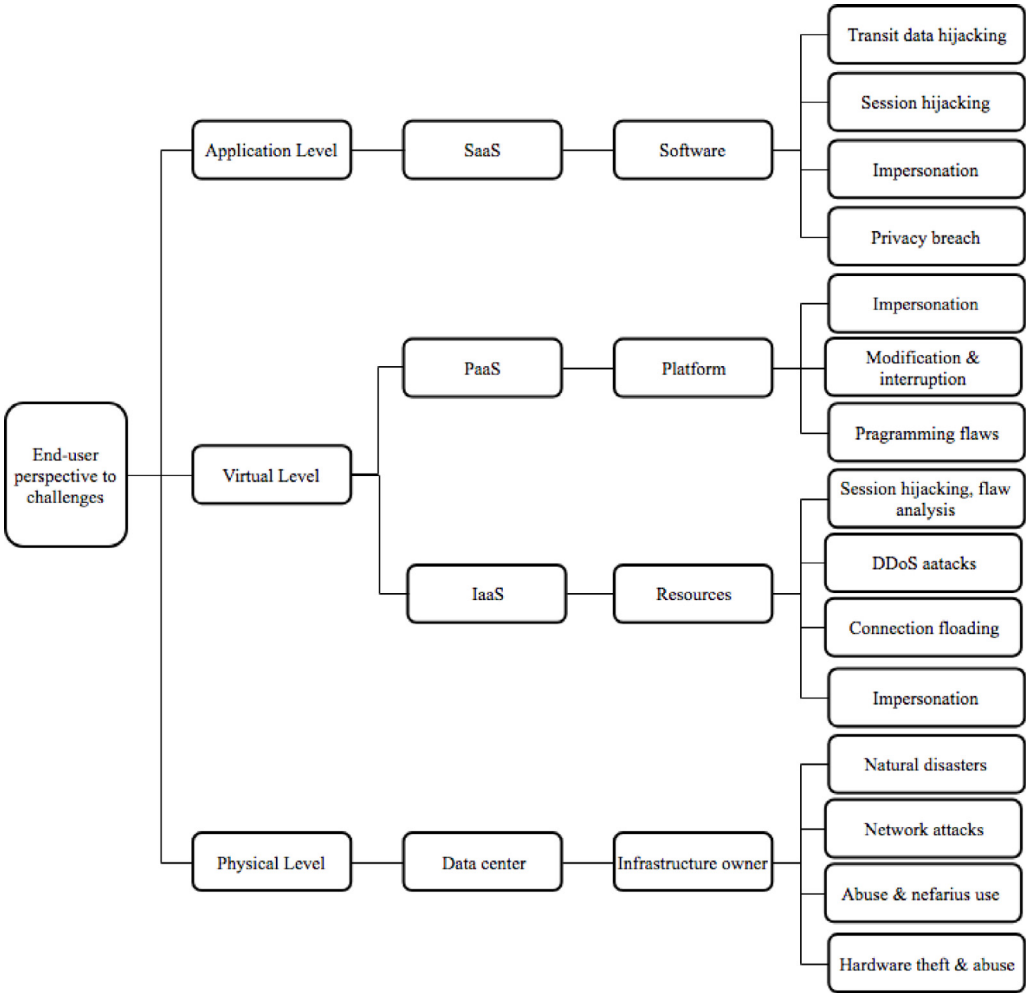


Fig. 15. An end user perspective taxonomy for cloud computing security challenges.

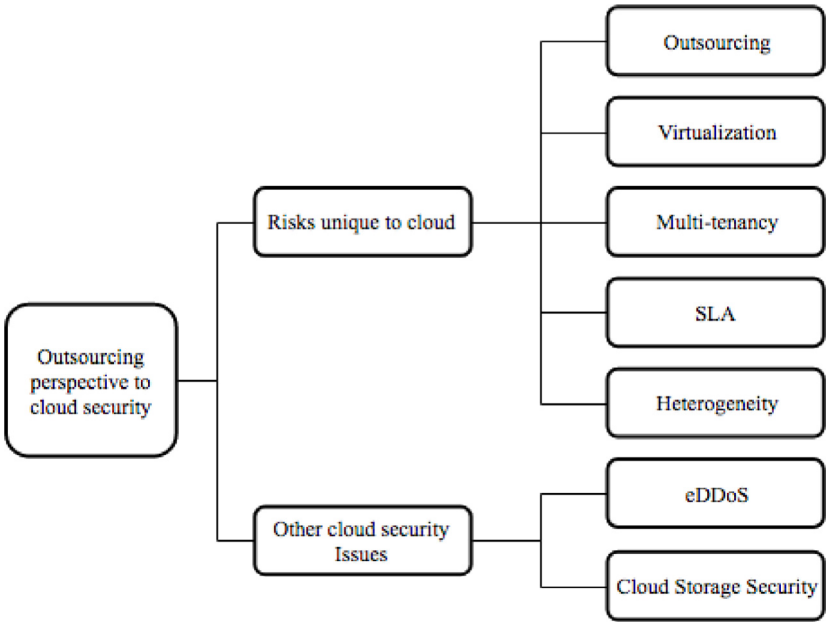


Fig. 16. An outsourcing perspective to cloud security challenges.

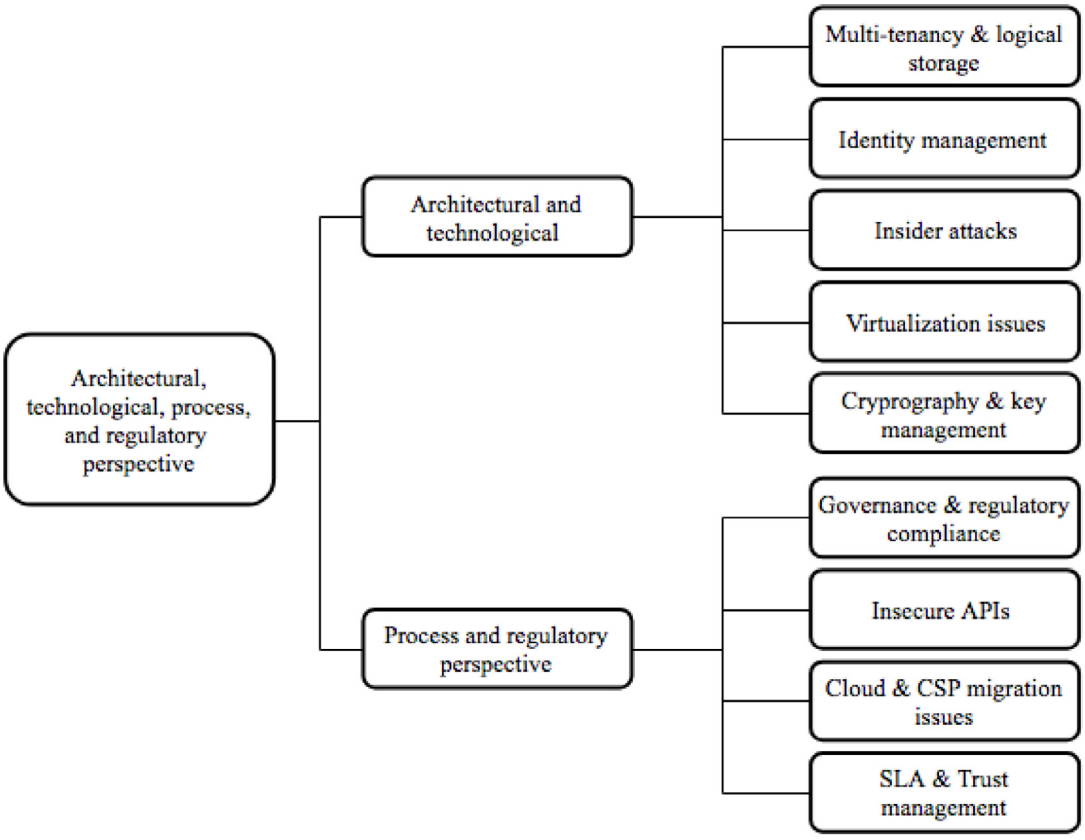


Fig. 17. Cloud security challenges from an architectural, technological, process and regulatory perspective.

introduces integration challenges, i.e. security integration on a multi-vendor platform [81].

Security issues unique to the logical structure of the cloud: As suggested by the definition of architecture; a logical organization of a conceptual structure,[7] we present our context of security challenges in the cloud as existing in, or between the logical components of the cloud and the logical interrelationships between these components. Thus, we view security issues existing in the cloud's architecture as technical and non-technical in nature. We consider cloud security issues that are a result of implementations of cloud concepts focusing on the infrastructure in the context of the "physical and organizational structures and facilities" (see Footnote 7) that constitute the cloud, according

[7] https://en.oxforddictionaries.com/definition/architecture.

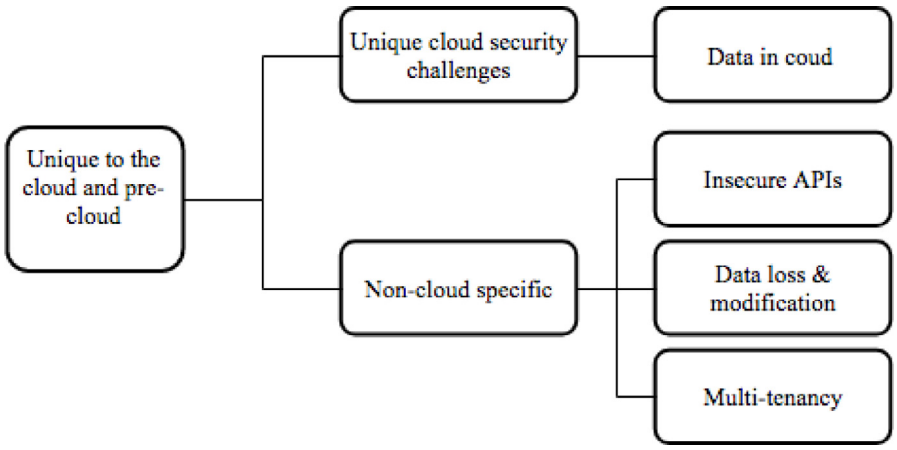


Fig. 18. Interpretation from a unique and pre-cloud perspective.

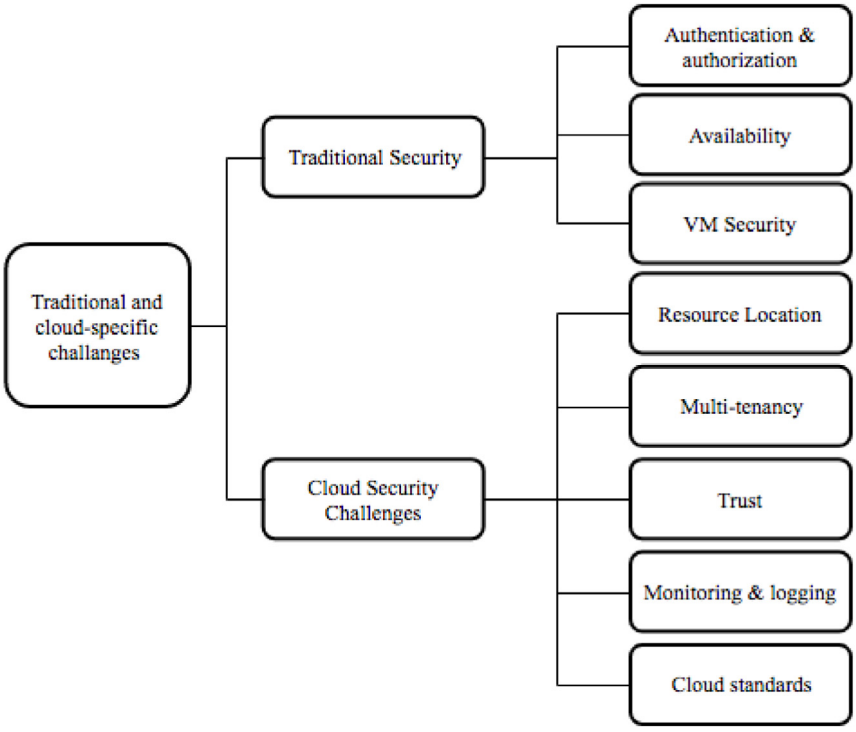


Fig. 19. A taxonomy illustrating our interpretation of traditional and cloud specific security challenges.

to NIST[8]'s conceptual model. For instance, in a scenario where cloud consumers utilize SaaS applications to process data, often without knowledge of how data is processed or where it resides, compliance and privacy issues arise [12]. Furthermore, legal challenges including e-discovery arise across jurisdictional boundaries. From a technical perspective, virtualization introduces vulnerabilities associated with isolating VMs on shared physical infrastructure, hypervisor vulnerabilities that may result in data leakages, malicious attempts to sniff traffic, compromised cryptographic keys and other confidential data [12]. Typically, one of cloud computing's main advantages for an organization is the reduction in management and maintenance costs associated with computing infrastructure, including the security. In this context, trust is assumed as shared between the cloud provider and the consumer [82]. However, considering vulnerabilities in multi-tenancy, virtualization, 3rd parties and shared infrastructure, trust concerns arise due to the subjective, context-based, imprecise and often transitive nature of trust [82]. According to [5], depending on the cloud model, trust is an obscure property due to the loss in the governance of data and applications associated with outsources services (see Figs. 9–11).

4.2. Holistic taxonomy

Current literature bespeaks a large and growing interest in classifying cloud security challenges. As evidenced in this paper, tremendous efforts also propose countermeasures, security frameworks and other recommendations to the said security challenges. However, this paper observes that security concerns are classified according to an aspect of the cloud or cloud component. Due to multiple perspectives, it is the view of the current authors that inadequately classified security issues will prevail despite much security spending. Fig. 12 summarizes these

8 http://www.nist.gov/itl/idms/.

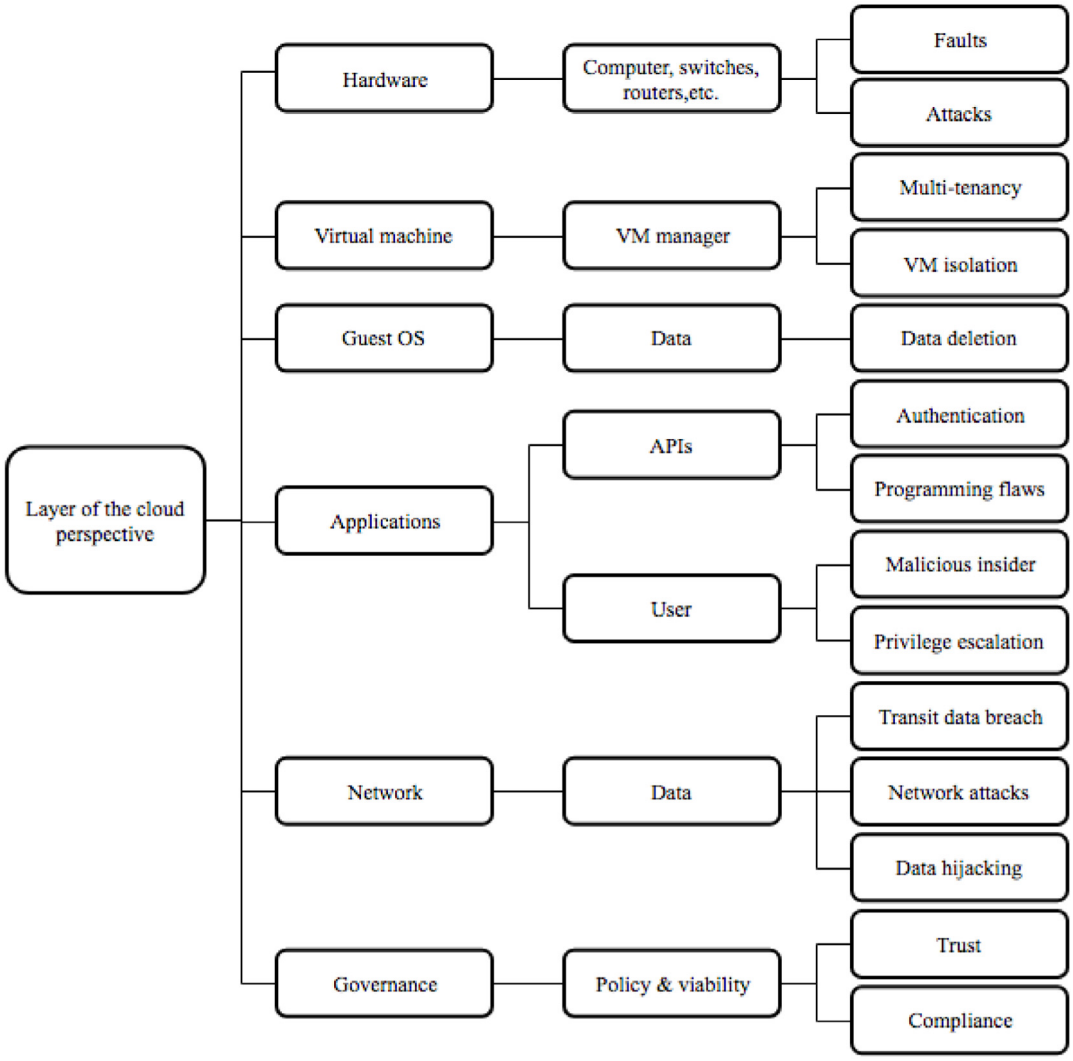


Fig. 20. A taxonomy illustrating our interpretation of cloud security challenges according to the layer of the cloud they affect.

perspectives for reference's sake and place the current paper's proposition into context.

This paper presents a holistic view of the security issues affecting cloud computing. Unlike taxonomies in current literature, it is anticipated that the holistic view facilitates comprehensive security analysis and the development of robust cloud security countermeasures. While holistic proposition is placed in retrospect to perspective-driven classifications, contributions including, [5,12,22,27,32,37,55,58,59] and [83] are substantial to the current proposition.

Building upon the analysis of cloud computing security challenges, their classifications and the important components of the cloud security paradigm, the categories upon which this paper's proposed holistic taxonomy are defined. Foremost, as this paper's origin/source hypothesis alludes, the base root of the holistic taxonomy comprises three main levels, herein coded A, B and C in Fig. 13. For reference's sake, the illustration (Fig. 2) identifies these. Subsequent levels, e.g. A1, B1, C1, etc. sub-levels e.g. A1-T, B1-T, C1-NT, etc. sub–sub-levels e.g. A1TD1-Att1, B1TD1-Att1, C1TD1-Att1, etc. branch out horizontally (from left to right) forming a tree-like structure as illustrated in Fig. 13 and detailed in Table 3 that follows. To capture the multiple perspectives obtained through research into the taxonomy generation, vertical categories (code and issue), herein named Cat 0, 1, 2, 3, 4, and 5, are integrated. From the root, Cat 0 represents the proposed three sources of cloud security incidents. Below are brief descriptions of the proposed categories which outline the new and unique opportunities each affords to the general cloud-wide concept:

- **Cat 0:** Regardless of perspective or view of the cloud, this category distinguishes security challenges based upon their source or their origin; challenges emanating from cloud's peripherals, including traditional security challenges which were in existence pre-cloud resurgence, challenges considered to originate from cloud implementations including new technologies and challenges which are inherent to the nature of the cloud architecture. This definition of Cat 0 is in line with [84] who claim security in the cloud as being both internal and external of the cloud. This paper takes the view that the ability to locate the source/origin of a security challenge presents a clear opportunity for applying specific security measures based upon that origin or source, and where necessary, tracing the source. Hence Same Origin Policy (SOP) can be applied at Cat 0, where monitoring of the original location of a request web request for instance, enabling validation of that requests [85].
- **Cat 1:** This category consists of two corresponding subclasses which provide slightly more detail into the nature of the challenges described in Cat 0. For instance, traditional security challenges and trends such as bring your own device (BYOD) as subsets of security challenges that originate

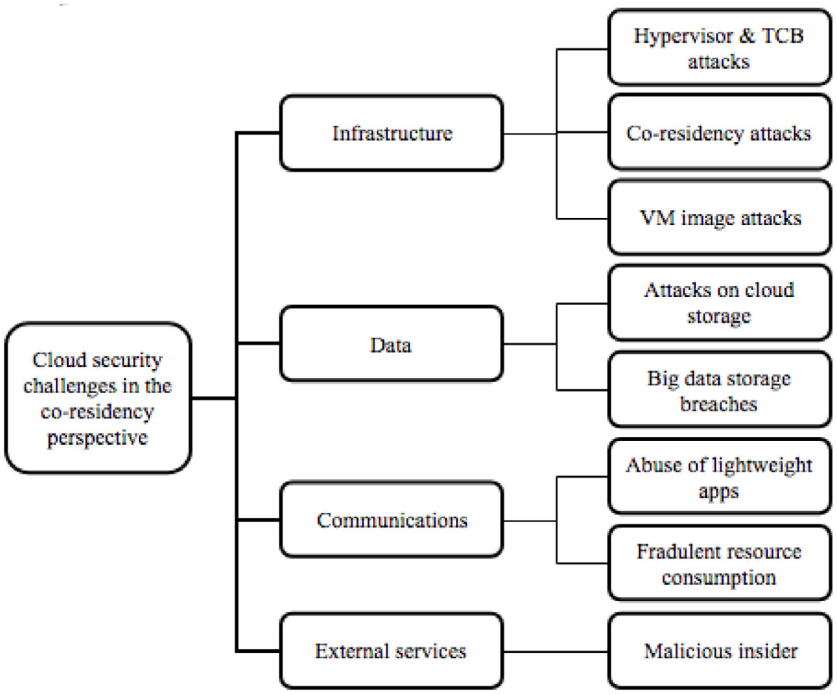


Fig. 21. A taxonomy of cloud security challenges from a co-residency perspective.

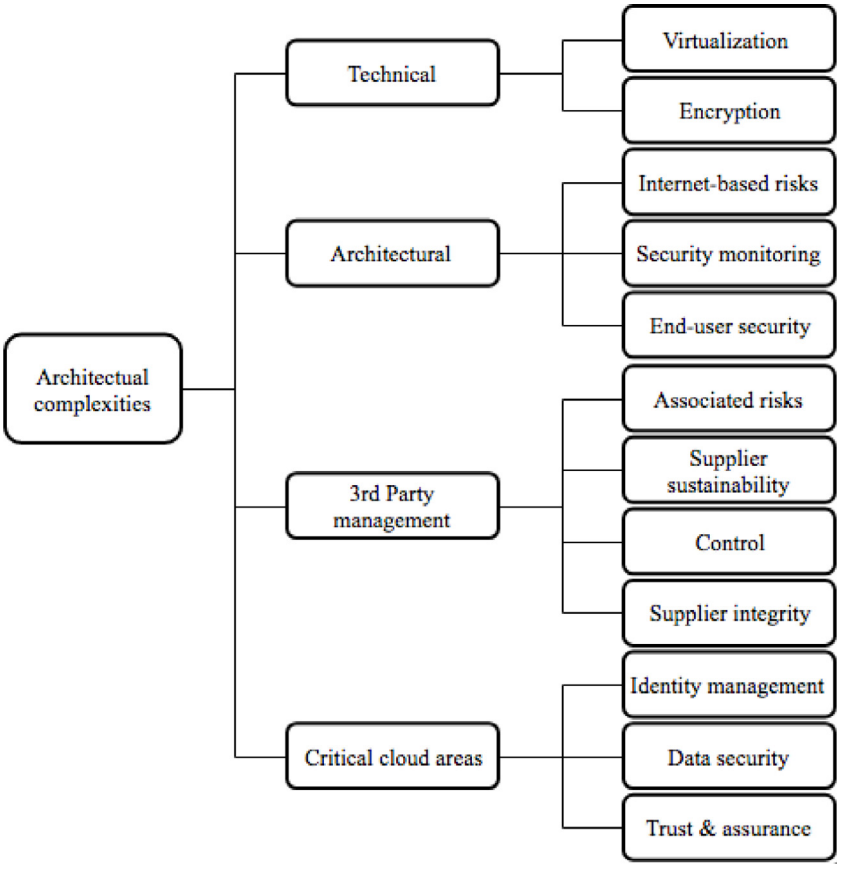


Fig. 22. A taxonomy illustrating cloud security challenges due to architectural complexities.

from the cloud's peripherals. In addition, challenges considered as architectural and business in nature including those which distinctly exist in the cloud due to the architecture of cloud computing, for instance, multi-tenancy. Likewise, infrastructural and business challenges to describe issues that are a result of cloud implementations, for instance control over OS and application settings that is prevalent in SaaS.

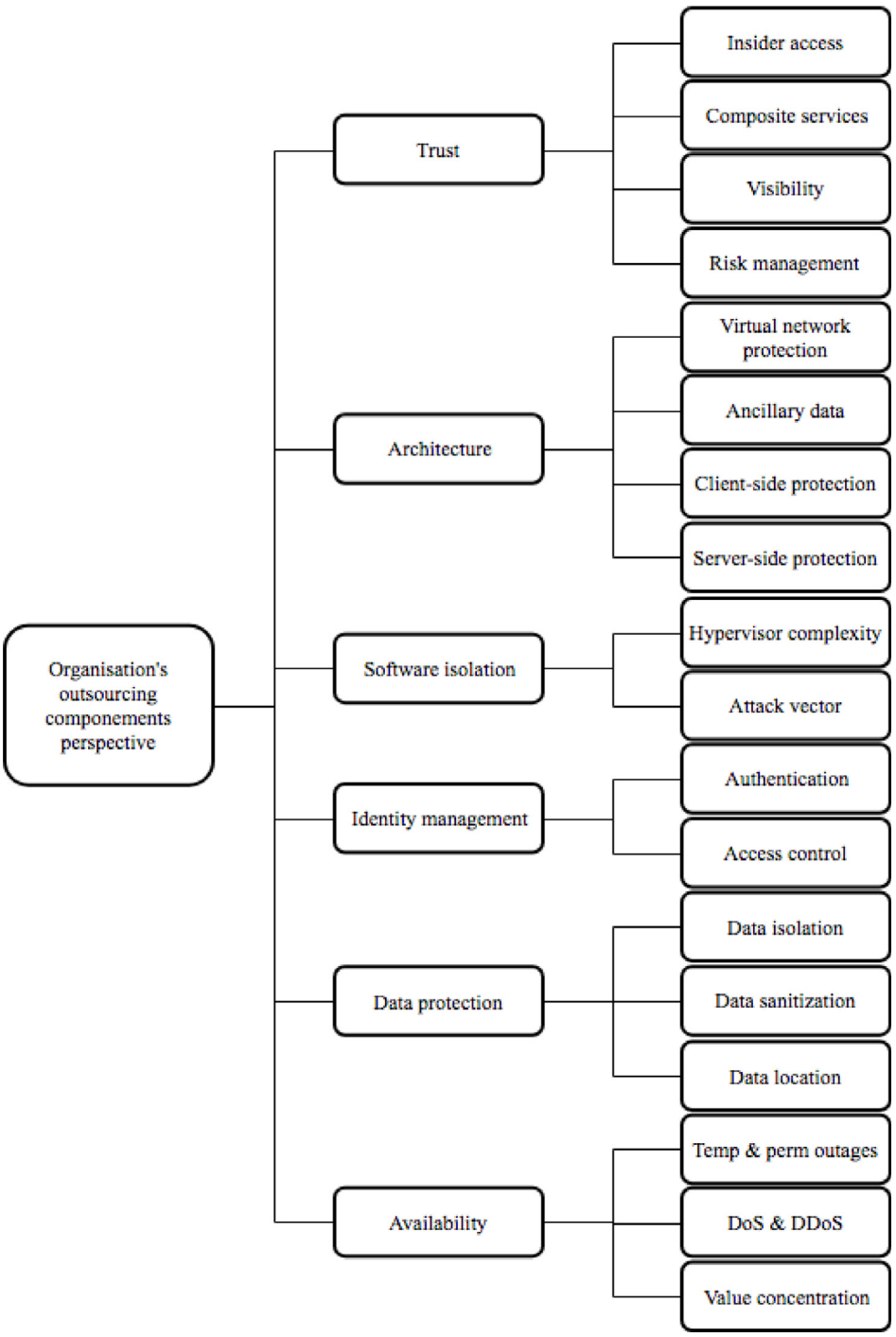


Fig. 23. A taxonomy of cloud security challenges highlighting the outsourcing components of an organization.

- **Cat 2**: Represents a common view that security in the cloud is considered as being technical or non-technical. By distinguishing security challenges in this manner, this paper anticipates efficient prioritizing and decision making, for instance business priorities that would attend to concerns such as governance and policy matters.
- **Cat 3**: This category provides detailed descriptions of the technical and non-technical aspects in the preceding in category (Cat 2). Put into perspective, Cat 3 describes traditional security challenges (Cat 1) emanating from cloud's peripherals (Cat 0) and technical in nature (Cat 2), but only exist upon elevation in the cloud (Cat 3). From an architectural perspective, Cat 3 describes technical challenges pertaining to the consumer and provider and non-technical challenges pertaining to the broker, carrier and auditor. Likewise, from an infrastructure perspective, technical challenges pertain to deployment and service models.
- **Cat 4:** This category describes attributes that have a direct impact on security, for instance, networking attributes in the traditional sense result in network attacks such as the man-in-middle or DoS. Similarly, attributes that describe data result in data breaches, etc. Virtual layer attributes result in multi-tenancy, virtual machine management (VMM) and hypervisor security issues.
- **Cat 5:** As we have illustrated throughout this paper, there are many security challenges that affect the CSP, consumer,

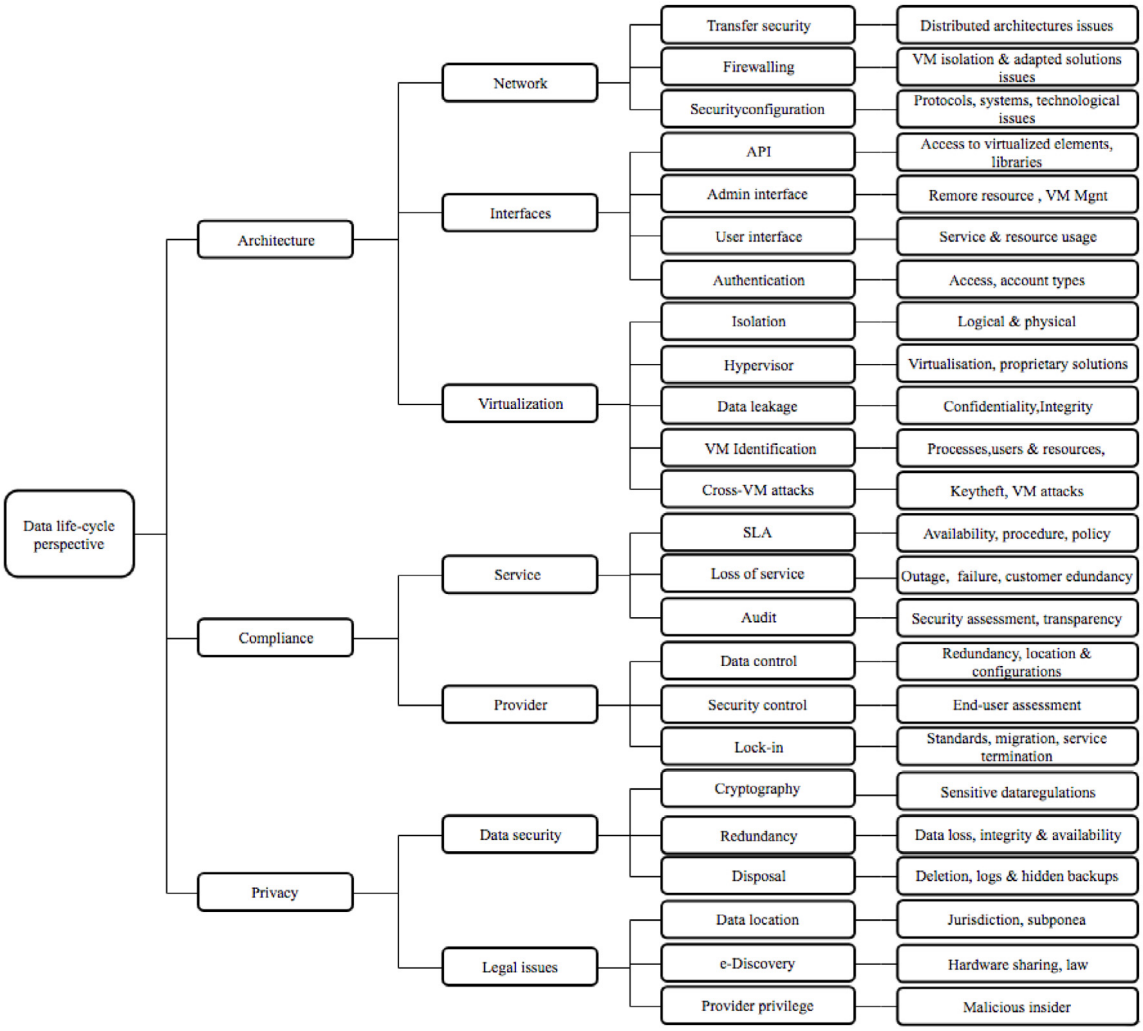


Fig. 24. A taxonomy illustrating cloud security challenges from a data lifecycle perspective.

carrier, auditor and the broker. This category identifies a spectrum of security challenges covering the entire cloud domain. We contend that this category is not exhaustive, thus, security challenges listed in this category exist for illustrative purposes.

4.3. Analysis

The goal of our proposed taxonomy is to enhance the security posture of cloud computing, both as a tool for security systems design and research. Focus should be firmly placed on identifying security challenges based on their source/origin, gradually progressing to the actual security incident. By considering source/origin as the root of the proposed classification and not the security issues first, this paper's considerations highlight a critical phase (planning) which is significant when designing and implementing security countermeasures. It is thus opinioned in this paper, that the proposed holistic taxonomy enables better planning for security design and provides contextual illustration of the relationship between cloud computing and its peripherals for research analysis. For instance, Cat 1 considers and allows for planning and designing solutions which should map any organization's objectives including their security requirements. For this reason, trends such as Big Data and BYOD are at the same level as business processes and procedures, as well as the security issues in the architecture and infrastructure. Thus, is one imagines a production environment, Cat 0 and Cat 1 attends to issues at the perimeter-level of security, thus enabling organizations to make use of their existing security technologies. This is an important addition considering deficiencies in that existing taxonomies including [58,69,86], and [55] to name a few. To address the limitations inherent to single-perspective approaches, the holistic taxonomy integrates Cat 3 as illustrative of NIST's view of cloud's computing; cloud entities, attributes and models.

To improve security in cloud computing environments, it is contingent upon how organizations are prepared to avoid or minimize the impact of insecurity. This readiness is what determines the appropriate security solution and the degree of proactiveness to ensure that unforeseen events or black swan events are well-prepared for. Employing the most appropriate countermeasures in the cloud includes applying the correct mechanisms (tools, techniques, procedures and approaches), correctly presented requirements and adequate policy that defines the lower and up boundaries of what is allowed and what is not allowed. These approaches can be matured with this paper's holistic taxonomy. Several techniques and approaches to secure cloud environment exist, some focusing on the technicality of achieving a security design, while others focus on the approach. For instance, CloudProtect is designed to provide privacy and confidentiality in the cloud [87]. [88] Conceptual Cloud Incident Handling model addresses security from the cost perspective of an incident handling investment, cost of incident detection and analysis, the cost of responding to an incident and post response cost.

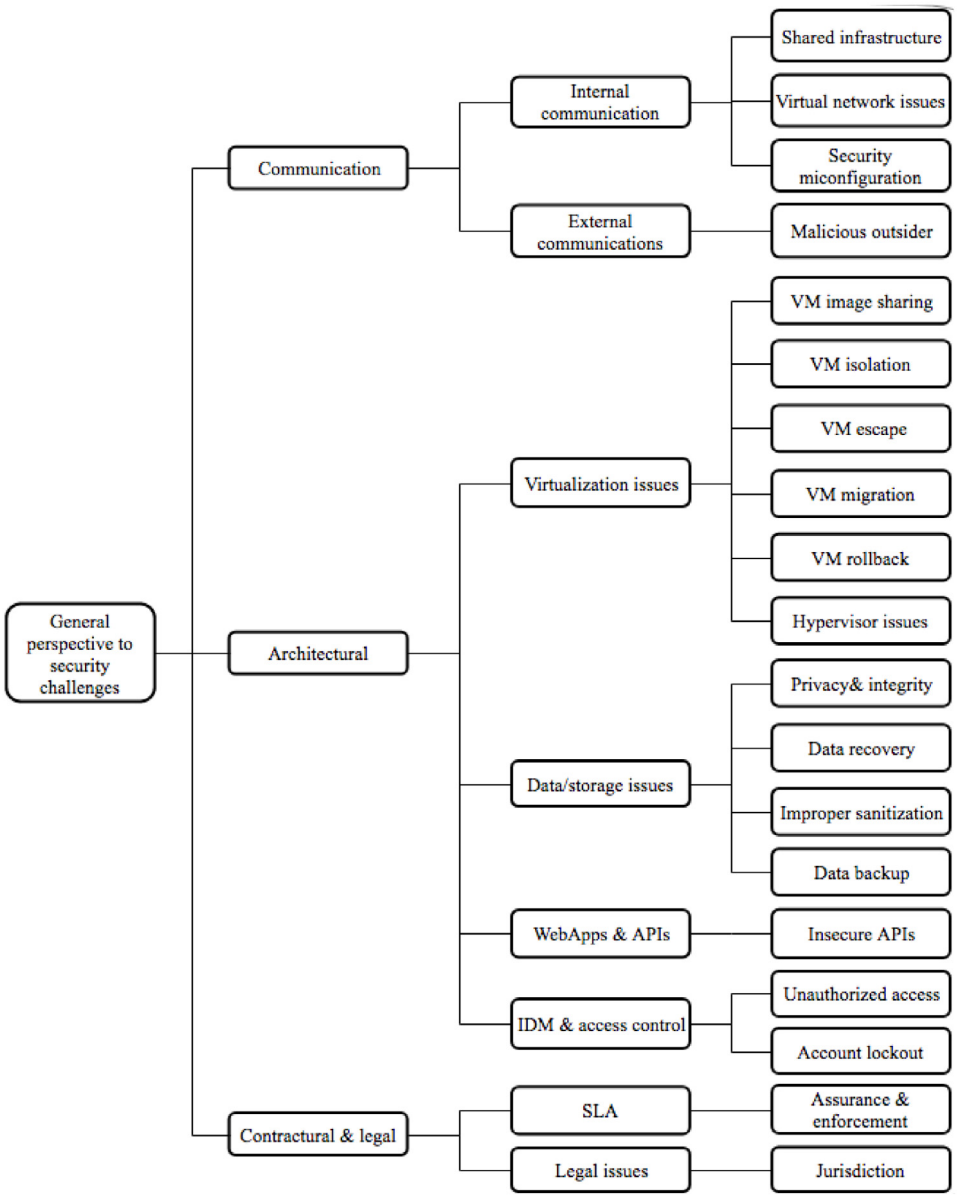


Fig. 25. A taxonomy of cloud security challenges by Ali et al. [2015].

Due to the volumes of literature on cloud security, is it clear that the current research does not represent every class of opinion in this continuum. However, this current research fuses consensus viewpoints of what constitutes the most prominent and current security concerns from academia and industry. It is our opinion that our paper provides substantial adds to the growing body of literature on cloud security challenges. Nonetheless, the proposed taxonomy highlights challenges that remain open. For instance, developing taxonomies based on interpreting corpus textual data is a tedious process and as such, prone to errors and omissions. However, this does not invalidate the contributions of this paper but rather provides a basis for further discussions. In fact, the current holistic taxonomy can be extended to include emergent phenomenon such a complexity and dynamicity of the environment. These phenomena are however not addressed in the current paper. The holistic approach to cloud security challenges proposed in the current paper is unambiguous as it integrates the entirety of cloud computing; services, entities, attributes, layers, characteristics, etc. linking all perspectives of the cloud into non-specific categories (Cat 0–Cat 5). By this manner of distinction, each category represents a branch of potential security incidents. This comprehensively organized taxonomy eliminates gaps introduced by perspective-driven views of the cloud and provides a basis for further research while aiding in developing security strategies.

Another clear opportunity is the possibility to enforce accountability in any cloud entity, including the enforcement of punitive or corrective measures through easier identification of the source or origin of a security incident. For an incident response point of view, the ability to identify the source/origin of a security incident means response teams spend more time implementing mitigation measures, rather than trying to identify the incident. From a defensive security point-of-view, this proposed holistic taxonomy highlights security boundaries, including where security systems can be placed.

Table 3
Detailed information for coding and issues in the categories and levels of the holistic taxonomy illustrated above in Fig. 13.

CAT 0		CAT 1		CAT 2		CAT 3		CAT 4		CAT 5	
Code	Issue	Code	Issue	Code	Issue	Code	Issue	Code	Issue	Code	Unique Issues
A	From cloud peripherals	A1	*Traditional*	A1-T	*Technical*	A1TD1	Elevated traditional issues	A1TD1-Att1	Network	AU*1	Network attacks, DoS
								A1TD1-Att2	Data	AU*2	Breaches
				A1-NT	*Non-technical*	A1NTD1	Processes & procedures	A1NTD1-Att1	Governance & Policy	AU*3	CIA & AAA
		A2	*Trends*	A2-T	*Technical*	A2TD1	BYOD	A2TD1-Att1	Data & Network	AU*4	Malicious software & outsider
						A2TD2	Big data	A2TD2-Att2	Data	AU*5	Privacy, isolation, breaches
				A2-NT	*Non-technical*	A2NT1	Outsourcing	A2NT1 -Att1	3rd parties	AU*6	Trust, control & compliance
B	Existing in cloud architecture	B1	*Architectural*	B1-T	*Technical*	B1TD1	Consumer	B1TD1-Att1	Virtual	BU*1	Multi-tenancy
								B1TD1-Att2	Network	BU*2	Malicious insider
								B1TD1-Att3	Data storage	BU*3	Malicious insider
						B1TD2	Provider	B1TD2-Att1	Virtual	BU*4	Hypervisor
										BU*5	VM management
								B1TD2-Att2	Network	BU*6	Availability
								B1TD2-Att3	Data storage	BU*6	Isolation
										BU*7	Deletion
										BU*8	Breaches
				B1-NT	*Non-technical*	B1NTD1	Broker	B1NTD1-Att1	Policy	BU*9	Compliance
								B1NTD1-Att2	Governance	BU*10	Data governance
						B1NTD2	Carrier	B1NTD2-Att1	Policy	BU*11	Service reliability & availability
								Att2	Governance	BU*12	Privacy
						B1NTD3	Auditor	B1NTD3-Att1	Policy		Monitoring & logging
								Att2	Governance	BU*13	Assurance
		B2	*Business*	B2-NT	Non-*technical*	B2NTD1	Processes & procedures	B2NTD1-Att1	Governance & Policy	BU*14	LSAs & Standards
C	Because of cloud infrastructure	C1	*Infrastructural*	C1-T	*Technical*	C1TD1	Deployment	C1TD1-Att1	Private	CU*1	Complex attacks
										CU*2	Availability-central failure
								C1TD1-Att2	Public	CU*3	Trust
										CU*4	Control
								C1TD1-Att3	Hybrid	CU*5	Compliance & control
										CU*6	Fault propagation
						C1TD2	Services	C1TD2-Att1	Software	CU*7	Data breaches, hijacking & deletion
								C1TD2-Att2	Platform	CU*8	Unauthorized users & insecure APIs
								C1TD2-Att3	Infrastructure	CU*9	DDoS, traffic analysis & abuse of cloud
		C2	Business	C2-NT	Non-technical	C2NTD1	Processes & procedures	C2NTD1-Att1	Governance & Policy	CU*10	LSA & standards

In order to determine effective measures for cloud security, future work could extend on current findings to explore suitable mechanisms for securing virtualized and distributed environments. For instance, it may be necessary to explore a grading system (e.g. usefulness and importance scales) applicable through the taxonomy (at each level and category). For instance, one could consider evaluating the usefulness of level A; Cat 0, Cat 1, Cat 2, and the level of importance to an infrastructure or an organization. One could simply apply a usefulness-importance

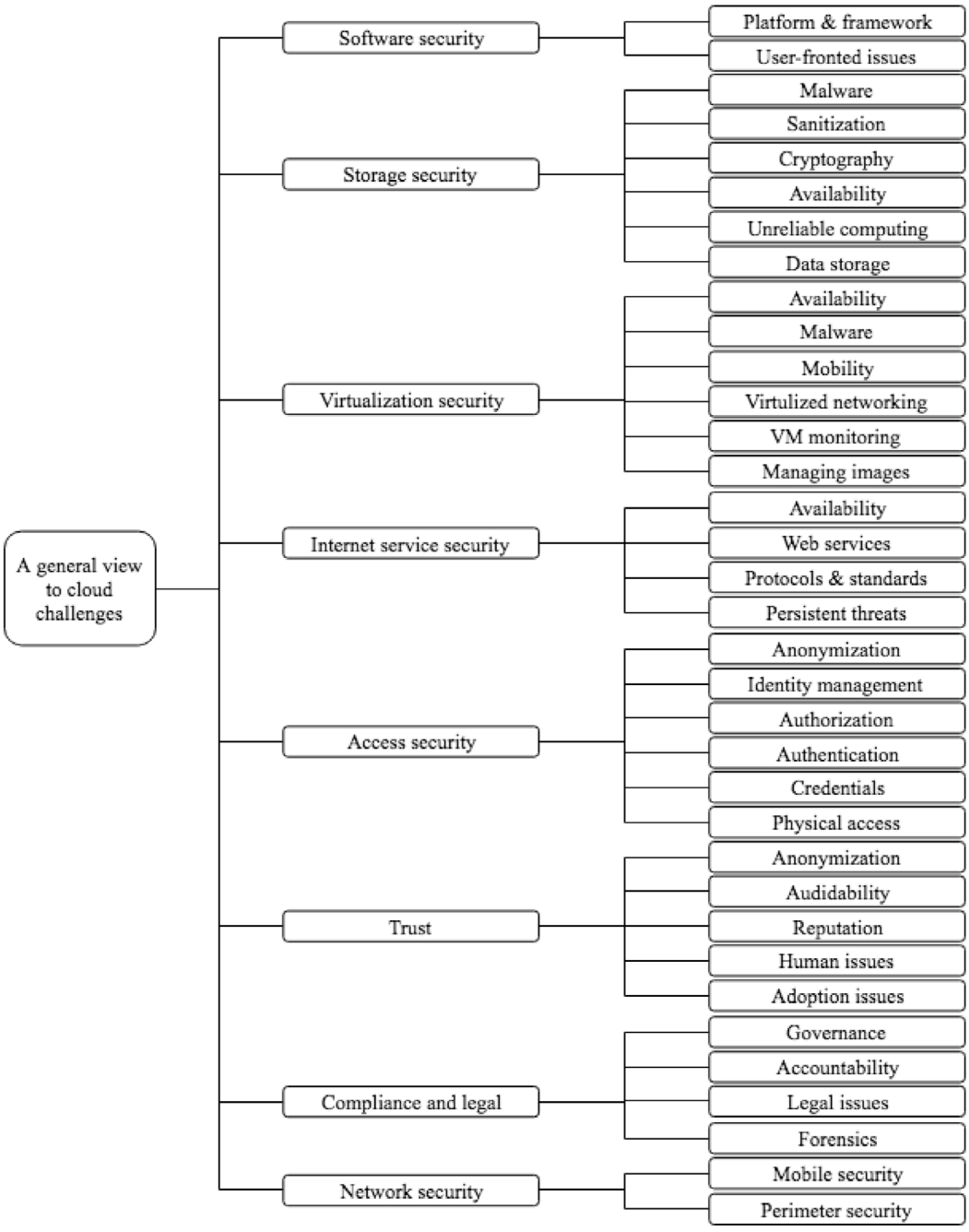


Fig. 26. A taxonomy illustrating our interpretation of a general view of cloud security challenges.

scale to facilitate the holistic approach suggested in this paper; vertically and horizontally, as shown in the illustration in Fig. 14.

5. Conclusions

Opportunities for technological innovation and advancement are abound in ideal cloud computing environment. However, the cloud paradigm and cloud's attributes introduce new challenges as dynamism and complexity renders static traditional security systems ineffective. Moreover, confidentiality is threatened by the very fact that data resident on the cloud provider's infrastructure is left at that provider's mercy, including the provider's employees. We share a common view with [69] that, the focus on achieving security is currently handled by legislation, contracts and good practices. This paper clearly demonstrates a lack of holistic and comprehensive classification of cloud security challenges, but rather multiple atomistic classifications. This is subsumed in the current paper, to suggest in part, the multi-faceted nature of the cloud. Nonetheless, despite an abundance of literature on cloud security, textual classifications fail to organize information into an easy, error-free, non-tedious and comprehensive manner useful for solutions design and research. To address this shortcoming, this paper synthesized available textual classifications to produce simple figures (See the Appendix section). By reconceptualizing classifications in this graphical format, this paper immensely contributes to the cloud continuum as it enhances visualization for the reader. As technology advances and the cloud evolves, the proposed holistic taxonomy is envisaged to be useful and scalable horizontally left to right and vertically up and down. It will be necessary in our future work nonetheless to

establish how cloud security challenges stack against the existing countermeasures, with the benefit of hindsight on this holistic view hypothesized here. With such a mapping, one can expect significant strides towards developing robust security approaches that can scale enough to overhaul current cloud security issues.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix

See Figs. 15–26.

References

[1] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, D. Sabella, On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration, IEEE Commun. Surv. Tutor. (2017).

[2] Amazon Web Services, Amazon Elastic Compute Cloud, Amazon EC2, Vol. 2010, Amaz. Web Serv. LLC, 2011.

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

[4] P. Mell, T. Grance, The NIST definition of cloud computing, 2011.

[5] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Gener. Comput. Syst. 28 (3) (2012) 583–592.

[6] N. Shahriar, R. Ahmed, S.R. Chowdhury, A. Khan, R. Boutaba, J. Mitra, Generalized recovery from node failure in virtual network embedding, IEEE Trans. Netw. Serv. Manag. 14 (2) (2017) 261–274.

[7] Gartner, Gartner research, 2015, [Online]. Available: https://www.gartner.com/en. (Accessed 20 February 2015).

[8] Cloud Security Allience, Cloud security allience, 2015, [Online]. Available: https://cloudsecurityalliance.org/. (Accessed 20 February 2015).

[9] Verizon, Data Breach Investigation Report, 2015, [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/. (Accessed 20 February 2015).

[10] M. Johns, Code-injection vulnerabilities in web applications-exemplified at cross-site scripting, IT-Inform. Technol. Methoden Innov. Anwend. Inform. Informationstech. 53 (5) (2011) 256–260.

[11] F. Lombardi, R. Di Pietro, Secure virtualization for cloud computing, J. Netw. Comput. Appl. 34 (4) (2011) 1113–1122.

[12] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, J. Netw. Comput. Appl. 34 (1) (2011) 1–11.

[13] A. Roy, S. Sarkar, R. Ganesan, G. Goel, Secure the cloud: From the perspective of a service-oriented organization, ACM Comput. Surv. 47 (3) (2015) 41:1–41:30.

[14] J.D. Howard, T.A. Longstaff, A Common Language for Computer Security Incidents, Sandia Natl. Lab, 1998.

[15] K. Malterud, Qualitative research: standards, challenges, and guidelines, Lancet 358 (9280) (2001) 483–488.

[16] S. Keele, Guidelines for performing systematic literature reviews in software engineering, 2007.

[17] C.A. Ardagna, R. Asal, E. Damiani, Q.H. Vu, From security to assurance in the cloud, ACM Comput. Surv. 48 (1) (2015) 1–50.

[18] C. Zott, R. Amit, L. Massa, Y. Zhu, Financial consumer protection and the global financial crisis, J. Consum. Res. 15 (2) (2012) 1–6.

[19] F. Liu, et al., NIST Cloud Computing Reference Architecture, Vol. 500, NIST Spec. Publ., 2011, p. 292.

[20] T. Baars, M. Spruit, Analysing the security risks of cloud adoption using the SeCA model: A case study, J. UCS 18 (12) (2012) 1662–1678.

[21] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, you, get off of my cloud, in: Proc. 16th ACM Conf. Comput. Commun. Secur., CCS '09, 2009, p. 199.

[22] Y. Liu, Y. Sun, J. Ryoo, S. Rizvi, A.V. Vasilakos, A survey of security and privacy challenges in cloud computing: Solutions and future directions, J. Comput. Sci. Eng. (2015).

[23] Y. Chen, V. Paxson, R.H. Katz, What's New About Cloud Computing Security, Rep. No.UCB/EECS-2010-5 January, vol. 20, no. 2010, Univ. California, Berkeley, 2010, pp. 2010–2015.

[24] L. Bilge, T. Strufe, D. Balzarotti, E. Kirda, All your contacts are belong to us: automated identity theft attacks on social networks, in: Proceedings of the 18th International Conference on World Wide Web, 2009, pp. 551–560.

[25] F. Ahamed, S. Shahrestani, A. Ginige, Cloud computing: Security and reliability issues, Commun. IBIMA 2013 (2013) 1.

[26] M. Henning, API design matters, Queue 5 (4) (2007) 24–36.

[27] K. Hashizume, N. Yoshioka, E.B. Fernandez, Three misuse patterns for cloud computing, Secur. Eng. Cloud Comput. Approaches Tools (2013) 36–53.

[28] A. Amittai, H. Sen, F. Bryan, G. Ramakrishna, Determinating Timing Channels in Compute Clouds, in: Proceedings of the 2010 ACM workshop on Cloud computing security workshop, 2010, pp. 103–108.

[29] Y. Xu, M. Bailey, F. Jahanian, K. Joshi, M. Hiltunen, R. Schlichting, An exploration of L2 cache covert channels in virtualized environments, in: Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, 2011, pp. 29–40.

[30] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, in: Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 199–212.

[31] R. Krebs, C. Momm, S. Kounev, Architectural concerns in multi-tenant SaaS applications, Closer 12 (2012) 426–431.

[32] F. Shahzad, State-of-the-art survey on cloud computing security challenges, approaches and solutions, Proced. Comput. Sci. 37 (2014) 357–362.

[33] P.G. Dorey, A. Leite, Commentary: Cloud computing-A security problem or solution? Inf. Secur. Tech. Rep. 16 (3) (2011) 89–96.

[34] Y. Demchenko, C. Ngo, C. De Laat, T.W. Wlodarczyk, C. Rong, W. Ziegler, Security infrastructure for on-demand provisioned cloud infrastructure services, in: Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on, 2011, pp. 255–263.

[35] A. Singh, K. Chatterjee, Cloud security issues and challenges: A survey, J. Netw. Comput. Appl. 79 (2016) (2017) 88–115.

[36] N.H. Hussein, A. Khalid, A survey of Cloud Computing Security challenges and solutions, Int. J. Comput. Sci. Inf. Secur. 14 (1) (2016) 52.

[37] M. Almorsy, J. Grundy, I. Müller, An analysis of the cloud computing security problem, 2016, arXiv:1609.01107 [cs].

[38] M. Daghmehchi Firoozjaei, J. (Paul) Jeong, H. Ko, H. Kim, Security challenges with network functions virtualization, Future Gener. Comput. Syst. 67 (2017) 315–324.

[39] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, Secur. Priv. IEEE 9 (3) (2011) 49–51.

[40] L. Bilge, T. Dumitras, Before we knew it: an empirical study of zero-day attacks in the real world, in: Proc. 2012 ACM Conf. Comput. Commun. Secur., CCS'12, 2012, pp. 833–844.

[41] B.B. Gupta, O.P. Badve, Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment, Neural Comput. Appl. (2017).

[42] O. Yevsieieva, S.M. Helalat, Analysis of the impact of the slow HTTP DOS and DDOS attacks on the cloud environment, in: 2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 - Proceedings, 2018.

[43] N. Gruschka, M. Jensen, Attack surfaces: A taxonomy for attacks on cloud services, in: Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010, 2010.

[44] A. Razzaq, K. Latif, H. Farooq Ahmad, A. Hur, Z. Anwar, P.C. Bloodsworth, Semantic security against web application attacks, Inf. Sci. (Ny) (2014).

[45] M. Ter Louw, V.N. Venkatakrishnan, Scripting attacks for existing browsers, in: Proceedings - IEEE Symposium on Security and Privacy, 2009.

[46] X. Li, Y. Xue, A survey on server-side approaches to securing web applications, ACM Comput. Surv. (2014).

[47] K.S. Schwaig, et al., Xml security, Secur. Priv. Trust Mod. Data Manag. 2 (2) (2014) 1–6.

[48] V.R. Mouli, K.P. Jevitha, Web services attacks and security- a systematic literature review, Procedia Comput. Sci. (2016).

[49] D. Hubbard, M. Sutton, Top Threats to Cloud Computing v1. 0, Cloud Secur. Alliance, 2010.

[50] L. Bello, A. Russo, Towards a taint mode for cloud computing web applications, in: Proceedings of the 7th Workshop on Programming Languages and Analysis for Security, 2012, p. 7.

[51] S. Kandula, D. Katabi, M. Jacob, A. Berger, Botz-4-sale: Surviving organized DDoS attacks that mimic flash crowds, in: Proceedings of the 2nd Conference on Symposium on Networked Systems Design & Implementation-Volume 2, 2005, pp. 287–300.

[52] A.C. Mora, Y. Chen, A. Fuchs, A. Lane, R. Lu, P. Manadhata, Top Ten Big Data Security and Privacy Challenges, Vol. 140, Cloud Secur. Alliance, 2012, November.

[53] S. Browne, M. Lang, Cloud security consciousness: A need for realisation, in: Entrepreneurial Small Firms, 2014.

[54] M.U. Farooq, M. Waseem, A. Khairi, S. Mazhar, A critical analysis on the security concerns of internet of things (IoT), Int. J. Comput. Appl. 111 (7) (2015).

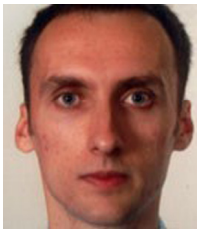
[55] M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: Opportunities and challenges, Inf. Sci. (Ny) 305 (2015) 357–383.

[56] M.T. Khorshed, A.B.M.S. Ali, S.A. Wasimi, Classifying different denial-of-service attacks in cloud computing using rule-based learning, Secur. Commun. Netw. 5 (11) (2012) 1235–1247.

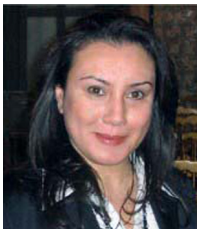
[57] F. Rocha, M. Correia, Lucy in the sky without diamonds: Stealing confidential data in the cloud, in: Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on, 2011, pp. 129–134.
[58] A. Roy, S. Sarkar, R. Ganesan, G. Goel, Secure the cloud, ACM Comput. Surv. 47 (3) (2015) 1–30.
[59] N. Gonzalez, et al., A quantitative analysis of current security concerns and solutions for cloud computing, J. Cloud Comput. 1 (1) (2012) 1–18.
[60] M.T. Khorshed, et al., Data security and privacy protection issues in cloud computing, Future Gener. Comput. Syst. 2 (1) (2012) 1–5.
[61] W. Jansen, T. Grance, Guidelines on Security and Privacy in Public Cloud Computing, Vol. 800, NIST Spec. Publ, 2011, p. 144.
[62] A. Bisong, M. Rahman, An overview of the security concerns in enterprise cloud computing, 2011, arXiv Prepr. arXiv:1101.5613.
[63] M.K. Srinivasan, K. Sarukesi, P. Rodrigues, M.S. Manoj, P. Revathy, State-of-the-art cloud computing security taxonomies - A classification of security challenges in the present cloud computing environment, in: Proc. Int. Conf. Adv. Comput. Commun. Informatics - ICACCI '12, 2012, p. 470.
[64] S. Ramgovind, M.M. Eloff, E. Smith, The management of security in cloud computing, in: Information Security for South Africa, ISSA, 2010 (2010) 1–7.
[65] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, Cloud computing-The business perspective, Decis. Support Syst. 51 (1) (2011) 176–189.
[66] F. Polash, A. Abuhussein, S. Shiva, A survey of cloud computing taxonomies: Rationale and overview, in: Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for, 2014, pp. 459–465.
[67] A. Botta, W. de Donato, V. Persico, A. Pescapé, Integration of cloud computing and internet of things: a survey, Future Gener. Comput. Syst. 56 (2016) 684–700.
[68] M. Díaz, C. Martín, B. Rubio, State-of-the-art, challenges and open issues in the integration of Internet of things and cloud computing, J. Netw. Comput. Appl. (2016).
[69] M.D. Ryan, Cloud computing security: The scientific challenge, and a survey of solutions, J. Syst. Softw. 86 (9) (2013) 2263–2268.
[70] C. Rong, S.T. Nguyen, M.G. Jaatun, Beyond lightning: A survey on security challenges in cloud computing, Comput. Electr. Eng. 39 (1) (2013) 47–54.
[71] M. Chraibi, H. Harroud, A. Maach, Classification of security issues and solutions in cloud environments, in: Proceedings of International Conference on Information Integration and Web-based Applications & Services, 2013, p. 560.
[72] W. Jansen, Cloud hooks: Security and privacy issues in cloud computing, in: System Sciences (HICSS), 2011 44th Hawaii International Conference on, 2011, pp. 1–10.
[73] I. Khalil, A. Khreishah, M. Azeem, Cloud computing security: A survey, Computers 3 (1) (2014) 1–35.
[74] N. Grant, T. Cadden, R. Mcivor, P. Humphreys, A taxonomy of manufacturing strategies in manufacturing companies in Ireland, J. Manuf. Technol. Manag. (2013).
[75] R.C. Nickerson, U. Varshney, J. Muntermann, A method for taxonomy development and its application in information systems, Eur. J. Inf. Syst. (2013).
[76] S. Pearson, A. Benameur, Privacy, security and trust issues arising from cloud computing, in: 2010 IEEE Second Int. Conf. Cloud Comput. Technol. Sci., 2010, pp. 693–702.
[77] R. Yu, et al., Cooperative resource management in cloud-enabled vehicular networks, IEEE Trans. Ind. Electron. 62 (12) (2015) 7938–7951.
[78] R. Chow, et al., Controlling data in the cloud, in: Proc. 2009 ACM Work. Cloud Comput. Secur., CCSW '09, 2009, p. 85.
[79] F. Sabahi, Cloud computing security threats and responses, in: Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, 2011, pp. 245–249.
[80] B. Grobauer, T. Walloschek, E. Stocker, Understanding cloud computing vulnerabilities, Secur. Priv. IEEE 9 (2) (2011) 50–57.
[81] H. Takabi, J.B.D. Joshi, G.-J. Ahn, Security and privacy challenges in cloud computing environments, IEEE Secur. Priv. (6) (2010) 24–31.
[82] D. Sun, G. Chang, L. Sun, F. Li, X. Wang, A dynamic multi-dimensional trust evaluation model to enhance security of cloud computing environments, Int. J. Innov. Comput. Appl. 3 (4) (2011) 200–212.
[83] D. Huang, H. Wu, Mobile cloud computing taxonomy, in: Mobile Cloud Computing, 2018.
[84] B.Y.M. Armbrust, et al., of cloud computing, Commun. ACM 53 (4) (2010) 50–59.
[85] J.C. R, W. Al-Hamdani, Who can you trust in the cloud?: a review of security issues within cloud computing, in: Proceedings of the 2011 Information Security Curriculum Development Conference, 2011, pp. 15–19.
[86] D.A.B. Fernandes, L.F.B. Soares, J.V. Gomes, M.M. Freire, P.R.M. Inácio, Security issues in cloud environments: a survey, Int. J. Inf. Secur. 13 (2) (2014) 113–170.
[87] C.A. Ardagna, R. Asal, E. Damiani, Q.H. Vu, From security to assurance in the cloud: A survey, ACM Comput. Surv. 48 (1) (2015) 2.
[88] N.H.A. Rahman, K.-K.R. Choo, A survey of information security incident handling in the cloud, Comput. Secur. 49 (2015) 45–69.

Siyakha N Mthunzi holds a B. Eng. degree in Computer and Networks Security from Staffordshire University. In April 2015, he joined the Ph.D. program in the School of Computing and Digital Technology at Staffordshire University. His research interests include areas of Bio-inspired design for Cyber Security and Distributed Networks, Cloud Computing, Survivability and Security, Edge and Fog Computing, Artificial Intelligence, and Internet of things. He is a Fellow of the Higher Education Academy.

Elhadj Benkhelifa is a Full Professor of Computer Science at Staffordshire University, UK/ He is the founding head of Cloud Computing and Applications Research Lab and the Research Lead for REF (Research Excellence Framework) for Computing and Informatics Unit of Assessment. Before that (2014–2016) Elhadj was the Faculty Director of the Mobile Fusion Applied Research Centre (45 Ph.D. students and 15+ Staff). Elhadj has published 120+ research papers in journals, conferences and book chapters and edited several conference proceedings and journals' special issues. He is the co-founder or number of successful IEEE international conferences and workshops. Elhadj' s research interest covers Artificial Life and biologically inspired systems, Cloud Computing including security and resilience, Mobile Cloud, Software Defined Systems, Cloud Forensics, IOT and Cloud, Fog and Mobile Edge Computing. Elhadj is also a Director at Yotta Laboratories Ltd and a Senior R&D Advisor to several companies in the UK.



Tomasz Bosakowski is a Senior lecturer at Staffordshire University in the School of Computing and Digital Tech. He holds M.Sc. and a Ph.D. Computer Science. Tomasz has lectured at Huddersfield University and an associate tutor at Edge Hill University. He is also a member of the university's Cisco teaching team and a qualified CISCO CCNA and CCNA Security instructor. Tomasz is also a member of the British Computer Society (BCS), and Associate Member of the BCS (AMBCS), 2011.



Chirine Ghedira Guegan is a full professor of computer sciences and co-head of the "service oriented computing" research team at Lyon Research Center for Images and Intelligent Information Systems associated with the French National Center for Scientific Research (CNRS) in Lyon, France. Her research interests include service-oriented architectures and computing; interoperability; complex, autonomic, and adaptive systems; context-aware computing; data services; privacy; and cloud computing. Chirine Ghedira Guegan has a research habilitation in computer science from Université de Lyon 1.

Mahmoud Barhamgi is an Associate Professor of Computer Science at Claude Bernard University Lyon 1. His research focuses on security and privacy preservation in service-oriented architecture, web, and cloud environments. Barhamgi received a Ph.D. in information and communication technology from Claude Bernard University Lyon 1. Contact him at mahmoud.barhamgi@univ-lyon1.fr.