Advances in Dynamical Systems and Applications.
ISSN 0973-5321, Volume 16, Number 2, (2021) pp. 1883-1919

https://www.ripublication.com/adsa.htm

A Systematic Literature Review of Cloud Computing Cybersecurity

Hanane BENNASAR
Mohamed V University, Laboratory of ENSIAS Rabat, Morocco

Mohammad ESSAAIDI
Mohamed V University, Laboratory of ENSIAS Rabat, Morocco

Ahmed BENDAHMANE
Abdelmalek Essaadi University, Laboratory of ENS, Tetouan, Morocco

Jalel BEN-OTHMAN
Paris13 Villetaneuse University Paris, Laboratory of L2TI, Paris, France

ABSTRACT

Cloud Computing is a large-scale distributed computing system which has initially emerged from financial systems. Security is usually listed as the number one concern for cloud computing adoption. Cloud security issues persistently rank above cloud reliability, network issues, availability and worries about the cloud financial profit. This paper proposes a systematic literature review which aims to provide an up-to-date and a comprehensive overview of cyber- security issues in cloud computing. A systematic literature review analyzes the peer-reviewed research papers published and indexed by Science Direct, Springer, Google Scholar, Web of Science, IEEE Xplore, etc. With the following string terms: Cloud computing issues, cloud computing cyber- security, threats to cloud computing, cloud computing risks, cloud computing solutions, and cloud computing recommendations. This literature review is conducted based on the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) methodology, which is used to create a systematic, accurate, and reliable overview of the literature. This yielded 1134 papers out of which 87 ultimately met inclusion criteria and were reviewed. From the Systematic Literature Review, it was possible to overview and identify the state-of-the-art main cloud computing cyber-security threats and challenges.

Keywords: Cloud Computing, Threats, Cybersecurity, Systematic Literature Review.

1. INTRODUCTION

The proposed Systematic Literature Review (SLR) aims to explore Cloud Computing cyber-security threats, risks and concerns together with the proposed approaches and solutions proposed to tackle them. This SLR is also very valuable to identify suggestions and paths for future relevant research work. The new cloud computing pattern offers numerous new advantages in a powerfully changing business world. To keep up the opposition, organizations genuinely need to think about the appropriation of cloud arrangements. In any case, the redistributing of business procedures, administrations and sensitive data comes recently developed and slightly many security challenges than known from different solutions gave over the Internet. Cloud computing is a model for empowering helpful, on-request system access to a shared pool of configurable computing assets that can be quickly provisioned and discharged with negligible administration exertion [1]. Though there are several advantages for adopting Cloud Computing solutions, there are still many critical issues and concerns that need to be solved. Among the biggest and the most important concern in this regard is cyber-security [2]. This is partly because Cloud Computing is based on distributed computing systems "shared and accessed" through the internet and involves several stakeholders such as cloud end-user client and Cloud Service Provider (CSP).

It is an established fact among researchers and consultants that Cloud Computing provides competitive advantages while the security is still susceptible to attacks and other threats particularly regarding resource pooling and virtualization. Furthermore, the user's availability weakness was pointed out while suggesting improved data encryption as an ensuing solution.

As there are many controls and few security components in distributed computing that can guaranty cloud security and privacy [3], there is an increasing need for security and trust in business cloud applications. Therefore, there is a need for progressively efficient components that guarantee the rightness and correctness of returned results from cloud assets to enhance the computations dependability and trust.

Virtualization is a basic concept in cloud computing. This is based on asset sharing procedure while hiding the details of underlying equipment to build computing asset usage in a productive and scalable way.

The authors of [4] describe how Cloud selection requires an attention of several essential factors. Generally, the internet / web associates and moves information from and to a customer and the service provider. In this virtualized system there are significant security and privacy concerns, risks and threats.

The remainder of this paper is organized as follows. Section 2 presented an overview of cloud computing service adoption; Section 3 is dedicated to the presentation of the background. Section 4 presented the methodological approach utilized for the literature selection, the method applied for investigation, provides the mapping results and the aim of the SLR. Finally, Section 5 provides a conclusion and explores further research possibilities.

2. OVERVIEW

During the last few years, there has been a rapid and an increasing development and adoption of cloud computing systems, technologies, applications and services. This is owing mainly to many benefits this technology offers for businesses and organizations. However, Cyber-security is considered among the most important issues and concerns for widespread adoption of cloud computing. Among the major issues related with Cloud Computing security we can mention data security, intrusions attacks, confidentiality and data integrity. The paper aim is to classify the challenges, the different approaches and solutions proposed to address them and the open problems that need to be addressed. This article will help researchers in their cloud computing cyber-security searches.

The Adoption of cloud computing services implies that a large part of system, applications, network and data are under a third-party control. Every year, The Cloud Security Alliance (CSA) organized a panel of industry experts in order to present the Cloud Computing Top Threats:

- Data Breaches: A Security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so [6].
- Data Loss: An error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing [5].
- Account Hijacking: A type of identity theft in which the hacker uses the stolen account information to carry out malicious or unauthorized activity [6].
- Insecure APIs: Web and cloud services allow third-party access by exposing application programming interfaces, and many developers and customers do not
- Adequately secure the keys to the cloud and their data [7].
- Denial of Service: An attempt to make a machine or network resource unavailable to its intended users [8].
- Malicious Intruders: Insider malicious activity bypassing firewall and other security model [9].
- Abuse of cloud Services: Allows interloper to start stronger attacks due to unidentified signup, lack of justification, and service fraud [10].
- Insufficient Due Diligence: Organizations adopting the cloud without fully understanding the associated risks, they increase many operational, architectural and contractual issues over responsibility and transparency [11].
- Shared Technology Issues: Allows one user to hinder other users' services by compromising hypervisor [11].
- System Vulnerabilities: Bugs in programs that attackers use to infiltrate a system to steal data, to take a control of the system or disrupting service operations [12].
- Advanced persistent threats (APTs): APTs are a parasitical form of cyber-attack that penetrates systems to create a dependable balance in the IT infrastructure of target firms.

- Insufficient identity, credential, and access management: Bad actors masquerading as legitimate users, operators, or developers can read, modify, and delete data [13].
- According to our detailed research, we identified more potential threats to cloud computing:
- Lock-in: The inability of a user to move their programs or data away from a cloud computing danger (cloud computing service provider) [14].
- Loss of governance: While adopting Cloud benefits, the Cloud Customer essentially surrenders control to the Cloud supplier on various issues which may affect security (Cloud Socket, 2019).
- Isolation Failure: A cloud tenant can influence another's resources due to Multi-tenancy and shared resources [33].
- Compliance Risks: The application, certification and Cloud Service Provider process can make potential risks for the Postal Service, if the CSP cannot provide evidence of their own compliance with the pertinent requirements [15].
- Access Problem: Cloud computing systems suffer from a problem of access to the data view that data is stored in different locations in the world.
- Natural disaster: A risk to cloud computing availability [16].
- Confiscated Computer System: When by law enforcement authorities confiscate computer systems, the centralization of capacity and shared area of physical equipment uncover more danger of undesired information revelation to distributed computing clients [15] [16].
- Supply chain failure: A Cloud supplier can convey portions of its creation chain to outsiders, or even, as a feature of its administration, utilize other Cloud Providers. Subsequently, a potential for falling disappointments is created [16].

Figure 1, Figure 2 and Figure 3 present relative ordering of different threats important in the years 2010, 2012 and 2016 simultaneously. Figure 4 presents potential cloud computing threats identified through deep research. As it evident, year after year, new threats were identified while there are those that have been removed or changed, over time.

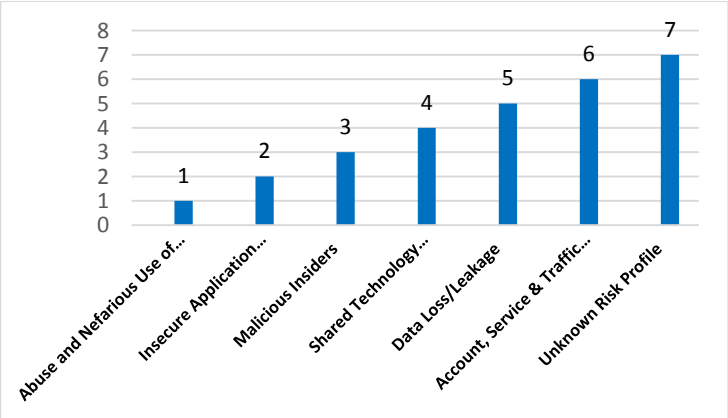

Figure 1: CSA Top Cloud Computing Threats, 2010

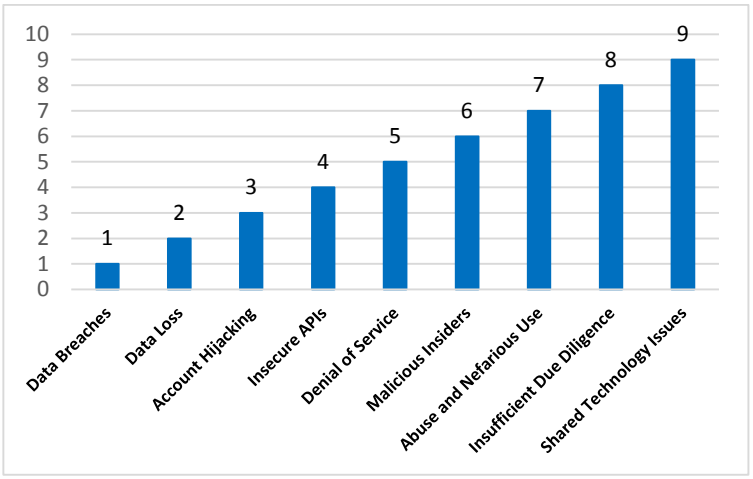

Figure 2: CSA Top Cloud Computing Threats, 2013

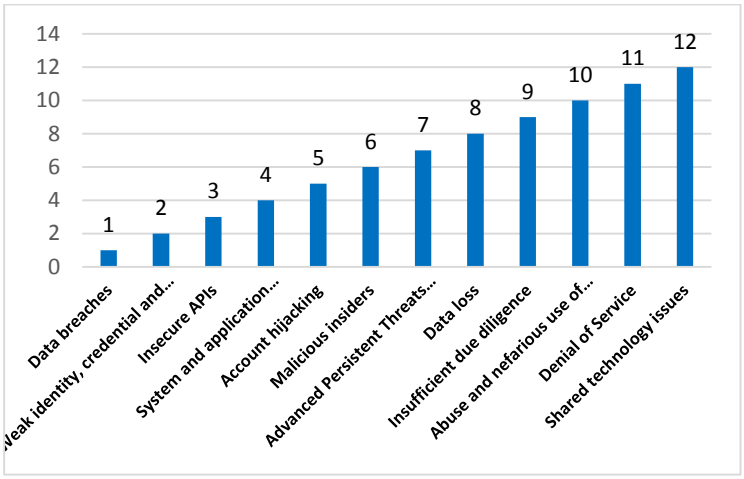

Figure 3: CSA Top Cloud Computing Threats, 2016

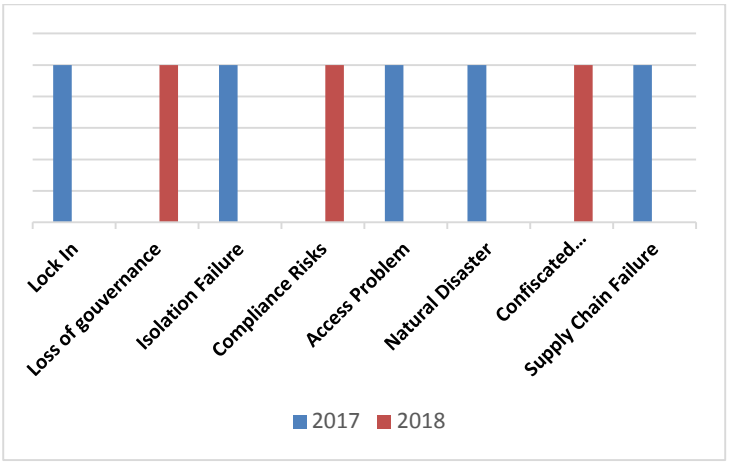

Figure 4: CSA Top Cloud Computing Threats,2017 & 2018

3. BACKGROUND (CLOUD COMPUTING SECURITY)

Researchers have addressed various parts of cloud security in their works, like cloud architectural components and associated attack vectors, cloud security issues and challenges, observed attacks, recognized dangers, proposed countermeasures, known vulnerabilities, etc.

Researchers [33] investigated Data security issues and solutions in distributed computing. Data security issues are broken down into four major categories, which are related to Confidentiality, Integrity and Availability (CIA), namely,

- Authentication and Access Control (AAC)
- Broken Authentication
- Session & Access
- Other Data Related Security Issues

Tao et. al., (Tao et al., 2012) developed a general structure for adequately homomorphic schemes of encryption. This structure guarantees full data confidentiality since computation tasks are completed on ciphertext while different methodologies are just ready to utilize plaintext. On the drawback, this structure battles with more slow execution contrasted with different components.

Fernandes et. al., [17] examined and arranged key cloud security themes, for example, attack, threats and vulnerabilities in late academic and industry publications. In addition, numerous showed cloud security issues concerning data, storage, framework, virtualization and access, they featured cybercrime as one all the more the present significant challenge. As cybercriminals stay aware of developing technologies, attacks become progressively modern since data put stored in public cloud are focuses with huge expected advantages. This situation is exasperated by the assorted variety of offered cloud arrangements, which are required to be streamlined sooner rather than later.

Ali et. al. [18] directed an itemized review of cloud computing security difficulties extended out by a concise diagram of versatile cloud figuring vulnerabilities. The security concerns were categorized into three major groups: challenges at communication level, challenges at engineering level and difficulties at authorities and legal dimensions. Accordingly, this paper features that cloud information security concerns resulting from the characteristic of multi-tenancy are central point hampering organizations of cloud computing adoption as was pointed out by [19] as well. These conclusions extend the research work done by [20].

G. Ramachandra et. al., [16] presented an overview on Security in Cloud Computing to understand the cloud components, security issues, risks, and solutions that may potentially alleviate the vulnerabilities in the cloud. Moreover, they indicated that there is a need for further research in systems development life cycle (SDLC) for cloud consumers to join different advancement and innovative development models and container systems, for example, Docker to improve security at an essential dimension.

M. Hawedi et. al., [15] propose a security architecture that offers flexible and effective security as a service paradigm for cloud tenants. The proposed security can be offered by outsiders to their occupants, or it may be utilized by the tenants to monitor their Virtual Machines (VMs).

4. METHODOLOGY AND CLASSIFICATION OF CLOUD COMPUTING SECURITY THREATS

This section gives a review of our methodological approach utilized for the literature selection, the method applied for investigation, provides the mapping results and the aim of the SLR.

This literature audit is led based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) approach (Moher et al., 2009) which is utilized to make an orderly,

exact, and reliable overview of the literature (Liberati et al., 2009). The process of gathering articles for examination is guided by a flow-chart that incorporates four phases, and the procedure for reporting a literature survey incorporates a 27-step checklist. PRISMA characterizes an efficient review as "a survey of a clearly formulated question that utilizes systematic and explicit techniques to distinguish, select, and basically assess pertinent research, also, to gather and break down information from the examinations that are incorporated into the review" (Liberati et al., 2009).

A literature search was led in the scientific databases such as Science Direct, Web of Science and Scopus, from 2009 to 2019, to define the peer-reviewed publications related to cloud computing cyber-security. The reference databases are used as archives of the principle scientific publications of effect and pertinence for the examined subject. Also, through manual research.

As the search procedure happens through indexing systems, a lot of characters (strings) that are to be looked up are characterized. For this set to be found in the query, sequence and completeness that is wanted, Boolean operators (AND, OR, NOT) are embedded. The Booleans are incorporated from computational algebra math and enable outcomes to be discovered that match the forced impediments and wanted by the keywords. To gather the applicable research papers, the characterized search keywords were: (“Cloud computing security issues” or “cloud computing security threats” or cloud computing security problems” or “cloud computing security risks”). Concerning this research, it was acknowledged that strings were a part of the papers’ titles, their keywords and abstracts. We excluded: case studies and thesis dissertations, comparison studies, books’ chapters, conferences’ reviews and editorials. The results of the search were imported to the citation manager Mendeley.

After applying the search strategies in the reported databases, 1085 potentially relevant articles were found, and 76 additional articles were searched manually from other sources. After the withdrawal of the duplicates, there were 115 papers that had their titles and abstracts analyzed. After this procedure, they left over 105 articles that were

read in their entirety, when the inclusion/exclusion criteria were applied. Then remaining 87 articles which were included in this review. The flowchart is presented in the Figure 5.

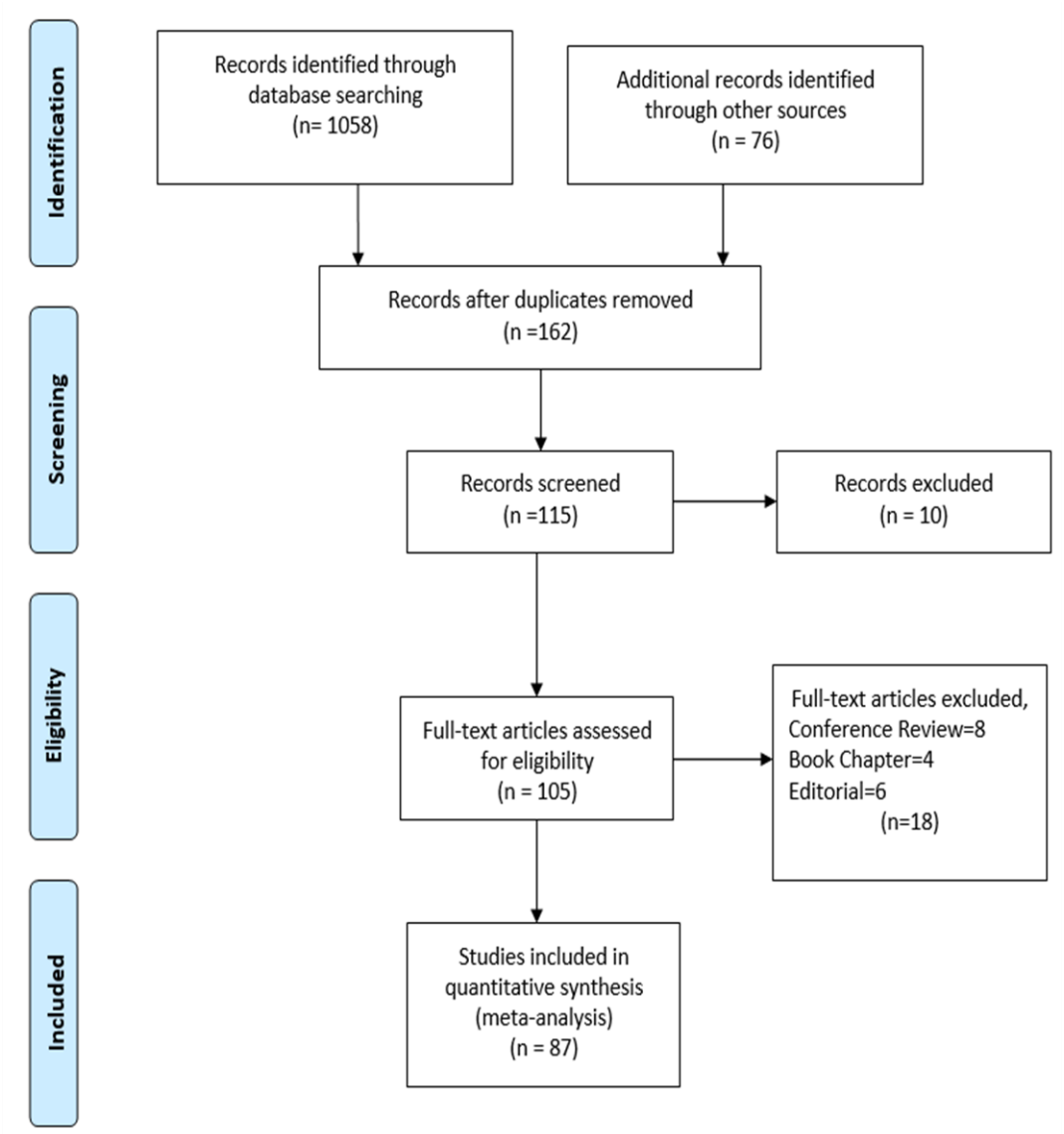

Figure 5: Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) flow diagram

Our main conclusions of the proposed systematic literature review are summarized in table 1 which are grouped by: Objectives, scope and results of the elaborated work; Year of publication; Country in which the research was conducted; Journal or conference where the paper was published; and finally, Inputs parameters for the model's evaluation.

Table 1: Summary of adherent articles

Reference	Objective/scope/Results	Year	Journal/conference	Country	Input Parameters
Wani et al. [27]	Providing performance comparison of seven popular symmetric algorithms: AES, DES, 3DES, Blowfish, RC4, IDEA, and TEA.	2019	Advances in Intelligent Systems and Computing	India	3DES; Symmetric key cryptography TEA
Basu et al. [28]	Covering Cloud security, Virtualization issues and solutions while other deal with the access control mechanisms with a proper interconnection between them and finally discussing a set of open problems in this domain.	2018	IEEE 8th Annual Computing and Communication Workshop and Conference CCWC 2018	India	Cloud computing; Virtualization
Kaura et al. [29]	Presenting the cloud services, risk associated with it and security measures in cloud computing.	2018	Proceedings of 2017 International Conference on Innovations in Information Embedded and Communication Systems ICIIECS 2017	India	Hybrid cloud; Infrastructure as a service (IaaS); Platform as a service (PaaS). [5]; Private cloud; Public cloud; Software as a service (SaaS)
Shanmugasundaram et al. [30]	Presenting a review on security issues in security standards for the cloud, infrastructure, access control, third party privacy, confidentiality, reliability and integrity of data. It portrays the techniques employed in addressing cloud security issues and its challenges.	2018	Proceedings of 2017 International Conference on Innovations in Information Embedded and Communication Systems ICIIECS 2017	India	Cloning; Cloud computing; Infrastructure; Service provider
Kaushik S. et al [31]	Presenting the various possible attacks, threats, risks and security concerns with the possible countermeasures that need to be understood related to the cloud. The current research also investigates that how different cloud frameworks are affected by which network attacks.	2018	International Journal of Networking and Virtual Organizations	India	Attacks; Risks; SaaS Security Software as a service Threats
Mehra N. et al. [32]	Discusses security issues, limitations of existing approaches, and possible solutions associated with cloud computing approach.	2018	Advances in Intelligent Systems and Computing	India	Cloud computing; Security issues; Services over Internet

Manoj Kumar M. et al. [33]	Identifying various design debt causes in a cloud computing system from various dimensions of design debt. Even though immature, un-ripen coded service accessible over the Internet using the cloud computing paradigm may work fine and be wholly tolerable to the patron	2018	Smart Innovation Systems and Technologies	India	Cloud computing security; Design debt; Design refactoring; Design smells; Multilateral cloud security architecture; Technical debt
Timothy D.P. et al. [34]	Designing a new security method by using a hybrid cryptosystem, for data security in the cloud. high security on data transmission over the internet and proper network access on demand to a shared tank of constructive computing resources, mainly net, server, and storage application.	2017	International Conference on Microelectronic Devices Circuits and Systems ICMDCS 2017	India	RSA; SHA-2; blowfish; cloud-computing; cryptosystem
Barona R. et al. [35]	Presenting cloud computing, different cloud models and primary security threats and data breach issues that are right now exploring in the cloud computing framework. investigates the noteworthy research and difficulties that presents data breach in cloud computing and provides best practices to service providers and additionally endeavors plan to influence cloud servers to enhance their main concern in this serious economic scenario.	2017	Proceedings of IEEE International Conference on Circuit Power and Computing Technologies ICCPCT 2017	India	Cloud computing; Data breach; Security services; Service providers
Sahil Sood S.K. et al. [36]	Cloud Computing offers scalable virtual computing resources in the form of web-services on pay-as-you-go model	2017	Proceeding - IEEE International Conference on Computing Communication and Automation ICCCA 2016	India	Genetic Engineering IDEs One-time ownership cost model Pay-as-you-go Virtual Computing"
Dhingra A.K. et al. [37]	Presenting potential of cloud computing with reference to Security, Privacy and Policy issues are examined as a part of major concern which makes the computing potential puny and review of existing	2016	2016 5th International Conference on Reliability Infocom Technologies and Optimization ICRITO 2016:	India	Cloud computing; Cloud policy; Cloud security; IaaS; PaaS; SaaS

	literature for security challenges and policies issues in cloud computing.		Trends and Future Directions		
Gandhi K. et al. [38]	Emphasizing on the area of cloud computing, identifying the benefits in this kind of systems and various threats related to cloud computing.	2016	Proceedings of the 10th INDIA Com	India	
Balaji V. et al. [39]	Dealing with a survey of big data with cloud computing security and the mechanisms that are used to protect and secure big data within the limitations.	2016	International Journal of Control Theory and Applications	India	Big data; Big data privacy; Cloud computing; Cloud provider; Cloud security
Singh H. et al. [40]	Introducing a comprehensive reasoning of the cloud's security problems and explores the possible security and data privacy problems from the perspective of the cloud architecture, its delivery and deployment models.	2016	International Journal of Control Theory and Applications	India	Adoption risk; Cloud barriers; Cloud computing; Cloud privacy; Cloud security; Data security
Ambekar K. et al. [41]	Presenting various characteristics of cloud computing with its extended support to the business model. Advanced security model using VPN and analyses its impact on the cloud computing system	2016	Advances in Intelligent Systems and Computing	India	Cloud computing; Virtual private network; Virtualization
Mallika N.M. et al. [42]	Presenting the proposed MDET based secret sharing scheme, in addition to identifying the related vulnerabilities and threats along with feasible solutions when compared to existing state of the art methods. © International Science Press.	2016	International Journal of Control Theory and Applications	India	Cloud Computing (CC) Security
Kulkarni P.et al. [43]	identifying the main vulnerabilities in this kind of systems and the most important threats found in the literature related to Cloud Computing and its environment as well as to identify and relate vulnerabilities and threats with possible solutions.	2015	International Conference on Communication and Signal Processing ICCSP 2015	India	Mobile Cloud Computing (MCC)

Narula S. et al [44]	Presenting the working of AWS (Amazon Web Service) cloud computing. AWS is the most trusted provider of cloud computing which not only provides very good cloud security but also provides excellent cloud services. Also, making cloud computing security as a core operation and not an add-on operation.	2015	International Conference on Advanced Computing and Communication Technologies ACCT	India	Amazon Web Service; Cloud Computing; Information Centric Security; Trusted Computing
Kaur R. et al. [45]	Analyzing the security issues, the definition of cloud computing and brief discussion to under cloud computing is presented, then it explores the cloud security issues and problem faced by cloud service provider. Thus, defining the Pixel key pattern and Image Steganography techniques that are used to overcome the problem of data security.	2015	International Conference on Computing for Sustainable Global Development INDIACom 2015	India	Cloud Computing; Cloud security; Image steganography; Pixel key pattern; Security issues
Sahil Sood S. et al. [46]	Designing a User Profiling System for Cloud environment using Artificial Intelligence techniques and studies behavior (of User Profiling System) and proposes a new hybrid approach, which will deliver a comprehensive User Profiling System for Cloud Computing security.	2015	Conference Proceeding - 2015 International Conference on Advances in Computer Engineering and Applications ICACEA 2015	India	Artificial Intelligence; Machine Learning; Multi-tenancy; Networking Systems; Pay-as-you-go Model
Yuvaraj M. et al. [47]	Presenting huge security risks associated When infrastructure, applications, data and storage are hosted by cloud providers, there are huge security risks associated with each type of service offered.	2015	Library Hi Tech News	India	Cloud computing; Traffic hijacking
Tripathi M.K. et al. [48]	focusing on inter-clouds for establishing trust in cloud computing environment. The aim is to promote the use of inter-clouds in cloud computing environment.	2015	Proceedings of 2014 IEEE International Conference on Advanced Communication Control and Computing Technologies ICACCCT 2014	India	Cloud computing; Single cloud trust

Kaur R. et al. [49]	Presenting a security model is proposed, implemented in Cloud Analyst to tighten the level of cloud storage security, which provides security based on different encryption algorithms with integrity verification scheme. making it difficult for the hacker to gain access of the authorized environment.	2014	Proceedings of the 2014 International Conference on Advances in Computing Communications and Informatics ICACCI 2014	India	AES; Blowfish; IDEA; SAES; SHA-1; Token
Gupta A. et al. [50]	Exploring the cloud security threats and also discusses the existing security approaches to secure the cloud environment. Also, proposing a novel Tri-mechanism for cloud security against data breach which provide all around security to the cloud architecture.	2014	International Conference on Control Instrumentation Communication and Computational Technologies ICCICCT 2014	India	Cloud Computing; Cloud security threats
Al-Anzi F.S. et al. [51]	focusing on the area, i.e. application security, information security, infrastructure security and security monitoring by giving our own security model. This model surely protects our organizational physical as well as virtual assets by providing better security options.	2014	International Conference on Data Mining and Intelligent Computing ICDMIC 2014	India	Cloud computing; Threat; security
Vikas S.Set al. [52]	analyzing the factors which will influence the widespread adoption of Mobile scientific discipline which we tend to go any to dialogue the counter claims in a trial to convert the reader that the advantages of Mobile scientific discipline outweighs its disadvantage.	2014	International Conference on Electronics and Communication Systems ICECS 2014	India	Cloud; Computing; Mobile; Security
Chalse R. et al. [53]	Presenting a detailed analysis of the cloud security problem. Also, the different problem in a cloud computing system and their effect upon the different cloud users are analyzed. It is providing a comparably scalable, position independent. Low cost platform for client's data.	2013	Proceedings - 5th International Conference on Computational Intelligence and Communication Networks CICN 2013	India	Cloud security; IaaS; PaaS; SaaS; data storage; integrity verification

Behl A. et al. [54]	introducing a detailed analysis of the cloud security problem. It investigates the problem of security from the cloud architecture perspective, the cloud characteristics perspective, cloud delivery model perspective, and the cloud stakeholder perspective. The paper investigates some of the key research challenges of implementing cloud-aware security solutions which can plausibly secure the ever-changing and dynamic cloud model.	2012	Proceedings of the 2012 World Congress on Information and Communication Technologies WICT 2012	India	Cloud; Cloud Computing; Cloud Security Model; Security; Security Challenges
Kanday R. et al. [55]	Presenting a survey of the different security and application aspects of cloud computing such as confidentiality, integrity, transparency, availability, accountability, assurance. © 2012 IEEE.	2012	Proceedings: Turing 100 - International Conference on Computing Sciences ICCS 2012	India	accountability; assurance; availability; cloud; confidentiality; integrity; security; transparency
Srinivasan M.K. et al. [56]	Analyzing the current security challenges in cloud computing environment based on state-of-the-art cloud computing security taxonomies under technological and process-related aspects.	2012	ACM International Conference Proceeding Series	India	Cloud Computing; Internet based Services; Secure Cloud Architecture; Security
Tripathi A. et al. [57]	Presenting the security issues that arise in a cloud computing framework. It focuses on technical security issues arising from the usage of cloud services and provides an overview of key security issues related to cloud computing with the view of a secure cloud architecture environment.	2011	2011 IEEE International Conference on Signal Processing Communications and Computing ICSPCC 2011	India	Cloud Computing; Internet based Services; Secure Cloud Architecture; Security
Verma A. et al. [58]	Cloud Computing has become another buzzword after Web 2.0. The phrase cloud computing originated from the diagrams used to symbolize the internet. Cloud computing is not a completely new concept	2011	Communications in Computer and Information Science	India	Cloud computing; Grid computing; Security

Jyoti S. [59]	Proposing virtualization as an engine to drive cloud-based security.	2011	Communications in Computer and Information Science	India	Cloud; Infrastructure-as-a-Service (IaaS); Platform-as-a-Service (PaaS) and Software-as-a-Ser; Virtualization
Abedin Z.U. et al. [60]	Presenting a Projected biometric coding to boost the confidentiality in Cloud computing for biometric knowledge. Mentioning virtualization for Cloud computing also as statistics coding and providing the safety weaknesses of Cloud computing and the way biometric coding will improve the confidentiality in Cloud computing atmosphere. The novel approach of biometric coding is to reinforce the biometric knowledge confidentiality in Cloud computing. Implementation of identification mechanism can take the security of information and access management in the cloud to a higher level.	2019	2nd International Conference on Computing Mathematics and Engineering Technologies iCoMET 2019	China	Biometric; Cloud computing; Computer security; Cryptography
Yang S. et al. [61]	Presenting the stream cipher algorithms and cloud computing security platforms to propose a hardware structure of reconfigurable nonlinear Boolean function. The entire architecture is verified on the FPGA platform and synthesized under the 0.18 CMOS technology the clock frequency reaches 248.7 MHz The result proves that the design is propitious to carry out the most nonlinear Boolean functions in stream ciphers which have been published compared with other designs the structure can achieve relatively high flexibility and it has an obvious advantage in the area of circuits and processing speed.	2019	International Journal of Information and Computer Security	China	AND terms; Adaptive logic module; Cloud computing; Computer security; Cryptography; Hardware structure; Information; LUT structure; Nonlinear Boolean function; Reconfigurable design; Security platform

Yan L. et al. [62]	Proposing a survey on potential threats and risks and existing solutions on cloud security and privacy. We also put forward some problems to be addressed to provide a secure cloud computing environment.	2018	ACM International Conference Proceeding Series	China	Cloud computing; Data security; Privacy; Security; Standards
Amara N. et al. [63]	Providing highlights cloud computing architectural principles cloud computing key security requirements cloud computing security threats and cloud computing security attacks with their mitigation techniques and future research challenges. © 2017 IEEE.	2018	Proceedings - International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery CyberC 2017	China	Cloud Computing; Mitigation Techniques; Security Attacks; Security Requirements; Security Threats
Yang A. et al. [64]	According to the security requirements of cloud computing fuzzy comprehensive evaluation model based on analytic hierarchy process was established and taking a cloud service platform as an example to evaluate its security	2016	Tongxin Xuebao/Journal on Communications	China	Cloud computing; Cloud security technical reference model; Security issues; Shared storage security solving techniques; Trusted cloud computing solving techniques
He J. et al. [65]	How to ensure network security for modern virtual machine-based cloud computing platforms is still an open question. This question becomes more important and urgent to solve as the fast development of cloud computing in recent years.	2016	Peer-to-Peer Networking and Applications	China	Fault tolerance
Yang Y. et al. [66]	Analyzing cloud security technology research directions and further development space of cloud security technology and standardization.	2015	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	China	Cloud computing

Ruo-Xin Z. et al. [67]	Drawing on cloud computing risk control security assess framework related to the international organizations based on China's classification protection assessment requirements the cloud computing security evaluation index system is built using of Delphi method and the weight of each index entry is calculated using the AHP (Analytic Hierarchy Process). The cloud security assessment model has been validated through examples and the results show that the proposed model can make quantitative assessment on secure cloud platform effectively with much more efficiency.	2014	Proceedings of the 9th International Conference on Computer Science and Education ICCCSE	China	Analytic hierarchy process
Ding W. et al. [68]	Introducing cloud computing system and its characteristics. As a new model which combines IT technologies and services cloud computing has basically been recognized by market while its security has drawn the users' attention.	2014	WIT Transactions on Information and Communication Technologies	China	Access control; Cloud computing; Internet; Security issue
Zhang N. et al. [69]	Giving an overview on cloud computing security. To clarify cloud security a definition and scope of cloud computing security is presented. An ecosystem of cloud security is shown to illustrate what each role in industry can do in turn. Then security impacts of cloud security for both customers and operators are analyzed. To overcome challenges from cloud security many state-of-the-art technical solutions e.g. continuation protection mechanism IDM data security and virtualization security are discussed. Finally, best practices on perspective of operator are summarized and a conclusion is conducted.	2013	Proceedings - International Conference on Information Technology and Applications ITA	China	Cloud Computing; Cloud security; Security as a service; data security

Lin C. et al. [70]	Analyzing and comparing the present research results of security model and mechanism in the cloud and proposing a security modeling method based on the multi-queue multi-server model.	2013	Jisuanji Xuebao/Chinese Journal of Computers	China	Cloud computing; Security architecture; Security measurement; Security mechanism; Security model
Xi C. et al. [71]	Introducing the security and protection method of digital libraries under the environment of the virtual cloud computing and puts forward security strategy and suggestions starting from the angle of the Virtualization security.	2013	Communications in Computer and Information Science	China	cloud digital libraries.
Yang S. et al. [72]	Discussing the four security properties this model can provides safe and high-efficient security underpinning for cloud service.	2012	Journal of Information and Computational Science	China	Cloud computing
Li H. et al. [73]	Presenting three typical definitions of cloud computing are listed. Security issues in cloud computing are analyzed. Novelties in cloud threat model new problems and new research directions in cloud computing environment are also outlined.	2012	Communications in Computer and Information Science	China	Cloud Computing
Xu X. et al. [74]	Discussing the architecture and tier of cloud computing analyzes the basic system structure of cloud computing platform designs a security framework of cloud computing platform describes the general process of such framework and discusses the principal functions of the key modules.	2012	Proceedings - 4th International Conference on Computational and Information Sciences ICCIS 2012	China	cloud computing
Liu W. et al. [75]	Introducing some cloud computing systems and analyzes cloud computing security problem and its strategy according to the cloud computing concepts and characters. The data privacy and service availability in cloud computing are the key security problem. Single security method cannot solve	2012	2nd International Conference on Consumer Electronics Communications and Networks CECNet 2012 - Proceedings	China	cloud computing

	the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system.				
Wang H. et al. [76]	Presenting cloud computing security management risk assessment and put forward a specific risk assessment methodology. It designed a typical environment of cloud computing conducted the experiment by the risk assessment methodology and analyzed the experiment results. The experiment showed that the risk assessment analysis methodology could effectively reveal the vulnerability and risk of security management in a cloud computing environment which is of great significance on the Cloud Computing Security Management Risks (CCSMR).	2012	Advances in Intelligent and Soft Computing	China	Cloud computing
Zhu H. et al. [77]	According to the analysis of theory the proposal is secured because the voiceprint templates are diverse cancelable and irreversible if the security parameters are secret. The experimental results demonstrated the authentication performance is unchanged. When the size of codebook is 32 FRR is 4% while the size of codebook is 64 FRR is 3.2%.	2011	Proceedings - International Conference on Cloud and Service Computing CSC 2011	China	
Tan X. et al. [78]	Proposing a cloud computing security reference framework. The purpose of this paper is attempted to bring greater clarity landscape about cloud computing security.	2011	Proceedings of International Conference on Electronic and Mechanical Engineering and Information Technology EMEIT 2011	China	cloud computing

Lv H. et al. [79]	Introducing cloud computing concepts and main features and analyzes the security of cloud computing and the security strategies are proposed for security issues related to cloud computing.	2011	Proceedings - International Conference on Intelligence Science and Information Engineering ISIE 2011	China	Cloud computing
Feng D. et al. [80]	Describing the great requirements in Cloud Computing security key technology standard and regulation etc. and provides a Cloud Computing security framework. This paper argues that the changes in the above aspects will result in a technical revolution in the field of information security.	2011	Ruan Jian Xue Bao/Journal of Software	China	Cloud computing
Wang C. et al. [81]	Supporting study of a method to solve cloud computing security issue with private face recognition. The method has three parts: user part provides face images	2010	International Conference on Computational Intelligence and Software Engineering CiSE	China	
Liu H. et al. [82]	Describing a model of overall cloud computing security risk assessment with a specific risk assessment analysis methodology. Tests of the risk assessment analysis methodology in a typical cloud computing environment show that the risk assessment analysis methodology can effectively reveal the overall vulnerability and risk in a cloud computing environment which is of great significance for the effective management of cloud computing security risks.	2010	Qinghua Daxue Xuebao/Journal of Tsinghua University	China	Cloud computing
Yan L. et al. [83]	Adopting federated identity management together with hierarchical identity-based cryptography (HIBC) not only the key distribution but also the mutual authentication can be simplified in the cloud. © 2009 Springer-Verlag.	2009	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	China	

Karame G.O. et al. [84]	Presenting new threats countermeasures and opportunities brought about by the move to cloud computing with a preference for unconventional approaches as well as measurement studies and case studies that shed light on the security implications of cloud infrastructure and use cases.	2017	Proceedings of the ACM Conference on Computer and Communications Security	United states	Cloud Computing; Security
Androulaki E. et al. [85]	Cloud computing is a dominant trend in computing for the foreseeable future	2016	Proceedings of the ACM Conference on Computer and Communications Security	United states	Cloud computing; Security
Kerschbaum F. et al. [86]	Analyzing the CCSW workshop aims to bring together researchers and practitioners in all security and privacy aspects of cloud-centric and outsourced computing.	2015	Proceedings of the ACM Conference on Computer and Communications Security	United states	Cloud computing; Privacy; Security
Oprea A. et al. [87]	Presenting cloud computing as a new paradigm for computing as a utility and refers to aggregation of virtualized computing resources managed by a service provider and dynamically allocated to tenants on demand.	2014	Proceedings of the ACM Conference on Computer and Communications Security	United states	Cloud computing; security
Khalil I.M. et al. [88]	Identifying 28 cloud security threats and presenting them into five categories. Also, authors present nine general cloud attacks along with various attack incidents and provide effectiveness analysis of the proposed countermeasures.	2014	Computers	United states	Attacks; Cloud computing; Cloud security; Insider attackers; Security vulnerabilities; Threats
Liu Y. et al. [89]	Ensuring that the service applications cloud software and the physical location of the cloud are secure. Furthermore, providers need to ensure that the service is secure on the client's side of the system.	2014	Proceedings - Pacific Asia Conference on Information Systems PACIS 2014	United states	Client-side security restriction; Cloud computing security; Mixed market competition; Profit-maximizing; Welfare

					maximizing
Sinha N. et al. [90]	Cloud computing offers an exceptional elasticity of resources and remarkable economic advantages in the Information Technology sector. It also provides an infrastructure for processing large and complex scientific data for data mining applications. While offering compelling throughput gains it also introduces several challenges related to security efficient storage of data and performance. We first present the basics and a brief history of cloud computing	2014	2014 23rd Wireless and Optical Communication Conference WOCC 2014	United states	cloud computing; data centers; data mining; performance; privacy; security; virtualization
Juels A. et al. [91]	Cloud Computing Security Workshop (CCSW) focuses on the security challenges and opportunities raised by cloud computing.	2013	Proceedings of the ACM Conference on Computer and Communications Security	United states	cloud computing; computer privacy; computer security
Barron C. et al. [92]	Presenting several types of attacks real-world cases are studied and the solutions that providers developed are presented. .	2013	Lecture Notes in Engineering and Computer Science	United states	Algorithms; Cloud computing security; Real-world cases; Security case studies
Panja B. et al. [93]	Presenting the largest security obstacles to defend against a Denial-of-Service (DOS) or Distributed Denial-of-Service (DDOS) attacks from taking down a cloud server.	2013	Recent Patents on Computer Science	United states	Bandwidth; Cloud computing; Denial of service
Capkun S. et al. [94]	Presenting the CCSW workshop aims to bring together researchers and practitioners in all security aspects of cloud-centric and outsourced computing to act as a fertile ground for creative debate and interaction in security-sensitive areas of computing impacted by clouds.	2012	Proceedings of the ACM Conference on Computer and Communications Security	United states	Cloud Computing; Security

Shi W. et al. [95]	Presenting MultiHype, a novel architecture that supports multiple hypervisors (or virtual machine monitors) on a single physical platform by leveraging many-core based cloud-on-chip architecture.	2012	CF '12 - Proceedings of the ACM Computing Frontiers Conference	United states	architecture; scalability; security; virtualization
Johnson III R.E. et al. [96]	Presenting used existing security tools. This paper will explore weaknesses in cloud security based on current commercial security tools. In addition, new methods and tools will be proposed to augment cloud security strategies.	2010	2010 International Conference on Information Society i-Society 2010	United states	Cloud security
Sumter L. et al. [97]	Presenting cloud computing concerns about internet security continue to increase	2010	Proceedings of the Annual Southeast Conference	United states	Cloud computing; Grid computing; Security; Software-As-A Service; Utility computing
Kang M. et al. [98]	Presenting how Cloud Security Certification System is implemented to solve the various cloud security problems in Korea.	2019	International Conference on Platform Technology and Service PlatCon 2019 - Proceedings	South Korea	CC certified product
Singh S. et al. [99]	Developing works on some public cloud and private cloud authorities as well as related security concerns. Additionally, it encompasses the requirements for better security management and suggests 3-tier security architecture. Open issues with discussion in which some new security concepts and recommendations are also provided.	2016	Journal of Network and Computer Applications	South Korea	Cloud computing
Masky M. et al. [100]	Introducing the Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE) Allegro methodology as a novel framework to identify risks for Cloud Computing.	2016	IEEE 2nd International Conference on Information Science and Security ICISS 2015	South Korea	Cloud Computing Security

Cagalaban G. et al. [101]	Addressing the security challenges by presenting a virtualization technique in M2M communications for cloud computing security. Then virtualization technique serves as security control mechanism for mobile devices which provides strong protection against the identified mobile threats as well as performance efficiency.	2012	Communications in Computer and Information Science	South Korea	Cloud Computing
Oh J. et al. [102]	Presenting comparison research between the difference of recognitions for the security priority in three areas between workers in private enterprise which are using cloud computing services and them in public institutions that has never used the services. It contributes to the establishment of strategies in aspect of security by providing guidelines to companies or agencies which want to introduce the cloud computing systems.	2012	International Journal of Security and its Applications	South Korea	Cloud computing
Shi W. et al. [103]	Presenting Multitype a novel architecture that supports multiple hypervisors (or virtual machine monitors) on a single physical platform by leveraging many-core based cloud-on-chip architecture.	2012	CF '12 - Proceedings of the ACM Computing Frontiers Conference	South Korea	architecture
Na S.-H. et al. [104]	Analyzing security threats and requirements for previous researches and propose service model and security framework which include related technology for implementation and are possible to provide resource mobility.	2010	Proceedings - 2010 IEEE Asia-Pacific Services Computing Conference APSCC 2010	South Korea	Component
Shirazi F. et al. [105]	Presenting that cloud security and privacy inherits most of the challenges existing in traditional security however it also introduces several new challenges around	2017	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and	Canada	Cloud computing

	virtualization trust legal privacy and data interoperability issues.		Lecture Notes in Bioinformatics)		
Benslimane Y. et al. [106]	Identifying the key themes and topics in cloud computing security. Findings from an analysis of 275 peer-reviewed publications show that cloud security solutions and cloud security challenges are the two most dominant themes. The other themes identified include guiding frameworks and methodologies and general security requirement.	2016	2015 IEEE 2nd International Conference on Information Science and Security ICISS 2015	Canada	Cloud computing security
Oprea A. et al. [107]	Presenting the Cloud computing as a new paradigm for computing as a utility and refers to aggregation of virtualized computing resources managed by a service provider and dynamically allocated to tenants on demand.	2014	Proceedings of the ACM Conference on Computer and Communications Security	Canada	Cloud, virtualization
Matrawy A. et al. [108]	Providing security in the new computing paradigm may be affected and that there might be some benefits that the cloud brings to the information security scene. In summary in this paper we attempt to initiate discussions around these important issues.	2011	CLOSER 2011 - Proceedings of the 1st International Conference on Cloud Computing and Services Science	Canada	Cloud; Security Paradigm
Zibouh O. et al. [109]	Proposing a new framework to secure cloud computing prevent security risks and improves the performance and the time of data processing. This framework combines between various powerful security techniques such secret sharing schema Fully Homomorphic Encryption (FHE) multi cloud approach and the implementation of a processing dispatcher which distributes a set of operations on FHE encrypted data between several processing engines.	2016	Journal of Theoretical and Applied Information Technology	Morocco	Cloud computing

Saadi C. et al. [110]	Proposing new cloud infrastructure architecture which combines IDS based on mobile agent sand using three types of honeypots in order to detect attacks to study the behavior of attackers increase the added value of Honeypot and IDS based mobile agents solve systems limitations intrusion detection improve knowledge bases IDS thus increase the detection rate in our cloud environment.	2016	Procedia Computer Science	Morocco	Attacks
Lemoudden M. et al. [111]	Discussing about enterprises are more and more moving to the cloud to take advantages of its economic and technological model. However, Privacy and Security issues are often cited as the main obstacle to the adoption of cloud computing for enterprises	2013	Journal of Theoretical and Applied Information Technology	Morocco	Cloud computing; security
Bouayad A. et al. [112]	Presenting the problem from the cloud architecture perspective the cloud offered characteristics perspective the cloud stakeholders' perspective and the cloud service delivery models perspective. Based on this analysis, authors detailed specification of the cloud security problem and key features that should be covered by any proposed security solution.	2012	CiSt 2012 - Proceedings: 2012 Colloquium in Information Science and Technology	Morocco	cloud computing

Following a thorough reading of the papers retained for this SLR and in accordance with its objectives, different threats to cloud computing systems were discussed which can be broken down into three categories given below;

Data Security: Data must be fittingly verified from the outside world. This is important to guarantee that data is ensured and is less inclined to damage. With cloud computing turning into a forthcoming trend, various vulnerabilities could emerge when the information is by and large aimlessly shared among the fluctuated frameworks in cloud computing. Guaranteeing data security and privacy in cloud computing implies the capacity to guarantee the standard key aspects of security, namely, confidentiality, integrity and accessibility. The fundamental prerequisites for data security are data integrity that alludes to the assurance that clients' data are not changed without approval [21]. In order to guarantee data integrity from both the supplier and supporter points of

view, secure encryption algorithms are commonly utilized. Nonetheless, encryption alone does not guaranty that data are not noxiously changed [22]. Because of the dynamic shared and circulated nature of the cloud, there is another vital requirement for cloud clients, specifically, privacy. This alludes to data security and exactness which permits ensuring private and delicate information. This implies the cloud framework ought to be available to approved authenticated clients any when, anywhere and through any platform. There are a few cyber-security threats that may confront a cloud service availability which are mainly network-based assaults, such as, Distributed Denial of Service (DDoS) attacks [93]. Furthermore, Cloud suppliers should keep up a suitable activity plan to manage these dangers and threats.

Cloud Network Infrastructure Security: A cloud service provider should be able to accept trustful network traffic, and to block malicious network traffic [23].

A cloud service provider should be able to accept trustful network traffic, and to block malicious one. The cloud network infrastructure security should be able to block and protect against Denial of Service (DoS) attacks, to detect and prevent intrusions and to allow logging and notification. DoS defenses are based on network security, which should effectively filter queries and identify invaders to prevent malicious attacks [24]. The intrusion detection and prevention systems IDS/IPS detect or block known malware attacks, virus signatures and spam signatures, but are also subject to false positives. Moreover, logging and notification allow cloud users to have some insight into the network's cyber-security health.

Cloud Applications Security: Organizations ought to shield their cloud-based applications from a wide range of cyber-security threats and attacks. Organizations ought to shield their cloud-based applications from a wide range of cyber- security threats and attacks. In addition, cloud applications security resembles web applications security when hosted in server centers. Numerous businesses propose single sign on (SSO) to enable the clients to access various individual cloud administrations [25]. Generally, it is difficult to update SSO arrangements accurately because it relies on a safe programming layer, which is required for several confirmation strategies.

5. DISCUSSION

This research work aims to provide a systematic literature review of cloud computing security, and hence, to get a holistic and up-to-date insight on its security threats and challenges. To this end, a total of 87 peer-reviewed papers were included representing three main axes of cloud computing security threats.

Aware of the importance of cloud security, many organizations including Cloud Security Alliance, National Institute of Standards and Technology and European Union Agency for Network and Information Security have published important reports highlighting the impact of cloud security issues.

Many researchers confirmed that security risks are considered as a noteworthy hindrance to cloud computing appropriation that are considered as a major hurdle impeding its advancement [26].

For instance, many researchers [113] for a Framework for secure cloud computing environments, trusted cloud services, and trusted service vendors for cloud security assurance. In addition, in order to ensure the correctness of users who can access the Cloud server, an effective and flexible distributed scheme with explicit dynamic data support, including, Kerberos authentication service and third party, was proposed.

It should be noted that the level of criticity of each issue is different. However, the most critical issues were widely reported while no experimental proof was accessible for different hindrances, so as information on these difficulties will increment, so will open doors for solutions.

6. CONCLUSION

The present work has done a methodical literature analysis in order to identify and classify the different threats of cloud computing security. The review covers the essential challenges through the main solutions to cloud computing cyber-security threats, the main different approaches, algorithms and techniques developed to address them, as well as the open problems which define the research directions in this area. We opted to classify them according to three main groups: Data Security, Cloud Network Infrastructure Security, and Cloud Applications Security. Furthermore, it was observed that, to answer the question raised in this SLR, 87 articles were analyzed. The main concern is that the state of maturity of cloud computing security is very encouraging and there are many research directions still open and which promise continued improvements of cloud security and privacy.

REFERENCES

[1] Rabia Latif, Haider Abbas, Saïd Assar, Qassim Ali, “Cloud Computing Risk Assessment: A Systematic Literature Review “, Future Information Technology, Chapter: 42, pp. 285-293,2014. DOI: 10.1007/978-3-642-40861-8_42.

[2] D. Garg, J. Sidhu, and S. Rani, “Improved TOPSIS: A multi-criteria decision making for research productivity in cloud security,” Comput. Stand. Interfaces, vol. 65, pp. 61–78, 2019. DOI: 10.1016/j.csi.2019.02.002.

[3] E. Zenker, M. Shahpas ,"A review of testing cloud security." International Journal of Internet under scienceonline.com, 2018. DOI: 10.1504/IJITST.2018.093661.

[4] T. Diaby, BB. Rad, Cloud computing : a review of the concepts and deployment models. Journal of Information Technology and Computer ; 2017. DOI: 10.5815/ijitcs.2017.06.07.

[5] PM. Mell, T.Grance,,NIST Definition of Cloud Computing, National Institute ; SP 800-145 ;2011. DOI: 10.6028/NIST.SP.800-145.

[6] F. Abazari, M. Analoui, H. Takabi, and S. Fu, “MOWS: Multi-objective

workflow scheduling in cloud computing based on heuristic algorithm," Simul. Model. Pract. Theory, vol. 93, pp. 119–132, 2019. DOI: 10.1016/j.simpat.2018.10.004.

[7] A. Lele, "Cloud computing," in Smart Innovation, Systems and Technologies, 2019.

[8] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," Comput. Electr. Eng., vol. 71, pp. 28–42, 2018. DOI: 10.1016/j.compeleceng.2018.06.006.

[9] D. Garg, J. Sidhu, and S. Rani, "Improved TOPSIS: A multi-criteria decision making for research productivity in cloud security," Comput. Stand. Interfaces, vol. 65, pp. 61–78, 2019. DOI: 10.1016/j.csi.2019.02.002.

[10] Y. Yu, A. Miyaji, M. H. Au, and W. Susilo, "Cloud computing security and privacy: Standards and regulations," Comput. Stand. Interfaces, vol. 54, pp. 1–2, 2017. DOI: 10.1016/j.csi.2017.03.005.

[11] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," J. Netw. Comput. Appl., vol. 79, pp. 88–115, 2017. DOI: 10.1016/j.jnca.2016.11.027.

[12] Huda Karajeh1, Mahmoud Maqableh2, Ra'ed (Moh'd Taisir) Masa'deh3, Security of Cloud Computing Environment,2014

[13] Peter Mell. 'The NIST Definition of Cloud ', Reports on Computer Systems Technology, sept., p. 7. 2011. DOI: 10.6028/NIST.SP.800-145

[14] Armbrust M et al Above the clouds: a Berkeley view of cloud computing. UC Berkeley Technical Report ,2009.

[15] M. Hawedi, C. Talhi, and H. Boucheneb, "Security as a service for public cloud tenants (SaaS)," Procedia Comput. Sci., 2018. DOI: 10.1016/j.procs.2018.04.143.

[16] G. Ramachandra, M. Iftikhar, and F. A. Khan, "A comprehensive survey on security in cloud computing," Procedia Comput. Sci., 2017. DOI: 10.1016/j.procs.2017.06.124

[17] D. B. Fernandes, L. B. Soares, J. Gomes, M. Freire, and P. M. Inácio, "Security issues in cloud environments: a survey," International Journal of Information Security, Vol. 13, pp. 113-170, 2014/04/01 2014.

[18] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," Information Sciences, Vol. 305, pp. 357-383, 2015. DOI: 10.1016/j.ins.2015.01.025.

[19] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," Computers & Electrical Engineering, Vol. 39, pp. 47-54, 2013. DOI: 10.1016/j.compeleceng.2012.04.015.

[20] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An

analysis of security issues for cloud computing," Journal of Internet Services and Applications, Vol. 4, p. 1, 2013. DOI: 10.1186/1869-0238-4-5.

[21] TURBAN, E. & KING, D. Electronic commerce global edition, person, 2012.

[22] Lifei, Wei Haojin, Zhu Zhenfu, Security and privacy for storage and computation in cloud computing, 2014. DOI: 10.1016/j.ins.2013.04.028.

[23] RABAI, L. B. A., JOUINI, M., AISSA, A. B. & MILI, A. A cyber security model in cloud computing environments. Journal of King Saud University - Computer and Information Sciences, 25, 63-75, 2013. DOI: 10.1016/j.jksuci.2012.06.002.

[24] Bryan Sullivan, Microsoft Said Tabet, Practices for Secure Development of Cloud Applications,2013.

[25] C. Mainka, V. Mladenov, J. Schwenk, On the security of modern Single Sign-On Protocols Second-Order Vulnerabilities in OpenID Connect, CoRR URL https://arxiv.org/pdf/1508.04324.pdf, [Accessed on 13-Apr-2018].

[26] E. Cayirci, A. Garaga, A. Santana de Oliveira and Y. Roudier, "A risk assessment model for selecting cloud service providers" In: Journal of Cloud Computing: Advances, Systems and Applications, 5(14), 2016. DOI https://doi.org/10.1186/s13677-016-0064-x.

[27] Wani, A.R., Rana, Q.P., Pandey, N ; Performance evaluation and analysis of advanced symmetric key cryptographic algorithms for cloud computing security ;Advances in Intelligent Systems and Computing, 742, pp. 261-271, 2019 ; DOI: 10.1007/978-981-13-0589-4_24.

[28] Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S., Sarkar, P.Cloud computing security challenges & solutions-A survey.2018 IEEE 8th Annual Computing and Communication Workshop and Conference, CCWC, 2018-January, pp. 347-356, 2018. DOI: 10.1109/CCWC.2018.8301700.

[29] Kaura, W.C.N., Lal, A.Survey paper on cloud computing security ;Proceedings of 2017 International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS 2017, pp. 1-6, 2018. DOI: 10.1109/ICIIECS.2017.8276134.

[30] Shanmugasundaram, G., Aswini, V., Suganya, G.A comprehensive review on cloud computing security.Proceedings of International Conference on Innovations in Information, pp. 50-71, 2018. DOI: 10.1109/ICIIECS.2017.8275972.

[31] Kaushik, S., Gandhi, C.Cloud computing security: Attacks, threats, risk and solutions (2018) International Journal of Networking and Virtual Organisations, 2018. DOI: 10.1504/IJNVO.2018.093926.

[32] Mehra, N., Aggarwal, S., Shokeen, A., Bura, D. Analyzing cloud computing security issues and challenges Advances in Intelligent Systems and Computing,

710, pp. 193-202,2018. DOI: 10.1007/978-981-10-7871-2_19.

[33] Manoj Kumar, M., Nandakumar, A.N.Exploring multilateral cloud computing security architectural design debt in terms of technical debtSmart Innovation, Systems and Technologies, 78, pp. 567-579, 2018. DOI: 10.1007/978-981-10-5547-8_59.

[34] Timothy, D.P., Santra, A.K. A hybrid cryptography algorithm for cloud computing security,2017 International Conference on Microelectronic Devices, Circuits and Systems, ICMDCS2017, 2017-January, pp. 1-5, 2017. DOI: 10.1109/ICMDCS.2017.8211728.

[35] Barona, R., Anita, E.A.M. A survey on data breach challenges in cloud computing security: Issues and threats.Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2017. DOI: 10.1109/ICCPCT.2017.8074287.

[36] Sahil, Sood, S.K., Mehmi, S., Dogra, S.Designing and analysis of user profiling system for cloud computing security using fuzzy guided genetic algorithm.Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016, art. no. 7813823, pp. 724-731, 2017. DOI: 10.1109/CCAA.2016.7813823.

[37] Dhingra, A.K., Rai, D.Evaluating risks in cloud computing: Security perspective 5th International Conference on Reliability, Infocom Technologies andOptimization, ICRITO 2016: Trends and Future Directions, art. no. 7785013, pp. 533-536, 2016. DOI: 10.1109/ICRITO.2016.7785013

[38] Gandhi, K., Gandhi, P. Cloud computing security issues: An analysis. Proceedings of the 10th INDIACom; 3rd International Conference on Computing for Sustainable Global Development, INDIACom 2016, art. no. 7724982, pp. 3858-3861, 2016.

[39] Balaji, V., Swarnalatha, P. A review paper on big data & cloud computing security issues International Journal of Control Theory and Applications, 9 (26), pp. 145-151, 2016.

[40] Singh, H., Manhas, P., Maan, D., Sethi, N.Cloud computing security and privacy issues- a systematic review International Journal of Control Theory and Applications, 9 (Specialissue11), pp. 4979-4992, 2016.

[41] Ambekar, K., Kamatchi, R.Enhanced user authentication model in cloud computing security. Advances in Intelligent Systems and Computing, 530, pp. 327-338, 2016. DOI: 10.1007/978-3-319-47952-1_26

[42] Mallika, N.M., Srinivasan, B. Multi-Clouds Computing security for distributed environment using Differential Evolution Threshold based secret sharing and data replication International Journal of Control Theory and Applications, 9 (2), pp. 717-729, 2016.

[43] Kulkarni, P., Khanai, R. Addressing mobile Cloud Computing security issues:

A survey. International Conference on Communication and Signal Processing, ICCSP 2015, art. no. 7322756, pp. 1463-1467, 2015. DOI: 10.1109/ICCSP.2015.7322756.

[44] Narula, S., Jain, A., Prachi Cloud computing security: Amazon web service.International Conference on Advanced Computing and Communication Technologies, ACCT, pp. 501-505,2015.

[45] Kaur, R., Kaur, J. Cloud Computing security issues and its solution: A review International Conference on Computing for Sustainable Global Development, INDIACom 2015, art. no. 7100438, pp. 1198-1200.

[46] Sahil, Sood, S., Mehmi, S., Dogra, S. Artificial intelligence for designing user profiling system for cloud computing security: Experiment Conference Proceeding - 2015 International Conference on Advances in Computer Engineering and Applications, ICACEA 2015, art. no. 7164645, pp. 51-58. DOI: 10.1109/ICACEA.2015.7164645.

[47] Yuvaraj, M. Security threats, risks and open source cloud computing security solutions for libraries ; Library Hi Tech News, 32 (7), pp. 16-18, 2015. DOI: 10.1108/LHTN-04-2015-0026.

[48] Tripathi, M.K., Sehgal, V.K. Establishing trust in cloud computing security with the help of inter-clouds ; Proceedings of 2014 IEEE International Conference on Advanced Communication, Controland Computing Technologies, ICACCCT 2014, art. no. 7019408, pp. 1749-1752. DOI: 10.1109/ICACCCT.2014.7019408.

[49] Kaur, R., Singh, R.P.Enhanced cloud computing security and integrity verification via novel encryption techniques Proceedings of the 2014 International Conference on Advances in Computing,Communications and Informatics, ICACCI 2014, art. no. 6968328, pp. 1227-1233. September 2014. DOI: 10.1109/ICACCI.2014.6968328.

[50] Gupta, A., Chourey, V. Cloud computing : Security threats & control strategy using tri-mechanism ;International Conference on Control, Instrumentation, Communication and Computational Technologies, ICCICCT 2014, art. no. 6992976, pp. 309-316. DOI: 10.1109/ICCICCT.2014.6992976.

[51] Al-Anzi, F.S., Yadav, S.K., Soni, J.Cloud computing: Security model comprising governance, risk management and compliance International Conference on Data Mining and Intelligent Computing, ICDMIC 2014, art.no. 6954232. DOI: 10.1109/ICDMIC.2014.6954232.

[52] Vikas, S.S., Pawan, K., Gurudatt, A.K., Shyam, G. Mobile cloud computing: Security threats ;International Conference on Electronics and Communication Systems, ICECS 2014, art.no. 6892511. DOI: 10.1109/ECS.2014.6892511

[53] Chalse, R., Selokar, A., Katara, A. A new technique of data integrity for analysis of the cloud computing security ;Proceedings - 5th International Conference on Computational Intelligence and Communication ;pp. 469-473, 2013. DOI:

10.1109/CICN.2013.103.

[54] Behl, A., Behl, K. An analysis of cloud computing security issues.Proceedings of the 2012 World Congress on Information and Communication Technologies,WICT 2012, art. no. 6409059, pp. 109-114.

[55] Kanday, R. A survey on cloud computing security ; Proceedings: Turing 100 - International Conference on Computing Sciences, ICCS 2012, pp. 302-311.

[56] Srinivasan, M.K., Sarukesi, K., Rodrigues, P., Manoj, M.S., Revathy, P.State-of-the-art cloud computing security taxonomies - A classification of security challenges in the present cloud computing environment ;ACM International Conference Proceeding Series, pp. 470-476, 2012. DOI: 10.1145/2345396.2345474.

[57] Tripathi, A., Mishra, A. Cloud computing security considerations ;IEEE International Conference on Signal Processing, Communications and Computing,ICSPCC 2011. DOI: 10.1109/ICSPCC.2011.6061557

[58] Verma, A., Kaushal, S.Cloud computing security issues and challenges: A survey Communications in Computer and Information Science, 193 CCIS (PART 4), pp. 445-454, 2011. DOI: 10.1007/978-3-642-22726-4_46.

[59] Jyoti, S., Manish, S., Rupali, G.Virtualization as an engine to drive cloud computing security ; Communications in Computer and Information Science, 169 CCIS, pp. 62-66, 2011. DOI: 10.1007/978-3-642-22577-2_9.

[60] Abedin Z.U. Guan Z. Arif A.U. Anwar U.An advance cryptographic solutions in cloud computing security. 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies, iCoMET 2019; 2019. DOI: 10.1109/ICOMET.2019.8673400.

[61] Yang S, Junwei S, Wei W. Reconfigurable design and implementation of nonlinear Boolean function for cloud computing security platform. Int J Inf Comput Secur 2019;11(2):145-159. DOI: 10.1504/IJICS.2019.098201.

[62] Yan L. Hao X. Cheng Z. Zhou R. ;Cloud computing security and privacy. ACM International Conference Proceeding Series; 2018.

[63] Amara N. Zhiqui H. Ali A. ;Cloud Computing Security Threats and Attacks with Their Mitigation Techniques. Proceedings - 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, 2018. DOI: 10.1109/CyberC.2017.37.

[64] Yang A-, Gao F, Bian M-, Yang S-. Cloud computing security evaluation and countermeasure based on AHP-fuzzy comprehensive evaluation. Tongxin Xuebao 2016;37:104-110. DOI: 10.11959/j.issn.1000-436x.2016255.

[65] He J, Dong M, Ota K, Fan M, Wang G. NetSecCC: A scalable and fault-tolerant architecture for cloud computing security. Peer-to-Peer Netw Appl 2016; 9(1):67-81. DOI: 10.1007/s12083-014-0314-y.

[66] Yang Y, Zhao C, Gao T. Cloud computing: Security issues overview and solving techniques investigation. Lect Notes Comput Sci 2015;8993:152-167. DOI: 10.1007/978-3-319-19848-4_10

[67] Ruo-Xin Z. Cui X.-J. Gong S.-J. Ren H.-K. Chen K. ; Model for cloud computing security assessment based on AHP and FCE. Proceedings of the 9th International Conference on Computer Science and Education, ICCCSE 2014; 2014. DOI: 10.1109/ICCSE.2014.6926454.

[68] Ding W. ; Cloud computing security study based on the mobile internet environment. WIT Transactions on Information and Communication Technologies; 2014. DOI: 10.2495/ISME20132593.

[69] Zhang N. Liu D. Zhang Y. ; A research on cloud computing security. Proceedings - 2013 International Conference on Information Technology and Applications; 2013. DOI: 10.1109/ITA.2013.91.

[70] Lin C, Su W-, Meng K, Liu Q, Liu W-. Cloud computing security: Architecture, mechanism and modeling. Jisuanji Xuebao 2013;36(9):1765-1784. DOI: 10.3724/SP.J.1016.2013.01765.

[71] Xi C. Cloud computing security in multi-processor virtualization environment. Commun Comput Info Sci 2013;391 PART I:427-435. DOI: 10.1007/978-3-642-53932-9_42.

[72] Yang S, Wang S. Research on ATN-based trusted cloud computing security model. J Inf Comput Sci 2012;9(18):5945-5952.

[73] Li H, Tian X, Wei W, Sun CC. A deep understanding of cloud computing security. Commun Comput Info Sci 2012;345:98-105. DOI: 10.1007/978-3-642-35211-9_13.

[74] Xu X. Yan J. ; Research on cloud computing security platform. Proceedings - 4th International Conference on Computational and Information Sciences; 2012. DOI: 10.1109/ICCIS.2012.238.

[75] Liu.W ; Research on cloud computing security problem and strategy. 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet 2012 - Proceedings; 2012. DOI: 10.1109/CECNet.2012.6202020.

[76] Wang H, Liu F, Liu H. A method of the cloud computing security management risk assessment. Adv Intell Soft Comput 2012;141 AISC:609-618. DOI: 10.1007/978-3-642-27948-5_81.

[77] Zhu H.-H. He Q.-H. Tang H. Cao W.-H. ; Voiceprint-biometric template design and authentication based on cloud computing security. Proceedings - International Conference on Cloud and Service Computing, CSC 2011. DOI: 10.1109/CSC.2011.6138538.

[78] Tan X. Ai B. The issues of cloud computing security in high-speed railway. Proceedings of International Conference on Electronic and Mechanical

Engineering and Information Technology; 2011. DOI: 10.1109/EMEIT.2011.6023923.

[79] Lv H. Hu Y. Analysis and research about cloud computing security protect policy. Proceedings - International Conference on Intelligence Science and Information Engineering; 2011. DOI: 10.1109/ISIE.2011.16.

[80] Feng D-, Zhang M, Zhang Y, Xu Z. Study on Cloud Computing security. Ruan Jian Xue Bao 2011;22(1):71-83. DOI: 10.13328/j.cnki.jos.004807].

[81] Wang C. Yan H. Study of cloud computing security based on private face recognition. 2010 International Conference on Computational Intelligence and Software Engineering; 2010. DOI: 10.1109/CISE.2010.5676941.

[82] Liu H, Wang H, Wang Y. Overall cloud computing security risk assessment analysis. Qinghua Daxue Xuebao 2010;50(SUPPL. 1):1521-1528.

[83] Yan L, Rong C, Zhao G. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. Lect Notes Comput Sci 2009;5931 LNCS:167-177. DOI: 10.1007/978-3-642-10665-1_15.

[84] G. O. Karame and A. Stavrou, "CCSW'17-2017 ACM cloud computing security," 2017, pp. 2627–2628. DOI: 10.1145/3133956.3137050.

[85] E. Androulaki and M. K. Reiter, "CCSW'16: 8th ACM Cloud Computing Security Workshop," Proc. 2016. DOI: 10.1145/2976749.2990480.

[86] F. Kerschbaum, C. Nita-Rotaru, and I. Ray, "CCSW 2015: The 7th ACM cloud computing security workshop," 2015, vol. 2015-Octob, pp. 1703–1704.

[87] A. Oprea, A. Turk, C. Nita-Rotaru, and ..., "Mosaic: A platform for monitoring and security analytics in public clouds," 2016 IEEE …, 2016. November 2016. DOI: 10.1109/SecDev.2016.025

[88] Khalil, I, Khreishah, A, Azeem, M. Cloud computing security: A survey. Computers. mdpi.com; 2014; DOI: 10.3390/computers3010001.

[89] Liu Y. Sheng X. Marston S.R.; Bridging the theory and practice of cloud computing security. Proceedings of the ACM conference on computer and communications security; 2014.

[90] Sinha N. Khreisat L AnonymousClient side cloud computing security: A mixed market analysis. Proceedings - pacific asia conference on information systems, PACIS 2014; 2014.

[91 Juels A. Parno B. AnonymousFifth ACM cloud computing security workshop (CCSW 2013). Proceedings of the ACM conference on computer and communications security; 2013. 1487 p. DOI: 10.1145/2508859.2509033.

[92] Barron C. Yu H. Zhan J. AnonymousCloud computing security case studies and research. Lecture notes in engineering and computer science; 2013. 1287 p.

[93] Panja B, Bhargava B, Pati S, Paul D, Lilien LT, Meharia P. Monitoring and

managing cloud computing security using denial of service bandwidth allowance. Recent Pat Comput Sci 2013;6(1):73-81. DOI: 10.2174/2213275911306010009.

[94] Capkun S. Kamara S. Anonymous4th cloud computing security workshop (CCSW 2012). Proceedings of the ACM conference on computer and communications security; 2012. 1060 p. DOI: 10.1145/2382196.2382329.

[95] Shi W. Lee J. Suh T. Woo D.H. Zhang X. AnonymousArchitectural support of multiple hypervisors over single platform for enhancing cloud computing security. CF '12 - proceedings of the ACM computing frontiers conference; 2012. 75 p. DOI: 10.1145/2212908.2212920.

[96] Johnson III R.E. AnonymousCloud computing security challenges and methods to remotely augment a cloud's security posture. 2010 international conference . DOI: 10.1109/i-Society16502.2010.6018819.

[97] Sumter L. AnonymousCloud computing: Security risk. Proceedings of the annual southeast conference; 2010. DOI: 10.1145/1900008.1900152 .

[98] Kang M. Kwon H.-Y.AnonymousA study on the needs for enhancement of personal information protection in cloud computing security certification system. 2019 international conference on platform technology and service, PlatCon 2019 - proceedings; 2019. DOI: 10.1109/PlatCon.2019.8669413.

[99] Singh S, Jeong Y-, Park JH. A survey on cloud computing security: Issues, threats, and solutions. JNetwork Comput Appl 2016;75:200-22. DOI: 10.1016/j.jnca.2016.09.002.

[100] Masky M. Young S.S. Choe T.-Y. AnonymousA novel risk identification framework for cloud computing security. 2015 IEEE 2nd international conference on InformationScience and security, ICISS 2015; 2016. DOI: 10.1109/ICISSEC.2015.7370967.

[101] Cagalaban G, Kim S, Kim M. A mobile device-based virtualization technique for M2M communication in cloud computing security. Commun Comput Info Sci 2012;339 CCIS:160-7. DOI: 10.1007/978-3-642-35264-5_23.

[102] Oh J, Yoon YB, Suh JR, Lee BG. The difference of awareness between public institutions and private enterprises for cloud computing security. Int J Secur Appl 2012;6(3):01-10.

[103] Shi W. Lee J. Suh T. Woo D.H. Zhang X. AnonymousArchitectural support of multiple hypervisors over single platform for enhancing cloud computing security. CF '12 - proceedings of the ACM computing frontiers conference; 2012. 75 p. DOI: 10.1145/2212908.2212920.

[104] Na S.-H. Park J.-Y. Huh E.-N. AnonymousPersonal cloud computing security framework. Proceedings - 2010 IEEE asia-pacific services computing conference, APSCC 2010; 2010. 671 p. DOI:10.1109/APSCC.2010.117.

[105] Shirazi F, Seddighi A, Iqbal A. Cloud computing security and privacy: An

empirical study. Lect Notes Comput Sci 2017;10272 LNCS:534-49. DOI: 10.1007/978-3-319-58077-7_43.

[106] Benslimane Y. Yang Z. Bahli B. AnonymousKey topics in cloud computing security: A systematic literature review. 2015 IEEE 2nd international conference on InformationScience and security, ICISS 2015; 2016. DOI: 10.1109/ICISSEC.2015.7371014.

[107] Oprea A. Safavi-Naini R AnonymousCCSW 2014: Sixth ACM cloud computing security workshop. Proceedings of the ACM conference on computer and communications security; 2014. 1560 p.

[108] Matrawy A. Liem C. Wiener M. Gu Y.X. Wajs A. AnonymousA new perspective on providing cloud computing security: A position paper. CLOSER 2011 - proceedings of the 1st international conference on cloud computing and services science; 2011. 650 p. DOI: 10.5220/0003449106500655.

[109] Zibouh O, Dalli A, Drissi H. Cloud computing security through parallelizing fully homomorphic encryption applied to multi-cloud approach. J Theor Appl Inf Technol 2016;87(2):300-7. Corpus ID: 27115275.

[110] Saadi C. Chaoui H. AnonymousCloud computing security using IDS-AM-clust, honeyd, honeywall and honeycomb. Procedia computer science; 2016. 433 p. DOI: 10.1016/j.procs.2016.05.189.

[111] Lemoudden M, Ben Bouazza N, El Ouahidi B, Bourget D. A survey of cloud computing security overview of attack vectors and defense mechanisms. J Theor Appl Inf Technol 2013;54(2):325-30. DOI: 10.1016/j.procs.2016.04.253.

[112] Bouayad A. Blilat A. Mejhed N.E.H. El Ghazi M. AnonymousCloud computing: Security challenges. CiSt 2012 - proceedings: 2012 colloquium in information science and technology; 2012. 26 p. DOI: 10.1109/CIST.2012.6388058.

[113] P. Belimpasakis and S. Moloney, "A platform for proving family oriented RESTful services hosted at home". In: Consumer Electronics, IEEE Transactions on, 55, pp. 690–698, 2009. DOI: 10.1109/TCE.2009.5174441.