universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Scientometric Analysis of literature on Auditing Cloud Computing“

verfasst von / submitted by

Charlotte Mann BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2020 / Vienna 2020

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 915
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Betriebswirtschaft
Betreut von / Supervisor:	ao. Univ.-Prof. Mag. Dr. Michaela Schaffhauser-Linzatti

Table of Content

Table of figures

List of Tables

Index of abbreviations

SLA	Service Level Agreement
CSP	Cloud Service Provider
DSR	Design Science Research
GDPR	General Data Protection Regulation
TPA	Third Party Audit/ Third Party Auditor
IoT	Internet of Things
IS	Information Systems
IT	Information Technology

1. Introduction

The word digitalization is on everyone's lips, likewise in current business environment. According to 77% of business cloud users the technology is significantly contributing to overall enterprise digitalization of internal processes and included in the development of digital business models. (KPMG, Bitkom Research GmbH, 2020) It is a mean for companies to enable business growth and innovation. However, as legacy security models remain and need to be reconfigured, despite increasing investments in cloud solutions the progress of adoption is slow. Security flaws need to be dissolved to unleash full value for enterprises. (McKinsey, 2018) Threats are including cloud outages due to technical disturbance, security incidents and external attacks. Many cloud-users have security concepts for various cloud scenarios however not all of them are recorded and coherent measures. Companies need to comply with data protection regulations, therefore transparent security architecture and controls and independent security certificates are important. (KPMG, Bitkom Research GmbH, 2020)

The loss of controllability is one reason why auditing cloud computing services is important to assure security and to make security communicable. Former accounting audits and IT audits must undergo strategic considerations and processes need to be extended to cover new risks emerging from the usage of cloud computing resources. (Chen & Yoon, 2010). In particular public auditing giving an additional third party access to data and infrastructure opens new and additional risks to privacy preservation. (Grandison, Thorpe, & Stenneth, 2013)

As Schumpeter stated in 1942 innovation is the "process of industrial mutation that incessantly revolutionizes the economic structure from within, incessantly destroying the old one, incessantly creating a new one" (Schumpeter, 1942). To increase effectiveness and efficiency enterprises are using information systems. (Hevner & Chatterjee, Design Science Research in Information Systems, 2010) With the increase of IT goods and services there comes a higher need for research. The growing societal infrastructure with increasing complexity created demands for new emphasizes in IT research. (Computer Science and Telecommunications Board; National Research Council, 2000) Research is essential as its leading to new ideas, testing and the amelioration of existing theories. (Mamun, Bishwajit Banik, & Hafsa, 2014)Technological advances are only developing through science research processes. (Hevner & Chatterjee, Design Science Research in Information Systems, 2010) Therefore research is inevitably a vital part of the innovation cycle leading to technological advancement.

In order to contribute to this cycle research publication on auditing cloud computing are assessed in this thesis by scientometric means. For innovation to be complete, innovation must be communicated effectively to others. That is the only way how sustainable change and innovation can take place. (Vinkler, 2010) Additionally, the persistence and long-term implementation of technology and innovation depends on how challenges are met. (Rasheed, 2013) Scientometry is a viable way to analyze the research conducted on the topic of auditing cloud computing to communicate results and enhance innovation communication. It provides information about research in a specific field, by a specific group of people or on a specific topic and provides a way to communicate sciences. It communicates innovation and progress by analyzing for example research productivity, publication patterns or theoretical trends.

The aim of this thesis is to support the information fluctuation in the field of auditing cloud computing by analyzing research productivity, publication pattern, citation and reference patterns and identifying key trends which are promising to lead towards an efficient cloud computing security. The overall aim is to communicate the safe handling of infrastructure and data and likewise elevate the usage and demand for services or products involving cloud computing services. Contributing to innovation as impetus of growth and development.

In chapter two the conceptual background of this thesis is discussed in further detail by defining cloud computing and auditing of cloud computing services and giving an overview of the associated risks and challenges. In chapter three the methodological theory of scientometrics is described before the actual analysis and results are presented in chapter four and five.

2. Conceptual Background of Auditing Cloud Computing Services

In this chapter fundamental concepts underlying this thesis are described by defining cloud computing in business context, revealing its risks and benefits. Furthermore, the importance and processes of auditing cloud computing services are narrowed down.

2.1 Defining Cloud Computing

Cloud computing is a computing area many companies have opted to integrate into their business operations. (Chou, Cloud Computing: A value creation model, 2015) Research often references the National Institute of Standards and Technology (NIST) who defines cloud computing as:

> *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. This cloud model is composed of five essential characteristics, three service models, and four deployment models.* (National Institute of Standards and Technology, 2011)

The five characteristics referred to in the NIST definition are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. (National Institute of Standards and Technology, 2011) When using Cloud Computing, companies choose to outsource their IT Infrastructure, wholly or partially, virtually to the cloud. (Chou, Cloud Computing: A value creation model, 2015) According to Hon, Millard and Walden cloud computing “provides flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand” (W.Kuan Hon, 2011). Hussain et al. describes cloud computing as a solution for on-demand computation and storage demand companies can use without devoting much time and dealing with high hardware investments upfront. Operationalization can start immediately. (Hussain & Al-Mourad, 2014)

The most well-known cloud computing providers are Amazon Web Services (AWS), Microsoft Azure and Google Cloud. (McKinsey, 2018) AWS is one of the biggest cloud platforms offering more the 175 different functions and services via its datacenters all over the world. (Amazon Web Services, Inc., 2020) It’s services are ranging from analytics, virtual reality, machine learning and Internet of Things (IoT) to storage. (Amazon Web Services, Inc., 2020) Amazon S3 is one of the most prominent data storage services on the market. (Tian, et al., 2019) Utilizing cloud storage services the cloud user being the

data owner is moving data from their local systems to the cloud. (Yang & Jia, An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, 2013) In this process the data owner loses the control over their data and many security hazards are imposed. Therefore, cloud storage auditing schemes were developed to increase its' security and reliability. (Yang & Xia, 2016) In chapter 2.2 the topic of auditing cloud computing services is continued.

According to the deployment model (Gurkok, 2017) clouds can be differentiated into Private, Community, Public and Hybrid Clouds providing different settings and levels of security (Pearson, 2009).

- **Private Cloud:** Operating a private cloud a company doesn't have to share hardware or infrastructure with other companies. The usage is exclusive to one organization, which can contain multiple users. Via private cloud the customer can use internal services like Intranet or data centers. As the company itself has operating authority over the cloud fault tolerance security can be influenced and controlled according to the company's requirements. (Chou, Cloud computing risk and audit issues, 2015)
- **Community Cloud:** Community clouds are based on shared concerns of the user like mission, security requirements or policy and compliance considerations. Individuals as well as multiple organizations can use such clouds. (Chou, Cloud computing risk and audit issues, 2015)
- **Public Cloud:** For public cloud services the cloud provider offers cloud infrastructure, which is located at the provider's premises, to any other organization for usage on a self-service, on demand, pay-per-use basis. (Chou, Cloud computing risk and audit issues, 2015)
- **Hybrid Cloud:** As implied this is a hybrid form of the afore mentioned three types of clouds. It combines various cloud infrastructures, adapting to individual needs and prerequisites. (Chou, Cloud computing risk and audit issues, 2015)

Additionally to the four deployment models three different service models can be distinguished. Those are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). (W.Kuan Hon, 2011)

- **IaaS:** Infrastructure provided through IaaS includes network, hardware and storage capacities. (Amazon Web Services, Inc., 2020)
- **PaaS:** PaaS agreements provide the companies with platforms to build, test and deploy custom applications, however the control over the applications remains with the client. (Chou, Cloud computing risk and audit issues, 2015)

- **SaaS:** The third service model SaaS provides companies with ready to use applications and software is accessible through a web browser. (Chou, Cloud computing risk and audit issues, 2015)

Both employment model and service model need to be taken into consideration when discussing cloud computing auditing in chapter 2.2.

The scope of a cloud service agreement among others specifying deployment and service mode are constituted in the Service Level Agreement (SLA). SLAs are the prevalent form of contract between the cloud service provider (CSP) and the user. It is defining the level of service the client can expect from the provider. It specifies on availability, performance and security. (Hussain & Al-Mourad, 2014) The SLA can serve as a trust base between the cloud provider and user. The adherence to the SLA can be checked by internal compliance checks and audits. Duncan and Whittington however criticize that most SLAs are too narrow in scope and too one-sided. (Duncan & Whittington, Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement, 2015) Not just that but the provider has an incentive to deceit the SLA at the clients costs to reduce costs and increase competitiveness in the very competitive cloud computing market. The provider can lower computational and storage space or move data or services to a lower quality of service level without letting the user know. As processes are run off-premise it becomes difficult for the client to check the commitment of the CSP and to identify contract breach. Clients can use third party auditors (TPA) as a mean to monitor the provider. When the client delegates the auditing task to a third-party specialist he checks periodically whether the CSP complies to the SLA. When a TPA is used as intermediary the provider also has reasons to attempt to deceit the TPA, for example by providing auditors with preferential accesses. (Hussain & Al-Mourad, 2014) The pivotal and challenging role of cloud computing auditing and third-party auditing are becoming apparent and are described in more detail in chapter 2.2.

2.2 Benefits and Risks of Cloud Computing

There are various benefits and different purposes for companies to adopt cloud computing technology which are facilitating economies of scale. They include on-demand access, flexibility, and least management from the user. This leads to cost savings, improvement of efficiency and scalability of service. Cloud computing adds to value creation of a business and becomes essential part for sustainable business continuity. Another benefit of cloud computing is mobility. Through virtualization, software becomes accessible anywhere giving employees the opportunity to work flexible in and out of office. (Chou, Cloud Computing: A value creation model, 2015) Additionally environmental sustainability

is enhanced by incorporating cloud computing technology as companies deploy less physical infrastructure devices and less energy because of scalability. (Chou, Cloud computing risk and audit issues, 2015) Please see table 1 for a comprising list of benefits.

However outsourcing processes to external vendors in general and outsourcing IT infrastructure using cloud computing in particular because of its of premise-virtual momentum bears increasing complexity and numerous risks that must be taken into consideration when incorporating it into business operations. (Chou, Cloud Computing: A value creation model, 2015) Those risks are pivotal when addressing the topic of auditing cloud computing services.

One drawback prominently mentioned in research are security concerns regarding the cloud. This is due to its virtual setting and the procession of partially sensitive data. (Chou, Cloud computing risk and audit issues, 2015) Additionally, loss of governance and compliance risks add to security considerations. (Rasheed, 2013) Companies face the risk, that cloud providers don't comply to enterprise policies, so that it loses reputation and credibility. The cloud provider itself holds the risk of processing personal data, and has legal liabilities, if it doesn't hold them it also faces loss of reputation and loss of user credibilitys. (Pearson, 2009)

Furthermore risks of authentication issues, problems with the compatibility with internal systems, dependency on system availability and business continuity appear. Another critical issue is the question of ownership of content and legal requirements that need to be met. (Chou, Cloud Computing: A value creation model, 2015) Leakage is a security risk to be face as well. The fact that data is processed and storage remotely and not on premise like before and the fact that users are using multiple different cloud platforms is causing additional security risks. (Pearson, 2009) Customers demand for secure cloud computing infrastructure to be willing to run mission-critical applications. (Foster, Zhao, Raicu, & Lu, 2017)

Rasheed specifies four data challenges that have to be taken into consideration. Those are data integrity, data confidentiality, data lineage respectively, data provenance and data remnance. To provide data integrity the data must be secured from unauthorized changes. To provide confidentiality data cannot be disclosed. To achieve data lineage respectively data provenance the computing history and origin of data must be accountable. Data remnance addresses the issue that even if data was deliberately deleted there is a possibility that residual data rests remain with the provider and can be leaked to third parties. (Rasheed, 2013) Those issues can lead to insecure cloud

frameworks (Thangavel, et al., 2016). Please refer to table 1 below for a consecutive list of benefits and risks of Cloud Computing.

Benefits of Cloud Computing	Risks of Cloud Computing
+ On-demand access	- Security issues
+ Flexibility	- Authentication issues
+ Less management duties	- Compatibility
+ Cost savings	- Dependency
+ Increase in efficiency and scalability	- Ownership debates
+ Value creation	- Data leakage/ Data integrity
+ Sustainable business continuity	- Data confidentiality
+ Mobility and accessibility	- Data lineage
+ Environmental sustainability	- Data remnance

Table 1: Overview of benefits and risks of cloud computing

2.3 Defining Auditing Cloud Computing

To overcome the risks of cloud computing solutions presented in chapter 2.2 and to incentive companies to fully use the potentials of cloud computing by cutting down adoption barriers to increase credibility and accountability is essential. To do so internal and external auditing processes can be utilized. Those processes must show the willingness and ability to process (personal) data in secure matters. (Martin Gilje Jaatun, 2016) Auditing is also essential to be legally compliant. (Chou, Cloud Computing: A value creation model, 2015) Before going into more detail regarding the auditing cloud computing processes the underlying principles of IT auditing are stated.

2.3.1 IT Audit

With the rise of cloud adoption in recent years concomitant security and risk issues are multiplying. Because of data breaches incidents in the past cybersecurity gains high attention in organizations. Simultaneously because of the rapid technological advancements of threats their control becomes more difficult. Audit and control processes are vital functions in detecting threats and identifying risks. (Al-Matari, Helal, A. Mazen, & Elhennawy, 2018) IT security audits enable the communication of level of customer data protection and company's standards for protection against threats. (Ryoo, Rizvi, Aiken, & Kissell, 2014) In order to do so IT auditors are responsible for the examination of a company's internal information system. They examine hardware, software, communication networks and interfaces. Risks negatively impairing operational processes should be identified and monitored. (Chou, Cloud computing risk and audit issues, 2015) There are different kind of threats and attacks which need to be identified

and prevented. Counteractions entail penetration testing, computer forensics and user awareness of information security. The latter is of particular importance as control issues often arise because of incorrect process execution or process weaknesses but not technological flaws. (Al-Matari, Helal, A. Mazen, & Elhennawy, 2018) Cloud computing auditing (more in chapter 2.3.2) is one form of IT Auditing but demands for customization. (Ryoo, Rizvi, Aiken, & Kissell, 2014) It can be seen as one focus of IT auditing among others like for example IT governance. (Chou, Cloud computing risk and audit issues, 2015)

The IT Auditor follows an externally compilated set of guidelines. (Chou, Cloud computing risk and audit issues, 2015) Existing law should be considered when making policy and technical choices. (Al-Matari, Helal, A. Mazen, & Elhennawy, 2018) Advances are often driven by best practice and user demands. The ISO security standard ISO 27001 is one of the prevalent guidelines in this field. (Rasheed, 2013) It is the "specification for an enterprise information security management system (ISMS)" (Al-Matari, Helal, A. Mazen, & Elhennawy, 2018). To obtain the certification a formal audit by an outside accreditor needs to be conducted. The implementation of several controls among others in the domains of cryptography and operations security need to be verified. (Al-Matari, Helal, A. Mazen, & Elhennawy, 2018) A systematic evaluation of risks, implementation of security controls embedded in an overarching management process must be documented. (Rasheed, 2013)

Another standard is the Payment Card Industry Security Standard (PCI DSS). This standard needs to be considered if handling customer credit card data. It requires the approval of a security specialists albeit the requirements are less strict then the requirements of ISO 27001. They include building and maintaining a secure network, protecting card holder data, integrating strong security measures and regular testing and monitoring of networks. (Rasheed, 2013) Furthermore the Sarbanes-Oxley Act (SOX) (2002) which was the responds to multiple accounting scandals in America should be taken into consideration. The Act requires storage times for specific financial records over multiple years. Organizations affected have to implement the necessary IT controls ensuring its security and risk-freeness. According to the Auditing Standard No. 2 an evaluation of the CSP's IT control environment is required. Additionally the Statement on Auditing Standards No. 70 (SAS 70) requires an auditor's report by the vendor's auditor. Other guidelines are provided by the Information Systems Audit and Control Association (ISACA). According to them cloud computing audit should cover the assessment of effectiveness of provider's internal controls and security, the identification of internal

control deficiencies and assessment of quality. (Chou, Cloud computing risk and audit issues, 2015)

Which standards and statements are required depends on the company's domicile, governance policy and the industry the company is operating in. As ISO 27001 and SAS 70 are more relevant for the Financial Sector, the Health Insurance Portability and Accountability Act is more applicable for organizations operating in the health service sector. (Mithani, Salsburg, & Rao, 2010) The appropriate audit approach can then be derived based on the applicable policy standards and organizational needs. (Chou, Cloud computing risk and audit issues, 2015)

2.3.2 Cloud Computing Service Auditing

The risks of cloud solutions described in chapter 2.2 explain the necessity of auditing processes for cloud computing services. Simultaneously the lack of auditability itself in various aspects of security is creating additional risks causing hesitation in adoption. Auditing is a vital mean to communicate the safe and compliant handling of security concerns to the customer. Rasheed identifies the following two key functions of security auditing – Firstly the 'security' aspect of the provider enabling secure data and infrastructure management and secondly enable the customer to verify those controls are in place and working ('auditing'). (Rasheed, 2013)

There are multiple ways to categorize cloud computing auditing. According to Chou companies can either audit their IT according to a value-added approach or a risk based audit approach (Chou, Cloud computing risk and audit issues, 2015) Before implementing cloud computing technology a company has to consider all risks and benefits respectively values that can be created through the incorporation of cloud computing services into business operation. (Ryoo, Rizvi, Aiken, & Kissell, 2014) Values that have to be considered in the value-added approach are amongst others increased flexibility, more efficient resource allocation and cost avoidance. (see table 1 chapter 2.2) Risks to be considered are authentication issues, data security and privacy, system availability, business continuity, ownership of content and other legal requirements. (Chou, Cloud computing risk and audit issues, 2015) Rasheed et al. distinguish between infrastructure security auditing and data security auditing. The first one reflecting the security controls of underlying systems which are relevant for all service levels in the cloud. The latter is concerning the confidentiality, integrity and availability of data with special criticality for PaaS and SaaS users relying on databases and platforms. In case of Infrastructure services (IaaS) the ability of auditing on the client's side is mostly given. (Rasheed, 2013)

However for this study most relevant is the distinction between private and public auditing. (Tian, et al., 2019) The privacy process within a company must be observable by the public and the user. Data transactions must meet data protection and privacy legislation and the accurate procedures need to be documented and must be showable. Therefore, internal audit should secure the underlying correct control process. The organization must appoint someone within the company responsible for this process. Its task is to monitor data accesses and modifications. (Pearson, 2009) In practice leading cloud providers approach internal cloud computing auditing by incorporating three processes. First being a sufficient risk management assessing and prioritizing risks and derive appropriate security and quality controls which build the second process of providing a secure cloud. In the third step those controls need to be monitored and evaluated. For this a compliance framework is in place to make sure the controls meet industrial and governmental standards. (Hussain & Al-Mourad, 2014)

Public auditing is referred to as Third Party Auditing (TPA) or external auditing. As monitoring a cloud provider's actions can be a burden for the client and difficult to conduct, TPAs are commonly utilized to facilitate cloud computing auditing. The TPA ensures the compliance of the CSP to the SLA providing the security and quality of service agreed on in the contract. (Hussain & Al-Mourad, 2014) Figure 1 shall depict the constellation and cohesions of the three involved parties – the CSP, the clients consisting of the data owner and the user and the TPA. A SLA is agreed on between the client and the CSP. The data owner delegates to the TPA the duty of auditing the provider who then reports his results back to the data owner. (Tian, et al., 2019)

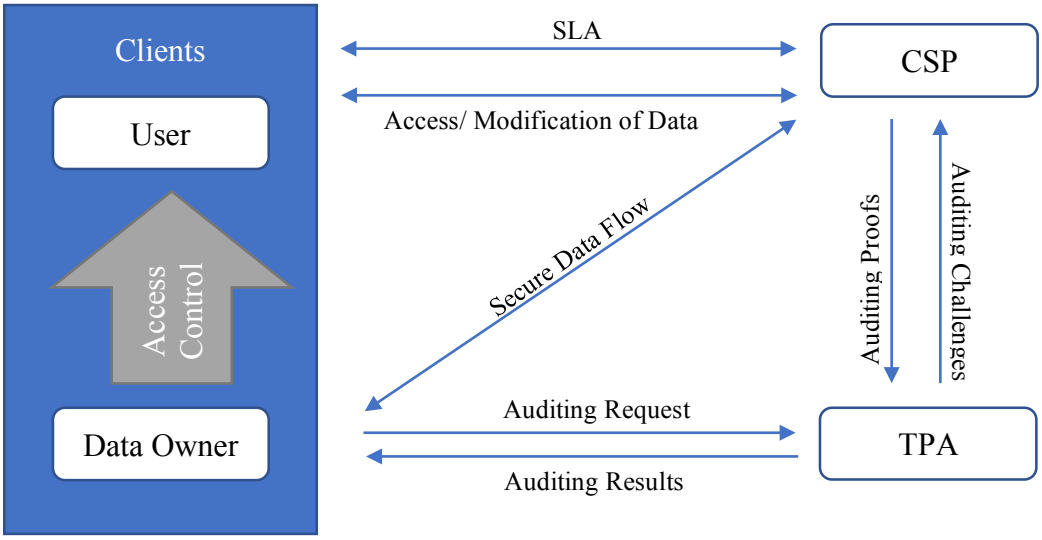

Figure 1: Relationship between CSP, User and TPA *(Tian, et al., 2019)*

The TPA checks unauthorized access of data by the provider or other users and checks for hardware failures or errors made by the CSP leading to data deletion. The challenge in this process is that the CSP can't reveal data to the TPA. This is very important for integrity being maintained. In general this is possible using six different algorithms. Figure 2 shall depict the process of Public Auditing in a simplified 5 step way. In the first step the client divides data that is going to be stored in the cloud into blocks and assigns public and private keys to those blocks enabling the TPA to audit data integrity without accessing actual data. In the second step if the client wants to check data integrity he sends a respective request to the TPA. The TPA then sends a challenge request to the CSP who generates the proof and responds to the TPA. Finally, the TPA verifies the provided proof and reports his results to the client. (Thangavel, et al., 2016)

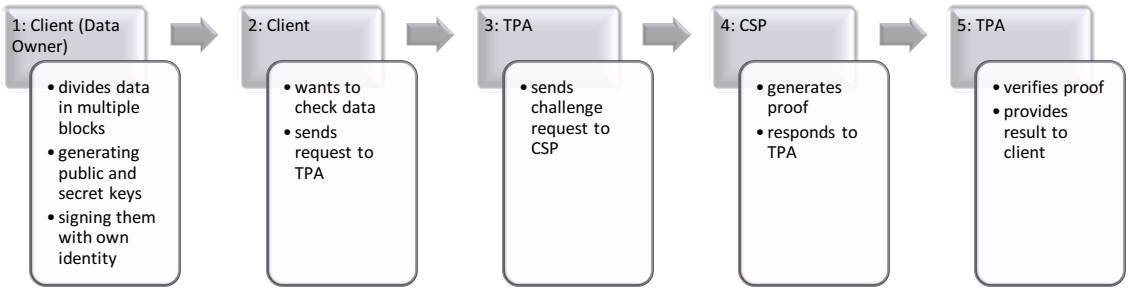

Figure 2: Public auditing process (Thangavel, et al., 2016)

2.3.3 Challenges, Properties and Techniques

However auditing processes of cloud infrastructures are challenging original IT audit frameworks as cloud services are always provided by an external provider and therefore companies rely on the outside vendor's support and control. In this regard building a trustworthy relationship between the cloud provider and the client is essential but challenging at the same time. (Chou, Cloud computing risk and audit issues, 2015) Cloud computing auditing holds various challenging implications and demands certain properties to respond to those.

The extend of audit actions depends on multiple factors like the service model (IaaS, PaaS or SaaS) or deployment model (Private, Community, Public and Hybrid Clouds) depending on different location selection, resource sharing options and openness of provision. (Chou, Cloud computing risk and audit issues, 2015) Private Clouds provide higher security and a better controllable environment. (Pearson, 2009) For IaaS customers, the implementation of own data auditing processes is easier than for SaaS or PaaS clients. (Rasheed, 2013)

Especially external audit processes conflict with the confidentiality aspect needed when working with personal data. Data leakage is one of the largest worriers in cloud computing practice. Problematic is also that there are different levels of security and privacy practice and checks implemented varying among different companies which have to be taken into consideration. (Pearson, 2009) Another challenge is the fact that cloud computing is a relatively new technology, which may hold weaknesses and immaturities not known yet. Also auditors need to be knowledgeable of all aspects of cloud computing and complete ongoing training to keep up to date with state of the art developments. It is also important for companies to manage the developed knowledge efficiently so it can be shared and distributed among the divisions. (Chou, Cloud computing risk and audit issues, 2015) Responsibility is another challenging question in this field. Organizational constructs can be very intricate and opaque and providing security means and documentation be tricky. (Pearson, 2009)

If the provider breaches a SLA contract he also has an interest and options to avoid the detection by the TPA. The CSP can deceive the TPA by launching a forge attack forging proofs challenged by the TPA, by replacing attack replacing the proofs of corrupted data or replay attacks using old proofs in order to pass the verification process. (Tian, et al., 2019) As the CSP wants to maintain its reputation he is interested in keeping contract breaches and security incidents private. This is possible because of the direct auditing

approach where the provider can control when to uphold the SLA and provide auditors with preferential access. (Hussain & Al-Mourad, 2014) Many of the underlying investigated literature name this issue showing weaknesses in public auditing models and are trying to overcome this issue.

Additionally new regulations like the General Data Protection Regulation (GDPR) (applicable since May 2018) and companies' compliance with privacy and data protection law depicts a new challenge, concerning national, company-based compliance efforts as well as the problematic trans-border data transfers. (Pearson, 2009) Within the EU the GDPR "encourages the free movement of personal data within the EU" (W.Kuan Hon, 2011).

Derived from the legislative requirements, organizational requirements, user requirements and identified challenges, auditing frameworks should hold certain properties. Desirable properties of public-auditing are the support for privacy preservation, auditing of dynamic data, batch auditing, auditing of multiple replicas and for auditing of shared data (Tian, et al., 2019) In terms of data handling the assurance of data integrity, data confidentiality, data lineage and provenance and data remnance have to be considered. (Rasheed, 2013) In order to provide secure TPA auditing the efficient audit should be possible without demanding a local copy of data preventing new vulnerabilities towards the user's data privacy. (Wang, Wang, Ren, & Lou, 2010)

Techniques to achieve those properties contain cryptography and remote data integrity checking for assuring data confidentiality and integrity. (Rasheed, 2013) For secure TPA auditing public key based homomorphic authentication with random masking can be used to conduct a privacy-preserving public cloud data auditing or bilinear aggregate signatures can be incorporated to extend to a multi-user setting (batch auditing). (Wang, Wang, Ren, & Lou, 2010) One way of increasing the security and efficiency of data security and the auditing process is batch auditing. In this form of audit the TPA performs multiple audits for different clients simultaneously. (Thangavel, et al., 2016) For privacy assurance, the homomorphic authenticator (HA) technique based on public key infrastructure (PKI) is often applied. To additionally minimize the risks of data leakage random masking technique or zero knowledge proof can also be incorporated. The dynamic nature of cloud data being accessed and updated frequently can be considered in dynamic auditing frameworks utilizing the Merkle hash tree (MHT) data structure. Batch Auditing and multiple-replica auditing can be facilitated via the bilinear aggregated signature technique. (Tian, et al., 2019)

3. Methodology - Conceptual Background of Scientometrics

In chapter two a picture was drawn of the concept of cloud computing and the underlying challenges of auditing cloud computing services to assure security, accountability and credibility. As auditing cloud computing is an evolving subject with high relevance for companies and developers it is a much-bespoken topic in current literature and research. Employing scientometric means to the scientific literature on the topic of auditing cloud computing is conducted in this thesis. Before the practical scientometric analysis is conducted in chapter 4 the methodological approach of scientometrics is being described theoretically.

3.1 Methodological description

In this subchapter, the science field scientometrics is being defined and described. Scientometrics is the study of science or more precisely the assessment of the dynamic evolvement of a discipline. It is related to the research fields bibliometrics and infometrics but in comparison solely assesses science and technology literature. (Hood & Wilson, 2001) Scientometric assessments are used to evaluate and improve an academic discipline. (Lewis, Templeton, & Luo, 2007) Underlying assumption of this meta-perspective on a discipline is that scientific activity is reflected through scientific publication. Empirical measures are applied to research output to explore the fundamentals of the publications and analyze general research activities like the development of key topics or socio-organizational structures. (Heilig & Voß, 2014) Additionally output is not only evaluated regarding growth, structure, interrelationships and productivity but it furthermore elaborates on broader aspects like the role science and technology plays in the national economy or the influences of governmental policies towards science. (Hood & Wilson, 2001)

Contribution to science is only made if something is given to the common fund of knowledge. Therefore, the aim of science is not only to produce knowledge but also to communicate it. That is what makes scientometrics as important as it is, being a science on science for science, processing scientific research for more efficient management of science. (Vinkler, 2010)

Assessing the impact of scientific information by conducting a scientometric assessment there is no absolute method to carry out to determine the absolute position of a research topic, author, institution etc. but only the relative position can be determined. There is not one single strict set of rules or directory to conduct scientometric assessment. Laws or rules cannot be regarded as hard. They should rather be regarded as trends. As science

is multidimensional it should always consider several aspects and therefore incorporate several indicators to encompass the entire momentum. (Vinkler, 2010)

3.2 Assessment plan and specifying the purpose of the assessment

The assessment plan underlying this analysis of literature was developed based on the theoretical introduction to scientometrics "The Evaluation of Research by Scientometric Indicators" by Peter Vinkler and other scientometric analysis like "Artificial Intelligence Research in India: A Scientometric Analysis" by Rishabh Shrivastava and Preeti Mahajan.

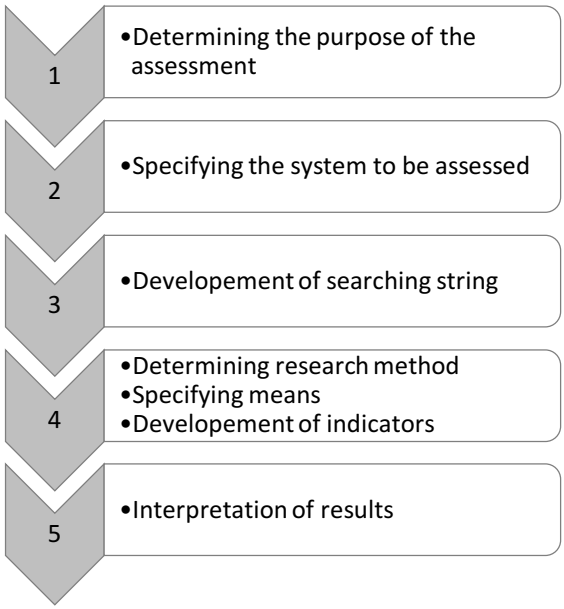

Figure 2: Assessment plan

The process of a scientometric analysis can be split up in multiple steps. (Vinkler, 2010) Figure 2 gives an overview of the five steps in the assessment planning process which are described in more detail in the following. In the first step the purpose of the assessment was specified. The objective of this assessment is to study the research performance in the field of auditing cloud computing. Aiming to precise the role of audit and identifying trends in this field. In the second step the system assessed needs to be further specified. Underlying base are publications on auditing cloud computing without further indicators like specific timeframe or geographical position. Restrictions were put on the selection of publications. All underlying publications were published in peer-reviewed sources. Those are for example IEEE, ACM, Elsevier, Springer, Wiley, Sage, INFORMS, Emerald, Inderscience, IGI and Taylor & Francis. Thirdly an appropriate searching string had to be developed to filter out the relevant literature. See table 2 (chapter 3.3) for the generic search queries that were developed. Rows in section B were removed in cleansing actions during the process because of inaccurate data records. The

data collection process is described in more detail in the next chapter 3.3 Dataset description.

Main part of developing the assessment plan is selecting methods and specifying indicators for each examination criterion. There are two main assessment methods used in scientometrics, peer review and method of quantitative indicators. The selection of method depends on the purpose and condition of the assessment and can also be based on personal preference. Structure and aiming of both are similar however there are differences. The method of quantitative indicators is mainly based on citation and can be carried out without limits on time and number of evaluators. Furthermore the latter does not highly follow determined provided structures and rules, it rather develops from within itself. As in the following assessment in the field often a mixture of both methods is applied and boundaries are fluent. (Vinkler, 2010, S. 199-200) For this assessment criterions that were chosen to be assessed in further detail are research productivity, reference and citation pattern, authorship structure, keywords, titles, topic, research question and proposed research outcome. For each criterion a set of indicators was developed to assess the data and develop results and trends. To assess the research productivity the total number of publications, the date of first paper published and the distribution of number of publications for each year is being analyzed. Various key figures were used to describe the publication pattern – the share between journal and conference publications, distribution of research sources, determining key outlets, analyzing the scientific field of the outlets, language distribution, country distribution, analyzing collaborative publications with regards to number of authors and countries. The citation and reference pattern is assessed by looking at the number of citations per paper and identifying key publications, the number of references and the average reference count depending on the citation count. Identifying key researchers and analyzing their nationality and citation count gives more information of the authorship. Additionally the keyword count and main keywords are being analyzed.

In the second part of the analysis quantitative and qualitative assessment techniques are used to assess title, topic, research question, research method and research outcome. Titles of the underlying publications are analyzed with regards to their word count and keywords used. Within the topic analysis the appearance of internal and external audit topics is being assessed to determine which topic is of more significance and what other topics appear. The research questions are being assessed by identifying main challenges and thereby trends in the challenges of auditing cloud computing. The proposed research outcomes are being assessed to identify key strategies and new trends in auditing cloud computing. Finally the research method used to find solutions to the set challenges differ

from publication to publication however trends in research methods applied can be identified.

In the last part of the assessment an interpretation of the results is obtained and connected to components outside of the system like science political issues.

3.3 Dataset description

In this thesis, scientific literature on the topic of auditing cloud computing is being assessed. The data collection process is described in the following. Underlying scientific publications are journal and conference publications. Book chapters and other are not included in the assessment. (Vinkler, 2010) Elicitation of relevant publications was conducted twice in 2018 and 2020.

		1)	2)	3)	2)	3)	
		Searching String	Google Scholar	Peer-reviewed	Google Scholar	Peer-reviewed	
			Until 2017	Until 2017	2018-2020	2018-2020	**Total**
A	Included	**"Cloud Computing Auditing"**	66	19	22	6	25
	Included	**"Cloud Computing Internal Auditing"**	1	0	2	0	0
	Included	**"Cloud Computing Audit"**	45	7	13	1	8
	Included	**"Auditing Cloud Computing"**	273	71	63	28	102
			385	**97**	**100**	**35**	**132**
B	To Broad	"Cloud Computing Data Protection"					
	Off-topic	"Cloud Computing IT Security"					
	Not feasible	"Cloud Computing Auditing" internal					
	Not feasible	"Cloud Computing Auditing" external					
	Not feasible	Cloud Computing "internal Auditing"					
	Not feasible	"Cloud Computing" "internal Auditing"					

Table 2: Searching String Framework and number of underlying publications

In order to determine the underlying scientific publications to be included in this assessment searching strings were developed (see table 2 column 1) Searching String).

Those searching strings provided a first indication of relevant literature on Google Scholar. The searching strings to be included further in this research were then to be narrowed down. The strings in section A "Cloud Computing Auditing", "Cloud Computing Internal Auditing", "Cloud Computing Audit" and "Auditing Cloud Computing" were further included in the analysis. The strings from section B were dropped and not further considered for the assessment because the searching strings were to broad, off-topic or not feasible.

In the next step, the numeric results on Google scholar were checked for each string to get a feeling if the framework provides enough publications as data basis. In total 385 (until 2017) and 100 (2018-2020) results were showing in Google scholar. (See columns 2) Google Scholar)

To ensure the quality of the data basis and the assessment only publications from peer reviewed sources were included. (See columns 3) Peer-Reviewed) Peer review is a principal procedure of quality judgement. (Vinkler, 2010) Peer reviewed sources taken into consideration in this assessment are amongst others IEEE, Elsevier, Springer, Wiley, Emerald, ACM, INFORMS, Inderscience, IGI and Taylor & Francis. After scanning the Google results for peer reviewed sources 132 (97 (until 2017) + 35 (2018-2020)) publications remained to be considered for this scientometric assessment.

4. Scientometric Assessment

Based on the afore acquired dataset (chapter 3.3) the 132 publications are analyzed regarding various metrics in the following. Those metrics include quantitative metrics regarding publication patterns and growth as well as qualitative metrics concerning the substantial focal points.

4.1 Measuring research productivity and research growth

The underlying literature of 132 publications covers a time span of 10 years from 2010 to 2020.

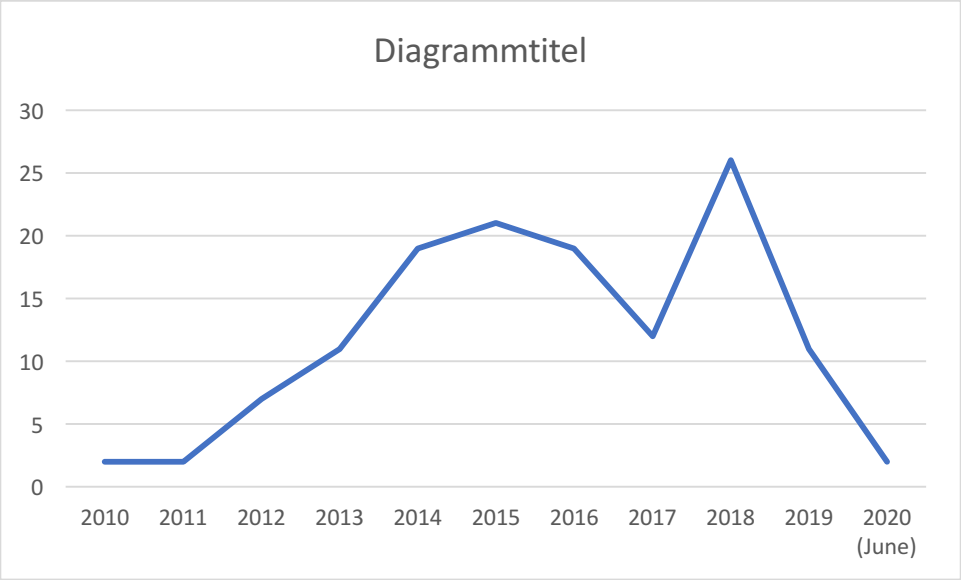

Figure 2: Annual distribution of publications

Figure 3 shows the distribution of number of publications for each year between 2010 and 2020 (as of June 2020). In the first two years 2010 and 2011 only two publications per year were countable. From 2012 onwards research starts to increase significantly to 7 in 2012, 11 in 2013, 19 in 2014 until 21 in 2015. In the years 2016 and 2017 research output is declining first to 19 then to 12 publications per year. This is followed by a steep incline of research output in 2018 with a total of 26 publication. After this peak the curve dropped again in 2019 to 11 publications. This year as of June 2020 only two relevant publication could be identified, despite the fact that this covers only half of 2020 it looks like the curve is further plummeting in 2020. So far two peaks of research output are visible, one in 2015 and one in 2018. Those could be interpreted as waves. If they are waves a higher output of research publications would be expected for 2021. Innovation happens in cycles or waves. The environment needs time to adapt, process and refine innovation. This also holds for cloud computing auditing techniques. Therefore an undulated course research

publications is feasible. A lasting decrease in publication output would be unexpected because of the topic's relevance for today's business world. If publication output stays at that level or further decreases the obstacles of auditing cloud computing will remain.

4.2 Analyzing the publication pattern

In this chapter, the publication pattern is being analyzed. The publication pattern describes the way literature on the topic of auditing cloud computing is being published. More precisely it includes looking at which outlets are predominantly chosen for publishing content on auditing cloud computing, the publication language predominantly used in this area, prevalent countries of publication and the number of authors per publication. Those key figures are giving an impression about where and how publication on the topic of auditing cloud computing are published.

4.2.1 Source and Outlet

Included in this analysis are solely scientific journal publications and conference publications. The pie chart in figure 4 depicts the share of both types of publications, showing the dominance of 93 conference publications to 39 journal publications which amounts to 70% and 30%. It can be concluded that literature on the topic of auditing cloud computing is predominantly published in conference outlets.

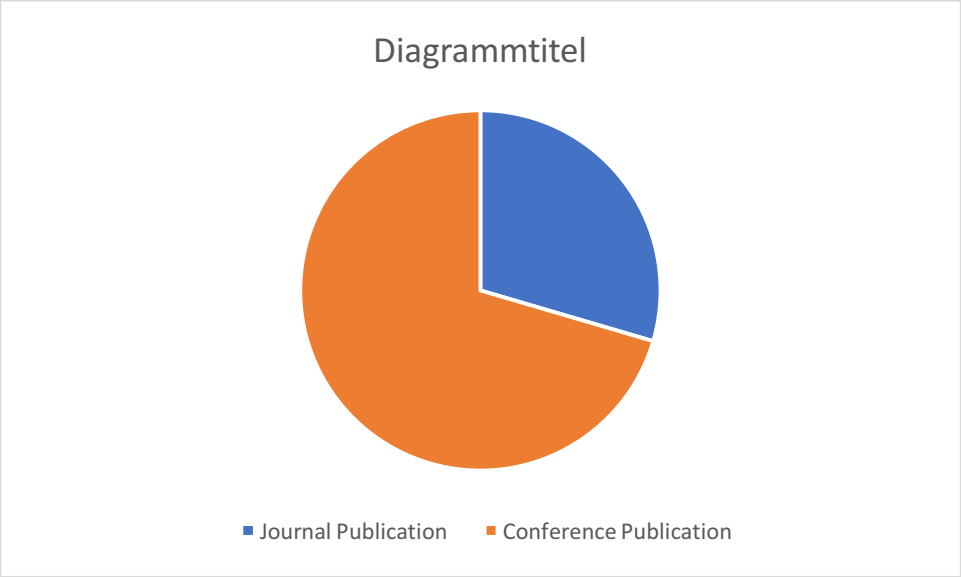

Figure 3: Share of conference and journal publications

Looking at the distribution of publications between the peer-reviewed outlets shows that the final data set was extracted from seven of them - IEEE, Springer, Inderscience, Elsevier, ACM, MDPI and Wiley - whereby IEEE is by far the most prominent source with 107 publications out of 132 in total which account for 81%. Figure 5 shows the distribution

between the 6 outlets in more detail. The second highest publication count was extracted from Springer with a count of twelve publications. The others provided between one and six publications each. IEEE seems to be the most prominent and comprehensive outlet of all.

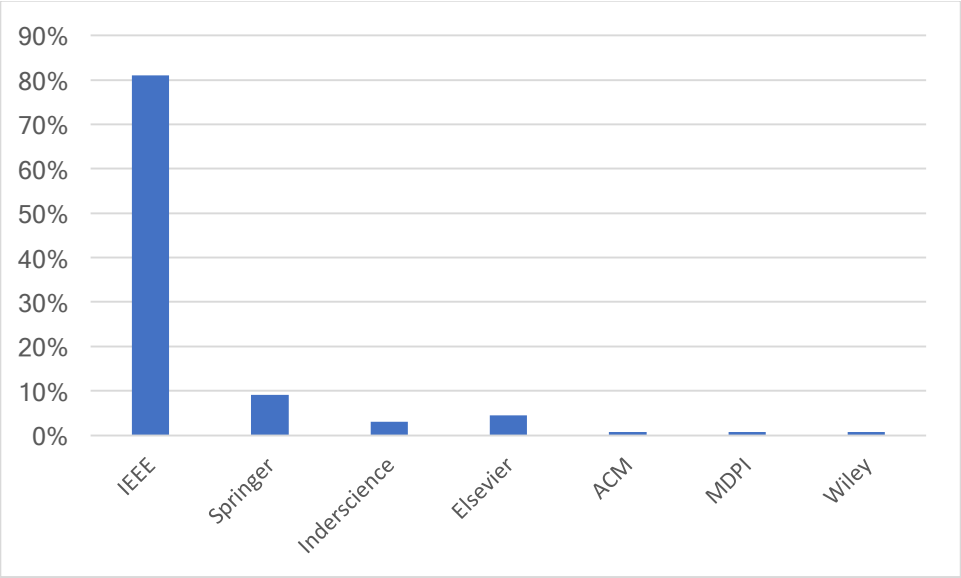

Figure 4: Distribution between peer reviewed sources

In the next step the individual outlets were analyzed. In total 78 different conference outlets and 26 different journal outlets were counted. The conferences with the highest count of publications is the International Conference on Cloud Computing Technology and Science (CloudCom) with four publications. (see table 3) In the proceedings of CLOUD, World Congress on Services and CICN respectively three of the underlying 78 conference publications were published. The mass of conference outlets appears only once (69 out of 78). There is a similar spread of journal publications with 24 out of 26 journals accounting for one or two publications. The two journals with a significantly higher publication contribution to the underlying publication base are the journal “IEEE Transactions on Information Forensics and Security” (6 publications) and “IEEE Access” (4 publications) (see table 3). This accounts to respectively 15% and 13% of the overall 39 journal publications.

Conference	Publications per Outlet
International Conference on Cloud Computing Technology and Science (CloudCom)	4
International Conference on Cloud Computing (CLOUD)	3
World Congress on Services	3
International Conference on Computational Intelligence and Communication Networks (CICN)	3
Journal	
IEEE Transactions on Information Forensics and Security	6
IEEE Access	4

Table 3: Most prominent Conference and Journal Outlets

Further analysed was also the field of the underlying publication outlets. For each publication in the data base it was recorded whether the outlet covers technical or business related topics. Figure 6 shows the outcome of this analysis - The very strong dominance of technical outlets, counting 124 of 132 publications were published in technical outlets. All key outlets (conference and journal) determined in the segment above are technical outlets. That finding is stringent with cloud computing and auditing cloud computing being an IT technology. But as the topic is also highly business relevant and an unneglectable issue in the adaption process of cloud computing technology it would have been expected that there would be more research done in business context to overcome this barrier and facilitate the secure incorporation of cloud solutions into business environments.

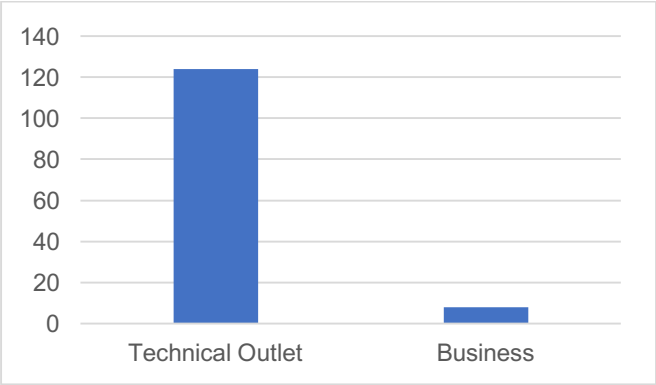

Figure 5: Distribution of technical and business outlets

4.2.2 Language and Country distribution

This chapter discusses the language and country distribution of the underlying publication base. All 132 publications were published in English language. More variation is found when looking at the country distribution. The 132 publications are assignable to 31 different countries. All continents America, Europe, Africa and Asia are represented. Table 4 shows the number of publications per country. It shows single country contributions (dark grey) and international collaborations (publications with up to four contributing countries). The 132 publications of the data base consist of 106 single country contributions and 26 international collaborations, which is a relation of 80% to 20%.

Country distribution	China	India	US	UK	Taiwan	Australia	Hong Kong	Germany	Canada	Saudi Arabia	Scotland	South Korea	Brazil	France	Pakistan	South Africa	Belgium	Colombia	Egypt	Greece	Israel	Italy	Jamaica	Malaysia	Marocco	NZ	Nigeria	Qatar	Romania	Sweden	Switzer-land
China	33	1	8		2	4	3		2			2								1											
India	1	33			2																										
US	8		9			1	1					2																			
UK				5																			1					1			
Taiwan	2	2			3																					1					
Australia	4		1			1	2																								
Hong Kong	3		1			2	2																								
Germany								4																							
Canada	2								1																						
Saudi Arabia										3																					
Scotland											3																				
South Korea	2		2									1																			
Brazil													1																		1
France														0			1					1									2
Pakistan															1																
South Africa																2															
Belgium																	0														
Colombia																		0								1					
Egypt	1																		1												
Greece																				0											
Israel														1			1				0										
Italy														1			1				1	0									
Jamaica			1											1									0								
Malaysia															1									0							
Marocco				1																					1						
NZ																										0					
Nigeria																		1									0				
Qatar			1																									0			
Romania													1																1		
Sweden														1																0	
Switzerland																															0
Single Country	33	33	9	5	3	1	2	4	1	3	3	1	1	0	1	2	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0
Collaboration* *Collaborations with up to 4 countries possible	17	2	10	1	3	4	3	0	2	0	0	2	1	2	1	0	1	1	0	1	1	1	1	1	0	1	1	1	0	1	1
Total	50	35	19	6	6	5	5	4	3	3	3	3	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Table 4: Country distribution

Table 5 lists the leading contributing countries explicitly. China and India are with 50 and 35 contributions (single country contributions and international collaborations combined) leading the list followed by the US with 19 contributions. The UK, Taiwan, Australia, Hong Kong and Germany show between 6 and 4 contributions. It is visible that China both in national publications as well as international collaborations is leading the board. In contrast India is rather less involved in international collaborations. The US shows an almost even ratio of 9 national and 10 international publications. Germany is the only of the listed countries not involved in any international collaboration. With a count of 17 and 10 the most international collaborations are showing the countries China and the US.

Country	National Collaborations	International Collaborations	Total
China	33	17	50
India	33	2	35
US	9	10	19
UK	5	1	6
Taiwan	3	3	6
Australia	1	4	5
Hong Kong	2	3	5
Germany	4	0	4

Table 5: Leading contributing countries

4.3 Examination of citation and reference patterns

Information on citation and reference count was directly extracted from the respected source of each underlying publication (eg. IEEE and Springer or the web page researchgate.com) and the outcome will be further analyzed in this chapter.

4.3.1 Citation Analysis

Number of citations lay between 0 and 261. The average number of citations is 13,33 citations per publication. Table 6 shows the distribution of citations, showing 36% of uncited publications and 43% publications with citation count ranging from one to ten. Those account to 80% of all 132 underlying publications. 16 publications are counting between 20 and 100 citations. The range between 11 and 20 and exceeding 100 are with 5% and 2% in single digit spectrum.

Citation Count	Number of Publication	Percentage (%)
Uncited	48	36%
1-10	57	43%
11-20	7	5%
20-100	16	12%
101-200	2	2%
201+	2	2%
Total	132	

Table 6: Distribution of citations

Four publications show a citation count above 100. (see table 6) Two of those publications were conducted by Hong Kong based research institutions, one in the UK and one was an international collaboration of China and Canada based researchers. Even though Hong Kong is listed among the leading contributing countries (table 5) it is far behind the leads China and India, therefore it is notable they are listed with most citations twice. Even though China is leading the list of contributing countries it is only represented regarding its citation count here with one collaborative contribution. Also standing out is the fact that even though most of publications are from conference outlets (70%), all four publications are journal publications. Also, all four publication are collaborations with two to three contributors.

Name of Publication	Year	Citation Count	Country	Outlet	Collaboration/Number of Authors
An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing	2013	261	Hong Kong/China	Journal	C/2
Data storage auditing service in cloud computing: challenges, methods and opportunities	2012	243	Hong Kong/China	Journal	C/2
A critical review of cloud computing: researching desires and realities	2012	142	UK	Journal	C/2
Oruta: privacy-preserving public auditing for shared data in the cloud	2014	113	China & Canada	Journal	C/3

Table 7: Publications with over 50 citations

This research was conducted over a period of two years from 2018 to 2020. The citation count was recorded once in 2018 and once in June 2020. Therefore, it is possible to additionally look at the citation growth over the last two years. The average citation count per paper increased from 8,59 to 13,33 which is an increase of just over 55%. For the literature that was collected in 2018 (97 publications) the overall citations increased from 822 to 1760 which is an increase of roughly 114%.

4.3.2 Reference Analysis

In this chapter the reference pattern of the underlying 132 publications is being analyzed. For three publications, no reference count was acquirable. 128 publications list 5 to 62 references. There is one outlier with 205 references. The outlier publication is “A critical review of cloud computing: researching desires and realities” by Venters and Whitley. Table 8 shows the distribution of references. With a count of 53, 40% of the underlying 132 publications list between 11 and 20 references. The average number of references per paper is 23,9.

Reference Count	Number of Publications
1-10	16
11-20	53
21-30	28
31-40	19
41-50	6
51-60	4
61-70	2
71-80	0
81-90	0
91-100	0
100 +	1

Table 8: Distribution of references per publication

Next the average number of references depending on the number of citations was analyzed. (see table 9) It shows that uncited papers feature the lowest average reference count (19). The average reference count increases with the citation count. Respectively it can be said that publications with high citation counts on average show a high reference count.

Citation Count	Number of Publication	Sum of References	Average references/ publication
Uncited	48	892	19
1-10	57	1252	22
11-20	7	223	32
20-100	16	465	29
101-200	2	238	119
201+	2	86	43

Table 9: Average number of references depending on citation count

4.4 Authorship Analysis

In this section, the authorship of the underlying publication was analysed. The number of contributing authors lies between one and nine authors. 125 of the 132 underlying publications were published by more than one author, accounting for 95%. Publishing in collaborations seems to be a dominating trend in comparison to the seven publications by only one author (5%). (see figure 5)

Figure 6: Share of collaborations

When looking at the distribution of author count (table 10) it becomes visible that a count of two and three authors is the most prominent author count with 45 and 33 publications. This statement is undermined by looking at the average number of authors per publications over the period covered which is 3.3 per paper. The trend towards collaborative publications becomes visible. In total 47 publications were published by more than three authors, only seven were non-collaborations with one author.

Number of Authors per Publication	Number of Publications
1	7
2	45
3	33
4	22
5	12
6	9
7	1
8	1
9	2

Table 10: Distribution number of authors per publication

In total 384 authors contributed to the 132 underlying publications. 347 researchers were solely involved in one single publication. 37 authors were involved in more than one publications with a range between two and three contributions. Whereby most of the 37 researchers were involved in two publications (31) and six in three publications. The six researchers publishing three papers were identified as key authors. Their names are Xiaofeng Chen, H. Zhu, B. Duncan, M. Whittington, Kan Yang and Jie Wu. (see table 11) Looking at the coherent countries is partially inconclusive as some authors (Yang and Wu) published for different universities in different countries. The authors Chen and Zhu solely published for Chinese institutions. The two authors from Scotland Duncan and Whittington both collaborated on three publications. The researcher Kan Yang is from Hong Kong but published one of his researches at a Canadian institution. Last but not least Je Wu published in the US and China. Looking at the citation count shows an average for the top authors of 40,4, which is a significantly higher average then the general citation average of 13,33 citation per publications (see chapter 4.3.1). Five of the 18 publications were published in journal outlets. Those 27,8% are consistent with the findings of the journal-conference-distribution which was analyzed in chapter 4.2.1.

Name author	Publication Count	Country	Title	Year	Outlet 1	Citation Count
Xiaofeng Chen	3	China	An Efficient Proof of Retrievability with Public Auditing in Cloud Computing	2013	Conference	7
			An Efficient Public Auditing Protocol With Novel Dynamic Structure for Cloud Data	2017	Journal	40
			Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation	2016	Journal	57
H. Zhu	3	China	Leveraging Cloud Computing for Privacy Preserving Aggregation in Multi-domain Wireless Networks	2012	Conference	1
			SecCloud: Bridging Secure Storage and Computation in Cloud	2010	Conference	56
			Third Party Auditing for Service Assurance in Cloud Computing	2017	Conference	2
B. Duncan	3	Scotland	Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement	2015	Conference	4
			Reflecting on Whether Checklists Can Tick the Box for Cloud Security	2014	Conference	7
			The Importance of Proper Measurement for a Cloud Security Assurance Model	2015	Conference	4
M. Whittington	3	Scotland	Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement	2015	Conference	4
			Reflecting on Whether Checklists Can Tick the Box for Cloud Security	2014	Conference	7
			The Importance of Proper Measurement for a Cloud Security Assurance Model	2015	Conference	4
Kan Yang	3	Hong Kong	An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing	2013	Journal	261
		Canada	Identity-preserving public auditing for shared cloud data	2016	Conference	4
		Hong Kong	Data storage auditing service in cloud computing: challenges, methods and opportunities	2012	Journal	243
Jie Wu	3	USA	Auditing cloud service level agreement on VM CPU speed	2014	Conference	5
		China	CDCAS: A Novel Cloud Data Center Security Auditing System	2014	Conference	4
		USA	Consistency as a Service: Auditing Cloud Consistency	2014	Journal	17

Tabelle 11: Identified key authors

4.5 Keyword Analysis

In this section, the keywords indicated in the underlying literature are being analyzed to identify focal points and trends of high importance in this research field. The keywords were extracted directly from the publications (authors keywords) or the outlet website (e.g. IEEE). In total 640 keywords were counted. After clearing for multiple mentions 328 different keywords were detected. Per publication, a range between two and twelve keywords was used. On average 4,9 keywords were used per paper. Besides the expected key keywords “Cloud Computing” and “Auditing” six other key keywords with more than ten mentions were identified. (see table 12) From the table below the topics of auditing, public auditing, security issues, data integrity issues, data storage which were mentioned in chapter 2 are confirmed as being key topics of today’s research regarding auditing cloud computing. The fact that besides the keyword “Public Auditing” also the keyword “TPA” (Third Party Auditor) is among the list of key keywords indicates a relevance of external auditing for cloud computing auditing.

Keyword (Group)	**Count**
Cloud Computing	70
Auditing	27
Public Auditing	24
Cloud Storage	23
Security	22
Data Integrity	14
Privacy Preservation	13
TPA	13

Table 12: Top 8 identified keywords (keyword groups)

4.6 Title Analysis

The 132 different titles were analyzed regarding their length and whether they are formulated as a question. Additionally, the titles were scanned regarding keywords used in the title, to help identify key trends.

The average word count is 10 words with a minimum count of four words and maximum count of 22 words. None of the titles were formulated as questions.

To identify the most prominent words used in the titles all titles were scanned for keywords. The keywords were selected based on apparentness and the keyword analysis in chapter 4.5. Table 13 shows the keywords and the respective count in the titles. The percentage term is based on the 132 publications in the data set and depicts the most used keywords. Apparent keywords are ‘Cloud’, ‘Cloud Computing’ and ‘Audit’ as the whole assessment is based on scientific literature on auditing cloud computing. Therefore, it was expected that those terms show high counts in the title analysis. The words ‘Cloud’ and ‘Audit’ show the highest counts with 113 and 98 appearances in the title. That are 86 % and 74 % of the 132 publications of the data set. The term ‘Cloud Computing’ has less counts (36) and is with 27% on the 6th rank of frequent title keywords. The words ‘Storage’, ‘Data’ and ‘Security’ are with 32, 31 and 30 percent the more suggestive ones as they give first insight which topics and challenges are the most prominently bespoken ones in scientific literature. This finding is congruent with the findings of the keyword analysis in chapter 4.5 where ‘Security’ shows the third highest count after ‘Cloud Computing’ and ‘Audit’. The terms ‘Public Auditing’ and ‘Privacy’ appear on 7th and 8th place with 29 and 22 counts. ‘Efficiency’ and ‘Integrity’ are also in the mid-range of keywords both counting 17 (13%) mentions. Whereby ‘Integrity’ already occurred in the keyword analysis ‘Efficiency’ is a new additional trend indicator. In the lower section of title keywords within a range between one and nine percent are the keywords ‘Dynamic’, ‘Cloud Audit’, ‘TPA’, ‘Data Integrity’, ‘Communication’, ‘SLA’ and ‘Personal’.

Keyword	Count	%
Cloud	113	86%
Audit	98	74%
Storage	42	32%
Data	41	31%
Security	39	30%
Cloud Computing	36	27%
Public Auditing	29	22%
Privacy	22	17%
Efficient/Effective	17	13%
Integrity	17	13%
Dynamic	12	9%
Cloud Audit	7	5%
TPA	7	5%
Data Integrity	4	3%
Communication	3	2%
SLA	3	2%
Personal	1	1%

Tabelle 13: Keywords Title

4.7 Topic Analysis

To analyze the researched topics on a high level in order to determine a focus on external or internal auditing or other topics for each of the 132 publications of the data set the topic was condensed in one short paragraph (see Appendix – 'Research Subject'). The topics were clustered during the data acquisition process. The publications were clustered regarding whether the topic relates to 'Audit' or/and to another topic ('Other'). And when it related to 'Audit' it was also captured whether it referred to 'External Audit', 'Internal Audit' or 'External and Internal Audit'. The terms external and internal audit were explained in chapter 2.2.

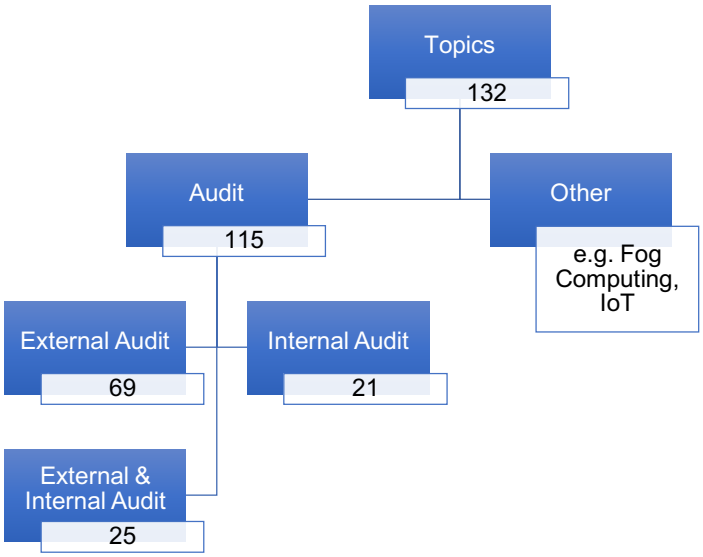

Figure 7: Outcome topic analysis overview

115 publication of the 132 publications of the data set address topics related to 'Auditing', leaving 17 papers with 'Other' main topics. 69 of the 115 'Audit'-related publications address a topic regarding 'External Auditing'. 21 are related to 'Internal Auditing' and 25 to both external and internal auditing. This shows the great relevance of external auditing in research literature. The 17 publications categorized as 'Other' are for the foremost addressing topics around the cloud e.g. about deploying cloud computing, assessing the risks of cloud computing. But also covering more diverse topics like IoT security or fog computing.

4.8 Analyzing the underlying research questions

Every research usually addresses a specified research question, a challenge in the underlying research field the research is aiming to contribution too with a solution or a refinement of an existing solution. The research questions of the underlying 132 publications are being analyzed in this chapter aiming to identify key research questions in the field of auditing cloud computing enabling the identification of key challenges that need to be overcome in the future. In order to do so the research question of each publication, which is usually mentioned within the abstract or at the beginning of the research paper, was outlined in one paragraph (see Appendix 'Research Challenge'). Those paragraphs were further analyzed by reading and keyword extraction.

From the overall assessment 8 key categories were derived. (see table 14) 32 publications are mentioning challenges regarding data. Those comprises amongst other data corruption, integrity, localization, loss, privacy, security, verification and unauthorized modification. General security concerns are raised in 17 publications. 16 publications

mention various challenges regarding the actual auditing schemes, let it be the challenges for existing audit schemes in terms of efficiency and speed, high costs for private auditing or the missing focus on batch auditing. Eleven publication raised concerns about the role and the actions of the TPA specifically querying privacy concerns due to their self-interest and the risk of local copies of outsourced data. Between eight and four publications address the challenges of access control, costs, attacks due to enlarged attack surface and internal threats, the burden and time requirements of computation and last but not least the flaws of the SLA risking deceit, being too narrow and lacking possibilities to detect disruption. The literature on those challenges is being analyzed in more detail below.

Research question – Challenge mentioned in underlying literature	Publication Count
Data	32
Security	17
Audit	16
TPA	11
Access Control	8
Costs	7
Attacks	6
Computation	5
SLA	4

Table 14: Identified key research challenges

As discussed in chapter 2 security and privacy concerns are considered one of the downsides of cloud computing technology. (Chen & Yoon, 2010) In his publication, Rasheed Hassan emphasizes that security concerns are one of the main causes for the reluctant usage of cloud computing services in companies. Those concerns are tied to the lack of audit options that customers have. (Rasheed, 2013). Likewise Zhou et al. are stressing how security and privacy concerns detain potential cloud computing users due to caveats regarding availability, confidentiality, data integrity control and audit. (Zhou M. , Zhang, Xie, Qian, & Zhou, 2010) The cloud user is concerned about their data stored in the cloud. Therefore, assuring privacy and security and creating trust on the user's side is a key challenge for the cloud computing provider. (Mythili & Anandakumar, 2013)

Data leakage and loss are named as one of the dominating challenges' cloud computing audit is facing. Data leakage violates data confidentiality that should be ensured by the provider. This needs to be supervened with the issue of data loss. (Hussain & Al-Mourad, 2014) Additionally, modification and deletion are issues that are being addressed. (Raja & Ramakrishnan, 2017) Especially in a shared cloud environment like a public cloud environment data leakage can occur. If data is stored in a place accessible by other applications, even if it's just temporarily, leakage is possible. As with the usage of cloud

services, let it be applications or infrastructure, with the transfer of data the control is transferred to the third party as well. This loss of control implies amongst others security and privacy challenges. Research agrees that auditability requires an extra layer of security to be applied to data. (Chen & Yoon, 2010)

Existing (IT) audit schemes are challenged by the new cloud computing environment. The notion of IT auditing and cloud computing auditing were described in chapter 2. According to David Chou IT auditing "should examine a company's internal information systems and their inputs, outputs, and processing components" (Chou, Cloud computing risk and audit issues, 2015). As cloud computing is changing the IT environment this change also challenges IT Auditing and adds additional new challenges. Because cloud computing is using external information systems resources auditing partially differs from traditional auditing. Depending on the deployment option for cloud services (Private, Public, Hybrid) the effect on auditing practice also shows in operational differences. To adapt to the cloud computing environment IT auditors must understand and consider the details of cloud computing and have to comply with regulations. From the underlying publications it can be deduced that the virtualized and complex environment (Chou, Cloud computing risk and audit issues, 2015), lack of tools (Oliveira, Sendor, Garaga, & Jenatton, 2013), the different cloud models (Konoor, 2016), low security setting's at the clients side (Yu, Ren, Wang, & Varadharajan, 2015), lack of near-real time audit schemes (Park, Spetka, Rasheed, Ratazzi, & Han, 2012), limitations of audit schemes (Tang, Qi, & Huang, 2016), and the burden of high computation power are challenging existing auditing schemes. (Zhang & Zeng, 2014) Supporting privacy and auditing simultaneously is difficult which is discussed by Grandison et al. Especially when client information is involved cloud computing service providers have to assure that sensitive data is secure simultaneously guaranteeing privacy requirements are met. To achieve that the creation of privacy-preserving audit logs and random privacy-preserving audit mechanisms have to be taken into consideration. Grandison et al. emphasize this demand for more technology enabling cloud users to confirm privacy and auditing protocols are being followed correctly. (Grandison, Thorpe, & Stenneth, 2013).

The involvement of TPAs is causing additional privacy concerns. The user must fear the reveal of sensitive information to the audit agent. Therefore, the provider needs to implement privacy preserving policies and techniques. Those techniques could encompass pseudonymization, pseudonym unlinkability or encryption. (López, Ruebsamen, & Westhoff, 2014) The examined publications show that giving a third party access to data and infrastructure bears different risks and creates new privacy concerns and threats. (López, Ruebsamen, & Westhoff, 2014) In some TPA auditing schemes local

copies of data need to be made to execute auditing processes. Baghel and Theng argue that for a convincing TPA auditing scheme it is necessary that those local data copies can be avoided. (Baghel & Theng, 2015) Another deficiency is the fact that TPA's can work in their self-interest and damage the company causing internal threats. (Rizvi & Cover, 2015)

Internal threats in conjunction with the menace of fraud, corruption and attacks are being mentioned as one critical aspect of cloud computing audit as well as the not improbable possibility of criminals trying to hack clouds to gain access to sensitive data. (Suganya & P. M. D. R. Vincent, 2017)

When looking at more recent research publications (between 2018 to 2020) it stands out that two publications are specifically mentioning the challenges created by handling images in the cloud. Sasmal and Pan mention the importance of trustable TPA in integrity checking of digital images. (Sasmal & Pan, Bit-Reversal Encryption Towards Secured Storage of Digital Image in Cloud Deployment, 2018) Kim argues that existing auditing schemes aren't considering the characteristics of cloud images and therefore are causing high computation, communication and storage costs. (Kim, Kim, Son, Wang, & Noh, 2018)

4.9 Analyzing the underlying research results

In this chapter the results and findings with respect to the research questions and challenges (chapter 4.8) shall be analyzed. The outcome of each publication was summarized in one paragraph (see appendix – 'Proposition') and then further analyzed. In a first step the paragraphs were categorized into propositions considering external audit, internal audit or others. Multiple assignment was possible. Please find the analysis in chapter 4.9.1. In a second step the technologies and techniques indicated in the paragraphs are being analyzed (chapter 4.9.2).

4.9.1 High-level Analysis

Based on the short summarized paragraph the results were classified into three different contextual groups – 'External Audit', 'Internal Audit' and 'Other'. Multiple classification was possible. As afore mentioned in chapter 2.2 cloud computing auditing is complex and multidimensional. The presorting and categorizing helps to identify structure, distribution and textual trends during the analysis. In total 88 publications were assigned to 'External Audit', 44 Publications to 'Internal Audit' and 16 publications to 'Other'. Multiple classification was possible.

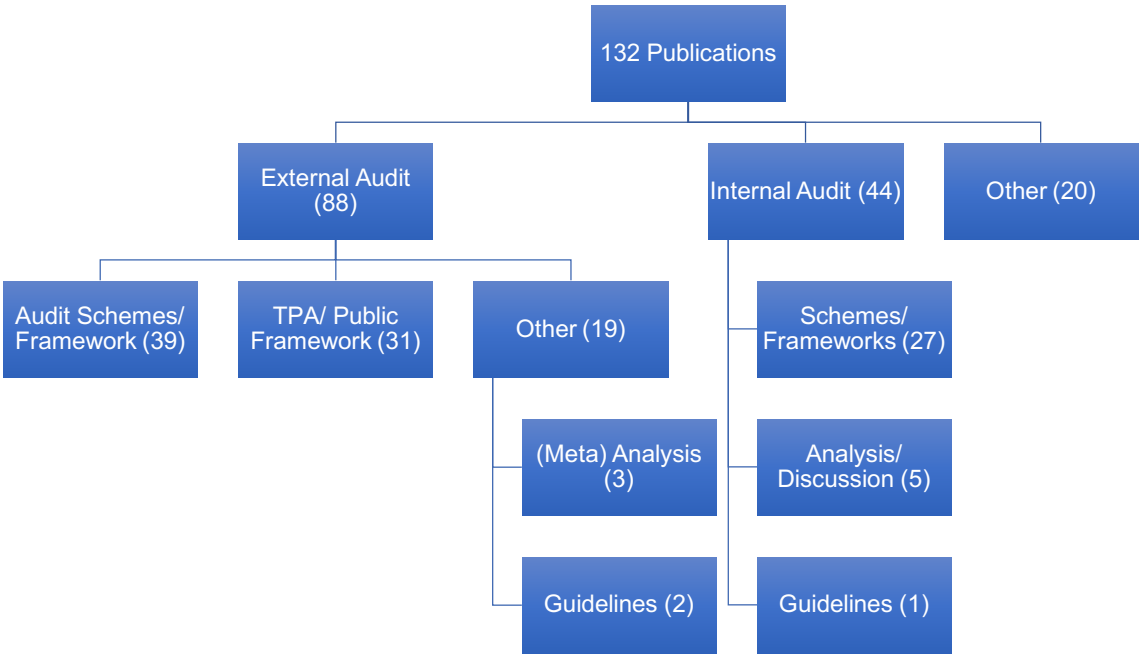

Figure 8: Analysis of results (high-level)

'External Audit' - 39 publications in the external audit section are mentioning a novel audit scheme or framework. 31 of the 88 publications are specifically suggesting a TPA or public audit framework which make roughly 24 % of the total 132 underlying publications. 19 publication were assigned to ('Other') addressing the topic of external audit, albeit not presenting practical frameworks but for example general guidelines, analysis or game theoretical approaches. Three of them concern analyses or discussions of cloud computing theory, audit concepts, risks, requirements and challenges. Two publications provide new general guidelines and additional measures for reference purposes (Chou, Cloud computing risk and audit issues, 2015) and to support management (Duncan & Whittington, The Importance of Proper Measurement for a Cloud Security Assurance Model, 2015). The rest of the solutions are individual ideas and concepts.

'Internal Audit' – Out of the 44 publication 27 publications propose frameworks or new audit schemes. In total six conduct analysis or propose guidelines. The other publication address miscellaneous individual ideas.

'Other' - In this section, the 20 publication not falling into the category of 'External' or 'Internal Audit' are being analyzed. They for example include proposals of new technologies that are built on cloud computing technology and therefore face the risks associated with cloud computing service. (Li, Tan, Chen, & Wong, 2013) The underlying research questions and the consecutive solutions are very diverse. Therefore no

overarching trends could be identified. In a large part the publications address cloud computing in general, auditing is only mentioned as a side notion. One publication examines how cloud computing technology and services can be utilized for the audit action itself. Also in this context disadvantages of cloud computing like high costs, information security and interest conflict are mentioned. (Huang, Lin, & Jian, 2014) Another publication provides guidance for the IT industry by developing a value creation model. (Chou, Cloud Computing: A value creation model, 2015)

4.9.2 Technical Trends

In a next step, the explicitly named technology in the summarized solution paragraph got extracted separately. Those technologies were then analyzed regarding their count reaching the following result.

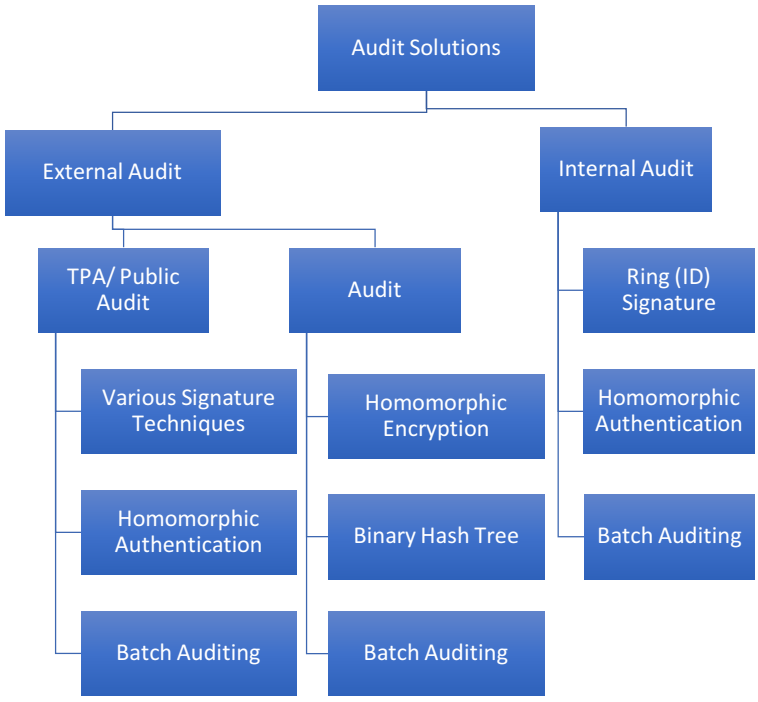

Figure 9: Analysis of results (technical-level)

In regards to the publications assigned to 'External Audit' the following key technologies were identified. From the 'TPA' or 'Public Audit' related publications three trends were identified being homomorphic authentication, various signatures and batch auditing. From the 'Audit'–related publications homomorphic encryption, the binary/hash trees and integrity checking protocol were identified as key technologies. The focal points of publications in the 'Internal Audit' section coincide in terms of homomorphic authentication and batch auditing and bring focus on one specific type of signature, being ring (ID) signature. The definition, functioning and type of application of those identified key technologies are outlined in the next paragraphs.

Batch Auditing - Audit schemes can be classified differently according to retrievability and data possession or the nature of data classification. Another classification categorizes schemes according to their audit mode. Here single auditing, sample auditing and batch auditing can be distinguished. (Yang & Xia, 2016) Batch auditing, meaning being able to support auditing for multiple owners and clouds, is one important requirement for cloud storage auditing involving a TPA. The auditor might either be asked by multiple data owners to conduct audit where if these requests can be combined and conducted as batch audit simultaneously leading to better system performance. Or on the other hand as data owners can distribute their data over multiple clouds the auditor faces the challenge of multiple servers for verification and therefore combining the challenge responses and conduct batch verification can lead to a reduction in computation cost. Therefore "batch auditing can greatly improve the auditing performance, especially in large-scale cloud storage systems" (Yang & Jia, An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing, 2013). It can improve both communication and computation efficiency and thus overall auditing efficiency. (He, Huang, Shi, & Wang, Public Integrity Auditing for Dynamic Regenerating Code Based Cloud Storage, 2016)

Cryptography - Cryptography is the umbrella term when talking about establishing data security, integrity, confidentiality, nonrepudiation, authentication and authorization. (Simpson, 2016) Amongst others it encompasses methods that secure data and information against unauthorized access. There are two major classes to distinguish - symmetric key/private key and public key cryptography – both are used to secure data transmission. Before employing a private or public key, the plaintext of a message or information is transformed into a ciphertext using an encryption algorithm. This ciphertext can only be decrypted by an authorized recipient. A key "is a secret number or other significant information which parametrizes an encryption or decryption algorithm" (Lam, Khoo, & Jiang, 2018).

Private Key cryptography - In a private key system knowing the encryption function and corresponding key allows to determine the decryption function. The same key is used for the encryption and decryption algorithm. It can be rapidly carried out and at the same time is resistant to attack. (Lam, Khoo, & Jiang, 2018)

Public Cryptosystems (RSA) - In a public key system "each user has a pair of encryption (public) and decryption (private) keys" (Lam, Khoo, & Jiang, 2018). A public key certificate is used to bind a user identification and public key. There are different public key cryptosystems available (see table 15) whereby the RSA cryptosystem is one of the most

widely used. It “assures message authenticity using digital signatures” (Lam, Khoo, & Jiang, 2018).

Public Key Cryptosystems
• RSA Cryptosystem • Elgamal Cryptosystem • Elliptic curve Cryptosystem • NTRU • Cramer-Shoup Cryptosystem • Pailler Cryptosystem • Goldwasser-Micali Cryptosystem • Identity-based encryption • Attribute-based encryption

Table 15: Public key cryptosystems (Lam, Khoo, & Jiang, 2018)

Those cryptosystems avail themselves of several core cryptographic applications. Those applications are used to achieve communication security. Table 16 shows a list of those mechanisms of which some are described in more detail below. Those cryptosystems and cryptographic mechanisms are often used to secure cloud computing providing confidentiality and auditability. (Lam, Khoo, & Jiang, 2018)

Cryptographic Applications
• Digital Signature • Message Authentication Code • Key Exchange • Homomorphic Encryption • Secret sharing • Conference key distribution • Oblivious transfer • Secure multi-party computation

Table 16: List of cryptographic applications

Cryptographic applications - Digital Signature - Is a commonly used application to provide information security. (Menezes, van Oorschot, & Vanstone, 1996) Like handwritten signatures a digital signature can be used to seal a document. Either to authenticate the identity of the document creator or signer or as affirmation of the verity of the unchanged content. (Simpson, 2016) The digital signature “in the form of a value dependent on some secret known only to the signer and on the message being signed” (Lam, Khoo, & Jiang, 2018). It can be added to a document. (Simpson, 2016) Besides authentication and data integrity assurance digital signatures can be used as certification

of public keys, enabling trusted third parties to bind the identity of a user to a public key. (Menezes, van Oorschot, & Vanstone, 1996) Digital signatures can be classified as in the following graphic (figure 10) whereby digital signatures with appendix require the original message input to verify. The second type of signature scheme recovers the content from the signature itself. Furthermore randomized schemes have an indexing set for signing > 1 or are otherwise deterministic. (Menezes, van Oorschot, & Vanstone, 1996)

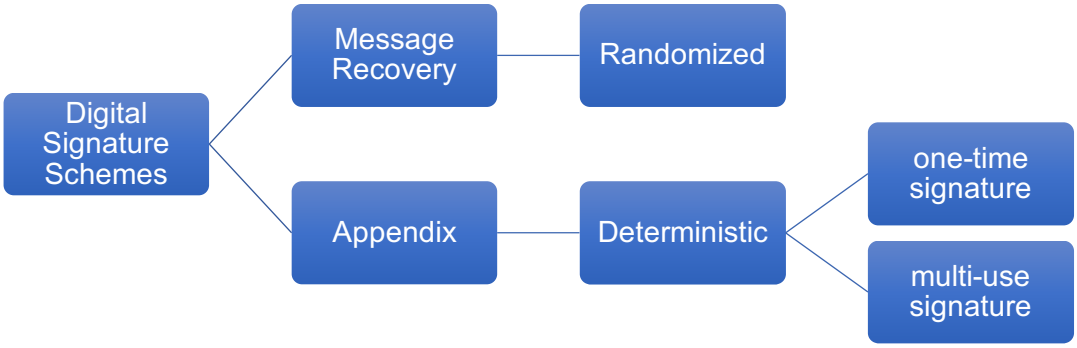

Figure 10: Classification of digital signature (Menezes, van Oorschot, & Vanstone, 1996)

There are different kind of digital signatures. (Menezes, van Oorschot, & Vanstone, 1996) Which is also showing in the results of the conducted scientometric analysis of solution proposals whereby various signature techniques were proposed. (Lam, Khoo, & Jiang, 2018)

Homomorphic Encryption - Homomorphic Encryption is "one solution to protect data privacy in cloud computing" (Lam, Khoo, & Jiang, 2018). It allows to conduct computations on ciphertext - encrypted plaintext. The ciphertext doesn't have to be decrypted to perform the computation, therefore the knowledge of the decryption key is not necessary. The computation is showing the same result as performed on the original text. (Lam, Khoo, & Jiang, 2018)

Hash (Tree) - A hash tree is built of hash values as leaves and one root hash building the top of the tree. In a binary tree scheme every node besides the leaves has two children. (Hwang & Chen, 2016) "Tree structures have been widely applied in dynamic data update operations" (Yang & Xia, 2016) and are used for dynamic verification assuring high efficiency. For the hashing usually cryptographic hash functions are being used. (Yang & Xia, 2016) A hash function maps an arbitrary length bit of information to a small fixed length output which makes it easier to conduct computations. Iteratively they are processing block by block. Purpose of those functions is the assurance of data integrity and message authentication. Common construction methods are the Merkle-Damgard construction and the Matyos-Meyer-Oseas construction. A group of cryptographic hash functions builds a secure hash algorithm and is used in commercial applications. (Lam,

Khoo, & Jiang, 2018) With regards to cloud auditing hash values and hash trees enable real time auditing by creating hash values after each file operation enabling instant identification of violations. One critical aspect is the involved high overhead for storing and turnaround time however there are efforts to reduce those means. (Hwang & Chen, 2016)

Beside the research emphasizes described above, when focusing on literature published between 2018 and 2020 three more research priorities could be identified. Nine publications mention the topic of Internet of Things (IoT) and fog computing which are correlating topics. The role of IoT in our everyday life is constantly increasing, the quantity of IoT devices is constantly increasing. The huge burden is already leading to latency issues and quality issues. In order to meet the ever-growing demand for storage capacities and strong, secure and fast inter-device connectivity the concept of fog computing is bringing cloud computing to a next level. Functionalities are moved closer to the end user and away from the central cloud. “Fog computing environment is envisioned for the future as a spatio-temporal network of end-user IoT devices, regional for service providers, and back-end global cloud service providers” (Kim, Kim, Son, Wang, & Noh, 2018).

4.10 Research Method Analysis

“IT research is what IT researchers do” (Sung, Hansen, & Helps, 2015). – In order to identify prevalent research designs used in the assessed research field the research methodologies of the underlying 132 publications were systematized and the interpretation conducted in this chapter. Research design can be defined as “systematic procedure which includes the designing, compiling, and analyzing of information (…)” (Habib, Pathik, & Maryam, 2014). The applied research method of each publication was registered in the overall data set (see appendix). In total twelve different research methods were identified. Those were modelling, analysis, discussion, examination, simulation, experiment, survey, literature review, investigation, review and recommendation, meta-analysis and case study. Figure 10 below shows the quantitative distribution of the eleven identified research methods and reveals that modelling is with a count of 95 appearances the most prominent research method used in the underlying publications. Between the other research methods, no large deviation appears. They appear between ten and one time.

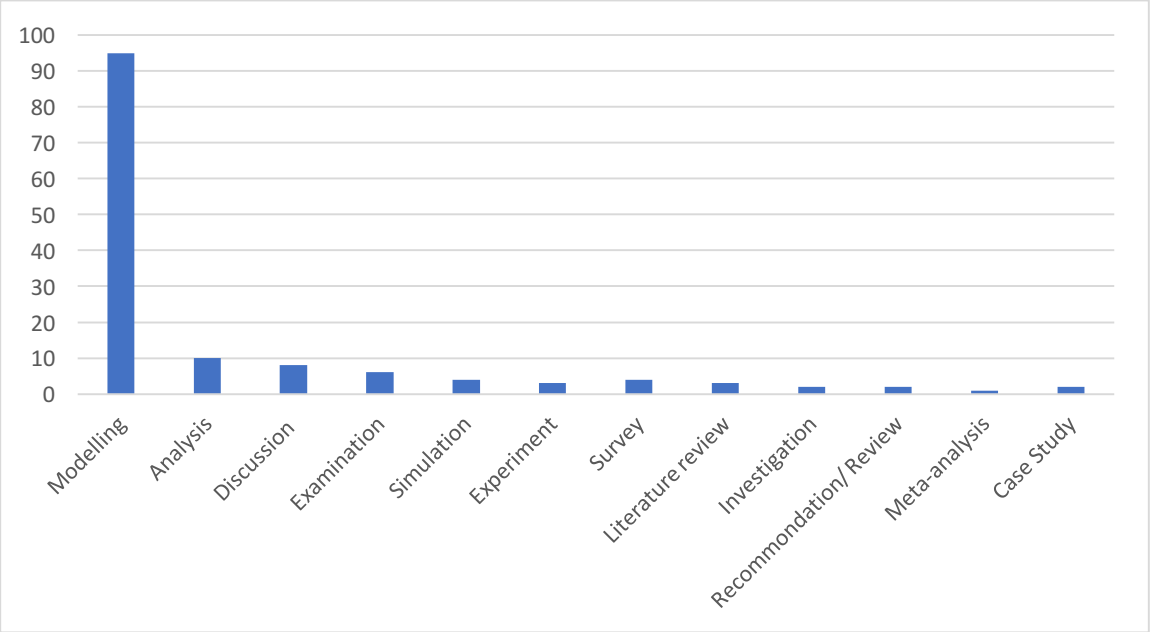

Figure 11: Distribution of research methods

There is comprehensive methodology and there are various ways to classify and distinguish different research types. It can be differentiated between descriptive and analytical research, between applied and fundamental research, between quantitative and qualitative methods and between conceptual and empirical research method. Additionally, mixed types of all the above can appear as result of research specificities as timeframe. (Kothari, 2004, S. 2-5) Most of the applied research models in information technology (IT) or information system (IS) research are empirical ones. (Rowe, 2012) This is supported by the findings of this analysis. Modelling as prevalent methodology and other methods like experiment and simulation show the dominance of empirical research in this field.

However, it must be considered that research in the field of information technology and hence wise cloud computing are highly technical and might be approached differently to natural or behavioral science topics. (Hevner, March, Park, & Sudha, 2004) Prevailing research type in IS research are research articles, notes, essays and commentary, reviews and issues and opinion papers. Prevailing empirical means in IS research are case study, experiment and survey. (Rowe, 2012) Survey and experiment were two of the identified prevailing research methods. None is prevalent however. Rowe (2012) suggests the following categorization for IS research genres: 1. Literature review 2. Theory Development & Research Essays 3. Empirical Research 4. Ethnographies & Narratives 5. Issues & Opinions. Rowe emphasizes the importance of literature reviews, a not essentially visible research method in IS research outlets, as it can help to identify research gaps, operating theories, frameworks and unrecognized assumptions, enabling to pave the way towards new research direction. Further Rowe argues for a more

accessible dealing with pure theory papers and ethnographies. (Rowe, 2012) Whereas theory papers are well represented in the 132 underlying research papers, ethnographies are not represented. Ethnographies by the means of narratives or story telling help to describe situations by observing reality with the result of identifying relationships and the quality of objects. Being a research methodology demanding much time and effort could be a reason why it's not a prominent research method in published literature. (Rowe, 2012)

Another prominent research methodology in IT and IS research is the Design Science Research (DSR) Paradigm. It aims to solve actual issues in today's technological and business world that show high relevance. In comparison behavioral science tries to predict and describe how entities in a business environment behave or will behave exposed to information technology. DSR aims to actively solve real problems that require creative and innovative solutions. Further distinguished must be the difference between high quality professional design, which applies already developed knowledge or techniques to a given problem, whereas in DSR completely novella solutions and techniques are being proposed to solve an issue or increase efficiency. (Hevner, March, Park, & Sudha, 2004)

Processes in research following the DSR paradigm can be broken down into three cycles. First of all the relevance cycle in which the environment to the issue is taken into consideration, therefore the requirements, the application domain, problems and opportunities are examined. The second cycle is the rigor cycle in which the knowledge base for the underlying examined problem is gathered. The third and main cycle is the actual design cycle where the actual DSR is being conducted, processes are developed and evaluated. (Hevner, March, Park, & Sudha, 2004)

The outcome of DSR is a constructed artefact which can be classified as construct, model, method, or instance. (Sangupamba, Prat, & Comyn-Wattiau, 2014) The findings of this research (72% modelling) are coherent with identifying DSR as a dominating research methodology in auditing cloud computing research.

Unfortunately DSR lacks a certain degree of development and concomitand sturdiness, as methodological support, detailed procedures and techniques and reference procedures are partially missing. (Braun, Benedict, Wendler, & Esswein, 2015) However as DSR incorporates technical, organizational and human components in building its artifact for a "class of similar business problem" (Braun, Benedict, Wendler, & Esswein, 2015) it seems to be highly relevant for research in the field of auditing cloud computing.

The results of this scientometric analysis are in line with literature on IS and IT research methodology, showing prevailing empirical methods, theory papers and modelling within the meaning of the DSR paradigm being used. After Rowe I agree that ethonographic narrative further focusing on artifact application in the real world would be reasonable. As auditing cloud computing is a topic not alone researchers but foremost enterprises and cloud users are involved an intersection with real-worl application is crucial. In order to advance progress scientific research and enterprises need to work close together. (Rowe, 2012)

5. Summary, conclusions and outlook

In this chapter the results of the above conducted scientometric analysis on the topic of auditing cloud computing services are summarized, contextualized and conclusions are drawn. (chapter 5.1) Eventually followed by an outlook. (chapter 5.2)

5.1 Summary of results

Summary of assessment outcome	
Underlying literature:	132 publications
Time span covered:	2010-2020
Distribution of publications:	Constant increase until 2015, wave shaped afterwards peaking in 2015 and 2018
Language:	100% English
Source/ Outlet Analysis: Key conference: Key journal outlet:	- 81% IEEE outlets - 70% conference and 30% journal publications - 94% outlets with technical focus International Conference on Cloud Computing Technology and Science (CloudCom) IEEE Transactions on Information Forensics and Security
Country analysis: International Collaborations: Leading contributing countries (overall): Leading contributing countries (national): Leading contributing countries (international):	 26 international collaborations, 106 national China, India, US, UK, Taiwan, Australia, Hong Kong, Germany China & India, US, UK, Germany, Taiwan, Hong Kong, Australia China, US, Australia, Taiwan & Hong Kong, India, UK, Germany
Citation and reference analysis: Average number of citation per publication: Average number of reference per publication:	 13,33 23,9
Authorship analysis: Number of publications with one author: Collaborations: Average number of authors per publication:	 7 (5%) 125 (95%) 3,3
Key authors:	Xiaofeng Chen, H. Zhu, B. Duncan, M. Whittington, Kan Yang, Jie Wu
Key Keywords:	Cloud Computing, Auditing, Public Auditing, Cloud Storage, Security, Data Integrity, Privacy preserving, TPA
Topic analysis (publications):	69 external audit, 21 Internal audit, 25 external and internal audit, 17 other
Key research questions:	Data, Security, Audit, TPA, Access Control, Costs, Attacks, Computation, SLA
Research results analysis: Technological trends:	External Audit: 39 frameworks, 31 TPA/ Public frameworks, 19 others (e.g. guidelines) Internal Audit: 27 frameworks, 5 Discussions, 1 guideline Others: 20 External Audit: Various Signature Techniques, Homomorphic Authentication/ Encryption, Batch Auditing, Binary Hash Tree Internal Audit: Ring (ID) Signature, Homomorphic Authentication, Batch Auditing
Research method analysis:	- dominance of empirical studies - 72% modelling - importance of DSR paradigm

Table 17: Summary of the assessment outcome

5.2 Interpretation and conclusions

In this research 132 scientific publications were analyzed by means of scientometry to evaluate research activities and publication structure and to identify the development of key topics. Additionally, the results are put into context to the role of science and technology in the national economy and governmental science politics.

When looking at the productivity and distribution of research growth it can be seen that the number of publications peeked in 2015 and 2018. The development curve could be interpreted as wave shaped. A lasting decrease of publications is not expected, rather another increase because of the topic's relevance for today's business world and dissolved challenges in the field of auditing cloud computing services. There are studies describing technological innovation evolving in a cyclist manner. (Lee, 2018) In that sense the curve of scientific publications is expected to also develop in cycles, increasing after the year 2020/2021.

In the set of research publications appears a strong dominance of conference publications (70%). This result is surprising as journal publications offer more flexibility and more room for elaboration. (Habib, Pathik, & Maryam, 2014) 81% of the publications were published in an IEEE outlet. 94% of all outlets are technical outlets, only the remainder is business or others focused. The most prominent conference and journal outlets in the research field of auditing cloud computing include the "CloudCom Conference" and the journal "IEEE Transactions on Information Forensics and Security". The strong dominance of technical outlets can be explained as cloud computing and relating auditing research is an IT topic and settled in technological science. Due to its high relevance in today's business world a higher shared distribution also in business related outlets would have been expected. Additionally, considering the highly interdisciplinary characteristic of the research field (Sung, Hansen, & Helps, 2015) a more balanced and wider scope of business focused research outlets would have been expected.

95% of publications were published by more than one author. The average author count is 3,3 authors per publication. The strong dominance of collaborations is visible. 106 publications are national publications, 26 are international collaborations. International research collaborations are one of the transmission mechanism to distribute technological innovation between firms as well as countries. (Fu, 2015) Those cross-cultural publications are creating new and additional dimensions, enriching the research outcome. (Habib, Pathik, & Maryam, 2014) Roughly one third of the underlying publications are international collaborations. This share is auspicious and indicates a certain degree of cross-country innovation distribution and collaboration. China is involved in 17

international cross-country collaborations, leading the list of international collaboration contributors.

The cross-cultural, interdepartmental collaborative and interdisciplinary nature of IT research (Sung, Hansen, & Helps, 2015) is confirmed by the here conducted scientometric analysis. Cross-cultural research has the potential to create new dimensions in research (Habib, Pathik, & Maryam, 2014), enabling reaction to the becoming more “complex, large-scale societal infrastructure” (Computer Science and Telecommunications Board; National Research Council, 2000). The outcome must be flexible being able to react to socio-economic changes. (Mori, 2014) Additional incentives are necessary in order to eliminate obstructions to collaborative research environments. (Computer Science and Telecommunications Board; National Research Council, 2000)

Furthermore for the underlying literature the publishing country, meaning the location of publishing research institution, was analyzed. China and India were identified as key publishing nations when looking at the number of publications per country on a quantitative perspective. China is involved with the most national and international contributions, whereas India shows the second most national contributions and the US the second most international contributions. China and India, the two strong competitors in the IT industry are often referred to as ‘Dragon and Elephant’. In this assessment in the field of auditing cloud computing services the Dragon’s (China’s) slight dominance becomes apparent. Chinas dominance in the IT area should be seen under the light of its state innovation policy and its social system - China and India are both socialistic states. The social system of a country has impact on its development route and trajectory. State innovation policy plays an important role in a country’s innovation trajectory. (Chen, Li, Lv, Chen, & Yang, 2019) China was forced to move from imitation to innovation in order to sustain long-term economic growth. (Fu, 2015) China reached a turning point where qualitative innovation-based growth is being focused. The long-term success of this new trajectory depends on economic, social and political factors. The required large-scale infrastructure is the result of China’s strong government orientation. (Chen, Li, Lv, Chen, & Yang, 2019) Federal government involvement in form of funding besides industry is essential for research. (Computer Science and Telecommunications Board; National Research Council, 2000) China’s high governmental involvement and systematic strategy towards innovation can be an explanation for their high contribution of their work in the underlying literature in the field of auditing cloud computing services.

Looking at the continental European contributions shows 21 publications in the underlying data set. The leading European contributors are the UK and Germany. How can the

comparatively little contribution of European countries be explained? When looking at the dominant cloud providers amazon, Google, Microsoft and IBM it becomes apparent that all of them are US companies. Europe's adapter position in this field could be an explanation for the comparatively low contributions. Technical focal points lie elsewhere.

Another examined aspect was the citation pattern. Citation count is a measure for quality and indicates the significance and reach of a publication. 36% of the underlying literature are uncited (as of June 2020). The average number of citations lays at 13,33 citations. The average is strongly influenced by a few outliers with a high number of citations. Three out of the four publications with the highest citation count ranging from 113 to 261 are Chinese contributions (two national contributions and one international collaboration with Canada). This is in line with the former identification of China as key publishing nation. Two of the publications with highest citation count are contributions by research institutions in Hong Kong which is a special administrative of China. Hong Kong also appears on the list of most contributing countries with a total of five contributions in the underlying literature. Hong Kong's government has prioritized and supported the innovation and technology industry from before the year 2000. Overall R&D expenditures and number of R&D employees increased significantly in the past enabling applied research and development and technology transfer by providing the necessary infrastructure. (S. Sanders, 2012) Additionally it becomes apparent that all four publications are collaborations of two to three authors and are journal publications. The latter is rather conspicuous as 70% of the underlying publications were identified as conference publications. This indicates that quality and reach of journal publications is higher. The average number of references per paper is 23,9. The average reference count increases with the citation count. Respectively it can be said that publications with high citation counts on average show a high reference count.

Six key authors were identified with three contributions each. Those authors are X. Chen and H. Zhu (China), B. Duncan and M. Whittington (Scotland/ UK), Kan Yang and Jie Wu publishing in research institutions in China/ Hong Kong, the US and Canada. This finding overlaps with the identified key contributing countries China, the US and UK. The average number of citations of the 18 publications of the identified key authors is with 40,4 significantly higher than the general average citation count (13,33).

Furthermore the research methodology was analyzed in chapter 4.10. The result shows the dominance of empirical studies conducting modelling and the importance of the design science research paradigm in this research field. Design Science Research is geared for Information Systems research. As an applied research domain, it helps creating artifacts

and solutions to solve problems and enhance application in the real world. Design science research has high relevance as it helps solving industry's problems in practice. (Alturki, Bandara, & Gable, 2012) DSR addresses unsolved problems or increases efficiency of existing solutions in unique and innovative ways. (Hevner & Chatterjee, Design Science Research in Information Systems, 2010) That's why it's highly relevant for research in cloud auditing practice.

In order to identify trends in the underlying publications in terms of subject, research questions and solutions in chapter 4.7-9 the necessary analyzes were conducted. The analysis of keywords allows to identify research trends and to predict relevance. (Barki, Rivard, & Talbot, 1988) The identified keywords are cloud computing, auditing, public auditing, cloud storage, security, data integrity, privacy preserving and TPA.. The result is refelcting the significance of public auditing schemes vie TPA to diminish security challenges and to preserve data integrity and privacy. As costumers are losing control over their data auditing techniques need to be created and developed by research that create an environment of security, privacy and trust. (Sangupamba, Prat, & Comyn-Wattiau, 2014) Especially in the field of data storage the development of auditing mechanisms is crucial in order to guarantee integrity and react to internal and external security threats. (Tian, et al., 2019) The focus on public or external auditing is additionally supported by the topic analysis also showing the dominance of external auditing schemes.

When analyzing the research questions of the underlying literature the before mentioned keywords were confirmed and further specified. The main challenges addressed besides the already mentioned topics of audit and TPA audit are concerning security topics with special regards to data and access control, (computation) costs, threat of attacks and the SLA. Those identified challenges in the field of auditing cloud computing is reflected in the solutions proposed by research with strong emphasis on external audit modelling. Key aspects of auditing schemes and techniques are various signature techniques, homomorphic authentication and encryption, batch auditing, (Binary) Hash trees, IoT and Fog computing. The findings of the underlying scientometric analysis conform Tian et al's request for the following trades in a public auditing mechanism – privacy preservation, supporting dynamic data and batch auditing and light weight overheads. "A practical public-auditing scheme should comprehensively support auditing for all types of cloud data and fulfill the corresponding security requirements" (Tian, et al., 2019).

5.3 Outlook

In practice cloud-computing adoption has been increasing rapidly and cloud-specific spending is expected to grow at more than six times the rate of general IT spending

through 2020. (McKinsey, 2018) With the increase of IT goods and services there comes a higher need for research. The growing, more “complex, large-scale societal infrastructure” creates demands for new emphasizes in IT research. (Computer Science and Telecommunications Board; National Research Council, 2000)

Research is so important as practice-based solutions are often specific to one individual issue. (Braun, Benedict, Wendler, & Esswein, 2015) Despite fixing security issues with unregistered patches and solutions, build in security for cloud infrastructure is needed and demands the focus of research. (Ramachandran, 2014) It shows that good research depends on telling a convincing story by adapting the method to the problem. Blindly following scientific methods is decisive. (Rowe, 2012)

The underlying scientometric assessment shows that in this research field cross-cultural and interdisciplinary practical application is significant. As there is a delay between academic research and practical application (Alturki, Bandara, & Gable, 2012) a look into enterprise practice is likewise important.

More and more new technologies are emerging, often based on public cloud solutions. IoT Applications, special data storage, AI and blockchain are some of those new trends. (McKinsey, 2018) Those are propelling advancements in cloud computing (services) leading to new challenges in terms of security, privacy and integrity. Together with a yet inconsistent international legal framework auditing cloud computing remains a topic of great interest in scientific research.

7. List of literature

Aguilera, X. M., Otero, C., Ridley, M., & Elliott, D. (2018). Managed Containers: A Framework for Resilient Containerized Mission Critical Systems. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (pp. 946-949). San Francisco, CA: IEEE.

Al-Aqrabi, H., & Hill, R. (2018). A Secure Connectivity Model for Internet of Things Analytics Service Delivery. *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)* (pp. 9-16). Guangzhou: IEEE.

Al-Aqrabi, H., Johnson, A., Hill, R., Lane, P., & Liu, L. (2019). A Multi-layer Security Model for 5G-Enabled Industrial Internet of Things. *Smart City and Informatization* (pp. 279-292). Singapore: Springer Singapore.

Al-Matari, O. M., Helal, I. M., A. Mazen, S., & Elhennawy, S. (2018). Cybersecurity Tools for IS Auditing. *2018 Sixth International Conference on Enterprise Systems (ES)* (pp. 217-223). Limassol: IEEE.

Alouane, N.-E., Abouchabaka, J., & Rafalia, N. (2016). A thick-cloud solution for data auditing in a cloud environment. *2016 International Conference on Electrical and Information Technologies (ICEIT)* (pp. 8-15). Tangiers: IEEE.

Alrabea, A. (2020, June). A Modified Boneh-Lynn-Shacham Signing Dynamic Auditing In Cloud Computing. *Journal of King Saud University - Computer and Information Sciences*, pp. 1-7.

Alturki, A., Bandara, W., & Gable, G. G. (2012). Design Science Research and the Core of Information Systems. *Design Science Research in Information Systems. Advances in Theory and Practice. DESRIST 2012. Lecture Notes in Computer Science* (pp. 309-327). Berlin, Heidelberg: Springer.

Asmah, A., & Kyobe, M. (2018). Towards an Integrative Theoretical Model For Examining IT Governance Audits., (pp. 18-22).

Baghel, S. V., & Theng, D. P. (2015). A Survey for Secure Communication of Cloud Third Party Authenticator. *2'ND INTERNATIONAL CONFERENCE ON ELECTRONICS AND COMMUNICATION SYSTEMS* (pp. 51-54). India: ICECS '2015.

Barki, H., Rivard, S., & Talbot, J. (1988). An Information Systems Keyword Classification Scheme. *MIS Quarterly*, 299-322.

Bi, J., & Liu, J. (2016). Cryptanalysis of a Privacy Preserving Auditing for Data Integrity Protocol. *International Conference on Information Security Practice and Experience* (pp. 37-47). Springer.

Bless, R., & Flittner, M. (2014). Towards corporate confidentiality preserving auditing mechanisms for Clouds. *2014 IEEE 3rd International Conference on Cloud Networking (CloudNet)* (pp. 381-387). Luxembourg: IEEE.

Braun, R., Benedict, M., Wendler, H., & Esswein, W. (2015). Proposal for Requirements Driven Design Science Research. In B. Donnellan, M. Helfert, J. Kenneally, D. VanderMeer, M. Rothenberger, & R. Winter, *New Horizons in Design Science: Broadening the Research Agenda* (pp. 135-151). Cham: Springer.

Carroll, M., van der Merwe, A., & Kotzé, P. (2011). Secure cloud computing: Benefits, risks and controls. *2011 Information Security for South Africa* (pp. 1-9). Johannesburg: IEEE.

Chen, X., Li, R., Lv, M., Chen, D., & Yang, L. (2019). Information Technology Industry in China. In Kung-Chung, Liu, & S. R. Uday, *Information Technology Industry in China* (pp. 71-92). Singapore: Springer Singapore.

Chen, Z., & Yoon, J. (2010). IT Auditing to Assure a Secure Cloud Computing. *6th World Congress on Services* (pp. 253-259). Miami, FL: IEEE.

Chou, D. C. (2015). Cloud computing risk and audit issues. *Computer Standards & Interfaces*, 137-142.

Chou, D. C. (2015). Cloud Computing: A value creation model. *Computer STandards & Interfaces*, 72-77.

Computer Science and Telecommunications Board; National Research Council. (2000). Expanding the Scale and Scope of Information Technology Research. In C. S. Board, & N. R. Council, *Making IT Better - Expanding Information Technology Research to Meet Society's Needs* (pp. 195-214). Washington, D.C.: NATIONAL ACADEMY PRESS.

Duncan, B., & Whittington, M. (2014). Reflecting on Whether Checklists Can Tick the Box for Cloud Security. *2014 IEEE 6th International Conference on Cloud Computing Technology and Science* (pp. 805-810). Singapore: IEEE.

Duncan, B., & Whittington, M. (2015). Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement. *Trustcom/BigDataSE/ISPA* (pp. 1088-1093). IEEE.

Duncan, B., & Whittington, M. (2015). The Importance of Proper Measurement for a Cloud Security Assurance Model. *7th International Conference on Cloud Computing Technology and Science* (pp. 517-522). Scotland: IEEE.

Flittner, M., Weigel, A., & Zitterbart, M. (2017). gAUDIT: A group communication-capable request-response middleware for auditing clouds. *2017 International Conference on Networked Systems (NetSys)* (pp. 1-8). Gottingen: IEEE.

Foster, I., Zhao, Y., Raicu, I., & Lu, S. (2017). Cloud Computing and Grid Computing 360-Degree Compared. *2008 Grid Computing Environments Workshop* (pp. 1-10). Austin, TX: IEEE.

Fu, X. (2015). *China's Path to Innovation.* Cambridge, UK: Cambridge University Press.

Gaikwad, V. A., & Babar, S. D. (2016). Forward secure E-Auction with Auditing Integrity. *2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)* (pp. 399-406). Pune: IEEE.

Gonzalez, N. M., Goya, W. A., Pereira, R. d., Langona, K., Silva, E. A., Melo de Brito Carvalho, T. C., . . . Sefidcon, A. (2016). Fog computing: Data analytics and cloud distributed processing on the network edges. *35th International Conference of the Chilean Computer Science Society (SCCC)* (p. 9). Chile: IEEE.

Grandison, T., Thorpe, S., & Stenneth, L. (2013). Simultaneously Supporting Privacy and Auditing in Cloud Computing Systems. *Ninth World Congress on Services* (pp. 290-297). IEEE.

Gupta, S., Gupta, S. C., Majumdar, R., & Rathore, Y. (2016). Measuring Cloud Security from risks perspective. *2016 6th International Conference - Cloud System and Big Data Engineering* (pp. 214-220). Noida: IEEE.

Gurkok, C. (2017). Securing Cloud Computing Systems. In *Computer and Information Security Handbook* (p. 897ff). Florida: Elsevier.

Gutte, V. S., & Deshpande, P. (2015). Cost and Communication Efficient Auditing over Public Cloud. *2015 International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 807-810). Jabalpur: IEEE.

Habib, M., Pathik, B. B., & Maryam, H. (2014). *Research Methodology - Contemporary Practices: Guidelines for Academic Researchers.* UK: Cambridge Scholars Publishing.

He, D., Zeadally, S., & Wu, L. (2018). Certificateless Public Auditing Scheme for Cloud-Assisted Wireless Body Area Networks. *SYSTEMS JOURNAL*.

He, K., Huang, C., Shi, J., & Wang, J. (2016). Public Integrity Auditing for Dynamic Regenerating Code Based Cloud Storage. *2016 IEEE Symposium on Computers and Communication (ISCC)* (pp. 581-588). Messina, Italy: IEEE.

He, K., Huang, C., Yang, K., & Shi, J. (2015). Identity-preserving public auditing for shared cloud data. *2015 IEEE 23rd International Symposium on Quality of Service (IWQoS)* (pp. 159-164). Portland, OR, USA: IEEE.

Heilig, L., & Voß, S. (2014). A Scientometric Analysis of Cloud Computing Literature. *IEEE Transactions on Cloud Computing*, 266-278.

Hevner, A., March, S., Park, J., & Sudha, R. (2004). Design Science Research in Information Systems. In A. Hevner, & S. Chatterjee, *Design Research in Information Systems, Integrated Series 9 in Information Systems* (pp. 9-22). Springer Science+Business Media.

Hood, W. W., & Wilson, C. S. (2001). The literature of bibliometrics, scientometrics, and informetrics. *Scientometrics*, 291-314.

Hou, J., Li, X.-Y., Jung, T., Wang, Y., & Zheng, D. (2018, July). CASTLE: Enhancing the Utility of Inequality Query Auditing Without Denial Threats. *IEEE Transactions on Information Forensics and Security*, pp. 1656-1669.

Houlihan, R., & Du, X. (2012). An effective auditing scheme for cloud computing. *2012 IEEE Global Communications Conference (GLOBECOM)* (pp. 1599-1604). Anaheim, CA: IEEE.

Houlihan, R., Du, X., Tan, C. C., Wu, J., & Guizani, M. (2014). Auditing cloud service level agreement on VM CPU speed. *2014 IEEE International Conference on Communications (ICC)* (pp. 799-803). Sydney, NSW: IEEE.

Huang, S. Y., Lin, C.-W., & Jian, Y.-F. (2014). The innovative application of cloud computing on auditing. *International Journal of Mobile Communications*, na.

Hui, Huaihai, McLernon, D., & Zaidi, S. A. (2018). Design of the Security Mechanism for a BPO Cloud Computing Platform. *9th IEEE International Conference on Software Engineering and Service Science* (pp. 1092-1095). Beijing, China: IEEE.

Huo, H., Jiang, T., Tan, S., & Tao, X. (2019, December 02). Efficient public integrity auditing with secure deduplication in cloud computing. *International Journal of Embedded Systems* .

Hussain, M., & Al-Mourad, M. B. (2014). Effective Third Party Auditing in Cloud Computing. *28th International Conference on Advanced Information Networking and Applications Workshops* (pp. 90-95). Saudi Arabia: IEEE.

Hwang, G.-H., & Chen, H.-F. (2016). Efficient Real-Time Auditing and Proof of Violation for Cloud Storage Systems. *2016 IEEE 9th International Conference on Cloud Computing (CLOUD)* (pp. 132-139). San Francisco, CA, USA: IEEE.

Hwang, S.-J., & Li, T.-L. (2018). Strategies to Improve Auditing Performance and Soundness for Cloud Computation. *International Conference on Security with Intelligent Computing and Big-data Services* (pp. 170-182). Springer.

Ismail, U. M., Islam, S., & Mouratidis, H. (2015). A Framework for Cloud Security Audit. *International Conference on Global Security, Safety, and Sustainability* (pp. 296-309). London: Springer.

Jiang, H.-C., Feng, C.-S., & Yuan, D. (2016). Enabling public and privacy-preserving auditability for cloud storage. *2016 International Conference on Machine Learning and Cybernetics (ICMLC)* (pp. 24-28). Jeju: IEEE.

Jiang, T., Chen, X., & Ma, J. (2016, August 01). Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation. *IEEE Transactions on Computers*, pp. 2363-2373.

Jin, Y., Gong, X., Li, P., & He, H. (2018). Data integrity verification based on hybrid cloud. *2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA)* (pp. 1557-1562). Wuhan: IEEE.

Kai, H., Chuanhe, H., Jinhai, W., Hao, Z., Xi, C., Yilong, L., . . . Bin, W. (2013). An Efficient Public Batch Auditing Protocol for Data Security in Multi-cloud Storage. *2013 8th ChinaGrid Annual Conference* (pp. 51-56). Changchun: IEEE.

Khalid, A., Shahbaz, M., & Khan, I. A. (2018, September 03). Intelligent use of fog devices in edge-cloud paradigm to assist in E-polling. *Concurrency and Computation - Practice and Experience*, p. 31:e4957.

Kharmate, P., & Suryawanshi, R. (2016). Cloud Based Two Tier Security Scheme for Store, Share and Audit Our Data into Cloud. *2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)* (pp. 116-121). Pune: IEEE.

Kim, D., Kwon, H., Hahn, C., & Hur, J. (2016, November). Privacy-preserving public auditing for educational multimedia data in cloud computing. *Multimedia Tools and Applications*, pp. 13077–13091.

Kim, Y., Kim, D., Son, J., Wang, W., & Noh, Y. (2018). A New Fog-Cloud Storage Framework with Transparency and Auditability. *2018 IEEE International Conference on Communications (ICC)* (pp. 1-7). Kansas City: IEEE.

Konoor, D. K. (2016). Auditing in Cloud Computing Solutions with OpenStack. *2016 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)* (pp. 176-176). Bangalore: IEEE.

Kothari, C. (2004). *Research Methodology: Methods & Techniques.* New Dheli: New Age International Publisher.

Lam, C. C., Khoo, K., & Jiang, S. (2018). Chapter 15: Cryptography. In K. H. Rosen, *Handbook of Discrete and Combinatorial Mathematics* (pp. 1069-1142). Boca Raton, FL, US.

Lee, H. L. (2018). Big Data and the Innovation Cycle, Lee. *Production and Operations Management*, 1642-1646.

Leonard Heilig, S. V. (2014). A Scientometric Analysis of Cloud Computing Literature. *IEEE Transactions on Cloud Computing*, 267-278.

Lewis, B. R., Templeton, G. F., & Luo, X. (2007). A Scientometric Investigation into the Validity of IS Journal Quality Measures. *Journal of the Association for Information Systems*, 619-633.

Li, B., Li, X., Tong, W., Wang, H., & Chen, J. (2020). A Survey on Tracing for Default of Cloud Service. *2019 IEEE International Conference on Computation, Communication and Engineering (ICCCE)* (pp. 17-20). Fujian P.R: IEEE.

Li, J., Tan, X., Chen, X., & Wong, D. S. (2013). An Efficient Proof of Retrievability with Public Auditing in Cloud Computing. *2013 5th International Conference on Intelligent Networking and Collaborative Systems* (pp. 93-98). Xi'an, China: IEEE.

Li, Z., & Liu, Y. (2017, June 20). A differential game-theoretic model of auditing for data storage in cloud computing. *International Journal of Computational Science and Engineering (IJCSE)*.

Liu, C., Ranjan, R., Zhang, X., Yang, C., Georgakopoulos, D., & Chen, J. (2013). Public Auditing for Big Data Storage in Cloud Computing - A Survey. *2013 IEEE 16th International Conference on Computational Science and Engineering* (pp. 1128-1135). Sydney: IEEE.

Liu, J., Huang, K., Rong, H., Wang, H., & Xian, M. (2015, July). Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage. *IEEE Transactions on Information Forensics and Security*, pp. 1513-1528.

Liu, Q., Wang, G., & Wu, J. (2014, March). Consistency as a Service: Auditing Cloud Consistency. *IEEE Transactions on Network and Service Management*, pp. 25-35.

Lohacha, A., & Karambir. (2019, February 21). ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. *Journal of Information Security and Applications*, pp. 1-12.

López, J. M., Ruebsamen, T., & Westhoff, D. (2014). Privacy-Friendly Cloud Audits with Somewhat Homomorphic and Searchable Encryption. *14th International Conference on Innovations for Community Services (I4CS)* (pp. 95-103). Germany: IEEE.

Majumdar, S., Madi, T., Wang, Y., Tabiban, A., Oqaily, M., Alimohammadifar, A., . . . Debbabi, M. (2019). User-Level Runtime Security Auditing for the Cloud. *Cloud Security Auditing*, pp. 71-102.

Mamun, H., Bishwajit Banik, P., & Hafsa, M. (2014). *Research methodology - contemporary practices: guidelines for academic researchers.* Newcastle upon Tyne: Cambridge Scholars Publishing.

Martin Gilje Jaatun, S. P. (2016). Enhancing accountability in the cloud. *International Journal of Information Management*, 1-11.

Massonet, P., Naqvi, S., Ponsard, C., Latanicki, J., Rochwerger, B., & Villari, M. (2011). A Monitoring and Audit Logging Architecture for Data Location Compliance in Federated Cloud Infrastructures. *2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum* (pp. 1510-1517). Shanghai: IEEE.

Mateescu, G., Vladescu, M., & Sgarciu, V. (2014). Auditing cloud computing migration. *2014 IEEE 9th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, (pp. 263-268).

Meera, G., & Geethakumari, G. (2015). A provenance auditing framework for cloud computing systems. *2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)* (pp. 1-5). Kozhikode: IEEE.

Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Chapter 11: Digital Signatures. In P. v. A. Menezes, *Handbook of Applied Cryptography* (pp. 425-488). Boca Raton, FL, US: CRC Press.

Min, Y., & Shi, W. (2019). Efficient Privacy-Preserving Certificateless Provable Data Possession Scheme for Cloud Storage. *IEEE Access*, pp. 122091-122105.

Mithani, M., Salsburg, M., & Rao, S. (2010). A Decision Support System for MOving Workloads to Public Clouds. *GSTF International Journal on Computing*, 150-158.

Modi, F. M., Desai, M. R., & Soni, D. R. (2018). A Third Party Audit Mechanism for Cloud Based Storage Using File Versioning and Change Tracking Mechanism.

2018 International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 521-523). Coimbatore: IEEE.

Mohanty, S., Pattnaik, P. K., & Kumar, R. (2018). Confidentiality Preserving Auditing for Cloud Computing Environment. *2018 International Conference on Research in Intelligent and Computing in Engineering (RICE)* (pp. 1-4). San Salvador: IEEE.

Mori, K. (2014). *Concept-Oriented Research and Development in Information Technology.* Hoboken, New Jersey: Wiley.

Muthuram, R., & Kousalya, G. (2014, January). A survey on integrity verification and data auditing schemes for data verification in remote cloud servers. *Electronic Government, an International Journal (EG)*, p. 408.

Mythili, K., & Anandakumar, H. (2013). Trust management approach for secure and privacy data access in cloud computing. *2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)* (pp. 923-927). Chennai: IEEE.

National Institute of Standards and Technology. (2011, September 01). *NIST - Computer Security Resource Center.* Retrieved June 2020, from SP 800-145 The NIST Definition of Cloud Computing: https://csrc.nist.gov/publications/detail/sp/800-145/final

Navajothi, R., & Fenelon, S. J. (2014). An efficient, dynamic, privacy preserving public auditing method on untrusted cloud storage. *International Conference on Information Communication and Embedded Systems (ICICES2014)* (pp. 1-6). Chennai: IEEE.

Ni, J., Yu, Y., Mu, Y., & Xia, Q. (2014, October). On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage. *IEEE Transactions on Parallel and Distributed Systems*, pp. 2760-2761.

Nix, R., Kantarcioglu, M., & Shetty, S. (2013). Toward a Real-Time Cloud Auditing Paradigm. *2013 IEEE Ninth World Congress on Services* (pp. 255-259). Santa Clara, CA: IEEE.

Oliveira, A. S., Sendor, J., Garaga, A., & Jenatton, K. (2013). Monitoring Personal Data Transfers in the Cloud. *2013 IEEE 5th International Conference on Cloud Computing Technology and Science* (pp. 347-354). Bristol: IEEE.

Olowu, M., Yinka-Banjo, C., Misra, S., & Florez, H. (2019). A Secured Private-Cloud Computing System. *International Conference on Applied Informatics* (pp. 373-384). Springer.

Pan, H., Liu, C., Duan, S., Han, P., Zhang, X., & Fang, B. (2019). Deep Learning Based Scene Text Reading for Cloud Audit Information Extraction. *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)* (pp. 686-693). Hangzhou, China: IEEE.

Park, J. S., Spetka, E., Rasheed, H., Ratazzi, P., & Han, K. J. (2012). Near-Real-Time Cloud Auditing for Rapid Response. *2012 26th International Conference on Advanced Information Networking and Applications Workshops* (pp. 1252-1257). Fukuoka: IEEE.

Pasquier, T. F.-M., Singh, J., Bacon, J., & Eyers, D. (2016). Information Flow Audit for PaaS Clouds. *2016 IEEE International Conference on Cloud Engineering (IC2E)* (pp. 42-51). Berlin: IEEE.

Patil Rashmi, R., & Sangve, S. M. (2015). Public auditing system: Improved remote data possession checking protocol for secure cloud storage. *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)* (pp. 75-80). Davangere: IEEE.

Patil, J., & Chaudhari, S. (2018). Privacy Preserving and Dynamic Audit Service for Secure Cloud Storage. *2018 International Conference on Smart City and Emerging Technology (ICSCET)* (pp. 1-6). Mumbai: IEEE.

Pearson, S. (2009). Taking Account of Privacy when Designing Cloud Computing Services. *Cloud'09* (pp. 44-52). Vancouver: ICSE'09 Workshop.

Pei, B., Chen, C., & Wan, C. (2014). A XOR Based Public Auditing Scheme for Proof-of-storage. *2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications* (pp. 558-565). Guangdong: IEEE.

Pereira, L., Ortiz, L., Rossi, D., Rosa, M., Fonseca, K., Prado, C., . . . Riella, R. (2018). Using Intel SGX to Enforce Auditing of Running Software in Insecure Environments. *2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)* (pp. 243-246). Nicosia: IEEE.

Prakash, G. L., Prateek, M., & Singh, I. (2018). Secure Public Auditing Using Batch Processing for Cloud Data Storage. *1st International Conference on Smart System, Innovations and Computing.* Springer.

Puthal, D., Sahoo, B., Mishra, S., & Swain, S. (2015). Cloud Computing Features, Issues, and Challenges: A Big Picture. *2015 International Conference on Computational Intelligence and Networks* (pp. 116-123). Bhubaneshwar: IEEE.

Raja, J., & Ramakrishnan, M. (2017). Public key based third party auditing system using random masking and bilinear total signature for privacy in public cloud environment. *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1200-1205). Madurai: IEEE.

Ramachandran, M. (2014). *Advances in cloud computing research.* New York: Nova Publishers.

Rao, K. P., Puneeth, R. P., & Shetty, S. (2018). A Novel Third Party Integrity Checker (TPIC) based Data Auditing for Security of the Dynamic Streaming Client Data in a Cloud Infrastructure. *2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)* (pp. 533-538). Msyuru, India: IEEE.

Rasheed, H. (2013). Data and infrastructure security auditing in cloud computing environments. *International Journal of Information Management*, 364-368.

Rishabh Shrivastava, P. M. (2016). Artificial Intelligence Research in India: A Scientometric Analysis. *Science & Technology Libraries*, 136-151.

Rizvi, S., & Cover, K. (2015). Third-Party Auditor (TPA): A Potential Solution for Securing a Cloud Environment. *2nd International Conference on Cyber Security and Cloud Computing* (pp. 31-36). USA: IEEE.

Rowe, F. (2012). Toward a richer diversity of genres in information systems research: new categorization and guidelines. *European Journal of Information Systems*, 469-478.

Ryoo, J., Rizvi, S., Aiken, W., & Kissell, J. (2014). Cloud Security Auditing: Challenges and Emerging Approaches. *IEEE Computer and Reliability Societies*, pp. 68-74.

S. Sanders, E. (2012). HONG KONG IN FOCUS: Asia's Research Hub. *Science 338 (suppl.)*, 1639–1657.

Sakthivel, S., & Dhiyanesh, B. (2013). A privacy-preserving storage security for spatial data in dynamics cloud environment. *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (pp. 1-6). Tiruchengode: IEEE.

Salma, T. (2013). A flexible distributed storage integrity auditing mechanism in Cloud Computing. *2013 International Conference on Information Communication and Embedded Systems (ICICES)* (pp. 283-287). Chennai: IEEE.

Sangupamba, O. M., Prat, N., & Comyn-Wattiau, I. (2014). Business Intelligence and Big Data in the Cloud: Opportunities for Design-Science Researchers. In M. Indulska, & S. Purao, *Advances in Conceptual Modeling. ER 2014. Lecture Notes in Computer Science* (pp. 75-84). Switzerland: International Conference on Conceptual Modeling.

Santana de Oliveira, A., Sendor, J., Garaga, A., & Jenatton, K. (2013). Monitoring Personal Data Transfers in the Cloud. *2013 IEEE 5th International Conference on Cloud Computing Technology and Science* (pp. 347-354). Bristol: IEEE.

Sasmal, S., & Pan, I. (2017). Mutual auditing framework for service level security auditing in cloud. *2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)* (pp. 297-302). Kolkata: IEEE.

Sasmal, S., & Pan, I. (2018). Bit-Reversal Encryption Towards Secured Storage of Digital Image in Cloud Deployment. *Advanced Computational and Communication Paradigms* (pp. 803-812). Singapore: Springer.

Schumpeter, J. A. (1942). *Capitalism, Socialism and Democracy.* London: Routledge.

Shaikh, S., & Vora, D. (2016). Secure cloud auditing over encrypted data. *2016 International Conference on Communication and Electronics Systems (ICCES)* (pp. 1-5). Coimbatore: IEEE.

Shara Monteleone, L. P. (2017). *From Safe Harbour to Privacy Shield.* Brussles: European Parliament Research Service.

Shen, J., Shen, J., Chen, X., Huang, X., & Susilo, W. (2017, October). An Efficient Public Auditing Protocol With Novel Dynamic Structure for Cloud Data. *EEE Transactions on Information Forensics and Security*, pp. 2402-2415.

Shirisha Reddy, K., & Balaraju, M. (2018). Comparative Study On Trustee Of Third Party Auditor To Provide Integrity And Security In Cloud Computing. *Materials Today: Proceedings* , pp. 557-564.

Simpson, W. R. (2016). Chapter 5 - Cryptography. In W. R. Simpson, *Enterprise Level Security: Securing Information Systems in an Uncertain World* (pp. 55-73). Boca Raton, FL, USA: CRC Press.

Subha, T., & Jayashri, S. (2017). Efficient privacy preserving integrity checking model for cloud data storage security. *2016 Eighth International Conference on Advanced Computing (ICoAC)* (pp. 55-60). Chennai: IEEE.

Suganthi, J., Ananthi, J., & Archana, S. (2015). Privacy preservation and public auditing for cloud data using ASS in Multi-cloud. *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (pp. 1-6). Coimbatore: IEEE.

Suganya, S., & P. M. D. R. Vincent. (2017). Improving cloud security by enhancing remote data integrity checking algorithm. *2017 Innovations in Power and Advanced Computing Technologies (i-PACT)* (pp. 1-6). Vellore: IEEE.

Suguna, M., & Shalinie, S. M. (2017). Privacy Preserving Data Auditing Protocol for Secure Storage in Mobile Cloud Computing. *IEEE WiSPNET 2017 conference* (pp. 2724-2729). India: IEEE.

Sung, K., Hansen, D., & Helps, R. (2015). Information Technology Research in the Academy: Insights from Theses and Dissertations. (pp. 5-10). US: Association for Computing Machinery.

Suryawanshi, R., & Shelke, S. (2016). Improving data storage security in cloud environment using public auditing and threshold cryptography scheme. *2016 International Conference on Computing Communication Control and automation (ICCUBEA)* (pp. 1-6). Pune: IEEE.

Tan, S., Tan, L., Li, X., & Jia, Y. (2014, September). An efficient method for checking the integrity of data in the Cloud. *China Communications*, pp. 68-81.

Tang, X., Huang, Y., Chang, C.-C., & Zhou, L. (2019). Efficient Real-Time Integrity Auditing With Privacy-Preserving Arbitration for Images in Cloud Storage System. *IEEE Access*, pp. 33009-33023.

Tang, X., Qi, Y., & Huang, Y. (2016). Reputation Audit in Multi-cloud Storage through Integrity Verification and Data Dynamics. *2016 IEEE 9th International Conference on Cloud Computing (CLOUD)* (pp. 624-631). San Francisco, CA: IEEE.

Thangavel, M., Varalakshmi, P., Preethi, T., Renganayaki, S., Subhapriya, G., & Zeenath Banu, A. (2016). A Review on Public Auditing in Cloud Environment. *International Conference On Information Communication And Embedded System(ICICES 2016)* (p. 6). India: IEEE.

Thosar, S. D., & Mhetre, N. A. (2015). Integrity checking privacy preserving approach to cloud using third party auditor. *2015 International Conference on Pervasive Computing (ICPC)* (pp. 1-4). Pune: IEEE.

Tian, H., Chen, Y., Jiang, H., Huang, Y., Nan, F., & Chen, Y. (2019, March 25). Public Auditing for Trusted Cloud Storage Services. *IEEE Security & Privacy*, pp. 10 - 22.

Torkura, K. A., Sukmana, M. I., Strauss, T., Graupner, H., Cheng, F., & Meinel, C. (2018). CSBAuditor: Proactive Security Risk Analysis for Cloud Storage Broker Systems. *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)* (pp. 1-10). Cambridge: IEEE.

Trueman, T. E., & Narayanasamy, P. (2015). Ensuring Privacy and Data Freshness for Public Auditing of Shared Data in Cloud. *2015 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)* (pp. 22-27). Bangalore: IEEE.

Udagatti, A. K., & Sunitha, N. R. (2016). Fault tolerant public auditing system in cloud environment. *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)* (pp. 359-362). Bangalore: IEEE.

Venkatesh, M., Sumalatha, M., & SelvaKumar, M. (2012). Improving Public Auditability, Data Possession in Data Storage Security for Cloud Computing. *International Conference on Recent Trends in Information Technology* (pp. 463-467). India: IEEE.

Venters, W., & Whitley, E. A. (2012). A critical review of cloud computing: researching desires and realities. *Journal of Information Technology*, pp. 179–197.

Vinkler, P. (2010). *The Evaluation of Research by Scientometric Indicators.* Witney: Chandos Publishing.

W.Kuan Hon, C. M. (2011). The problem of 'personal data' in cloud computing: What information is regulated? - the cloud of unknowing. *International Data Privacy Law*, 211-228.

Wang, B., Li, B., & Li, H. (2012). Oruta: privacy-preserving public auditing for shared data in the cloud. *2012 IEEE Fifth International Conference on Cloud Computing* (pp. 295-302). Honolulu, HI: IEEE.

Wang, C., Wang, Q., Ren, K., & Lou, W. (2010). Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. *2010 Proceedings IEEE INFOCOM* (pp. 1-9). San Diego, CA: IEEE.

Wang, F., Xu, L., & Gao, W. (2019, September). Comments on “SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social

Systems Against Malicious Auditors". *EEE Transactions on Computational Social Systems*, pp. 854-857.

Wang, L., & Li, T. (2015). Virtual Resource Allocation and Composition for Data Stream Processing of Online Auditing in Cloud Computing. *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing* (pp. 806-813). Liverpool: IEEE.

Wang, X., Zhang, J., Wang, M., Zu, L., Lu, Z., & Wu, J. (2014). CDCAS: A Novel Cloud Data Center Security Auditing System. *2014 IEEE International Conference on Services Computing* (pp. 605-612). Anchorage, AK: IEEE.

Wang, Y., Wu, Q., Qin, B., Shi, W., Deng, R. H., & Hu, J. (2017, April). Identity-Based Data Outsourcing With Comprehensive Auditing in Clouds. *IEEE Transactions on Information Forensics and Security*, pp. 940-952.

Waqas, A., Yusof, Z. M., & Shah, A. (2013). Fault tolerant cloud auditing. *5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)* (pp. 1-5). Rabat: IEEE.

Wei, L., Zhu, H., Cao, Z., Jia, W., & Vasilakos, A. V. (2010). SecCloud: Bridging Secure Storage and Computation in Cloud. *30th International Conference on Distributed Computing Systems Workshops* (pp. 52-62). Genova: IEEE.

Wu, J., Li, Y., Wang, T., & Ding, Y. (2019). CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing. *IEEE Access*, pp. 160482-160497.

Xiao, C., Jia, W., Zhu, H., Du, S., & Cao, Z. (2012). Leveraging Cloud Computing for Privacy Preserving Aggregation in Multi-domain Wireless Networks. *International Conference on Wireless Algorithms, Systems, and Applications.* Berlin, Heidelberg: Springer.

Yan, Z., Yu, X., & Ding, W. (2017). Context-Aware Verifiable Cloud Computing. *IEEE Access*, pp. 2211-2227.

Yang, K., & Jia, X. (2011, July 16). Data storage auditing service in cloud computing: challenges, methods and opportunities. *World Wide Web*, pp. 409–428.

Yang, K., & Jia, X. (2013). An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing. *Transactions on parallel and distributed systems* (pp. 1717-1726). Hong Kong: IEEE.

Yang, L., & Xia, L. (2016). An Efficient and Secure Public Batch Auditing Protocol for Dynamic Cloud Storage Data. *2016 International Computer Symposium (ICS)* (pp. 671-675). Chiayi, Taiwan: IEEE.

Yang, Y., Guo, L., Zhong, Z., & Zhang, M. (2018, October). Selection of Technological Innovation for Service-Orientated Enterprises. *Sustainability*, p. 3906.

Yang, Y., Huang, Q., & Chen, F. (2019). Secure Cloud Storage Based on RLWE Problem. *IEEE Access*, pp. 27604-27614.

Yang, Y., Zhao, C., & Gao, T. (2015). Cloud Computing: Security Issues Overview and Solving Techniques Investigation in Intelligent Cloud Computing. *Intelligent Cloud Computing*.

Yu, H., & Yang, Z. (2018). Decentralized and Smart Public Auditing for Cloud Storage. *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)* (pp. 491-494). Beijing, China: IEEE.

Yu, J., Ren, K., Wang, C., & Varadharajan, V. (2015, June 1). Enabling Cloud Storage Auditing With Key-Exposure Resistance. *IEEE Transactions on Information Forensics and Security*, pp. 1167-1179.

Yu, Y., Ni, J., Au, M. H., Mu, Y., Wang, B., & Li, H. (2015, November). Comments on a Public Auditing Mechanism for Shared Cloud Data Service. *IEEE Transactions on Services Computing*, pp. 998-999.

Zhang, H., Li, P., & Zhou, Z. (2015). Performance Difference Prediction in Cloud Services for SLA-Based Auditing. *2015 IEEE Symposium on Service-Oriented System Engineering* (pp. 253-258). San Francisco Bay, CA: IEEE.

Zhang, J., & Zeng, W. (2014). Self-Certified Public Auditing for Data Integrity in Cloud Storage. *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing* (pp. 267-273). Guangdong: IEEE.

Zhang, X., & Xu, C. (2014). Efficient Identity-Based Public Auditing Scheme for Cloud Storage from Lattice Assumption. *2014 IEEE 17th International Conference on Computational Science and Engineering* (pp. 1819-1826). Chengdu: IEEE.

Zhang, Y., Li, X.-Y., & Han, Z. (2017). Third Party Auditing for Service Assurance in Cloud Computing. *GLOBECOM 2017 - 2017 IEEE Global Communications Conference* (pp. 1-6). Singapore: IEEE.

Zhang, Y., Zhang, H., Hao, R., & Yu, J. (2018, November). Authorized identity-based public cloud storage auditing scheme with hierarchical structure for large-scale user groups. *China Communications*, pp. 111-121.

Zhao, W., Qiang, L., Zou, H., Zhang, A., & Li, J. (2018). Privacy-Preserving and Unforgeable Searchable Encrypted Audit Logs for Cloud Storage. *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (pp. 29-34). Shanghai: IEEE.

Zheng, W., Lai, C.-F., He, D., Kumar, N., & Chen, B. (2020, April 29). Secure Storage Auditing with Efficient Key Updates for Cognitive Industrial IoT Environment. *IEEE Transactions on Industrial Informatics*, pp. 1 - 1.

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey. *2010 Sixth International Conference on Semantics, Knowledge and Grids* (pp. 105-112). Beijing: IEEE.

Zhou, Z., Zhang, H., Yu, X., & Guo, J. (2015). Audit meets game theory: Verifying reliable execution of SLA for compute-intensive program in cloud. *2015 IEEE International Conference on Communications (ICC)* (pp. 7456-7461). London: IEEE.

Zou, T., Wu, J., & Wan, C. (2012). An AAA based publicly auditable proof-of-storage scheme for cloud computing. *2012 7th International Conference on Computing and Convergence Technology (ICCCT)* (pp. 1226-1230). Seoul: IEEE.

Internet Sources

Amazon Web Services, Inc. (2020). *aws*. Retrieved July 2020, from Explore the AWS platform, cloud products, and capabilities: https://aws.amazon.com/?nc1=h_ls

Amazon Web Services, Inc. (2020). *aws*. Retrieved July 2020, from Cloud Computing with AWS: https://aws.amazon.com/what-is-aws/?nc1=h_ls

Amazon Web Services, Inc. (2020). *aws*. Retrieved June 2020, from What is cloud computing?: https://aws.amazon.com/de/what-is-cloud-computing/?nc1=f_cc

DSB. (2018, 5 12). *DSB: Datenschutzbehörde*. Retrieved from DSB: Datenschutzbehörde Republik Österreich: https://www.dsb.gv.at

Jolly, L. (2018, 5 12). *Thomson Reuters: Practical Law*. Retrieved from Thomson Reuters: Practical Law: https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

KPMG, Bitkom Research GmbH. (2020). *KPMG.* Retrieved June 2020, from KPMG: https://hub.kpmg.de/studie-cloud-monitor-2020?utm_campaign=Cloud-Monitor%202020&utm_source=AEM

McKinsey. (2018, April 12). *McKinsey Digital*. Retrieved June 2020, from Cloud adoption to accelerate IT modernization: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/cloud-adoption-to-accelerate-it-modernization

RIS. (2018, 5 12). *RIS*. Retrieved from RIS: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597

Abstract - English

The rise of cloud computing services in private as in business environments has been on the rise for years and there is no slowdown in sight. The popularity of cloud computing services can be ascribed to its various advantages in terms of cost reduction and flexibility increase. Its many benefits in terms of scalability make many entities incorporate external cloud solutions in their IT infrastructure. Clouds are one main driver of companies' digitalization strategies.

When it comes to auditing there are differences between internally and externally provided services. Therefore Cloud services are challenging the existing IT audit environment. Audits are important to monitor and evaluate the selection of new technology, assure regulatory compliance, test confidentiality, data integrity, availability and security. Monitoring and evaluation supports the integration of new technology and the success of cloud strategies. Furthermore it's a strong communication tool used to assure and to communicate certain security standards to the customer. The trust between cloud provider and user is enhanced.

Research in this field is essential as its leading to new solutions, testing and amelioration of technological advancements and a vital part of the innovation cycle. For innovation to be complete, innovation must be communicated effectively to others. That is the only way how sustainable change and innovation can take place.

In order to contribute to this cycle, in the scope of this thesis the current standing of research on the topic of auditing cloud computing services is being analyzed via scientometric means. Scientometric analysis is a viable way on analyzing the research conducted in a specific field, by a specific group of people or on a specific topic and provides a way to communicate results and enhance innovation. In this work it endorses the communication of innovation and progress by analyzing research productivity and growth, publication patterns, citation and reference pattern as well as authorship, keyword and content. Additionally, to identifying the development of key topics and solution proposals the results are put into context to the role of science and technology in the national economy and the influence of governmental science politics on research output is captured.

Abstract - German

Die Benutzung und das Angebot an Cloud Computing Lösungen ist seit Jahren auf dem Vormarsch und ein Ende ist nicht in Sicht. Der Erfolg und die weite Verbreitung von Cloud Computing Lösungen ist auf die Vielzahl seiner Vorteile zurückzuführen. Aus Unternehmenssicht sind vor allem die hohe Flexibilität und Möglichkeiten der Kostenreduzierung hervorzuheben. Aufgrund der hervorragenden Skalierbarkeit bauen immer mehr Unternehmen auch externe Cloud Computing Lösungen in ihre internen IT Strukturen ein. Cloud Services stellen einen wesentlichen Teil vieler Digitalisierungsstrategien dar.

Für die Auditierung von Cloud Computing Services ist die Verwendung von internen oder externen Lösungen möglich. Das wachsende Angebot an Cloud Services stellt eine Herausforderung für bestehende IT Audit Prozesse dar. Regelmäßige und einheitliche Auditprozesse sind wichtig um die Einführung neuer Technologien zu Monitoren und zu kontrollieren, die Compliance dieser mit geltenden Vorschriften zu verifizieren und die Verfügbarkeit, Vertraulichkeit, Integrität und Sicherheit von Daten sicherzustellen. Des Weiteren kann es auch als Kommunikationsmittel gesehen werden, um den konformen und sicheren Umgang mit Daten nicht nur zu kontrollieren sondern auch an den Kunden zu kommunizieren. Das Vertrauen zwischen Cloud Anbieter und Nutzer wird so gestärkt.

Forschung in dem Feld ‚Auditierung von Cloud Computing Services' ist wichtig, da es zu Verbesserungen und neuen Lösungen führt. Es ist wesentlicher Teil des Innovationskreislaufes. Auch wesentlich für diesen Kreislauf ist die effektive und vollständige Kommunikation von Forschungsergebnissen. Nur so können nachhaltige Veränderungen und Innovation stattfinden.

An diesem Punkt setzt diese Masterarbeit an, in deren Rahmen Forschungsergebnisse im Bereich ‚Auditierung von Cloud Computing Services' mit Hilfe scientometrischer Kennzahlen analysiert wird. Die scientometrische Analyse ist eine anerkannte Methode um, besonders im Bereich IT, Forschungsergebnisse in einem bestimmten Forschungsfeld, einer Personengruppe oder einem bestimmten Thema zu analysieren. Es trägt zur Kommunikation von Forschungsergebnissen bei und somit zum anhaltenden Innovationszyklus. Hierfür werden in dieser Arbeit verschieden Kennzahlen bzgl. Anzahl an Veröffentlichungen, Veröffentlichungsmuster, Autorenschaft, Zitier- und Referenzenmuster, Keywords und Inhalt analysiert um Trend-Themen und –Lösungsansätzen zu identifizieren. Zusätzlich werden die Ergebnisse im Zusammenhang

mit der volkswirtschaftlichen Rolle für Wissenschaft und Technologie und dem Einfluss von staatlichen Wissenschafts- und Forschungsstrategien gesetzt.

Appendix – Database

Database (132 publications) including - Publication Count, Title, Authors (A1-A9), Number of Authors, Collaboration (C), International C (I), Language, Journal (J) / Conference (C), Source 1 (Outlet), Source 2 (Outlet Title), Citations (2018 & 2020), References, Keywords, Researched subject, Research challenge, Research Approach and Proposition.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
1	SecCloud: Bridging Secure Storage and Computation in Cloud	2010	Lifei Wie, Haojin Zhu, Zhenfu Cao, Weiwei Jia, Athanasios V. Vasilakos	5	C	I (China, Greece)	English
2	IT Auditing to Assure a Secure Cloud Computing	2010	Zhixiong Chen, John Yoon	2	C		English
3	A Monitoring and Audit Logging Architecture for Data Location Compliance in Federated Cloud Infrastructures	2011	Philippe Massonet, Syed Naqvi, Christophe Ponsard, Joseph Latanicki, Benny Rochwerger, Massimo Villari	6	C	I (Belgium, France, Italy, Israel)	English
4	Secure cloud computing: Benefits, risks and controls	2011	Mariana Carroll, Alta van der Merwe, Paula Kotzé	3	C		English
5	An AAA based publicly auditable proof-of-storage scheme for cloud computing	2012	Tao Zou, Jian Wu, Changsheng Wan	3	C		English
6	Leveraging Cloud Computing for Privacy Preserving Aggregation in Multi-domain Wireless Networks	2012	Chengxin Xiao, Weiwei Jia, Haojin Zhu, Suguo Du, Zhenfu Cao	5	C		English
7	A critical review of cloud computing: researching desires and realities	2012	Will Venters, Edgar A. Whitley	2	C		English
8	An effective auditing scheme for cloud computing	2012	Ryan Houlihan, Xiaojiang Du	2	C		English
9	Data storage auditing service in cloud computing: challenges, methods and opportunities	2012	Kan Yang, Xiaohua Jia	2	C		English
10	Improving public auditability, data possession in data storage security for cloud computing	2012	M. Venkatesh, M.R. Sumalatha, C. Selvakumar	3	C		English
11	Near-Real-Time Cloud Auditing for Rapid Response	2012	Joon S. Park, Edward Spetka, Hassan Rasheed, Paul Ratazzi, Keesook J. Han	5	C		English
12	Monitoring Personal Data Transfers in the Cloud	2013	Anderson Santana de Oliveira, Jakub Sendor, Alexander Garaga, Kateline Jenatton	4	C	I (France/ Switzerland)	English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
1	C	IEEE	30th International Conference on Distributed Computing Systems Workshops	35	56	29	Cloud computing, Designated verification, Privacy preserving, Batch verification, Data storage secure
2	C	IEEE	6th World Congress on Services	14	17	21	Clouds, Communities, Cloud computing, Security, Computational modeling, Availability, Computer architecture
3	C	IEEE	International Parallel & Distributed Processing Symposium	1	47	13	Cloud computing, federated architectures, monitoring mechanisms, logging architecture, compliance issues
4	J	IEEE	Information Security for South Africa	31	61	35	Cloud computing, benefits, controls, risks
5	C	IEEE	7th International Conference on Computing and Convergence Technology (ICCCT)	0	0	18	Proof-of-storage, Cloud Computing, Publicly Auditable
6	C	Springer	International Conference on Wireless Algorithms, Systems, and Applications	1	1	9	Privacy Aggregation, Cloud Computing, Participatory Sensing
7	J	Springer	Journal of Information Technology	103	142	205	Cloud computing, services, latency, hybrid clouds, scalability, security
8	C	IEEE	Global Communications Conference (GLOBECOM)	5	6	20	Cloud computing; performance; auditing
9	J	Springer	World Wide Web	79	243	56	Data storage auditing, data owner auditing, third party auditing, cloud computing
10	C	IEEE	International Conference on Recent Trends in Information Technology	12	16	10	Data Storage, Public Auditing, Cloud Computing
11	C	IEEE	26th International Conference on Advanced Information Networking and Applications Workshops	9	9	29	Cloud computing, monitoring, auditing, rapid response, security
12	C	IEEE	5th International Conference on Cloud Computing Technology and Science	3	5	21	Auditing, Cloud computing, Security, Accountability, Compliance, Data tracking

Count	Researched Subject	Research Challenge	Research Approach	Proposition
1	Studying the interaction between cloud user and cloud service providers (CSPs) in cloud as a non-cooperative differential game.	The new paradigm of data hosting service is facing many new security challenges.	Simulation, Game formulation	Complex decision making processes and interactions between cloud user and CSPs are analysed. The simulation results provide a reference for users and CSPs in setting appropriate energy consumption and optimal strategies.
2	Introducing Provenance Management to Cloud Environments and depicting its challanges.	Cloud environments are susceptible to major security risks. Security and auditing of cloud systems is of great relevance.	Digital Forensic (post-incident investigation)	Proposition of a framework which aims at performing secure provenance audit of clouds across applications and multiple guest operating systems.
3	Analysis of existing auditing schemes and developement of a more efficient AAA-based scheme.	Existing schemes are very costly.	Analysis of the efficiency of bilinear map based schemes	Proposition of a light weight publicly auditable Proof-of-storage Scheme for cloud computing.
4	Comparative assessment of Outsourcing and auditing IT Infrastructure and Cloud Computing.	The virtualized environment of Cloud Computing challanges the IT auditing practice.	Examination	Developement of practical general guidelines for Cloud Computing audit for reference purposes.
5	Discovering the value creation and challenges confronted by cloud computing's practice.	Value creation ist essential and challangeable in every business. With increased usage of Cloud Computing by companies the examination of ist value creation is needed.	Modelling	Value creation Model discussion various effects of the implementation of Cloud Computing, providing guidance to the IT industry. Security Issues and Auditing are adressed.
6	Security Analytics and Intelligence for Cyber Physical Systems	Cloud service provider may invade data privacy and provide inaccurate data processing results. Therefore challange of cloud computing verification.	Modelling	Context-aware verifiable computing scheme based on full homomorphic encryption by deploying an auditing protocol to verify the correctness of the encrypted data processing results.
7	Chosen plaintext-attack on homomorphic encryption auditing scheme.	Data integrity and confidentiality can not be sufficiently provided by homomorphic encryption scheme.	Experiment	Applying LLL algorithm twice on two small deimension lattices shows that user data can be recovered.
8	Analysing Audit isues from three different perspectives, distinguishing between infrastructure security and data security.	For adopting Cloud Computing, security and espacially the lack of auditability, is still an obstacle.	Analysis	Most risks are easy to overcome but some may remain challanges that need to be overcome in the future.
9	Indirect Third Party Auditing of Cloud Service Provider adhereing the Service Level Agreements.	Cloud Service provider can deceipt the SLA to reduce costs.	Modelling	A crowdsourced TPA Model based on indirect auditing to detect CSPs deception of SLA.
10	Demystification of concepts of fog computing, edge computing and cloudlets using refernces from academia and industry.	Fog computing is not a novelty. Much can be learned when considering former concepts like edge computing.	Survey	Analysis of terminology, dimension of performance, security and governance and identification of related topics and main research areas.
11	Provide honest and genuine data sharing in E-Auctioning.	Validity of information, reasonableness and insurance of data propriator.	Modelling	Utilizing forward ring ID signatures security and a Third Party Auditor to ensure validity and reasonability.
12	Enabling privacy preserving outsourced data aggregation for multi-domain wireless networks.	Data leakage	Modelling	Novel hybrid cloud based privacy preserving outsourced data aggregation framework including the pro-active privacy preserving data aggregation and passive privacy preserving data aggregation schemes.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
13	Trust management approach for secure and privacy data access in cloud computing	2013	K. Mythili, H. Anandakumar	2	C		English
14	A flexible distributed storage integrity auditing mechanism in Cloud Computing	2013	T.J. Salma	1			English
15	A privacy-preserving storage security for spatial data in dynamics cloud environment	2013	S. Sakthivel , B. Dhiyanesh	2	C		English
16	An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing	2013	Kan Yang, Xiaohua Jia	2	C		English
17	An Efficient Proof of Retrievability with Public Auditing in Cloud Computing	2013	Jin Li, Xiaofeng Chen, Xiao Tan, Duncan S. Wong	4	C	I (China, Hong Kong)	English
18	An Efficient Public Batch Auditing Protocol for Data Security in Multi-cloud Storage	2013	He Kai, Huang Chuanhe, Wang Jinhai, Zhou Hao, Chen Xi, Lu Yilong, Zhang Lianzhen, Wang Bin	8	C		English
19	Fault tolerant cloud auditing	2013	Ahmad Waqas, Zulkefli Muhammed Yusof, Asadullah Shah	3	C	I (Pakistan, Malaysia)	English
20	Public Auditing for Big Data Storage in Cloud Computing - A Survey	2013	Chang Liu, Rajiv Ranjan, Xuyun Zhang, Chi Yang, Dimitrios Georgakopoulos, Jinjun Chen	6	C		English
21	Simultaneously Supporting Privacy and Auditing in Cloud Computing Systems	2013	Tyrone Grandison, Sean Thorpe, Leon Stenneth	3	C	I (USA, Jamaica)	English
22	Toward a Real-Time Cloud Auditing Paradigm	2013	Robert Nix, Murat Kantarcioglu, Sachin Shetty	3	C		English
23	Data and infrastructure security auditing in cloud computing environments	2014	Hassan Rasheed	1			English
24	Effective Third Party Auditing in Cloud Computing	2014	Mohammed Hussain, Mohamed Basel Al-Mourad	2	C		English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
13	C	IEEE	International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)	3	13	13	CIA, Cloud Computing auditing, Logging, BASE64
14	C	IEEE	International Conference on Information Communication and Embedded Systems (ICICES)	0	1	10	Data integrity, dependable distributed storage, error localization, data dynamics, Cloud Computing
15	C	IEEE	4th ICCCNT	3	4	8	Auditing, Cloud Computing, Cloud Storage, Privacy
16	J	IEEE	Transactions on Parallel and Distributed Dystems	153	261	30	Storage auditing, dynamic auditing, privacy-preserving auditing, batch auditing, cloud computing
17	C	IEEE	5th International Conference on Intelligent Networking and Collaborative Systems	4	7	20	Servers, Cloud computing, Security, Computational modeling, Protocols, Memory, Educational institutions
18	C	IEEE	8th Annual ChinaGrid Conference	5	8	22	Data Integrity, Batch Auditing, Data Corruption Identification, Multi-cloud Storage
19	C	IEEE	5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)	5	6	8	Cloud Computing, Security, Services, Auditing, Tiered Auditing, Fault Tolerant Auditing
20	C	IEEE	16th International Conference on Computational Science and Engineering	6	6	32	Cloud computing, big data, data security, integrity verification, public auditing
21	C	IEEE	Ninth World Congress on Services	1	1	32	Auditing, Cloud Computing,Privacy
22	C	IEEE	Ninth World Congress on Services	0	0	15	Cloud auditing, machine learning, real time processing, security
23	J	Elsevier	International Journal of Information Management	25	43	32	Cloud computing, Security audit, Data integrity, Standards compliance
24	C	IEEE	28th International Conference on Advanced Information Networking and Applications Workshops	1	6	16	Cloud computing, web-service auditing, quality of service

Count	Researched Subject	Research Challenge	Research Approach	Proposition
13	Demonstrating compliance to data transfer constraints.	Lack of tools to support accountable data localization and transfer across cloud software, platform and infrastructure services, usually run by data processors.	Experiment	Framework for automating the collection of evidence that obligations with respect to personal data handling are being carried out in what concerns personal data transfers.
14	Ensuring data intactness in Mobile Cloud Computing using Trusted Third Party Auditors.	Because of loss over control over data security and privacy remote data correcteness has to be ensured periodically with minimum overhead. It must be insured that private data is not reveiled to the TPA.	Experimental Analysis	Privacy Preserving Data Auditing Protocol using blockless and stateless verification to ensure that private data is not reveiled to the TPA.
15	Verifying the integrity of outsourced data in cloud storage technology.	Protecting the data from unauthorized access, data privacy preservation, modification and deletion of original data.	Modelling	Data Privacy preservation model using Third Party Auditing (TPA) without demanding the local copy of data, and any additional burden using bilinear aggregate signatures.
16	Taking data storage and computational security into consideration for Cloud security.	Computation security is often taken into consideration by other work.	Analysis and simulations	Developement of a framework achieving data storage and computation security using designated verification technique and batch verification technique.
17	Public auditing of outsourced data to verify data integrity.	Once the data leaves the owner premises, there is no control of data to the data owner.	Modelling	Multisector public auditing system by utilizing a linear combination of homomorphic linear authenticator tags of the file blocks.
18	Using information systems as auditing tool.	Often high costs, information security or interest conflicts leads to reluctant usage.	Conceptualization	Conceptualization of an auditing concept based on Cloud Computing SaaS technology and anylysis of the benefits of using cloud computing on auditing.
19	To Assure privacy and prevent data leakage security mechanisms have to be in place.	Challenges in achieving privacy and a trust based cloud.	Modelling	Introduction of a novel approach based on an CIA framework, using Logs and Base 64 algorithm to enhance information for the data owner and security.
20	Security management serves to protect the end-user's data but also ensures the tracability of the data processing which is nessesarry for compliance auditing.	Within federated Cloud Infrastructures, where data can migrate from one country to another, the data owner should be able to locate his data at any time.	Modelling	Logging architecture where provider monditors the Virtual machines and share his information with the user so he can create the audit logs required for compliance auditing.
21	Investigation of the concept and deployment of Clod Computing with the arising security problems.	All prominent Cloud security issues.	Modelling	Rendering a comprehensive Cloud Computing Security technical reference model which is composed of associated cloud security solving techniques that result from inevitably multi-faceted cloud security issues.
22	Achieving greater security and privacy by broadening the scope of Service Level Agreements.	SLA's are too narrow in scope and too one-sided to serve as an ultimate assurance instrument. Do far it doesn't meet the new requirements of corporate responsibility, as ist focus lies on availability.	Investigation/Examination of topic	Additionally to availability SLA's have to adress accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security.
23	The risky adoption of Cloud Computing Services.	The adoption of Cloud Computing Services comes with multilayered risks regarding Management, Operation and Technology.	Discussion and Recommondation	Mitigation strategies to avoid risk, like for example implementing end-to-end-encryption or audit controls.
24	Including additional privancy preserving concepts into software agent-based audit systems for clouds.	Using audit agents in cloud-adopted digital evidence collection frameworks causes new privacy concerns.	Proposition of framework	The framework proposes to use Somehow Homomorphic Encryption and Key Searchable Encryption to support privacy in the audit proces.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
25	The innovative application of cloud computing on auditing	2014	Shaio Yan Huang, Ching-Wen Lin, Yi-Feng Jian	3	C		English
26	Cloud Computing: Security Issues Overview and Solving Techniques Investigation in Intelligent Cloud Computing	2014	Yu Yang, Chenggui Zhao, Tilei Gao	3	C		English
27	Privacy-friendly cloud audits with Somewhat Homomorphic and Searchable Encryption	2014	José M. López, Thomas Ruebsamen, Dirk Westhoff	3	C		English
28	Reflecting on Whether Checklists Can Tick the Box for Cloud Security	2014	Bob Duncan, Mark Whittington	2	C		English
29	A XOR Based Public Auditing Scheme for Proof-of-storage	2014	Bei Pei, Changsong Chen, Changsheng Wan	3	C		English
30	An efficient method for checking the integrity of data in the Cloud	2014	Tan Shuang, Tan Lin, Li Xiaoling, Jia Yan	4	C		English
31	An efficient, dynamic, privacy preserving public auditing method on untrusted cloud storage	2014	R. Navajothi, S. Jean Adrien Fenelon	2	C		English
32	Auditing cloud computing migration	2014	Georgiana Mateescu, Marius Vlădescu, Valentin Sgârciu	3	C		English
33	Auditing cloud service level agreement on VM CPU speed	2014	Ryan Houlihan, Xiaojiang Du, Chiu C. Tan, Jie Wu, Mohsen Guizani	5	C	I (USA, Qatar)	English
34	CDCAS: A Novel Cloud Data Center Security Auditing System	2014	Xueying Wang, Jun Zhang, Mingbo Wang, Lijun Zu, Zhihui Lu, Jie Wu	6	C		English
35	Cloud Security Auditing: Challenges and Emerging Approaches	2014	Jungwoo Ryoo, Syed Rizvi, William Aiken, John Kissell	4	C		English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
25	J	Inderscience	International Journal of Mobile Communications	0	0	18	Cloud Computing, Auditing, mobile Communication, CAAT, Computer-assisted audit techniques, EAMs, embedded audit modules, COA, continous online auditing
26	C	Springer	International Conference on Intelligent Cloud Computing	0	0	38	Cloud computing, Security issues, Trusted cloud computing solving techniques, Shared storage security solving techniques, Cloud security technical reference model
27	C	IEEE	14th International Conference on Innovations for Community Services (I4CS)	2	3	20	Cloud Computing, Audit, Evidence, Computing on Encrypted Data, Somewhat Homomorphic Encryption, Searchable Encryption
28	C	IEEE	6th International Conference on Cloud Computing Technology and Science	3	7	61	Security, standards, compliance, assurance, audit
29	C	IEEE	9th International Conference on Broadband and Wireless Computing	0	0	18	XOR, Publicly Auditable, Proof-of-storage
30	J	IEEE	China Communication	0	0	24	Cloud computing, storage security, public auditability, provable data integrity
31	C	IEEE	International Conference on Information Communication and Embedded Systems (ICICE)	3	5	11	Cloud Computing, Public Auditing, Privacy Preserving, dynamic data
32	C	IEEE	9th International Symposium on Applied Computational Intelligence and Informatics (SACI)	1	3	8	Cloud computing, Computer architecture, Best practices, Computational modeling, Companies
33	C	IEEE	Communication and Information Systems Security Symposium	2	5	15	Cloud computing, Service Level Agreement, auditing, CPU
34	C	IEEE	International Conference on Services Computing	4	4	21	Cloud security auditing, log collection and analysis, autonomous rule, cloud data center
35	J	IEEE	Security & Privacy	13	27	15	Cloud computing, Information systems, Encryption, Privacy, Computer security, Organizational aspects

Count	Researched Subject	Research Challenge	Research Approach	Proposition
25	Cloud Security is often approached through standard compliane. Compliance is checked by internal audit using checklists.	Using Checklists generally comes with weaknesses, which are exacerbated by the nature of Cloud Computing.	Examination	Examination of problems regarding usage of checklists and adapting checklist model regarding the needs of Cloud Computing.
26	Cloud security can only be met by an Assurance model (not technical solutions only) given that the right measurements are in place.	Consistant measures for accountability, assurance, audit, confidentiality, compliance, integrity, privacy, responsibility and security are important.	Examination/ Examplification	A generic set of measures is not enough. The paper give examples of how management can measure for example security properties.
27	Assessing the impact of cloud computing on enterprises.	It is important to evaluate claims made in existing literature and critically review these against empirical evidence from the field.	Literature review	Framework within which to locate existing and future research on cloud computing characteristics that are important for cloud users to identify research questions.
28	Enforcing the quality of dependable cloud storage services for users through storage correctness insurance and data error localization.	Security in Ccloud data storage.	Modelling	Effective and flexible distributed scheme withe explicit dynamic data support, including block update, delete, and append.
29	Developing a language for describing the properties necessary for cloud security audit through a metamodel.	Ability of users to ascertain the security posture of cloud service providers to adequately safeguard data and applications.	Analysis	Audit framework that entails a set of concepts such as goals, constraint, plan and evidence to enable cloud users to identify their migration goals and introduce constraints that must be satisfied by a cloud provider.
30	Private virtual infrastructure (PVI), cloud management and security model.	Simultaneously achieving fine-grandness, scalability and data confidentiality of access control.	Modelling	Interactive PDP protocolusing challange-response algorithms and verifications protocol supporting dynamic operation.
31	Privacy preservation public auditing schemes by Trusted Third Party Auditor (TTPA).	Insecure cloud frameworksbecause of modification or corruption in data by unauthorized users.	Literature review	Analysis of ideas and audit schemes by various researchers.
32	Efficient Multilevel Security of Cloud Storageing.	TPA audit should not bring new privacy threats and should be possible with haven local copies of data.	Survey	Auditing solution using Kerberos as TPA, RSA algorithm for secure communication, MD5 algorithm to verify data integrity and data centers.
33	Ensuring the data storage correctness and integrity.	Because of lack of access control and data may tamper by malicious users, business organisations hesitate to use cloud computing.	Analysis	Analysisng various integrity procedures in terms of security and performance.
34	Efficient data auditing while controlling the cloud fees.	Many existing cloud storage security schemes did not consider the cloud fees into account or provide cost analysis.	Modelling	New regenerating code-based model for cloud data integrity protection that can surely conduct data auditing operation with the minimum cost possible.
35	Revising public auditing schemes.	Current public auditing schemes are bilinear map based and costly.	Modelling	More efficient XOR based public auditing scheme.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
36	Consistency as a Service: Auditing Cloud Consistency	2014	Qin Liu, Guojun Wang, Jie Wu	3	C	I (China, USA)	English
37	Efficient Identity-Based Public Auditing Scheme for Cloud Storage from Lattice Assumption	2014	Xiaojun Zhang, Chunxiang Xu	2	C		English
38	On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage	2014	Jianbing Ni, Yong Yu, Yi Mu, Qi Xia	4	C		English
39	Oruta: privacy-preserving public auditing for shared data in the cloud	2014	Boyang Wang, Baochun Li, Hui Li	3	C	I (China,Canada)	English
40	Self-Certified Public Auditing for Data Integrity in Cloud Storage	2014	Jianhong Zhang, Weina Zeng	2	C		English
41	Towards corporate confidentiality preserving auditing mechanisms for Clouds	2014	Roland Bless, Matthias Flittner	2	C		English
42	A provenance auditing framework for cloud computing systems	2015	G. Meera, G. Geethakumari	2	C		English
43	Cloud computing risk and audit issues	2015	David. C. Chou	1			English
44	Cloud computing: A value creation model	2015	David C. Chou	1			English
45	Enhancing Cloud Security and Privacy: Broadening the Service Level Agreement	2015	Bob Duncan, Mark Whittington	2	C		English
46	The Importance of Proper Measurement for a Cloud Security Assurance Model	2015	Bob Duncan, Mark Whittington	2	C		English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
36	J	IEEE	TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT	8	17	25	Cloud storage, consistency as a service (CaaS), two-level auditing, heuristic auditing strategy (HAS)
37	C	IEEE	17th International Conference on Computational Science and Engineering	1	3	25	Cloud storage, public auditing, lattice-based cryptography, post-quantum cryptography
38	J	IEEE	Transactions on Parallel and Distributed Systems	16	31	5	Auditing protocol, cloud storage, data integrity, security analysis
39	J	IEEE	Transactions on Cloud Computing	50	113	33	Public auditing, privacy-preserving, shared data, cloud computing
40	C	IEEE	Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing	1	1	18	Cloud computing, self-certified cryptography, integrity checking, security proof
41	C	IEEE	3rd international conference on Cloud Networking (CloudNet)	1	3	26	Cloud Security, Auditing, Non-Repudiation, Commitments, Transparency
42	C	IEEE	International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)	0	2	23	Cloud computing, Virtual machining, Cryptography, Monitoring, Digital forensics
43	J	Elsevier	Computer Standards & Interfaces	1	23	33	Cloud computing Auditing, Risk factors Audit standards
44	J	Elsevier	Computer Standards & Interfaces	28	49	28	Cloud computing, Value creation model, Risk analysis, IT auditing standards
45	C	IEEE	IEEE Trustcom/BigDataSE/ISPA	4	4	58	Security, privacy, standards, compliance, assurance, audit, service level agreements, cloud service providers, responsibility, accountability, agency theory, stewardship theory
46	C	IEEE	7th International Conference on Cloud Computing Technology and Science (CloudCom)	3	4	36	Security, privacy, standards, compliance, assurance, audit, measurement, cloud service providers, service level agreements

Count	Researched Subject	Research Challenge	Research Approach	Proposition
36	Monitoring performance and behaviour of the cloud.	Existing schemes are vulnerable to timed scrubbing attacks.	Modelling	Modification of the Linux auditing deamon-audit, using System Management Mode and Trusted Platform Module.
37	Independent audit service to check data integrity.	Existing remote integrity checking methods can only serve for static archieve data, but cloud data can be updated dynamically.	Modelling	Efficient and pricavy-preserving auditing framwork supporting data dynamic operations and batch auditing.
38	Securing Cloud storage data efficiently.	Existing schemes fail to provide public validation, impartiality, stateless validation and privacy protection efficiently all at once.	Modelling	Secure audit scheme supporting dynamic operation and transparent verification, using BLS short signature, sequence-enforced B+ Hash Tree structure, random mask and bilinear aggregate signature technology.
39	Creating secure and reliable data storage over unreliable service providers.	Burden of generating a constant amount of meta-data at the client side in order to audit data integrity.	Modelling	Based on bilinear schemes, simple and efficient audit service for public verification of untrusted and outsourced storage.
40	The role of the cloud user in verifying data integrity in cloud storage.	The computational burden is too huge for the users to compute the public authentication tags of file blocks that are needed by TPA.	Modelling	New cloud architecture with two independent cloud server, storage server and cloud audit server, to pre-process the data before uploading and later verifying it.
41	Auditing outsourced data.	Efficien dynamic support directed at cloud data are missing.	Modelling	Proposition of an efficient public auditing protocol with global and sampling blockless verification as well as batch auditing.
42	Auditing in multiple Cloud environments.	Many integrity auditing protocols focus on the single cloud environment or don't support batch auditing.	Modelling	Auditing scheme using homomorphic ciphertext verification and recoverable coding approach achieves quick identification of corrupted data.
43	Securing Cloud storage with efficient auditing services.	Existing remote integrity checking protocols can not serve for dynamic data.	Modelling	Novel auditing framework supporting the dynamic operations, which is efficient and provably secure in random oracle model.
44	Auditing Service Level Agreements in semi-honest Cloud model with help of a Cloud Service Broker (CSB).	User loose direct control over task and can not verify integrity.	Modelling	Proposition of a program structure mapping model called concept tree foolowed by a fine-grained CSB audit.
45	Assessing the impact of migrating to a cloud encironment.	Cloud environment can introduce significant risks within a company.	Modelling	Developement of a web based migration assessment tool (MAT) that assists the internal auditor in the pre-migration process.
46	Auditing of Service Level Agreements for CPU cheating.	Cloud service provider have incentives to cheat on the Service Level Agreement to increase their profits.	Modelling	TPA framework based on an algorithm using CPU intensive calculation and matrix multiplication to detect cheating by CSP.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
47	A Framework for Cloud Security Audit	2015	Umar Mukhtar Ismail, Shareeful Islam, Haralambus Mouratidis	3	C		English
48	A survey for secure communication of cloud third party authenticator	2015	Sawan V. Baghel, Deepti P. Theng	2	C		English
49	Audit meets game theory: Verifying reliable execution of SLA for compute-intensive program in cloud	2015	Zhigang Zhou, Hongli Zhang, Xiangzhan Yu, Junwu Guo	4	C		English
50	Cloud Computing Features, Issues, and Challenges: A Big Picture	2015	Deepak Puthal, B.P.S. Sahoo, Sambit Mishra, Satyabrata Swain	4	C	I (India, Taiwan)	English
51	Comments on a Public Auditing Mechanism for Shared Cloud Data Service	2015	Yong Yu, Jianbing Ni, Man Ho Au, Yi Mu, Boyang Wang, Hui Li	6	C	I (China, Hong Kong, Australien)	English
52	Cost and Communication Efficient Auditing over Public Cloud	2015	Vitthal S. Gutte, Priya Deshpande	2	C		English
53	Enabling Cloud Storage Auditing With Key-Exposure Resistance	2015	Jia Yu, Kui Ren, Cong Wang, Vijay Varadharajan	4	C	I (China, Hong Kong, USA, Australia)	English
54	Ensuring Privacy and Data Freshness for Public Auditing of Shared Data in Cloud	2015	Tina Esther Trueman, P. Narayanasamy	2	C		English
55	Integrity checking privacy preserving approach to cloud using third party auditor	2015	Sonali D. Thosar , Nalini A. Mhetre	2	C		English
56	Performance Difference Prediction in Cloud Services for SLA-Based Auditing	2015	Hongli Zhang, Panpan Li, Zhigang Zhou	3	C		English
57	Privacy preservation and public auditing for cloud data using ASS in Multi-cloud	2015	J. Suganthi, Ananthi J, S. Archana	3	C		English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
47	C	Springer	Safety and Sustainability: Tomorrow's Challenges of Cyber Security	0	0	19	Cloud computing, Security, Audit, Evidence, Control, Constraint, Secure plan
48	C	IEEE	2nd International Conference on Electronics and Communication Systems (ICECS)	2	2	13	Public Auditing, Cloud Computing, Third Party Auditor, Multilevel database, Data center
49	C	IEEE	Communication and Information Systems Security Symposium	1	2	17	Auditing, compute-intensive program, cloud computing, game theory, service level agreement
50	C	IEEE	International Conference on Computational Intelligence and Networks	46	92	42	Cloud computing, Cloud security, Virtualization, Workflow scheduling, Data integrity, Public auditing
51	J	IEEE	TRANSACTIONS ON SERVICES COMPUTING	12	22	6	Cloud storage, data integrity, security analysis
52	C	IEEE	International Conference on Computational Intelligence and Communication Networks (CICN)	0	0	12	Cloud Computing, Storage technology, security, database, storage management
53	J	IEEE	Transactions on Information Forensics and Security	37	72	38	Data storage, cloud storage auditing, homomorphic linear authenticator, cloud computation, key-exposure resistance
54	C	IEEE	IEEE International Conference on Cloud Computing in Emerging Markets	0	0	10	Cloud servers, data sharing, data owner, preserving privacy, fresh data, TPA, auditing, HARS
55	C	IEEE	International Conference on Pervasive Computing (ICPC)	2	3	10	Integrity, public auditability, blockless verification, privacy preserving
56	C	IEEE	Symposium on Service-Oriented System Engineering	4	4	16	Cloud computing; performance prediction, SLA
57	C	IEEE	International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)	2	2	11	Cloud computing, Aggregates, Servers, Public key, Data privacy, Conferences

Count	Researched Subject	Research Challenge	Research Approach	Proposition
47	Auditing Clouds based on the Cloud Auditing Data Federation (CADF) standard.	Different Cloud models, complex environments and orchestrated operations depict difficulties for auditing.	Analysis	Based on CADF using OpenStack audit records can be generated, which can be stored for and reviewed in the future.
48	Auditing Cloud data centers.	Security concerns as traditional auditing is not suitable for the new cloud environment.	Modelling	Novel auditing scheme based on an agent model controlled by a set of rules dynamically addapting to different scenarios. Using a log analysis model and correlative analysis algorithm to extract security.
49	Cloud-assisted WBANs (small sensors monitoring real-time parameters of patients' physiology remotely).	Integrity of patients' data stored in the Cloud is very important.	Modelling	Novel certificateless public auditing (CLPA) scheme, with provable security withstanding adverseries.
50	Conquering security issues of existing auditing systems with remote verification technique.	Schemes require presence of data owners to manage authentication and permission of open examining by TPA.	Modelling	Novel scheme using auditing based on the token generation and proxies ensuring data privacy and reducing computational overhead.
51	Cloud computing Technology	Fundamental concerns regarding communication, virtualization, data availability and integrity, public auditing, scientific application and information security.	Analysis	Precise the current open challanges regarding Cloud architecture, security issues and future implications.
52	Customization of IT security for Cloud Computing Models.	Data and security are managed by a third party.	Analysis	Description of challanges and three schools of thoughtt regarding cloud auditing.
53	Revising the public auditing protocol for shared data PANDA.	Panda is insecure in the sense that a cloud server can hide data loss without being detected.	Analysis and Modelling	Adequate approach to remedy the weakness without losing any features of the original protocol.
54	Replication technique in Cloud storage service.	It is expensive to achieve strong consistency on a worldwide scale.	Modelling	Novel Consistency as a service model, consisting of a large data cloud and multiple smaller auditing clouds applying a two-level auditing architecture.
55	Auditing mechanism for cost and communication efficiency.	Storage Space and data security.	Modelling	Audit scheme using TPA and digital signatures.
56	Auditing integrity of data storage.	Security risks because of interest divergence in identities and interests.	Survey/ Literature Analysis	Identifying requirements and challanges and analysis of performance and security of existing audit schemes.
57	Post-quantum secure public auditing.	Quantum computer attacks - data lost attacks and tamper attacks from provider.	Modelling	Novel scheme using preimage sampleable functions and inhomogeneous small integer solution assumption (ISIS).

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
58	Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage	2015	Jian Liu, Kun Huang, Hong Rong, Huimei Wang, Ming Xian	5			English
59	Public auditing system: Improved remote data possession checking protocol for secure cloud storage	2015	Rashmi R. Patil, S. M. Sangve	2	C		English
60	Third-Party Auditor (TPA): A Potential Solution for Securing a Cloud Environment	2015	Syed Rizvi, Katie Cover, Abdul Razaque	3	C		English
61	Virtual Resource Allocation and Composition for Data Stream Processing of Online Auditing in Cloud Computing	2015	Lei Wang, Tuo Li	2	C	I (China, USA)	English
62	Identity-preserving public auditing for shared cloud data	2015	Kai He, Chuanhe Huang, Kan Yang, Jiaoli Shi	4	C	I (China, Canada)	English
63	Cryptanalysis of a Privacy Preserving Auditing for Data Integrity Protocol	2016	Jingguo. Bi, Jiayang Liu	2	C		English
64	Fog computing: Data analytics and cloud distributed processing on the network edges	2016	Nelson Mimura Gonzalez, Walter Akio Goya, Rosangela de Fatima Pereira, Karen Langona, Erico Augusto Silva, Tereza Christina Melo de Brito Carvalho, Charles Christian Miers, Kjan-Erik Mangs, Azimeh Sefidcon	9	C	I (Sweden, Brazil)	English
65	Forward secure E-Auction with Auditing Integrity	2016	Vidya A. Gaikwad, Sachin D. Babar	2	C		English
66	Measuring Cloud Security from risks perspective	2016	Savy Gupta, Subhash Chand Gupta, Rana Majumdar, Y.S. Rathore	4	C		English
67	A review on public auditing in cloud environment	2016	M. Thangavel, P. Varalakshmi, T. Preethi, S. Renganayaki, G.R. Subhapriya, A. Zeenath Banu	6	C		English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
58	J	IEEE	Transactions on Information Forensics and Security	18	32	33	Cloud storage, regenerating codes, public audit, privacy preserving, authenticator regeneration, proxy, privileged, provable secure
59	C	IEEE	2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)	1	3	21	Cloud service provider, third party auditor, data dynamics, data posession checking, Security
60	C	IEEE	2nd International Conference on Cyber Security and Cloud Computing	4	6	14	Cloud computing, cloud auditing, data privacy, ntegrity, authentication, public verifier, insider threats
61	C	IEEE	2015 IEEE International Conference on Computer and Information Technology (CIT)	1	1	14	Online auditing, cloud computing, data stream processing, virtual resource allocation, service composition
62	C	IEEE	23rd International Symposium on Quality of Service (IWQoS)	0	4	20	Data Integrity, Shared Data, Public Auditing, Batch Auditing.
63	C	Springer	International Conference on Information Security Practice and Experience (ISPEC)	0	1	14	Cloud computing, Homomorphic encryption, Auditing protocol, LLL algorithm, Chosen-plaintext attack
64	C	IEEE	35th International Conference of the Chilean Computer Science Society (SCCC)	2	15	51	Mobile networks, Fog computing, edge computing, cloudlet, data analytics, distributed processing
65	C	IEEE	International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)	0	0	12	Authentication, Data Sharing, Platform as Service(PAAS), Forward Security, E-Auction, Public Auditing
66	C	IEEE	6th International Conference - Cloud System and Big Data Engineering (Confluence)	0	0	10	Cloud Computing, SaaS, PaaS,IaaS
67	C	IEEE	International Conference On Information Communication And Embedded System(ICICES)	0	1	20	Cloud Computing, Privacy, Integrity, Unauthorized access, Trusted Third Party Auditor

Count	Researched Subject	Research Challenge	Research Approach	Proposition
58	Privacy preserving auditing schemes (Oruta, Knox).	Risk of active adversaries - arbitrary modification of data.	Modelling	Solution scheme using proof responses verified by TPA.
59	Mutual nonrepudiation between user and service provider.	In existing solutions hash values of files need to be cashed leading to overhead.	Modelling	Novel scheme in which a sclice of binary hash tree is transferred to the client device for real-time auditing using a proof of violation. (POV) scheme.
60	Reduction of consequences of client's key exposure.	When low security settings at the clients side the client's secret key for auditing can not ensure integrity.	Modelling	Auditing protocol with key-exposure resilience using binary tree structure, preorder traversal technique and novel authenticator construction.
61	Securing integrity of data in cloud storage.	If cloud storage is vulnerable it looses clients.	Modelling	Public privacy-preserving audit scheme, based on BLS signature and random sampling.
62	Shared data storage services, in particular update sites and read-only sites.	Data integrity and the identity of the user needs to be secured by the provider and the user must be able to make changes to the data stored therefore data must be up to date at all times.	Modelling	Method ensuring integrity and data freshness using homomorphic authenticable ring signatures and Overly tree algorithm.
63	Cloud Computing service models, security & privacy threats and auditing strategies.	General concerns reagarding security. Privacy, auditing etc.	Analysis	In terms of auditing suggesting a conjunctive approach of fault tolerance and tiered strategy.
64	Data protection in Cloud storageing.	Trusting a Third party Auditor fully isn't the right idea.	Modelling	Introduction of a semi trusted TPA who when generating wrong or biased results get reported to the Cloud provider by the user.
65	Using request-respons communication patterns for auditing.	Not suitable for group communication patterns.	Modelling	Novel group communication-capable request-response middleware beinging together Request-response Reliability and group communication which is able to handle changes in the composition of the group.
66	Cloud Storage systems.	Integrity, controllable outsourcing, and origin auditing concerns in existing Cloud storage systems.	Modelling	Proposition of data outsourcing scheme (IBDO) allowing users to authorize dedicated proxies and facilitating comprehensive auditing.
67	Coud Storage integrity auditing.	Existing integrity auditing schemes are often not identity-preserving and have high auditing costs.	Modelling	Public Auditing scheme supporting user revocation without re-signing signatures computed by revoken users using batch auditing.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
68	A thick-cloud solution for data auditing in a cloud environment	2016	Alouane Nour-Eddine, Iabouchabaka Jaafar, Rafalia Najat	3	C		English
69	An Efficient and Secure Public Batch Auditing Protocol for Dynamic Cloud Storage Data	2016	Liu Yang, Lili Xia	2	C		English
70	Auditing in Cloud Computing Solutions with OpenStack	2016	Divya K. Konoor	1			English
71	Cloud Based Two Tier Security Scheme for Store, Share and Audit Our Data into Cloud	2016	Priya Kharmate, Ranjeetsingh Suryawanshi	2	C		English
72	Efficient Real-Time Auditing and Proof of Violation for Cloud Storage Systems	2016	Gwan-Hwan Hwang, Hung-Fu Chen	2	C		English
73	Enabling public and privacy-preserving auditability for cloud storage	2016	Hong-Chun Jiang, Chao-Sheng Feng, Ding Yuan	3	C		English
74	Fault tolerant public auditing system in cloud environment	2016	Anusha Koteppa Udagatti, N. R. Sunitha	2	C		English
75	Information Flow Audit for PaaS Clouds	2016	Thomas F. J.-M. Pasquier, Jatinder Singh, Jean Bacon, David Eyers	4	C	I (UK, New Zealand)	English
76	Privacy-preserving public auditing for educational multimedia data in cloud computing	2016	Daeyeong Kim, Hyunsoo Kwon, Changhee Hahn, Junbeom Hur	4	C		English
77	Public integrity auditing for dynamic regenerating code based cloud storage	2016	Kai He, Chuanhe Huang, Jiaoli Shi, Jinhai Wang	4	C		English
78	Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation	2016	Tao Jiang, Xiaofeng Chen, Jianfeng Ma	3	C		English
79	Reputation Audit in Multi-cloud Storage through Integrity Verification and Data Dynamics	2016	Xin Tang, Yining Qi, Yongfeng Huang	3	C		English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
68	C	IEEE	2nd International Conference on Electrical and Information Technologies lCEIT	0	0	13	Cloud storage, data tracking location, cloud refunding
69	C	IEEE	International Computer Symposium (ICS)	1	1	32	Cloud storage, Public auditing, Dynamic update operation
70	C	IEEE	International Conference on Cloud Computing in Emerging Markets	0	0	0	Cloud computing, Standards, Databases, Industries, Libraries
71	C	IEEE	International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)	0	1	15	Cloud storage, public audit, Data integrity, Third Party Auditor (TPA), Data privacy preserving
72	C	IEEE	9th International Conference on Cloud Computing	1	2	19	Cloud storage, cloud security, nonrepudiation, real-time auditing, proof of violation, service-level agreement
73	C	IEEE	International Conference on Machine Learning and Cybernetics (ICMLC)	0	0	19	Data storage, Preserve privacy, Public audit, Cloud computing
74	C	IEEE	2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)	0	0	11	Cloud Storage, Regenerating Code, Public Audit, Proxy
75	C	IEEE	International Conference on Cloud Engineering	6	12	62	Security, Context, Cloud computing, Metadata, Monitoring, Kernel, Databases
76	J	Springer	Multimedia Tools & Application	4	8	20	Privacy preserving auditing, Fully dynamic auditing, Cloud computing, Homomorphic hash, Educational multimedia
77	C	IEEE	Symposium on Computers and Communication (ISCC)	0	0	24	Data Integrity, Data Availability, Public Auditing, Data Dynamics
78	J	IEEE	TRANSACTIONS ON COMPUTERS	14	57	47	Public integrity auditing, dynamic data, victor commitment, group signature, cloud computing
79	C	IEEE	Conference Publication: 9th International Conference on Cloud Computing	0	2	15	Cloud storage, reputation, audit, MHT

Count	Researched Subject	Research Challenge	Research Approach	Proposition
68	Remote data integrity checking.	Attackers can hack the cloud information sometimes even though a data integrity checking protocol was installed.	Modelling	Proposition of an unused successive cloud auditing technique providing uninterrupted certificates to the user, verifying the data with help of fresh data integrity checking protocol.
69	Third Party Authenticator working in behalf of the cloud user.	Threat of security of sensitive outsourced data.	Modelling	Two schemes - Public Auditing in which homomorphic linear authenticator with random masking is used for auditing process and secondly Threshold Cryptography in which Capability List is used to ensure the data access control.
70	Integrity checking of remotely stored data to assure data storage security.	High computation time, little dynamic operation possible in existing models.	Modelling	A RSA based storage security system providing identification of misbehaving server with maximum probability detection, redducing computing time and support of dynamic operation.
71	Tracing information flows within Cloud infrastructur.	To tackle issues of data management a specified policy to control and track data is needed.	Modelling	Based on CamFlow Control Architecture an extended version providing dada-centric audit logs using standard graph processing tools is presented.
72	Data integrity verification.	Need of blockless verification, verifying correctness of data without having any knowledge of the data.	Modelling	Privacy preserving auditing model leading to less communication overhead.
73	Using IT auditing to secure Cloud Computing.	Security, Privacy, regulation and compliance concerns.	Modelling	General framework using checklists by following data flow and ist life cycle.
74	Provision of network security and infrastructure and service quality.	Users demand forsecurity and quality have to be checked mutually with provider's demand for information about clients' activities and applications running.	Modelling	Interactive framework that keeps track of different service modules from both end using message passing and roll back modules.
75	Security and privacy in Cloud Computing.	Lack of near-real time audit schemes, providing timely evaluation results and rapid response.	Discussion	Discussion of risks and Aanalysis of existing Cloud auditing approaches depicted with a case study.
76	Revising the dynamic auditing protocol to ensure the integrity of outsourced data.	The dynamic auditing protocol can have security flaws when an active adversary is involved in the cloud environment who can arbitrarily modify the the cloud data and produce a valid auditing proof to pass the audit verification.	Revision	Suggested solution to remedy this weakness without losing any features of the original protocol.
77	Auditing shared data across multiple users.	Difficulty of preserving personal privacy and confidential information during the auditing process.	Modelling	Proposition of a novel public auditing scheme, preserving privacy using signatures to enable the verification of data integrity.
78	Performance prediction for computationintensive applications.	Cloud users don#t have the knowledge to detect SLA disruption.	Modelling	Proposition of a performance prediction model, which can accurately predict the time cost of user applications on cloud.
79	Movement towards multi-clouds.	Traceability is a major issue in public auditing shared data done by exploiting Aggregate Signature Scheme.	Modelling	A Multi-clouds Database Model (MCDB) which is based on Multi-clouds service providers is used instead of single provider.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
80	Improving data storage security in cloud environment using public auditing and threshold cryptography scheme	2016	Reshma Suryawanshi, Santosh Shelke	2	C		English
81	Secure cloud auditing over encrypted data	2016	Sarah Shaikh, Deepali Vora	2	C		English
82	Efficient privacy preserving integrity checking model for cloud data storage security	2017	T. Subha, S. Jayashri	2	C		English
83	A differential game-theoretic model of auditing for data storage in cloud computing	2017	Zhi Li, Yanzhu Liu	2	C		English
84	Context-Aware Verifiable Cloud Computing	2017	Zheng Yan, Xixun Yu, Wenxiu Ding	3	C		English
85	Privacy preserving data auditing protocol for secure storage in mobile cloud computing	2017	M. Suguna, S. Mercy Shalinie	2	C		English
86	Public key based third party auditing system using random masking and bilinear total signature for privacy in public cloud environment	2017	J. Raja, M. Ramakrishnan	2	C		English
87	A survey on integrity verification and data auditing schemes for data verification in remote cloud servers	2017	R. Muthuram, G. Kousalya	2	C		English
88	An Efficient Public Auditing Protocol With Novel Dynamic Structure for Cloud Data	2017	Jian Shen, Jun Shen, Xiaofeng Chen, Xinyi Huang, Willy Susilo	5	C	I (China, Australia)	English
89	gAUDIT: A group communication-capable request-response middleware for auditing clouds	2017	Matthias Flittner, Alexander Weigel, Martina Zitterbart	3	C		English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
80	C	IEEE	International Conference on Computing Communication Control and automation (ICCUBEA)	1	2	16	Cloud computing, Cryptography, Servers, Access control, Protocols, Data privacy
81	C	IEEE	International Conference on Communication and Electronics Systems (ICCES)	0	0	11	Cloud computing, ElGamal algorithm, Public Auditing, SHA-256, TPA
82	C	IEEE	8th International Conference on Computational Intelligence and Networks	0	4	17	Auditing, cloud storage, data, integrity, privacy preserving, TTPA, Security
83	J	Inderscience	International Journal of Computational Science and Engineering	0	0	24	Differential game, cloud auditing, feedback Nash equilibrium, cloud security, data integrity checking
84	J	IEEE	IEEE Access	5	14	41	Cloud computing, full homomorphic encryption, privacy protection, verifiable cloud computing
85	C	IEEE	International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)	0	0	16	Mobile Cloud Computing, Auditing, Data Integrity, Bilinear Pairing, Merkle Hash Tree
86	C	IEEE	International Conference on Intelligent Computing and Control Systems	0	0	23	Cloud computing, third part Authentication, secure data storage, Data privarcy preservation, Bilinear aggregation
87	J	Inderscience	Electronic Government, an International Journal	0	0	/	Data storage auditing, cloud computing, integrity, privacy preserving, dynamic auditing
88	J	IEEE	TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY	7	40	44	Auditing protocol, cloud storage, dynamic databases, batch auditing
89	C	IEEE	International Conference on Networked Systems (NetSys)	0	0	22	Cloud computing, Monitoring, Unicast, Virtual machining, Reliability engineering

Count	Researched Subject	Research Challenge	Research Approach	Proposition
80	Adoption of cloud storage service by distance learning systems.	Challenging security issues in terms of data confidentiality and integrity.	Modelling	Public auditing protocol for educational multimedia data outsourced in the cloud storage using random values and homomorphic hash function.
81	Auditing data integrity in regenerating-code-based Cloud Storage.	So far only usable in private ausiting which comes with great online burden for the Cloud user.	Modelling	Proposition of a privacy-preserving public auditing scheme for regenerating-code-based Clouds using a novel homomorphic authenticator.
82	Authenticator-based efficient data integrity verification.	Efficiency and security in data integrity verification.	Metaanalysis	Analysis of main aspects, problems, research motivation, methodologies and achievements and a blueprint for future developement.
83	Securing intactness of data stored in clouds.	Conventional integrity mechanisms such as digital signature are not suitable.	Modelling	Proposition of auditing schme, using a Third party auditor allowing multiple times verification and reducing overhead.
84	Using regenerating codes to check for data integrity in cloud storaging.	Existing schemes only support static data limiting data availability and dynamic data operationandand have high auditing costs.	Modelling	Proposition of an adapted auditing schme for regenerating code based cloud computing using corrupted server localization and updated matrix and index mechanisms.
85	Auditing new collaborative cloud platforms.	Existing schemes are not secure against the collusion of Cloud Storage Server and revoked group users.	Modelling	Design of an efficient and reliable audit scheme including group data encryprion and decryption and securing user revocation.
86	Evaluation of reliability in multi-cloud storages.	Previously used integrity audits have limitations.	Modelling and Simulation	Proposition of a new reputation audit scheme, which in comparison to previous models is a pre-audit model and refelcts the historical quality of data.
87	Audit schemes to assure data intergrity, security, privacy and availability on cloud servers.	Data owner loose physical control over their data and need assurance of data intergrity, security, privacy and availability on cloud servers.	Modelling	Proposition of a new audit schme based on integrity verification strategy using a public key cryptographic algorithm.
88	Standards, policies and controls to to protect and safeguard systems and data.	New risks and opportunities for security exploits.	Discussion	Analysis of benefits, risks and mitigation control and recommondation for the mitigation process.
89	Verification of data integrity.	Former public audit schemes claims high computation from the auditor, which might become a burden.	Modelling	Proposition of a new public audit scheme with public verifiability and self-certified signature scheme in order to reduce computation effort.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
90	Identity-Based Data Outsourcing With Comprehensive Auditing in Clouds	2017	Yujue Wang, Qianhong Wu, Bo Qin, Wenchang Shi, Robert H. Deng, Jiankun Hu	6	C		English
91	Improving cloud security by enhancing remote data integrity checking algorithm	2017	S. Suganya, P. M Durai Raj Vincent	2	C		English
92	Mutual auditing framework for service level security auditing in cloud	2017	Soumitra Sasmal, Indrajit Pan	2	C		English
93	Third Party Auditing for Service Assurance in Cloud Computing	2017	Yanru Zhang, Xiang-Yang Li, H. Zhu	3	C	I (China, USA/South Korea)	English
94	Strategies to Improve Auditing Performance and Soundness for Cloud Computation	2018	Shin-Jia Hwang, Tsung-Lin Li	2	C		English
95	Secure Public Auditing Using Batch Processing for Cloud Data Storage	2018	G. L. Prakash, Manish Prateek, Inder Singh	3	C		English
96	Certificateless Public Auditing Scheme for Cloud-Assisted Wireless Body Area Networks	2018	Debiao He, Sherali Zeadally, Libing Wu	3	C	I (China, USA)	English
97	User-Level Runtime Security Auditing for the Cloud	2018	Suryadipta Majumdar, Taous Madi, Yushun Wang, Yosr Jarraya, Makan Pourzandi, Lingyu Wang, Mourad Debbabi	7	C		English
98	Privacy Preserving and Dynamic Audit Service for Secure Cloud Storage	2018	Jaaruti Patil , Sangita Chaudhari	2	C		English
99	Design of the Security Mechanism for a BPO Cloud Computing Platform	2018	Huaihai Hui, Des McLernon, Ali Zaidi	3	C		Englsih

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
90	J	IEEE	Transactions on Information Forensics and Security	5	37	34	Cloud storage, data outsourcing, proof of storage, remote integrity proof, public auditing
91	C	IEEE	Innovations in Power and Advanced Computing Technologies (i-PACT)	0	0	15	Cloud computing, Protocols, Organizations, Servers, Bandwidth
92	C	IEEE	3rd International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)	0	0	14	Audit policy, client-server, cloud computing, roll back mechanism, service auditing
93	C	IEEE	GLOBECOM 2017 - 2017 IEEE Global Communications Conference	0	2	20	Cloud computing, Contracts, Data privacy, Computer science, Data processing
94	C	Springer	International Conference on Security with Intelligent Computing and Big-data Services	0	0	14	Merkle hash trees, Cloud auditing, Cloud computing, Cloud storage, Digital signature schemes
95	C	Springer	1st International Conference on Smart System, Innovations and Computing	0	0	13	Security, Authenticator, Public auditing, Integrity, Storage as a service
96	J	IEEE	SYSTEMS JOURNAL	6	24	31	Auditing, cloud computing, protocol, security, wireless body area networks (WBANs)
97	J	IEEE	Transactions on Information Forensics and Security	0	2	59	Cloud security, security auditing, compliance verification, runtime verification, user-level security, OpenStack
98	C	IEEE	International Conference on Smart City and Emerging Technology (ICSCET)	/	0	14	Cloud Storage, Third Party Auditor, Public Auditing, Privacy Preserving, Integrity, Data Dynamic, Batch Auditing
99	C	IEEE	IEEE International Conference on Software Engineering and Service Sciences (ICSESS)	/	0	7	Security Meohanism.Claud Computing;BPO

Count	Researched Subject	Research Challenge	Research Approach	Proposition
90	Protecting security and privacy in the cloud.	Simultaneously supporting privacy and and auditing is problematic.	Discussion	Discussion of guiding principles, fundamental concepts and and threat models for current cloud computing systems and proposition of an respective infrastructure.
91	Revising Wie et al.'s cloud computing auditing scheme.	The assumtion that the cheating adversary always gives the random response for the auditing challenges is impractical.	Modelling	The off-line easy-auditor improving strategy, the function-based improving strategy, and mixed strategy are proposed.
92	Verifiable computing techniques.	Because of information asymmetry the correctness and completeness of data processing, computation and mining becomes an issue.	Discussion	A trusted third party auditor is used to gain trust in the cloud and combined with a contract theoretical penalty scheme.
93	Authentication of public verification.	A third party auditor can act act in self interest damaging and cause internal threats.	Discussion	Developement of an auditing method to ensure the integrity of Third Party Auditors to reduce the possibility of insider threats.
94	Cloud Auditing.	Audit mechanisms have to deliver quick results, analysis and response.	Examination	Online mashine learning algorithms can be used to provide audit data and might be emloyed in distributed computing environment.
95	Using Cloud Computing in the Critical Infrastructure Sector demands for additional measures to increase trust and accountability.	The CI Sector is characterized by additional strict regulatory constraints leading to technical means.	Discussion	Presentation of mechanisms to verify the adherence of cloud technologies to CI policies without compromising the providers confidentiality.
96	Runtime security auditing to increase trust in Cloud provider's compliance with security properties.	Existing runtime auditing techniques do not offer a practical response time to verify a wide-range of user-level security properties.	Modelling	Proposition of runtime security auditing framework including common access control and authentication mechanisms.
97	Online auditing as an important tool for national governance.	Data Stream processing remains a problem in online auditing.	Modelling	Proposition of a hierarchical online audit framework incorporating effiecient virtual resource scheduling, composition strategy and dynamic resource allocation showing improvement in reliabiity and availability.
98	Validation of data stored in the cloud using a Third Party Auditor (TPA).	Developing audit scheme holding the abilities of privacy preserving, public auditing, data integrity.	Modelling	New privacy preserving and dynamic public audit service utilizing various signatures and Merkle Hash Tree enabling batch auditing and dynamic data operation.
99	Deploying a rigid authentication and access control model for IoT Security.	New connected devices (IoT) have created a new dimension of se-curity challenges.	Modelling/ Framework	Novel light-weight authentication and authorization framework suitable for distributed IoT environment using Elliptical Curve Cryptography (ECC) and Message Queuing Telemetry Transport (MQTT).

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
100	Selection of Technological Innovation for Service-Orientated Enterprises	2018	Yang Yang, Lin Guo, Zhuling Zhong, Mu Zhang	4	C	I (China, Australia)	English
101	Cybersecurity Tools for IS Auditing	2018	Osamah M. Al-Matari , Iman M.A. Helal , Sherif A. Mazen , Sherif Elhennawy	4	C		English
102	Comparative Study On Trustee Of Third Party Auditor To Provide Integrity And Security In Cloud Computing	2018	K. Shirisha Reddy, M. Balaraju	2	C		English
103	Confidentiality Preserving Auditing for Cloud Computing Environment	2018	Suneeta Mohanty, Prasant Kumar Pattnaik, Raghvendra Kumar	3	C		English
104	Authorized identity-based public cloud storage auditing scheme with hierarchical structure for large-scale user groups	2018	Yue Zhang, Hanlin Zhang, Rong Hao, Jia Yu	4	C		English
105	Decentralized and Smart Public Auditing for Cloud Storage	2018	Haiyang Yu, Zhen Yang	2	C		English
106	CSBAuditor: Proactive Security Risk Analysis for Cloud Storage Broker Systems	2018	Kennedy A. Torkura, Muhammad I.H. Sukmana , Tim Strauss, Hendrik Graupner, Feng Cheng , Christoph Meinel	6	C		English
107	A Novel Third Party Integrity Checker (TPIC) based Data Auditing for Security of the Dynamic Streaming Client Data in a Cloud Infrastructure	2018	Krishna Prasad Rao, R.P. Puneeth, Shashank Shetty	3	C		English
108	Using Intel SGX to Enforce Auditing of Running Software in Insecure Environments	2018	L. Pereira, L. Ortiz , D. Rossi, M. Rosa, K. Fonseca, C. Prado, L. Rust, A. Britto, R. Riella	9	C		English
109	Data integrity verification based on hybrid cloud	2018	Yu Jin, Xin Gong, Peng Li, Heng He	4	C		English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
100	J	MDPI	Sustainability	/	3	40	Technological innovation; service-orientated enterprises; service innovation; sustainable competitive; DEMATEL method; ANP method; mVIKOR method
101	C	IEEE	2018 Sixth International Conference on Enterprise Systems (ES)	/	0	41	Cybersecurity, Penetration Testing, Vulnerability Assessments, Forensics
102	C	Elsevier	International Conference on Processing of Materials, Minerals and Energy	/	3	8	Cloud Storage Provider, Third Party Audit, Information Technology Audit
103	C	IEEE	2018 International Conference on Research in Intelligent and Computing in Engineering (RICE)	/	0	29	Auditing, Cloud User, Cloud Service Provider(CSP), Third Party Auditor(TP A)
104	J	IEEE	China Communications	/	0	26	Cloud storage, cloud storage auditing, large-scale users, third party auditor
105	C	IEEE	2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)	/	1	16	Blockchain, cloud auditing, data integrity checking, smart contract
106	C	IEEE	2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)	/	2	39	Cloud-Security, Cloud Audit, Security Metrics, Security Risk Assessment, Secure Configuration
107	C	IEEE	2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)	/	0	20	Cloud Auditing, Cloud Computing, Cryptography, Data Auditing, Data Integrity, Data Security
108	C	IEEE	2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)	/	0	11	Sgx, cloud-base toolchain, software auditing, software measurement, smart-metering
109	C	IEEE	13th IEEE Conference on Industrial Electronics and Applications (ICIEA)	/	0	18	Cloud Storage, Provable Data Possession, Private Cloud, Batch Auditing

Count	Researched Subject	Research Challenge	Research Approach	Proposition
100	Security of Cloud Computing Platforms (CCP), Business Process Outsourcing Cloud Computing Platform (BPO-CCP) in particular.	Virtualization security, cloud data security, access control, user authentication and authorization, and cloud computing auditing within BPO-CCP.	Modelling	Analyzing, modelling and application of an Security Mechanism for the BPO CCPs.
101	Risks of rapidly growing cloud computing migration.	Risks and concerns of outsourcing IT functions to third-party providers of BPO services.	Modelling	Modified Boneh-Lynn-Shachame Dynamic Auditing (MBLSSDA) algorithm executing batch audit processes enabling Third Party Auditing (incorporating homomorphic authenticator, random marking).
102	Auditing unconstrained storage cloud.	Data corruption in the cloud.	Modelling	Secure storage (batch) auditing supporting efficient key updates which can be used in cognitive industrial IoT environment.
103	Technological innovation startegy for service-orientated enterprises.	Appropriate and effective decision making for service-oriented enterprises.	Frameworke/Scheme	Evaluation criteria system for selecting a technological innovation scheme based on the four-dimensional model of service innovation and useing the hybrid multi-criteria decision model (MCDM), identifying Beacons technology as the best service innovation scheme.
104	User behaviour Auditing.	Internal threats of Cloud Computing.	Modelling & Evaluation	Information extraction method extracting audit information by remote desctop protocol via deep learning based scene text reading.
105	Public Data Auditing.	Customers may not fully trust that cloud service providers meet their legal expectations for data security.	Modelling & Review	Building an architecture of public data auditing whilst reviewing existing methods and discussing trends.
106	Storing data to cloud server promotes integrity auditing and data deduplication research topics.	Recent schemes did not support aggregating authentication tags of different users leading to heavy computation costs.	Modelling	Efficient public auditing scheme with secure deduplication using the idea of aggregate signature, supporting batch auditing.
107	Cybersecurity as an enterprise-wide issue requiring protection from malicious attacks to protect information assets.	Information systems auditing is becoming more difficult due to the rapidly developing technological threats.	Comparative Study	Comparative study of the capabilities of most of the available automated cybersecurity auditing tools for frontend cloud computing.
108	Cloud services for storrageing between user, provider and TPA.	Cloud services for storaging come with security issues and conflicts between the client and service provider.	comparative analysis	Reliable data storage providing computing resources in the form of service rather than a product and utilities.
109	Data storage in Cloud Computing Environment.	Maintenance of data privacy, integrity, confidentiality and data availability.	Modelling	Confidentiality preserving Auditing scheme to check the integrity of user's data along with TPA authentication and non-repudiation.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
110	Comments on "SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors"	2018	Feng Wang, Li Xu, Wei Gao	3	C		English
111	Bit-Reversal Encryption Towards Secured Storage of Digital Image in Cloud Deployment	2018	Soumitra Sasmal, Indrajit Pan	2	C		English
112	CASTLE: Enhancing the Utility of Inequality Query Auditing Without Denial Threats	2018	Jiahui Hou, Xiang-Yang Li, Taeho Jung, Yu Wang, Daren Zheng	5	C	I (China, US)	English
113	A New Fog-Cloud Storage Framework with Transparency and Auditability	2018	Yeojin Kim, Donghyun Kim, Junggab Son , Wei Wang, Young Tae Noh	5	C	I (China, US; South Korea)	English
114	Privacy-Preserving and Unforgeable Searchable Encrypted Audit Logs for Cloud Storage	2018	Weiwei Zhao, Li Qiang, Huanying Zou, Aixin Zhang, Jianhua Li	5	C		English
115	Intelligent use of fog devices in edge-cloud paradigm to assist in E-polling	2018	Adnan Khalid, Muhammad Shahbaz , Imran Ahmed Khan	3	C		English
116	Towards an Integrative Theoretical Model For Examining IT Governance Audits	2018	Alexander Ekow Asmah, Michael Kyobe	2	C		English
117	Managed Containers: A Framework for Resilient Containerized Mission Critical Systems	2018	Xavier Merino Aguilera, Carlos Otero, Matthew Ridley, David Elliott	4	C		English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
110	J	IEEE	IEEE Transactions on Computational Social Systems	/	1	10	Certificateless public key cryptography, cloud storage, data integrity auditing, provable data possession (PDP), storing one block attack
111	C	Springer	International Conference on Advanced Computational and Communication Paradigms (ICACCP)	/	0	12	Bit-reversal encryption, Cloud auditing, Cloud computing, Digital image, Privacy preservation
112	J	IEEE	IEEE Transactions on Information Forensics and Security	/	2	28	Query auditing, privacy-preserving query, denial threats
113	C	IEEE	2018 IEEE International Conference on Communications (ICC)	/	1	22	Cloud computing, Edge computing, Memory, Computer architecture, Security, Electronic mail, Computer science
114	C	IEEE	5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)	/	0	8	Searchable encryption, audit log, privacy, unforgeability
115	J	Wiley	Concurrency and Computation - Practice and Experience	/	1	16	Cloud computing, computer networks, data communication, distributed computing, edge computing, E-electoral system, fog computing, grid computing
116	C	ACM	11th International Conference on Theory and Practice of Electronic Governance	/	0	35	IT governance, IT auditing, COBIT 5, Governance Mechanisms
117	C	IEEE	11th International Conference on Cloud Computing (CLOUD)	/	1	14	Linux containers, availability, moving target defense, cyber survivability, virtualization

Count	Researched Subject	Research Challenge	Research Approach	Proposition
110	Identity-based public cloud storage auditing schemes with help of Private Key Generator (PKG) and TPA.	Undesirable for large-scale users since the PKG and the TPA might not be able to afford the heavy workload.	Modelling	Authorized identity-based public cloud storage auditing scheme using a hierarchical Private Key Generator structure for large-scale user groups.
111	Auditing to provide integrity of outsourced data in storaged data in the cloud.	centralized auditing framework is vulnerable and as a third party, the auditor cannot be fully trusted	Modelling	Decentralized and smart public auditing scheme eliminating the involvement of the TPA and improving the reliability by using protocol for automatic data integrity checking in a decentralized environment based on a smart contract.
112	Increasing volume of data in the cloud and data duplication.	Cloud server stores only a unique copy of outsourced data and the corruption or missing of the unique copy may bring immeasurable loss.		confidentiality-preserving deduplication cloud storage with public cloud auditing (CPDA) achieving secure file deduplication on encrypted file, realizing secure authentication tag deduplication using the convergent encryption and random masking techniques.
113	Cloud storage as means for the storage and management of images requires real-time integrity audit.	Existing schemes do not take the characteristics of cloud images into account and thus take enormous computations, communications, and storage to generate, transfer, and store authentication data.	Modelling	Audit scheme specific to cloud images with fair arbitration support based on adaptive reversible watermarking algorithm which provides a fixed embedding capacity for images to embed authentication and adopting Diffie-Hellman key exchange scheme.
114	Cloud Storage Brokers (CSB) provide seamless and concurrent access to multiple Cloud Storage Services (CSS) while abstracting cloud complexities from end-user.	Several security challenges including enlarged attack surfaces, malicious insider threats, security complexities due to integration of disparate components and API interoperability issues.	Modelling	Novel cloud security system that continuously audits CSB resources, to detect malicious activities and unauthorized changes using continuous snapshotting mechanism, chaos engineering, security metrics for risk analysis.
115	outsourcing of streaming client data in the cloud infrastructure, many store the mission critical data into the data centre's various remote locations to reduce data storage and management cost.	New security challenges often arise causing threat to the data stored in the cloud (eg data integrity).	Modelling	Third Party Integrity Checker (TPIC) based data auditing for security of the dynamic streaming client data, containing digital signatures generated by the Hash function allowing to trust the third party checker by not storing the actual data and allowing checking of periodically changing dynamic data.
116	Auditing of Running Software in Insecure Environments.	Insecure environments	Modelling	Audit system using Intel SGX processor, cloud-based toolchain, SGX-based binary loader, Linux kernel.
117	Cloud storage as one of the main means of Cloud computing.	Public cloud server is not a trusted third party, and the security of data is a cause for concern. Private auditing brings a lot of computing burden to the user.	Modelling	Improving Yan's scheme, enabling batch auditing, developing a new data model for the integrity of remote data validation also introducing a private cloud.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
118	A Secure Connectivity Model for Internet of Things Analytics Service Delivery	2018	Hussain Al-Aqrabi, Richard Hill	2	C		English
119	A Third Party Audit Mechanism for Cloud Based Storage Using File Versioning and Change Tracking Mechanism	2018	Falguni M. Modi, Megha R. Desai, Dishant R. Soni	3	C		English
120	Secure Cloud Storage Based on RLWE Problem	2019	Yang Yang, Qing Huang, Fei Chen	3	C		English
121	Efficient public integrity auditing with secure deduplication in cloud computing	2019	Huixia Huo, Tao Jiang, Shichong Tan, Xiaoling Tao	4	C		English
122	ECC based inter-device authentication and authorization scheme using MQTT for IoT networks	2019	Ankur Lohachab	1			English
123	Public Auditing for Trusted Cloud Storage Services	2019	Hui Tian, Yuxiang Chen, Hong Jiang, Yongfeng Huang, Fulin Nan, Yonghong Chen	6	C	I (China, US)	English
124	CPDA: A Confidentiality-Preserving Deduplication Cloud Storage With Public Cloud Auditing	2019	Jiaojiao Wu, Yanping Li, Tianyin Wang, Yong Ding	4	C		English
125	Efficient Real-Time Integrity Auditing With Privacy-Preserving Arbitration for Images in Cloud Storage System	2019	Xin Tang, Yongfeng Huang, Chin-Chen Chang, Linna Zhou	4	C	I (China, Taiwan)	English
126	Efficient Privacy-Preserving Certificateless Provable Data Possession Scheme for Cloud Storage	2019	Yang Ming, Wenchang Shi	2	C		English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
118	C	IEEE	IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)	/	0	23	Cloud computing, distributed systems, security, authentication, trust, multiparty, Internet of Things
119	C	IEEE	2018 International Conference on Inventive Research in Computing Applications (ICIRCA)	/	0	7	Cloud computing, Third Party Auditor, Security, Data Integrity
120	J	IEEE	IEEE Access	/	2	29	Integrity auditing, lattice cryptography, RLWE, secure cloud storage
121	J	Inderscience	International Journal of Embedded Systems	/	0	na	Efficient integrity auditing, secure deduplication, aggregate signature, batch auditing, cloud computing
122	J	Elsevier	Journal of Information Security and Applications	/	6	40	Iot, Authentication, Authorization, ECC, MQTT,Cloud, Fog
123	J	IEEE	IEEE Security & Privacy	/	2	29	Cloud computing, Digital forensics, Security, Servers, Data privacy, Outsourcing, Data processing
124	J	IEEE	IEEE Access	/	0	30	Cloud storage, secure deduplication, public cloud auditing, batch verification
125	J	IEEE	IEEE Access	/	0	36	Real-time auditing, fair arbitration, privacy-preserving, reversible watermarking, Diffie-Hellman key exchange
126	J	IEEE	IEEE Access	/	0	34	Cloud storage, privacy preserving, provable data possession, certificateless cryptography

Count	Researched Subject	Research Challenge	Research Approach	Proposition
118	Ensuring the integrity of the outsourced data in the rapid development of cloud storage and quantum computing.	Heavy cryptographic operations making the efficiency of existing schemes low and extensibility poor.	Modelling	Designing secure cloud storage (SCS) protocols based on ring learning utilizing vector variables to generate data block tags supporting data dynamics and batch auditing.
119	Protect the integrity of the data stored in the cloud.	Integrity of the data stored in the cloud.	Commentary & Modelling	Improved Zhang et al.'s proposed certificateless data integrity auditing scheme.
120	Cloud storage.	File owner is always concernd about data security like privacy and unauthorized access to third party and wants to ensure the integrity data during communication process.	Modelling	Framework based on third party auditor which checks the integrity and correctness of data during audit process using design custom hash.
121	Majority of digital records are transferred to cloud-based storage.	Creating a concern for data security.	Modelling	Bit-reversal encryption mechanism for privacy preservation of digital image data (different types) deployed on cloud simple and easy to implement.
122	Query auditing problem in outsourcing scenario.	Difficulty of removing denial threats, or lack the analysis of utility.	Modelling	Inequality query auditing scheme that evaluates the risk of answering a query based on the query history and determines whether a newly arrived query should be answered correctly against a denial threat.
123	Fog-cloud storage overcoming the limits of central cloud storage.	It is not straightforward to directly apply an existing audit scheme for a cloud storage to a fog-cloud storage.	Modelling	New fog-cloud storage architecture achieving much higher throughput providing transparency. Providing a stronger audit scheme naturally coupled with the initial data upload process ot suffer from the replay attack.
124	Audit logs in icloud computing and cloud storage require to protect the confidentiality of data and the privacy of users.	Security properties, such as privacy-preserving, searchability, verifiability and unforgeability and computation load.	Modelling	Privacy-preserving and unforgeable searchable encrypted audit log scheme based on PEKS immune to the collusion tamper or fabrication conducted by server and user.
125	Provable data possession schemes ensuring that a cloud server provider proves to a third party auditor that it is truthfully storing data from the data owner.	Management issue of the certificates and the identity-based provable data possession scheme causes an inherent key escrow problem.	Modelling	Efficient privacy-preserving certificateless provable data possession scheme based on certificateless cryptography and elliptic curve cryptography being unforgeable against adaptive chosen message attacks.
126	Private clouds.	Data loss & breaches, service vulnerabilities, insufficient due diligence, identity, access and credential management, poor footprint tracking for threats & malicious insider attacks threatening network security.	Modelling	Secured Private-Cloud Computing System using advanced features of HTML, CSS, JAVASCRIPT, & JQUERY, PHP & MYSQL restricting access to cloud resources only to trusted members.

Count	Titel	Year	Authors	Number of Authors	Collaboration (C)	International (I) (Countries)	Language
127	A Secured Private-Cloud Computing System	2019	Modebola Olowu, Chika Yinka-Banjo, Sanjay Misra, Hector Florez	4	C	I (Colombia, Nigeria)	English
128	A Multi-layer Security Model for 5G-Enabled Industrial Internet of Things	2019	Hussain Al-Aqrabi, Anju P. Johnson, Richard Hill, Phil Lane, Lu Liu	5	C		English
129	Deep Learning Based Scene Text Reading for Cloud Audit Information Extraction	2019	Hezhong Pan, Chuanyi Liu, Shaoming Duan, Peiyi Han, Xinyi Zhang, Binxing Fang	6	C		
130	A Survey on Tracing for Default of Cloud Service	2019	Bo Li, Xiaojian Li , Wencan Tong, Hailan Wang, Jing Chen	5	C		English
131	A Modified Boneh-Lynn-Shacham Signing Dynamic Auditing In Cloud Computing	2020	Adnan Alrabea	1			English
132	Secure Storage Auditing with Efficient Key Updates for Cognitive Industrial IoT Environment	2020	Wenying Zheng, Chin-Feng Lai, Debiao He, Neeraj Kumar, Bing Chen	5	C	I (India, China, Taiwan)	English

Count	Journal (J)/ Conference (C)	Source 1 (Outlet)	Source 2 (Outlet title)	Citations (as of 2018)	Citation (as of June 2020)	Number of References	Keywords
127	C	Springer	International Conference on Applied Informatics	/	0	19	HTML (Hypertext Markup Language), (CSS) Cascading Style Sheet, JSON (JavaScript object Notation)
128	C	Springer	International Conference on Smart City and Informatization	/	2	29	Internet of Things, 5G, Security, Physical Unclonable Functions, Analytics
129	C	IEEE	Fourth International Conference on Data Science in Cyberspace (DSC)	/	0	45	Cloud audit, scene text reading, text detection, text recognition, synthetic data generation
130	C	IEEE	IEEE International Conference on Computation, Communication and Engineering (ICCCE)	/	0	18	Correlation, Cloud computing, Heuristic algorithms, Electric breakdown, Monitoring, Security, Diseases
131	J	Elsevier	Journal of King Saud University - Computer and Information Sciences	/	0	17	Cloud Computing, Auditing, Security, Multiple Batch, Cloud Security
132	J	IEEE	IEEE Transactions on Industrial Informatics	/	0	29	Cognitive computing, big data, industrial IoT, cloud computing, auditing

Count	Researched Subject	Research Challenge	Research Approach	Proposition
127	Latency issues in cloud networks.	Due to the vast geographical distribution of cloud networks and end user nodes, transmission of data provides problems of latency and delay that can cause major hazards in applications that require real-time processing.	Case Study	Analyzing mock E-poll held under the Election commission of Pakistan using the newly proposed Fog Computing Paradigm to allow fast processing of real-time data.
128	Enterprise Governance of IT (EGIT) for both public and private enterprises increases the requirement for regular audits.	Paucity of IT auditing studies focusing on EGIT.	Conceptual Modelling (gestalt theory)	Integrative theoretical framework for examining EGIT and conceptual model to guide further research.
129	Secure communications between Industrial Internet of Things (IIoT) devices that operate in 5G-enabled environments.	5G networks enable greater data throughput and lower latency, which presents new opportunities for the secure authentication of business transactions between IoT hardware.	Modelling	Flexible and secure model for IIoT components in 5G environments using the (NIST) seven layer model of CC and Physically Unclonable Function (PUF) hardware.
130	Protecting containerized mission critical systems mostly based on cloud-based images that need to be always-on-always-connected.	Unable to guarantee uncompromisable security and given that systems will inevitably be attacked, we must emphasize resiliency and mission survivability.	Modelling	Work-in-progress to create a framework for cloud-based container resiliency using Linux containers expanding upon the generic container model with additional layers that enhance security and increase auditability.
131	After default, tracing can provide evidence for the final determination of responsibility attribution dispute.	Existing results of tracing are difficult to directly apply to the tracing research of cloud services default.	Survey	Surveys the research status of tracing towards cloud service accountability mechanism.
132	IoT is fuelling innovation in the way individuals and even machines can interact to exchange knowledge eg analytics.	Combination of network connectivity and emerging distributed models of service orchestration is allowing the creation of new ways of measuring, monitoring and analysing performance.	Modelling	Model of connectivity that enables analytics services to be consumed across individual system components inspired by NISTseven layer CC model.