Information Security Accountability in the Cloud Computing Context—A Comprehensive Review

Zahir Ahmed Al-Rashdi, Martin Dick, Rahma Ahmed Al-Rashdi, and Younis Al-Husaini

Abstract Accountability is a main concern for information security within cloud computing; it represents the trust in service relationships between clients and cloud service providers. Without evidence of accountability, a lack of trust and confidence in cloud computing is to be expected from decision-makers. Furthermore, a lack of accountability is considered as an added level of risk, especially since a client's essential services are controlled and managed by a third party. Therefore, this new outsourcing paradigm increases the challenge of maintaining data security and confidentiality, supporting data and service availability, and demonstrating compliance. This chapter presents a literature review on IS accountability. It sets out the different definitions of IS responsibility from the existing literature. This chapter reviews information security and cloud issues, and related security issues and how they relate to IS accountability in the context of cloud computing. The concept of Cloud computing along with the different types of cloud services is thoroughly described. The factors of accountability are also reviewed in this chapter. This chapter is made up of two main sections. The first section will focus on information security and explore IS Accountability in cloud services provisions. The second section will elaborate on the conceptual drivers of IS Accountability. These factors are Transparency, Responsibility, Assurance and Remediation. Finally, accountability for Cloud computing service relationships and all other aspects associated with IS Accountability will also be identified and explained.

Keywords Cloud computing · Information security · Information security accountability · Cloud service provision · Outsourcing · Accountability elements

Z. A. Al-Rashdi (✉)
Information Security Department, Sultan Qaboos University, Muscat, Oman
e-mail: zaher21@squ.edu.om

M. Dick · Y. Al-Husaini
RMIT University, Melbourne, VIC, Australia

R. A. Al-Rashdi
Keio University, Tokyo, Japan

R. Montasari et al. (eds.), *Challenges in the IoT and Smart Environments*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-87166-6_8

1 Introduction

This review provides an explanation of what Information Security Accountability (IS Accountability) in a Cloud computing context is, and how government organisations can ensure that it is present in Cloud computing service relationships. Although information security and privacy in relation to Cloud computing has received a great deal of attention from researchers in the field of information systems (Infosyss) [14, 71] and information security [72], yet, information security accountability in Cloud computing has not been studied in great depth. Furthermore, many of the studies concentrate on technical aspects such as encryption and preventive controls. Although technical aspects for cloud security and privacy have been actively researched, the focus on detective controls in relation to cloud accountability and auditability is scarce. Encryption and other privacy protection techniques will only manage a part of this problem. In addition, there is the problem of ensuring that security obligations are implemented by cloud service providers. According to Gartner, globally end-user expenditure on public cloud services would rise 18.4% to $304.9 billion in 2021, up from $257.5 billion in 2020 [23]. Thus, the enormous growth in moving businesses to Cloud computing, due to its flexibility, cost-effectiveness, scalability, and the perceived benefits of transference of data security and the absence of a specific Cloud computing accountability framework, highlights the growing need for research in this area. Research is needed into accountability and auditability of cloud service providers to affect both preventive and detective measures in ways that promote transparency, governance, and the accountability of the cloud service providers.

1.1 Evolution of Accountability

The principle of accountability is found in the well-known OECD Guidelines; in the laws of the European Union ("EU"), the EU member states, Canada and the United States; in emerging governance such as the APEC Privacy Framework and the Spanish Data Protection Agency's Joint Proposal for an International Privacy Standard. The Organisation for Economic Co-operation and Development (OECD) established accountability as a principle of data protection in 1980 and since then has played an increasingly important and visible role in privacy governance. The emergence of the accountability principle places responsibility on organisations as data controllers to comply with measures that give effect to all of the OECD principles [75]. In the European Union, the principle of accountability initially considered privacy protection including the implementation of processes by organisations, which in turn assessed how much data was to be collected, the usefulness and the usability of the collected data and the protection level required to ensure information security. The transfer of data outside the EU has been managed to ensure safe transfers of sensitive and personal data, which was addressed in the EU accountability principle in the data governance section [77]. In February 2009, The Spanish Data Protection Agency's established a basis for data transfers and created the Joint Proposal for an International Privacy Standard, which included the principle of accountability [78, 79]. The office of the Privacy Commission of Canada established the first principle of accountability in 2009 under Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) that soon became part of the law that relates to processing, storing and transferring data domestically and outside the Canadian border [76]. In the United States, the government has acted initiatively to enhance the principle of data protection and accountability by imposing legal obligations, Under the Gramm-Leach-Bliley Act, and the Safeguards Rule, enforced by the Federal Trade Commission, requires financial institutions to have a security plan to protect the confidentiality and integrity of personal consumer information [89]. The Center for Information Policy Leadership (CIPL) is working hard on the accountability approach in the digital world because much data has been migrated to cloud environments. CIPL has paid more attention to improving accountability in the public cloud and mobile services by presenting the main risk element associated with these two cloud environments [29, 62].

1.2 What is Information Security Accountability?

Accountability is a core concern for information security in Cloud computing, it represents the trust in service relationships between clients and cloud service providers (CSPs) [9]. Without evidence of accountability, a lack of trust and confidence in Cloud computing [11] is developed by decision-makers and considered as an added level of risk, which means a lack of accountability increases [9], especially since a client's essential services are controlled and managed by a third-party. Consequently, this new method of outsourcing renders the process of maintaining data security and privacy, supporting data and service availability, and demonstrating compliance far less transparent [27]. This makes it difficult for users to understand, influence and determine what security obligations are implemented by CSPs.

Many researchers indicate that accountability should be given more attention and treated as a high priority issue in terms of security [45, 50] as it affects the quality of service (QoS) [5, 56] as well as the grade of service (GoS) [5]. Generally, most users are seeking Assurance that their QoS and GoS requirements are satisfied and that their operations are not hindered due to congested cloud resources. Providing the required assurance measures and guarantees for both QoS and GoS is a challenging task. Furthermore, accountability—along with trust—are two major concepts that are considered foundational for potential users wishing to embrace cloud services.

In the remainder of this chapter, Sect. 2 outlines the importance of information security for organisations and investments into information and communication technologies. We also discuss cloud computing and related issues such as: cloud deployment models and cloud services, adoption drivers, and current issues of cloud computing. Then, Sect. 3 provides insight into information security accountability to discuss in detail the relationship between accountability and cloud computing within an organisational context. Section 4 covers information security accountability conceptual factors. Lastly, the conclusion is shared in Sect. 5.

2 Literature Review

2.1 Importance of Information Security

Information is considered the most valuable and crucial asset to any organisation, and hence, must be properly protected [25]. The use of information is evolving at an unprecedented rate and Escherich [21], a principal research analyst at Gartner, emphasises that information within an organisation is vitally important and has to be thoroughly protected. However, downloads and the use of many different types of software that process this information, brings along more threats to organisations [38]. For example, attackers can use malicious tools to gain access to various valuable information resources and services such as identities and credentials. This information can be used by attackers to gain profit illegally [22]. It is also evident that the need for information security for both personal and institutional use has rapidly increased due to the proliferation of communication media, electronic storage and transmission of information [93]. Some important reasons for this growth are due to the "increase in electronic applications in businesses as well as in daily life, the sharing of information on network systems, the accessibility of information from many points, the increasing threat of loss of information, and most importantly, the increases in personal and corporate losses" [20].

2.2 Organisations and Investments in Information Technology

Many researchers have proposed that all investments of business operations and IT should be integrated into their business values and should be aligned with organisational strategy [16, 41]. For example, Croteau and Raymond [17] confirm that the investment in IT and business processes should be coordinated to achieve a proper strategic plan with a good integration process. Ju et al. [32] propose that the correlation between strategic factors, organisational factors, and technology alliance have a great impact on an organisation's competitiveness. However, Markus [41] argues that approaching success and improvements in terms of functions and performance is difficult whether or not IT is required. There is a resistance to investing in technology in most organisations due to a lack of information, human resources, and cost of implementing internal security management systems.

2.3 Organisations and Information Security Concerns

Information systems security remains the most challengeable task to IT leaders, executives and professionals [19]. Maintaining Infosys security in organisations is more than just a technical matter. There are other aspects of Infosys, such as organisational "grounded principles and values" [19], which need to be considered. There are various studies in the literature which emphasise that Infosys security is more effective in terms of management if it goes beyond technical aspects [57]. For example, Puhakainen and Siponen [57] state that employee refuses to comply with information security policy should be considered as a real information security threat. Furthermore, Straub and Welke [69] state that there are several values to be measured in terms of protecting information resources at any organisation. Segev et al. [64] outline that the main key of protecting Infosys security is not technical but that it should be accomplished by studying the key managerial elements featuring each organisation.

Tan and Hunter [74] suggest that a mix of social and organisational factors must be considered as effective values to be employed by Infosys stakeholders. These organisational and social factors indicate people's assumptions, accountability, and values towards Infosys security issues [47]. Keeney and Keeney [34] state that re-evaluating these social factors can help to discover some hidden objectives. Trompeter and Eloff [82] argue that in addition to technical and organisational factors, ethics and personal accountability must be considered throughout the implementation of any ISMS. However, In the context of this review, the researcher will focus mainly on the challenges of information security accountability in the cloud computing context.

2.4 Cloud Computing Service Provisions

Cloud computing relates to the use of online computing services and is considered an on-demand IT service or product based on the business model. Users and businesses can use software and hardware through cloud services, including SaaS, PaaS and IaaS with the management of third parties at a remote location [68]. Characteristics include: manageability, access method, performance, multi-tenancy, scalability, data availability, control, storage efficiency [83], advanced security technologies [67], on request allocation and reallocation of resources, virtualised storage and networking facility, enabling sharable resources "as a service" model, the flexibility of moving an organisation's data through data centres, cost-effectiveness, reducing the responsibility of maintaining data locally, and resources made customisable on the web [92]. In addition, the computing resources and data are automatically maintained through software that is managed and controlled by CSPs [63].

According to the National Institute of Standards and Technology (NIST), Cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction"[42].

2.5 Cloud Computing Deployment Models and Cloud Computing Services

The cloud infrastructure can be subdivided into four layers: the physical layer, the infrastructure layer, the platform layer and the application layer. In addition, cloud computing is made up of four models: public, private, hybrid and community. Each of these models is divided into three service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) as demonstrated in Figs. 1 and 2 respectively [4, 12].

The rapid growth of Cloud computing has created a paradigm shift in technology since the whole IT infrastructure has become available as a service including within smart city sectors [3]. Despite the fears of losing control by different users about data stewardship especially health and financial data, there are a number of notable commercial and individual cloud computing services, including Google (Email Service), Microsoft Azure and Yahoo [84]. Ko et al. [36] state that Google, Microsoft (Azure) and Amazon (EC2/S3) are the current prominent cloud providers in the world. For example, Microsoft Office 365 provided by Microsoft is the most popular case of SaaS service provided to the public, Google Apps is a good example of PaaS and Amazon Web Services is a good example of an IaaS [46].

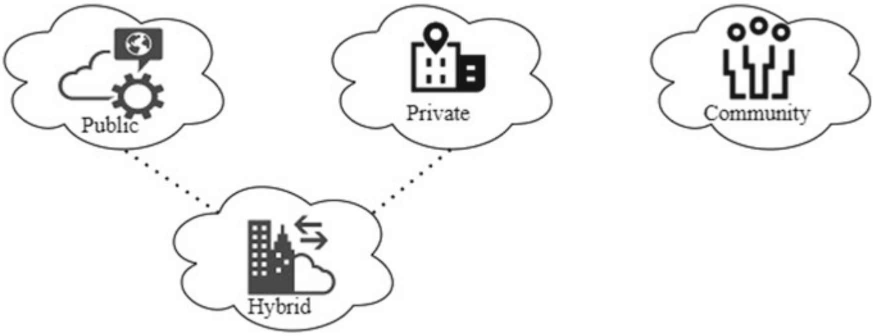

Fig. 1 Cloud computing deployment models

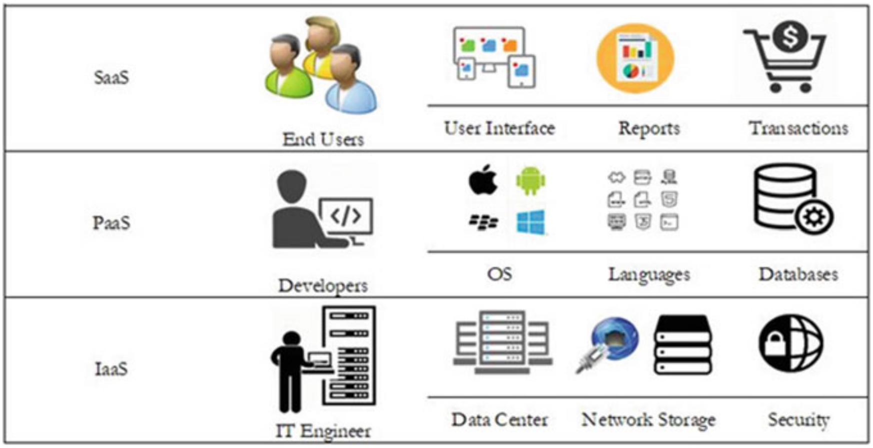

Fig. 2 Cloud computing services

2.6 A Motivation for Cloud Migration

Cloud computing relates to the use of online computing services and is considered an on-demand IT service or product based on the business model. Users and businesses can use software and hardware through cloud services, including SaaS, PaaS, and IaaS with the management of third parties at a remote location [84]. Characteristics include: manageability, access method, performance, multi-tenancy, scalability, data availability, control, storage efficiency [35, 88], advanced security technologies [35], on request allocation and reallocation of resources, virtualised storage and networking facility, enabling sharable resources "as a-service" model, the flexibility of moving an organisation's data through data centres, cost-effectiveness, reducing the responsibility of maintaining data locally, and resources made customisable on the web. In addition, the computing resources and data are automatically maintained through software that is managed and controlled by the CSP [63]. Overall the sharing of resources represents the main benefits of Cloud computing by sharing large pools of resources such as compute cycles, or virtual CPUs (VCPUs), storage and software services [44, 59]. However, sharing resources increases concerns towards security with end users, particularly with respect to data or applications hosted in the cloud provider's data centres [33].

2.7 Current Issues for Cloud Computing

In recent years, the demand for migration to clouds is ever-increasing due to the growing number of personal data including bookmarks, photographs, media and music files, are accessed remotely via a network [94]. Cloud computing has expanded

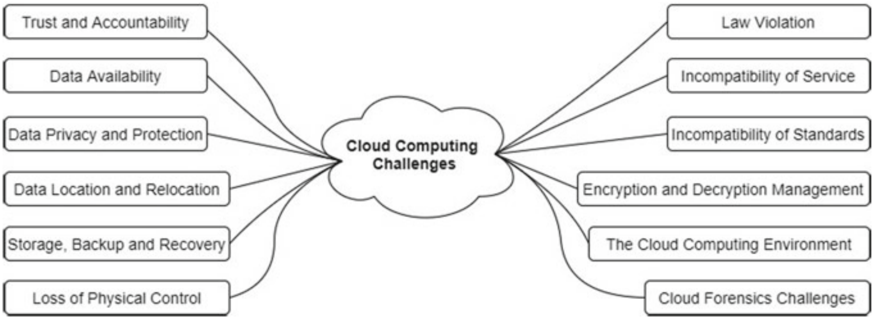
Trust and Accountability
Data Availability
Data Privacy and Protection
Data Location and Relocation
Storage, Backup and Recovery
Loss of Physical Control
Cloud Computing Challenges
Law Violation
Incompatibility of Service
Incompatibility of Standards
Encryption and Decryption Management
The Cloud Computing Environment
Cloud Forensics Challenges

Fig. 3 Cloud computing challenges

into one of the fastest-growing portions of the IT industry and has become a promising business concept where a huge amount of information—for both individuals and enterprises—is placed. This transformation of data distribution and storage in the cloud has generated a real concern towards data privacy and data protection. It has also raised questions about how safe the cloud environment is. This question is considered by most organisations before deciding on deploying their business into the cloud [70].

After reviewing more than eighteen case studies by the researcher about cloud computing, between 2009 and 2021, it was revealed that there are many challenges and security issues associated with cloud migration [58, 92]. These challenges, as shown in Fig. 3 and discussed in subsequent sections, have a significant impact on users' decisions to move their activities to the clouds.

2.8 Cloud Computing Challenges

From the above-mentioned cloud computing challenges presented in Fig. 3, it is clear that migrating data to the cloud is not an easy task to achieve in terms of decision making and implementation. Decision-makers should ensure that accountability mechanisms are in place to provide clients with control and transparency over data in the cloud. This includes enabling the customer to choose and select its cloud provider based on the criteria of reliability and IS responsibility and vice versa. When this happens, trust and accountability are fully implemented. In addition, data availability must also be ensured where client data are usually stored in 'blocks', usually in different locations and on different servers. This would contribute negatively to the availability of data and could constitute a genuine concern for the availability of uninterrupted and uninterrupted data provisions. Confidentiality and data protection are other aspects that must be taken into account, as confidentiality and data protection include confidentiality, integrity and availability. A proper practice, privacy policies and information system procedures must be clearly stated in the service level agreement (SLA) [60] to assure the client of data safety. The integrity mechanisms should be implemented by the CSP to ensure that data will not be modified to any extent. The client should be made aware of any data loss or change [13] and the right information should be made available to the right people [66]. Furthermore, the CSPs should inform the client about the data location (where the data will be stored, for example, in Australia or the US or India), this should be clearly mentioned in the SLA [18, 40]. Furthermore, the customer must be aware of the possibility of moving or transferring their data from one cloud to another [18]. The consumer needs to be sure about the whole cloud computing environment. The physical and political environment surrounding the data centre and how safe it is (data location) The consumer needs assurance about the availability of adequate data storage systems in place, at least RAID (Redundant Array of Independent Discs) systems. This can be accomplished by having the latest technology in storage, backup and retrieval systems. Recovery systems should be regularly updated and maintained to restore information as early as possible in the event of a malfunction. This is part of the emergency plan agreed to in SLA to manage events and respond to incidents.

Consumers are generally concerned about the loss of physical control as data and resources are shared with CSP in whole or in part. Sometimes governments never comply with privacy laws when it comes to accessing other people's data, indicating a clear breach of the law [37]. This includes the limitation of collecting citizens' data that resides/goes into storage, the duration of time to keep data and some financial, banking protocol, and that the customer's data should remain within the country. From a technical perspective, consumers are also concerned with the issue of compatibility, such as the incompatibility of services between different service providers. This is especially true when the customer decides to switch between cloud providers. For example, Microsoft, Cloud and Google Cloud are both incompatible with one another and incompatible with current standards and code of practice across the various clouds. Another conflict is emerging between the CSP and its associated consumers in terms of encryption and decryption management. It's about who should take control of encryption and decryption, the customer or the cloud provider? The consumer has to be clearly informed about the process and procedures the CSP will follow in case of data breach and how the investigation or what is known as a cloud forensics process will be maintained. This is a real challenge, as more than one-third party will host the data at any time and everyone will share the responsibility of hosting customer data. Cloud forensic investigations require complex procedures and special tools, along with the exceptional skills a digital forensic investigator must possess to conduct this type of investigation [1, 6]. Since digital forensics is one of the key elements of law enforcement (LEA) [7], CSP collaboration is vital. Therefore, the relationship between digital forensic investigators and CSPs must be framed to enhance trust between the two parties and ensure the highest level of preservation of the integrity of digital evidence [8]. In addition to the above-mentioned points, the studies also revealed some logistical issues such as service level agreement issues (SLA) [43], costing models, charging models [48], what to migrate [15], and cloud interoperability issues.

As part of this review, this chapter will focus on the challenges of IT security accountability. Information security practitioners believe that cloud ownership is the first “building block” that each organization must implement to improve cloud data protection. Ko et al. [36] and Lynn et al. [39] believe that cloud accountability is one of the evolving issues in cloud security and needs to receive the greatest attention. In addition, scholars also believe that accountability is incorporated directly with all the other information security challenges outlined above, and has a great impact on the implemented mechanisms, which in turn ensures responsible decision-making towards information security management and protection of data [24, 36].

3 Information Security Accountability

The review revealed four main components of Information Security accountability in relation to Cloud computing service provision, and showed that in order to be an accountable organisation, the four components should be fully implemented. As can be seen in the descriptions of these factors, as illustrated in Fig. 4, there are inherent interactions between the four components (Responsibility, Assurance, Transparency and Remediation) which means that they should all be addressed simultaneously; Uniqueness implementing each component is likely to cause failure in relation to IS Accountability. ISPs who wish to be held accountable should be aware of these four

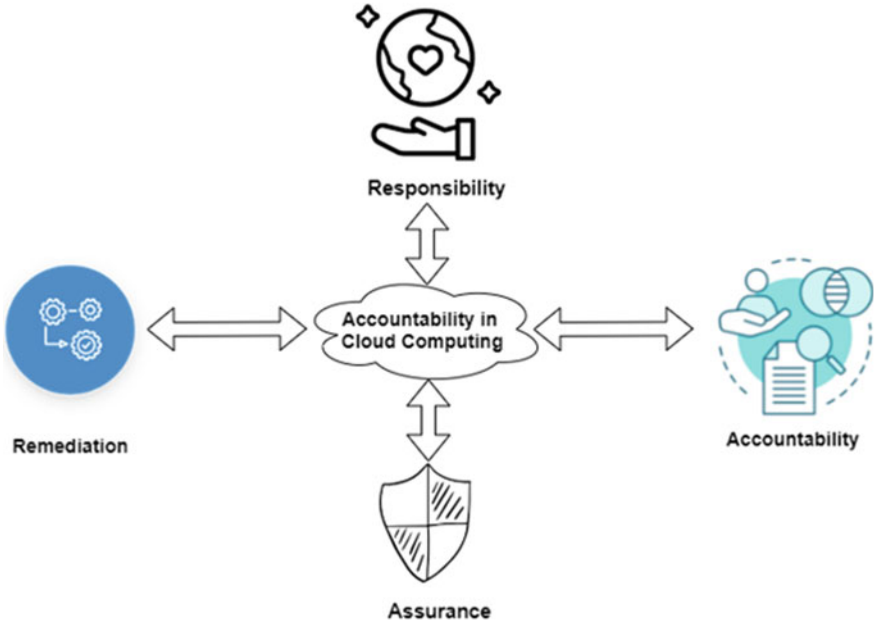

Fig. 4 The four central components of Accountability in the existing literature

core elements of accountability and be prepared to demonstrate to customers that they have achieved them. However, this does not mean that there is a singular method for implementing all four factors or any individual factor—the nature of the organisation, its industry context, the type of data collected, the business model, and the potential risks that data usage raises for clients all have an impact on the method chosen for implementing these factors [24, 52]. The following section details four different areas associated with accountability. First, the organization and accountability of end-users are briefly presented. Second, there is a discussion on what accountability means. Lastly, the conceptual factors for IS responsibility are listed and discussed.

3.1 Organisations and End Users' Accountability

People will remain the most responsible party in mitigating human risks posed by malicious tools [2]. There is social responsibility in combating threats and therefore, all parties should work together to mitigate the risks of malicious threats and that includes governments, ISPs, end-users, and international bodies.

3.2 What Is Accountability and How Does It Relate to Cloud Computing and ISMSs

Accountability is a global term that has been used and presented for a number of years in computer science, finance and public governance, and is becoming more incorporated into business regulatory programs. However, recently the term accountability has emerged in terms of a worldwide privacy and data protection framework [55]. The research effort on accountability has produced a considerable number of definitions. These definitions embody different spheres of accountability research. Both academics and practitioners have different views and interpretations of accountability. For example, accountability in computer science according to scholars is referred to a limited and imprecise requirement that is met by reporting and auditing mechanisms [52]. Yao et al. [91], considers accountability as a way of making the system accountable and trustworthy by the combination of mechanisms. Accountability should be approached by having mechanisms that concentrate on a broader scope of the legal issues [89]. For example, Vedder and Naudts [85] suggested calling for accountability mechanisms that transcend the mechanisms that are inherent in regulation. Authors like Jaatun et al. [28] proposed to develop accountability mechanisms that would diversify processes, non-technical mechanisms and tools that would support accountability practices. Rush [61] defines accountability as the reporting and auditing of mechanisms and obligating an organisation to be answerable for its actions.

Vithanwattana et al. [86] identified accountability as the process of tracking users' activity in a continuous manner while accessing resources in the system. The users would be tracked against the systems they accessed, which systems they were granted access to, what type of information they accessed, the amount of data transferred during their access, time spent on the system and when they disconnected from the system.

Muppala et al. [44] refer to accountability as the adherence to accepting the ownership and responsibility towards all actions in a standardised way as regulated by an acknowledged organisation such as the Organisation for Economic Cooperation and Development (OECD) who published privacy guidelines in 1980. However, Ko et al. [36] consider accountability as one out of the four components of trust in Cloud computing. The remaining three are security mechanisms (e.g. encryption), privacy (the protection of personal or confidential data not to be exposed) and auditability. A reasonable definition for accountability has been provided by the Galway project of privacy regulators and privacy professionals. To them, accountability is defined to as the commitment towards safeguarding personal information with an obligation to act as a responsible steward by taking responsibility for protecting, managing and appropriating use of that information beyond mere legal requirements, and to be held accountable for any misuse of that information [76].

The Centre for Information Policy Leadership in the United States has identified accountability in relation to privacy as "the acceptance of responsibility for personal information protection. An accountable organisation must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. The outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws. Done properly, it should promote trust and confidence on the part of consumers, and thereby enhance competitive and reputational advantages for organisations" [78, 79].

Pearson [53] stated certain conditions need to be met in order to provide an improved basis of trustworthiness in the Cloud computing environment, which automatically enhances accountability.

This review uses the definitions of accountability offered by several authors [76, 86]. These definitions cover the central components of accountability namely Transparency, Responsibility, Assurance, and Remediation. For example, organisations are required to demonstrate a certain level of acknowledgement and assumption of Responsibility by introducing or having in place appropriate policies and procedures along with promoting good practices for correction and remediation in case of failure and misconduct [52]. In addition, in terms of data protection, organisations should be held responsible for any decision made about the protection of data by report, explanation, enhancing Transparency, considering liability and be made answerable for the consequences [44]. Governance and ethical dimensions along with promoting the implementation of practical mechanisms are all parts of accountability, whereas legal aspects and guidance should be interpreted for data protection [77]. The above definitions are used as the basis of this comprehensive review because the definitions incorporate the protection of organisational assets and personal privacy.

However, none of these studies has mentioned the role of the ISMS in controlling all aspects of accountability in Cloud computing. This indicates that the need to employ an ISMS in order to control all aspects of security challenges in Cloud computing is a trend in today's world. Accountability in relation to cloud service provision needs to be examined and investigated with regards to its integration with ISMSs.

Therefore, accountability and ISMSs are interconnected with each other, since both of them are designed to satisfy the same approach towards information security management and data protection. Their main goals are to ensure the protection of organisational assets and personal privacy regardless of the difference in processes and procedures followed to achieve each approach.

4 Conceptual Factors

The Centre for Information Policy Leadership has identified accountability as "a demonstrable acknowledgement and assumption of responsibility for having in place appropriate policies and procedures, and promotion of good practices that include correction and remediation for failures and misconduct. It is a concept that has governance and ethical dimensions. It envisages an infrastructure that fosters responsible decision-making, engenders answerability, enhances transparency and considers a liability. It encompasses expectations that organisations will report, explain and be answerable for the consequences of decisions about the protection of data. Accountability promotes the implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection of data" [77].

As mentioned previously, this review uses the definition of Accountability offered by several authors [76, 78, 79]. In particular, these definitions cover the central components of accountability: Transparency, Responsibility, Assurance and Remediation. These definitions are used as the basis of this review because they incorporate the protection of organisational assets and personal privacy. Figure 4 shows the overall interactions between these four key components in terms of achieving accountability. It should be noted that the double arrows indicate that the four factors interact with each other and are not necessarily independent of each other.

4.1 Responsibility

Responsibility in the context of accountability for Cloud computing service provision is the acknowledgement and assumption of responsibility by CSPs that they have introduced or have in place appropriate policies and procedures [26]. Responsibility is achievable by ensuring the existence of obligatory and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards. The accountable CSP should develop, implement and communicate to clients a set of data privacy policies that are informed by appropriate external criteria recognised by laws, regulations or the industry's best practices [81]. In addition, the accountable CSP should be prepared to provide clients with [87] and also design and deploy a set of procedures to implement effective and practical written policies according to the circumstances of each organisation—such as what data is collected, how it is used, and how systems and organisations are connected.

Responsibility is considered one of the most important factors of IS Accountability to adequately manage the relationship between CSPs and clients. The accountable organisation (CSPs) should have a data privacy program in place to establish, demonstrate and test its accountability. Each organisation should demonstrate a level of Responsibility and a willingness to be accountable for any misconduct in its data practices, policies and procedures, which should be implemented based on external legislative criteria [30], and generally accepted principles or the industry's best practices. All policies and procedures must be approved at the highest level of the organisation, and senior management should demonstrate their commitment towards motivating Responsibility, which in turn encourages accountability.

4.2 Assurance

Assurance, in terms of Accountability for Cloud computing service provision, is to comply with governance and ethical measurements along with promoting the implementation of practical mechanisms that are commonly considered key parts of accountable processes and procedures [54]. In addition, Assurance is considered as the main tool of evidence that provides valuable information to risk management where this evidence would be used by providing confidence to stakeholders that the qualities of service and stewardship with which they are concerned are being managed and maintained appropriately [54]. The following factors are part of Assurance in relation to accountability for the provision of Cloud computing services:

- Staffing and delegation
- Education and awareness
- Mechanisms to manage IS accountability in the cloud computing environment
- Ongoing risk assessment and mitigation
- Program risk assessment oversight and validation
- Event management and complaint handling
- Internal enforcement.

Appropriately trained personnel will ensure the validity of the CSP's privacy program and assign the right resources to the right personnel [77]. Small and medium-sized organisations should ensure that these delegations are in line with their specific activities and circumstances, such as the nature, size and sensitivity of their data holdings. Once properly implemented, the client-CSP relationship will be enhanced;

CSPs will provide their employees with appropriate training and be assigned responsibility for the privacy program [30]. Education and awareness is another element of assurance that improves IS accountability to the CSP.

An effective education and awareness program will ensure that staff of an organization and on-site contractors are kept informed of data protection obligations. Such ongoing education and awareness will enhance the CSP's employees' capabilities and increase their understanding of the essentiality of protecting clients' data to avoid data leakage consequences such as job dismissal. It is clear that this process will increase the level of trust between clients and their CSPs. The implementation of a number of CSP mechanisms improves the assurance factor, which increases IS accountability. Implementing mechanisms directly impacts on managing IS accountability in the cloud environment. The review identified several mechanisms that, according to the researchers, support IS empowerment in a cloud computing environment [30, 31]. The mechanisms are considered tools and activities to implement and monitor IS accountability objectives. In addition, Jena and Mohanty [31] have discussed the importance of cloud auditors being used in online dispute resolutions (ODR) in the cloud environment where data is remotely controlled as part of the compliance process during the Remediation stage. The importance of cloud auditors as an effective mechanism was discussed by Jaatun et al. [30]. For example, mechanisms to clarify compliance with respect to extraterritorial legislative requirements and provide a list of certifications required should be handled by the cloud auditor, as they are considered to be the main actor to perform audits and certifications, to monitor accountability levels of cloud providers and to make sure that collection of implicitly collected data is made transparent [30].

Another aspect of assurance is the constant assessment and mitigation of risks. CSP and their associated clients agreed that to be an accountable CSP, processes are needed to understand the related risks to privacy that may occur from the implementation of new solutions, products, services, technologies or business models. The results of ongoing risk assessment and mitigation should be taken into account in the measures taken by the organization to mitigate potential client risks. In addition, these organizations should further demonstrate how these decisions are taken and what actions are taken to mitigate the risk. By having such steps in place, including precise processes and procedures to arrest ongoing risk and mitigation, CSPs will be perceived positively by clients in terms of accountability, and are likely to be branded as a trustworthy party. In addition, having a solid program risk assessment oversight and validation in place enhances the trust and confidence of CSP accountability as it assures clients that constant reviews are set in place. Ongoing reviews of an organization's confidentiality and accountability program need to be considered by clients and CSPs in order to be viewed as a responsible organization. This will ensure that the needs of an organization are consistently met through sound data management and protection decisions that promote and respect privacy outcomes. Information security practitioners believe that a review of the exchange of such programs between PSPs and clients will improve trust and validate CSP programs, which in turn will lead to a responsible partnership. In addition, security experts believe that implementing complaint management and handling systems is seen as an added value to cloud clients. Decision-makers believe that a responsible organisation should put in place procedures that effectively respond to requests for information, complaints and data protection breaches [30]. A timely response to any inquiry, complaint or violation in terms of data protection will establish an image of support between clients and CSPs, which in turn will strengthen accountability between them. The matter of support between clients and their CSPs can sometimes become complicated and often leads to contract termination, which means a loss of trust between clients and CSPs. The in-house application is another assurance factor that enhances IS accountability in cloud computing environments. IT experts believe that accountable organisations should have in place methods to enforce internal policy, ensuring that any breaches to those internal data protection rules by employees—such as IS Accountability practitioners—property or misuse of data, are subject to sanctions, including discharge [9, 77]. In this case, this internal application is directly linked to CSPs and the reinforcement of these aspects of the application will increase the likelihood that customers choose to use this CSP.

As a whole, assurance and accountability are interrelated. Based on corporate culture, each organization must establish performance systems to be viewed as a responsible organization, and the following characteristics represent successful performance systems: (1) they are consistent with the organisation's culture and are integrated into business processes; (2) they assess risk across the entire data life cycle; (3) they include training, decision-making tools and monitoring; (4) they apply to outside vendors and other third parties, to ensure that personal data obligations are met no matter where the data is processed; (5) they allocate resources in places where the risk to individuals is greatest; and (6) they are a function of an organisation's policies and commitment. In Europe, North America and Asia–Pacific seal programs are used where they play the role of third-party accountability agents, which provides external oversight by making Assurance and verification reviews a requirement for participating organisations.

4.3 Transparency

To ensure transparency in the context of accountability for providing cloud computing services, a series of issues need to be addressed. The results of each review, including changes in rules and procedures, should be communicated to customers in a clear and timely manner [73]. Information should be properly communicated to client organizations and regulators in a rigorous and cost-effective manner [51]. As part of this process, the outcome of assessment measures or audits should be reported to the appropriate employee within a client organisation, and where necessary corrective action should be taken [27, 49]. Transparency involves reporting and explaining decisions taken to protect data. It also means that acceptance of liability and remedies are clearly presented to customers [10]. Transparency between clients and their CSPs is an essential element towards achieving accountability in Cloud computing, as most clients want to know who is handling their data as well as how, where and when it is used. Sharing such information between clients and CSPs increases trust, which increases accountability [30]. A level of transparency must be demonstrated among clients and organizations. Clients should have rights to the data collected by editing it. They also have the right to stop using certain data where it is not appropriate or to correct the data collected where it is inaccurate. However, there may be limits on disclosing information in certain circumstances.

4.4 Remediation

To implement corrective actions that ensure accountability for cloud service delivery, there is a need for a range of corrective action processes. According to The Centre for Information Policy Leadership [84] remediation is "the method by which an organization provides recourse to persons whose privacy has been put in jeopardy." In this context, a responsible organization should use its best practices in remedial action and redress in the event of failure and misconduct [52, 65]. In addition, an accountable organisation should have a specific remediation mechanism that suits each organisation according to their data holdings, and the way the data is used and appropriated for a specific issue. These mechanisms should be readily accessible to clients, and the lead organization should be able to handle complaints in an effective and efficient manner. The redress mechanisms would vary depending on the culture and the industry. Therefore, decisions about redress should be made locally.

However, these remediation mechanisms would need to be developed in consultation with a range of experts, regulators, civil society, and representatives of both public and private sector organisations [90]. Corrective actions complement accounting processes and procedures to ensure business continuity in the event of a malfunction. When failure occurs, individuals should have access to a recourse mechanism. For instance, a third-party agency might be needed to address and resolve the failure that has occurred. Customers must be aware of the processes and procedures that must be followed in the event of failure.

5 Conclusion

This review has sought to understand how IS Accountability in Cloud computing can be conceptualised. Initially, this review used an extensive analysis of the literature relating to Cloud computing and accountability for information security to develop a model of the key conceptual elements (Responsibility, Transparency, Assurance and Remediation) (see Sect. 2.15) relating to this issue. The objective of this review was to understand what an organization needs to do to achieve IS responsibility in a cloud context. It should be noted that this differs from information security because an organization considered to be responsible for information security may still have corresponding violations. In fact, some aspects of information security and accountability, such as remedial actions, may never come into play if such a breach does not occur. In order to determine if an organization is responsible for its information security, the first step is to identify and define the core elements of IS accountability. The review found that these four elements were viewed by IS accountability practitioners as core elements of IS accountability.

This reviewer provided a more detailed definition of IS accountability based on the revealed literature. This definition will assist in the research of IS Accountability by providing a common understanding of the concept. The researcher examined the meaning of IS Accountability to determine whether the four components of the earlier IS Accountability in Cloud model could be expanded. Achieving IS Accountability is a complex task for any organisation. The first step is to understand the elements of IS Accountability. It is important to realise that though there are four elements, the level to which any element needs to be implemented in an organisation, is highly context-dependent. A level of transparency for an organization with an acceptable level of accountability may not be sufficient for another organization. Overall, it needs to be understood, that the four-element model is not prescriptive and that it must be used in a context-sensitive way that is dependent on the needs of the specific organisation that is attempting to achieve IS Accountability.

References

1. AL-Husaini Y, Al-Khateeb H, Warren M, Pan L (2018) A model to facilitate collaborative digital forensic investigations for law enforcement: the royal Oman Police as a case study. In: Paper presented at the 2018 cyber forensic and security international conference, Nuku'alofa, Kingdom of Tonga, pp 21–23
2. Abraham S, Chengalur-Smith I (2010) An overview of social engineering malware: trends, tactics, and implications. Technol Soc 32(3):183–196
3. Ahmadi-Assalemi G, Al-Khateeb H, Epiphaniou G, Maple C (2020) Cyber resilience and incident response in smart cities: a systematic literature review. Smart Cities 3(3):894–927. https://doi.org/10.3390/smartcities3030046
4. Ahmed ZE, Saeed RA, Mukherjee A (2019) Challenges and opportunities in vehicular cloud computing. In: Cloud security: concepts, methodologies, tools, and applications. IGI Global, pp 2168–2185
5. Akintoye SB, Bagula A (2019) Improving quality-of-service in cloud/fog computing through efficient resource allocation. Sensors 19(6):1267
6. Al-Husaini Y, Al-Khateeb H, Warren M, Pan L, Epiphaniou G (2020) Collaborative digital forensic investigations model for law enforcement: Oman as a case study. In: Security and organization within IoT and smart cities. CRC Press, pp 157–180
7. Al-Husaini Y, Warren M, Pan L (2018) Cloud forensics relationship between the law enforcement and cloud service providers. In: Paper presented at the CWAR 2018: proceedings of the 17th Australian cyber warfare conference
8. Al-Husaini Y, Warren M, Pan L, Gharibi MA (2019) Cloud forensics investigations relationship: a model and instrument
9. Al-Rashdi Z, Dick M, Storey I (2017) Core elements in information security accountability in the cloud
10. Ali MB, Wood-Harper T, Ramlogan R (2020) A framework strategy to overcome trust issues on cloud computing adoption in higher education. In: Modern principles, practices, and algorithms for cloud security. IGI Global, pp 162–183

11. Bass C (2019) The criteria cybersecurity decision makers use to evaluate the trustworthiness of a cloud computing storage service for financial data: a qualitative study. Colorado Technical University
12. Bouzerzour NEH, Ghazouani S, Slimani Y (2020) A survey on the service interoperability in cloud computing: client-centric and provider-centric perspectives. Softw Pract Exp 50(7):1025–1060
13. Brumă LM (2020) Data security methods in cloud computing. Inf Econ 24(1)
14. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I (2009) Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Futur Gener Comput Syst 25(6):599–616
15. Chang H (2013) Is ISMS for financial organizations effective on their business? Math Comput Modell 58(79):79–84
16. Chang SE, Ho CB (2006) Organizational factors to the effectiveness of implementing information security management. Indus Manag Data Syst
17. Croteau A-M, Raymond L (2004) Performance outcomes of strategic and IT competencies alignment†. J Inf Technol 19(3):178–190
18. Daniel E, Vasanthi N (2019) LDAP: a lightweight deduplication and auditing protocol for secure data storage in cloud environment. Clust Comput 22(1):1247–1258
19. Dhillon G, Torkzadeh G (2006) Value-focused assessment of information system security in organizations. Inf Syst J 16(3):293–314
20. Dodge RC Jr, Carver C, Ferguson AJ (2007) Phishing for user security awareness. Comput Secur 26(1):73–80
21. Escherich M (2014) Gartner survey shows U.S. consumers have little security concern with BYOD
22. Fossi M, Egan G, Haley K, Johnson E, Mack T, Adams T, Wood P (2011) Symantec internet security threat report trends for 2010. Semant Rep 16:20
23. Gartner (2020) Gartner forecasts worldwide public cloud end-user spending to grow 18% in 2021. https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021
24. Ghosh S (2020) Addressing accountability in cloud computing: a qualitative study of business cloud consumers. Wilmington University, Delaware
25. Hong KS, Chi YP, Chao LR, Tang JH (2003) An integrated system theory of information security management. Inf Manag Comput Secur
26. Ilten C, Kroener I, Neyland D, Postigo H (2012) Managing privacy through accountability. Springer
27. Ismail UM, Islam S (2020) A unified framework for cloud security transparency and audit. J Inf Secur Appl 54:102594
28. Jaatun MG, Pearson S, Gittler F, Leenes R, Niezen M (2016) Enhancing accountability in the cloud. Int J Inf Manag
29. Jaatun MG, Pearson S, Gittler F, Leenes R, Niezen M (2020) Enhancing accountability in the cloud. Int J Inf Manag 53:101498
30. Jaatun MG, Tøndel IA, Moe NB, Cruzes DS, Bernsmed K, Haugset B (2017) Accountability requirements for the cloud. In: Paper presented at the 2017 IEEE international conference on cloud computing technology and science (CloudCom)
31. Jena T, Mohanty J (2017) Cloud security and jurisdiction: need of the hour. In: Paper presented at the proceedings of the 5th international conference on frontiers in intelligent computing: theory and applications
32. Ju TL, Chen S-H, Li C-Y, Lee T-S (2005) A strategic contingency model for technology alliance. Indus Manag Data Syst 105(5):623–644
33. Kalpana P, Singaraju S (2012) Data security in cloud computing using RSA algorithm. Int J Res Comput Commun Technol IJRCCT. ISSN: 2278-5841.
34. Keeney RL, Keeney RL (2009) Value-focused thinking: a path to creative decisionmaking. Harvard University Press

35. Kelf S (2020) The security risks created by cloud migration and how to overcome them. Netw Secur 2020(4):14–16
36. Ko RK, Jagadpramana P, Mowbray M, Pearson S, Kirchberg M, Liang Q, Lee BS (2011) TrustCloud: a framework for accountability and trust in cloud computing. In: Paper presented at the 2011 IEEE world congress on services
37. Lee G, Epiphaniou G, Al-Khateeb H, Maple C (2019) Security and privacy of things: regulatory challenges and gaps for the secure integration of cyber-physical systems. In: Paper presented at the third international congress on information and communication technology, Singapore
38. Liu T, Guan X, Qu Y, Sun Y (2012) A layered classification for malicious function identification and malware detection. Concurr Comput Pract Exp 24(11):1169–1179
39. Lynn T, van der Werff L, Fox G (2020) Understanding trust and cloud computing: an integrated framework for assurance and accountability in the cloud. In: Data privacy and trust in cloud computing. Palgrave Macmillan, Cham, pp 1–20
40. Manral B, Somani G, Choo K-KR, Conti M, Gaur MS (2019) A systematic survey on cloud forensics challenges, solutions, and future directions. ACM Comput Surv (CSUR) 52(6):1–38
41. Markus ML (2004) Technochange management: using IT to drive organizational change. J Inf Technol 19(1):4–20
42. Mell P, Grance T (2011) The NIST definition of cloud computing
43. Morin J, Aubert J, Gateau B (2012) Towards cloud computing SLA risk management: issues and challenges. In: Paper presented at the system science (HICSS), 2012 45th Hawaii international conference
44. Muppala J, Shukla D, Patil S (2012) Establishing trust in public clouds'. J Inform Tech Softw Eng 2:e107
45. Mwenya JK, Brown I (2019) Cloud privacy and security issues beyond technology: championing the cause of accountability
46. Olaloye F, Adeyemo A, Edikan E, Lawal C, Ejemeyovwi J (2019) Cloud computing in education sector: an extensive review. Int J Civil Eng Technol 10:3158–3171
47. Orlikowski WJ, Gash DC (1994) Technological frames: making sense of information technology in organizations. ACM Trans Inf Syst (TOIS) 12(2):174–207
48. Pal R, Hui P (2012) Economic models for cloud service markets. In: Distributed computing and networking. Springer, pp 382–396
49. Patel P, Ranabahu AH, Sheth AP (2009) Service level agreement in cloud computing
50. Pearson S, Wainwright N (2013) An interdisciplinary approach to accountability for future internet service provision. Int J Trust Manag Comput Commun 1(1):52–72
51. Pearson S, Charlesworth A (2009) Accountability as a way forward for privacy protection in the cloud. In: IEEE international conference on cloud computing, pp 131–144
52. Pearson S (2011) Towards accountability in the cloud. In: Proceedings of the IEEE internet computing, pp 64–69
53. Pearson S (2017) Strong accountability and its contribution to trustworthy data handling in the information society. In: Paper presented at the IFIP international conference on trust management
54. Pearson S, Luna J, Reich C (2015) Improving cloud assurance and transparency through accountability mechanisms. In: Guide to security assurance for cloud computing. Springer, pp 139–169
55. Pearson S, Tountopoulos V, Catteddu D, Südholt M, Molva R, Reich C et al. (2012) Accountability for cloud and other future internet services. In: Paper presented at the 4th IEEE international conference on cloud computing technology and science proceedings
56. Potluri S, Rao KS (2020) Improved quality of service-based cloud service ranking and recommendation model. Telkomnika 18(3):1252–1258
57. Puhakainen P, Siponen M (2010) Improving employees' compliance through information systems security training: an action research study. MIS Q 34(4)
58. Purnaye P, Kulkarni V (2021) A comprehensive study of cloud forensics. Arch Comput Methods Eng 1–14.

59. Rashid ZN, Zeebaree SR, Shengul A (2019) Design and analysis of proposed remote controlling distributed parallel computing system over the cloud. In: Paper presented at the 2019 international conference on advanced science and engineering (ICOASE)
60. Raza MR, Varol A (2020) QoS parameters for viable SLA in cloud. In: Paper presented at the 2020 8th international symposium on digital forensics and security (ISDFS); The Best Practices Act of 2010 and Other Privacy Legislation, 2010 (2010)
61. Rush B (2010) The Best Practices Act of 2010 and Other Privacy Legislation, 2010
62. Ryan P, Crane M, Brennan R (2020) Design challenges for GDPR RegTech. arXiv preprint arXiv:2005.12138
63. Saravanan N, Mahendiran A, Subramanian NV, Sairam N (2012) An implementation of RSA algorithm in google cloud using cloud SQL
64. Segev A, Porra J, Roldan M (1998) Internet security and the case of Bank of America. Commun ACM 41(10):81–87
65. Shetty J, Babu BS, Shobha G (2020) Proactive cloud service assurance framework for fault remediation in cloud environment. Int J Electr Comput Eng 10(1):2088–8708
66. Singh HP, Singh R, Singh V (2020) Cloud computing security issues, challenges and solutions (2516-2314)
67. Sreenivas V, ArunaKumari B, VenkataRao J (2012) Enhancing the security for information with virtual data centers in cloud. In: Future wireless networks and information systems. Springer, pp 277–282
68. Sreenivas V, Narasimham C, Subrahmanyam K, Yellamma P (2013) Performance evaluation of encryption techniques and uploading of encrypted data in cloud. In: Paper presented at the 2013 fourth international conference on computing, communications and networking technologies (ICCCNT).
69. Straub DW, Welke RJ (1998) Coping with systems risk: security planning models for management decision making. MIS Q 441–469
70. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11
71. Sun P (2020) Security and privacy protection in cloud computing: discussions and challenges. J Netw Comput Appl 160:102642
72. Tabrizchi H, Rafsanjani MK (2020) A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput 76(12):9493–9532
73. Takabi H, Joshi JB, Ahn G-J (2010) Security and privacy challenges in cloud computing environments. In: IEEE security & privacy, no 6, pp 24–31
74. Tan FB, Hunter MG (2002) The repertory grid technique: a method for the study of cognition in information systems. MIS Q 26(1); Data Protection Accountability: The Essential Elements (2009a)
75. The Centre for Information Policy Leadership (2009a) Data protection accountability: the essential elements, Hunton & Williams LLP, US
76. The Centre for Information Policy Leadership (2009b) Galway project plenary session introduction, US
77. The Centre for Information Policy Leadership (2010) Demonstrating and measuring accountability – the accountability project – Phase II Paris, France, France
78. The Centre for Information Policy Leadership (2011a) Getting accountability right with a privacy management program, Hunton & Williams LLP, Washington, DC
79. The Centre for Information Policy Leadership (2011b) Implementing accountability in the marketplace a discussion document accountability Phase III - The Madrid Project, Hunton & Williams LLP, Madrid
80. The Centre for Information Policy Leadership T. (2020) Are our privacy laws asking too much of consumers and too little of businesses? http://www.informationpolicycentre.com/2/post/2019/12/are-our-privacy-laws-asking-too-much-of-consumers-and-too-little-of-businesses.html
81. Toney SB, Kadam SU (2013) Cloud information accountability frameworks for data sharing in cloud—a review. Int J Comput Trends Technol 4(3)

82. Trompeter CM, Eloff JHP (2001) A framework for the implementation of socio-ethical controls in information security. Comput Secur 20(5):384–391
83. Vairagade RS, Vairagade NA (2012) Cloud computing data storage and security enhancement. Organization 1:2
84. Vaishnav J, Prasad N (2021) Security aspects in cloud tools and its analysis—a study. In: Inventive systems and control. Springer, pp 927–937
85. Vedder A, Naudts L (2017) Accountability for the use of algorithms in a big data environment. Int Rev Law Comput Technol 31(2):206–224
86. Vithanwattana N, Mapp G, George C (2017) Developing a comprehensive information security framework for mHealth: a detailed analysis. J Reliab Intell Environ 3(1):21–39
87. Wang C, Wang Q, Ren K, Lou W (2010) Privacy-preserving public auditing for data storage security in cloud computing. In: Paper presented at the INFOCOM, 2010 Proceedings IEEE
88. Wang Z, Yan W, Wang W (2020) Revisiting cloud migration: strategies and methods. In: Paper presented at the Journal of Physics: conference series
89. Weitzner DJ, Abelson H, Berners-Lee T, Feigenbaum J, Hendler J, Sussman GJ (2008) Information accountability. Commun ACM 51(6):82–87
90. Wong T-S, Chan G-Y, Chua F-F (2019) Adaptive preventive and remedial measures in resolving cloud quality of service violation. In: Paper presented at the 2019 international conference on information networking (ICOIN)
91. Yao J, Chen S, Wang C, Levy D, Zic J (2010) Accountability as a service for the cloud. In: Paper presented at the 2010 IEEE international conference on services computing
92. Yellamma P, Narasimham C, Sreenivas V (2013) Data security in cloud using RSA. In: Paper presented at the 2013 fourth international conference on computing, communications and networking technologies (ICCCNT)
93. YenimanYildirim E, Akalp G, Aytac S, Bayram N (2011) Factors influencing information security management in small-and medium-sized enterprises: a case study from Turkey. Int J Inf Manage 31(4):360–365
94. Zissis D, Lekkas D (2012) Addressing cloud computing security issues. Future Gener Comput Syst 28(3):583–592