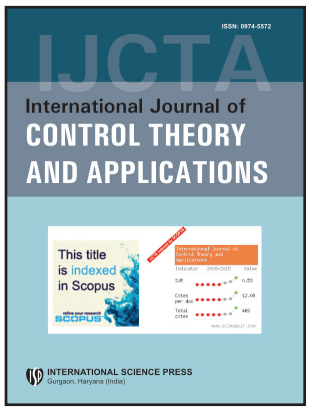

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 9 • Number 43 • 2016

Security in Cloud Computing: A Systematic Literature Review

Babak Bashari Rad[a], Eric Zenker[b] and Bogoreh Mohamed Robleh[c]

[a]School of Computing, Asia Pacific University of Technology and Innovation (APU), Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia. Email: babak.basharirad@apu.edu.my

[b-c]School of Technology, Asia Pacific University of Technology and Innovation (APU), Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia. Email: [b]zenker.eric@gmail.com; [c]bogoreh04gmail.com

Abstract: The cloud computing paradigm entails great opportunities for cost saving, tailored business solutions, state-of-the-art technical capabilities and systems as well as anytime worldwide access for organisations over the Internet. Hence, more and more clients shift their applications, business processes, services and data to the cloud. As a consequence thereof, customers hand over control and authority towards third-party cloud service providers. These circumstances raise various security concerns aggravated by multi-tenancy and resource pooling hampering cloud solution adoption. Most academic researchers examined cloud computing related security concerns either focused on technical specific (e.g. virtualisation), service model and legal issues. Beginning with introducing and defining key terms in cloud environments, especially cloud security, this survey systematically reviews technical and non-technical cloud computing security challenges in recent academic literature. The authors provide a general and consistent overview accompanied by obtaining current approaches to defining comprehensive industry standards. Additionally, gaps in previous related works are revealed, thus future research implications are pointed out. This paper fosters the understanding and relations of current security issues in cloud computing partly because the authors link academia and industry perspectives where suitable.

Keyword: Cloud Computing, Cloud Services, Cloud Security, Security, Security Challenges.

1. INTRODUCTION

With increasing research findings and emerging new technologies, IT capabilities need to be updated ever faster and frequent to stay competitive. On the one hand, this leads to boosted investments to stay up-to-date, but on the other hand, resources become more efficient. One approach to maximising the output is titled distributed systems. Besides, grid computing is a paradigm leveraging the usage of combined capabilities in heterogeneous, distributed networks. This long-known approach, however, is used for project-oriented tasks, whereas the relatively new paradigm cloud computing utilises resources in an efficient service manner [1].

In fact, cloud computing has revived and reinforced the traditional concept of outsourcing. The internet leverages the exploitation of on-demand and pay-per-use services, which result in cost savings and a stronger focus

on core business processes. Moreover, organisations are more flexible in terms of changing market conditions and quicker decision making speed. Additionally, enterprises benefit from cloud computing advantages, such as higher portability and scalability, to keep up with ongoing globalisation. In a nutshell, "clouds" have arisen to one of the most important and reasonable technologies for businesses in the 21st century [2, 3].

Cloud adoption necessitates an awareness of several essential factors in the Modern world. In general, the internet is the medium that connects and transfers data from and to a client and the service provider. In this virtualised network emerge major concerns regarding security as customers hand over control to a third-party [4]. Table I shows that security issues are highest rated among significant challenges within the adoption of cloud computing [5].

Singh et. al., [3] recently stated the cloud paradigm provides competitive advantages whereas the security is still vulnerable to attacks and other threats especially regarding resource pooling and virtualisation. Krishna et. al., [6] revealed the weakness of user accessibility while proposing enhanced data encryption as an eventual solution.

Table 1
Cloud computing adoption challenges [5]

S. No.	*Challenge*	*Percentage*
1	Security	63 %
2	Integrability	57 %
3	Performance	55 %
4	Compliance & Regulations	48 %
5	Lock-in	46 %
6	Cost transparency	44 %
7	Location	31 %

The objective of this survey is to investigate and consistently review recent publications on cloud computing and security issues as well as to outline major current cloud computing security challenges. First and foremost, the authors define general terms used in cloud environments. Subsequently, security issues are categorised and successively examined. Finally, previous related works are assessed and potential weak spots revealed.

2. CLOUD COMPUTING

Although "cloud computing" has only been invented around 2008/2009, the relatively new term is widely used in the industry and academics alike. Thus, it emerged to be a buzz word leading to different interpretations and misunderstandings. Therefore, the U.S. National Institute of Standards and Technology (NIST) brought out general and minimalist definitions for terms used regarding cloud computing to facilitate a comprehensive and mutual understanding. Referring to the NIST, is cloud computing "[…] a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources […] that can be rapidly provisioned and released with minimal management effort or service provider interaction." [7]. Figure 1 illustrates in greater detail the various classifications of the cloud paradigm on the basis of deployment and service models.

Furthermore, the pay-as-you-go paradigm distinguishes by five main characteristics according to NIST [7].

- *Resource pooling:* Within a multi-tenant model are technical capabilities virtually and physically pooled to dynamically service various client demands.
- *Broad network access:* Capabilities are accessible via standardised network mechanisms by heterogeneous platforms of clients.

- *Rapid elasticity:* To serve scaled consumer demands, technical resources can be flexible offered and released.
- *On-demand self-service:* Computing capabilities are, sans human interaction, automatically provisioned and consumed as need.
- *Measured service:* Capabilities are automatically controlled by metering measurements to tweak resource utilisation.

Beyond, in the recent research literature, two additional characteristics regarding cloud computing security had been added to the NIST standard.

- *Multi-Tenancy:* This non-essential characteristic had been added by the Cloud Security Alliance (CSA) and comprises the multiple and inter-organisational client use of a single capability [8, 9].
- *Auditability and certifiability:* Referred to Multi-Tenancy, measures enable affiliates to check the degree of service compliance [10].

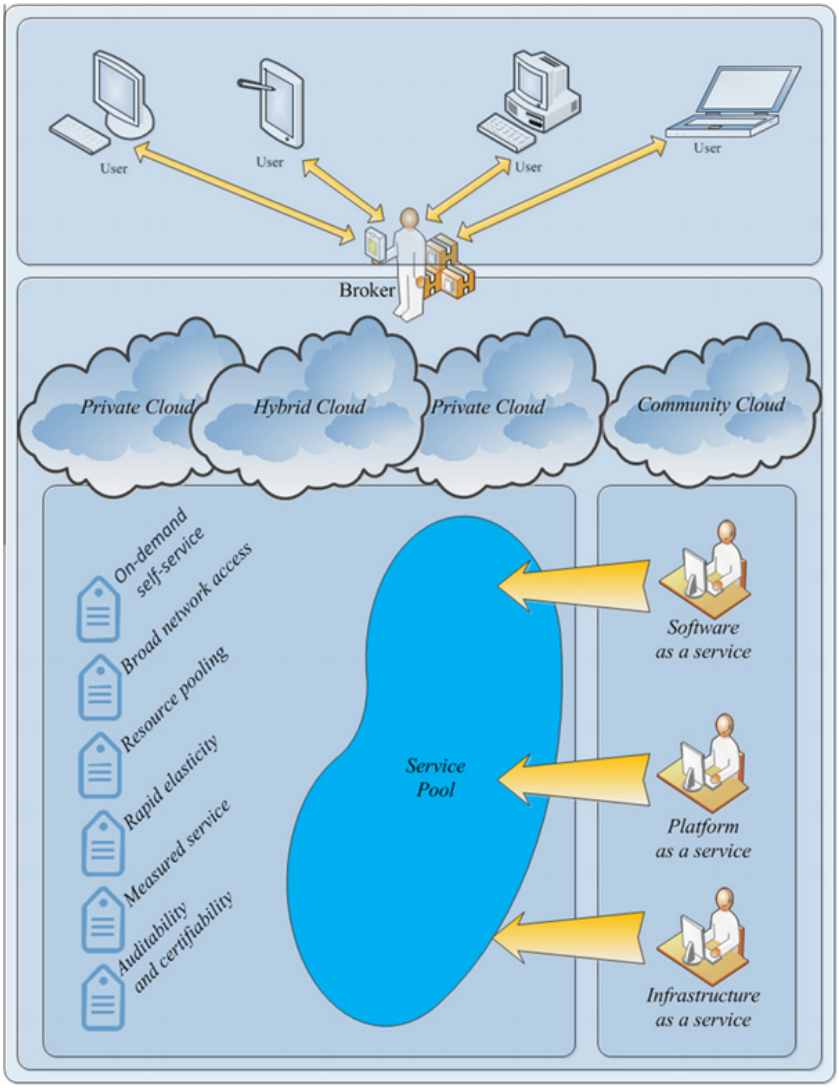

Figure 1: Cloud computing big picture [10]

A. Service Models

Available cloud solutions can be furthermore classified within three different service models. However, a few slightly distinct or extended models have recently emerged [11].

- *Software as a Service (SaaS):* A client utilises online-provisioned application software sans any authority to control underlying capabilities, operating systems or infrastructure.
- *Platform as a Service (Paas):* A supplier allocates an infrastructure, including technical capabilities sans dedicating control over the operating system or infrastructure to consumers to deploy customised or own applications.
- *Infrastructure as a Service (IaaS):* This approach only provides a plain computing infrastructure as well as technical resources for clients to virtually run their own operating systems and applications.

In chronological order, increase severity and skill as well as knowledge requirements to adopt those cloud computing solutions. Additionally, these models seem to be not tailored enough towards market demands. Thus, several distinct service models, known as A*nything as a Service (AaaS)*, emerged from the established ones. AaaS is a collective and an interchangeable model in respect of specific resources [1, 3]. Examples are *Data Integrity as a Service (DIaaS), Database as a Service, Provenance as a Service, Security as a Service, Logging as a Service, Big Data as a Service, Storage as a Service,* etc. [12]. Some major security-relevant models are following explained.

- *Network as a Service (NaaS):* NaaS is a framework, which enables customers to access existing network infrastructure. This model leverages the deployment of multicast protocols and customised routing, which results in redundancy elimination, smart caching and data aggregation [13].
- *Cloud storage as a Service:* This model is characterised by overcoming deficits of on-premises storage like risk extenuation via disaster recovery and long-term retention fostering business continuity [12].
- *Backend as a Service (BaaS):* In this model the database server steps in the classic application server to mainly enable web and mobile applications to directly interact [14].

B. Deployment Models

The infrastructure of a cloud solution is reflected in three, by NIST, defined deployment models.

- *Private cloud:* Services are not publicly offered to multiple clients within a single organisation by an on or off premises data centre [15].
- *Community cloud:* This model extends private clouds while providing access to a particular community with mutual interests.
- *Public cloud:* This model is designed for open general public use, thus, it is only and inevitably provisioned by a third-party vendor over the Internet.
- *Hybrid cloud:* This model combines the advantages of at least two specific cloud computing models by bounding them as unique entities with the use of standardised technology to facilitate portability [16].

Virtualisation is a common technology nowadays used in cloud computing environments. Thus, a new deployment model emerged in the recent literature.

- *Virtual private cloud:* This deployment model distinguishes itself in terms of a private constellation inside a public environment and makes other than the private cloud use of virtual private networks

(VPNs). However, the advantage is the on-demand use of pooled capabilities similar to the public cloud [1, 3].

3. SECURITY CHALLENGES

Nowadays cloud computing is omnipresent in every aspect of businesses. Therefore, it is essential to be aware of security concerns in cloud environments as they are major concerns faced by organisations. In general, the adoption of cloud solutions goes along with giving the control of data into the hands of a third party aggravated by the access of a large amount of users over the internet [8]. In general cloud security is distinguished by a wide collocation of policies, technologies and deployed checks to secure application software, access, data as well as the underlying infrastructure [17]. The cloud security reference model in Figure 2 clarifies the infrastructure, operations, entities and actors in cloud environments.

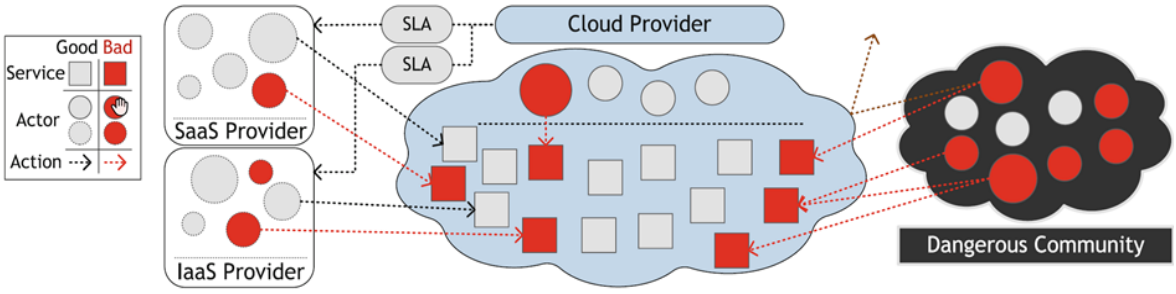

Figure 2: Cloud security reference model [1]

In a nutshell, providers offer services hosted in their own data centres, whereas customers outsource their processes and data with a transition of own control as well as authority. Providers are entirely responsible for managing their allocated resources, however, they may re-outsource certain activities likewise. Between customers and providers are service level agreements (SLAs) contracted to determine the terms and conditions of provisioned services. Moreover, this model exemplifies internal and external vulnerabilities [1]. Following, the authors are going to break down from rough to detailed the current situation regarding security in cloud computing.

A. Standards

In the recent past, standards in terms of cloud service provider interoperability to facilitate the consistent and homogenous migration between different cloud models had been introduced. To name but a few IEEE Cloud Computing Standard Study Group (IEEE CCSSG), Open Cloud Consortium (OCC) or Cloud Security Alliance (CSA) [11]. However, none of those standards is widely and generally accepted by the industry as a common one due to different interests and focus areas of the institutions. As these approaches lack defined guidelines for free data movement and compatibility among clouds, no inter-cloud standard has been established [11].

B. Service Level Agreements

As a result of missing standards, the industry applied the use of SLAs for direct and specific determinations between a vendor and a customer. These are widely known, accepted and used for classical outsourcing, which cloud services basically are. However, SLAs in general only specify minimum levels and until last did not consider integrity and confidentiality [11]. On the downside, everything not covered in SLAs and usually unexpected triggers disputes about consequences in case of breach and counteractive measures. Moreover, other than consistent standards, SLAs differ from provider to provider and are pre-defined, not negotiable contracts [8].

C. Infrastructure

Cloud solutions deliver one consistent front-end for clients to use the provider's services. Albeit the storage of data is mostly unknown to customers because the infrastructural network is distributed around the globe [18]. As a consequence thereof, various governmental policies apply in terms of privacy and breach, for example, within the European Union and other third countries regulated in the "safe harbor principle" 2 agreements [11].

However, this distribution fosters the characteristic resource pooling of cloud computing, resulting in sharing of technical and infrastructural capabilities to lower cost and maximise performance as well as efficiency. Nevertheless, these circumstances leverage cross-tenant attacks [8].

D. Virtualisation

The authors categorise virtualisation under security issues rather than Singh et. al., [3] who count it as an established characteristic of cloud computing. However, many recent publications revealed various related security concerns, thus, virtualisation is distinguished in virtual networks and virtualisation itself. A virtual network is logically built over a physical network as visualised in Figure 3. Accordingly, pooled technical resources at the provider's site are dedicated to the specific client.

Hence, virtual networks exacerbate physical protection and security mechanisms to monitor traffic and detect possible threats. In general, those mechanisms use pattern recognition to analyse anomalies albeit jimmied by the abstraction level [8].

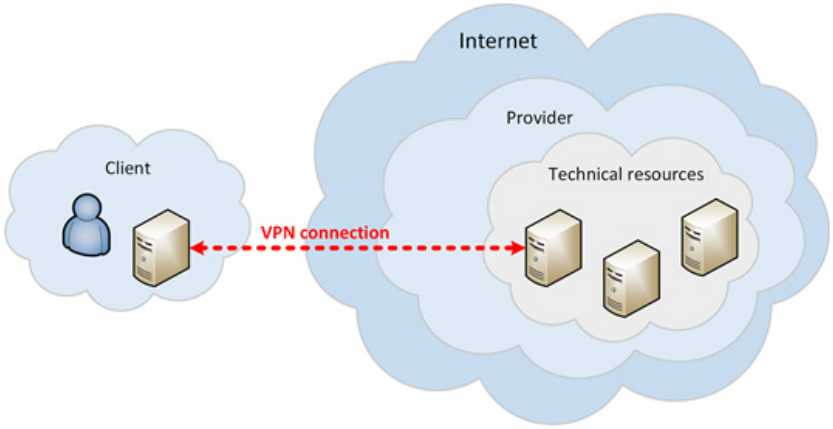

Figure 3: Virtual network [1]

In addition, not only the network is virtualised but also the operating systems, services and applications pooled in virtual machines (VMs). Figure 4 illustrates two different approaches for virtualised systems.

VM files, also known as images, can be pre-defined and easily copied and moved as well as instantly switched on and off to facilitate scalability [1]. On the contrary, compromised images can be easily widespread. Hypervisors are responsible for allocating and isolate hardware capabilities for one or multiple VMs. Thus, hypervisors are single points of failures [4]. However, entire virtual and logical isolation is so far not achieved and used virtualisation software cannot assure bug-freedom. In greater detail, VMs lack appropriate encryption mechanisms of large-sized files. As switching VMs on and off on demand is easy and convenient, the number of such instances can rapidly grow, which hampers the consistent maintenance of updates and security patches [1].

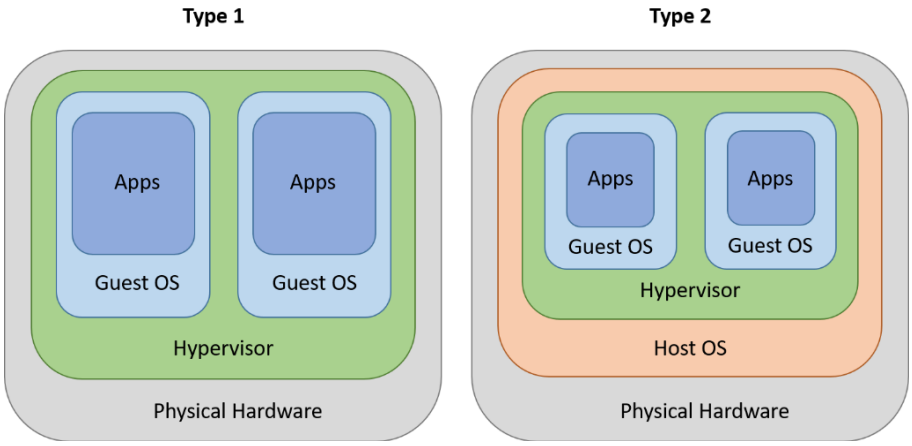

Figure 4: Types of virtualised systems [19]

E. Availability, Confidentiality and Integrity

The security of cloud environments and stored data underlies three key information technology principles: availability, confidentiality and integrity. Availability in cloud computing is mainly affected by external attacks. Besides those, which will be discussed later on, especially in cloud environments, providers sustainability and backup services are relevant [20].

Data confidentiality needs to consider key strengths and encryption algorithms. On the other side, cloud confidentiality describes the confidential keeping of clients computing task and data from both contractors. However, the characteristic of multi-tenancy can cause data confidentiality and privacy breaches because of lacks of strong authentication of several clients on the same platform, using the same capabilities [16].

Integrity in cloud environments concerns computing and data alike. Data integrity describes the unaltered condition and if so the detection of changes. Data stored on servers in the cloud may be modified or falsely administered. Attackers could especially target the loss of data control to take any advantages. On the other hand, computing integrity is the correct execution of programs without any alteration of other harmful influences. Since clients have no control of used servers, providers may deploy outdated and insecure source code [9]. Zafar et. al., [12] suggest the use of data integrity schemes to timely identify data deletion or corruption facilitating taking actions for data recovery.

F. Backup and Recovery

The need for data recovery results from natural, human or technical disasters causing an outage of provided services at the third party [3]. To prevent such occurrences, provider back up data to other servers or data centres for quick and seamless recoveries. However, the backup locations must be secured against tampering and unauthorised access as well [8]. In some cases, provider source out the backup service to subcontractors. Logically, those subcontractors have one backup methods and privacy policies to be concerned about. In terms of a total data centre breakdown affecting multiple clients, in the recent past untrustworthy providers' collated clients' data with wrong ownership [4].

G. Identity Management

Client access in cloud environments is one of the major concerns as they can cause internal as well as external frauds such as brute-force and dictionary attacks [1]. The difficulty is to restrict the access for only authorised

clients plus the delimitation of private and public accessible data stored locally or at a third-party's site [2]. To do so identity management has to ensure valid access from multiple client platforms and locations [3]. The CSA published a general best practice guide addressing these concerns [4]. Ali et. al., [8] recommend to use open standards like OAuth in combination with the especially for cloud environments developed cryptography method Attribute Based Encryption (ABE). Furthermore, ABE has been recently extended with a set based arrangement to ease the customisation of user attributes. Another extension of this method adds a hierarchical structure of users resulting in a root-level authority mechanism. Other approaches focus more on decentralisation or role-based authentication [8].

Zissis & Lekkas [16] emphasise on certificate-based attribute access control to facilitate scalability and flexibility.

4. PREVIOUS RELATED WORKS

Sharma et. al., [2] debated an overview of cloud computing types, security concerns and data protection approaches in cloud computing. They grouped security challenges into six categories: information security, design, portability, access & identity and trust & privacy. Among the types of cloud computing security issues, they discussed more in detail authentication and identity management. To encounter those security challenges they suggested an identity-based authentication framework renouncing certificate-based protocols. However, the main focus was on passwords neglecting other user attributes. Moreover, this hierarchy framework makes no use of open standards. Ali et. al., [8] conducted a much more detailed and recent survey on authentication.

Tao et. al., [21] developed a universal framework for amply homomorphic schemes of encryption. This framework ensures full data confidentiality because computation tasks are carried out on ciphertext whereas other approaches are only able to use plaintext. On the downside, this framework struggles with slower performance compared to other mechanisms.

Rong et. al., [11] discussed cloud computing in general and related security concerns. In addition, as there is no solution to cover and solve all issues they emphasised on SLAs and accountability in terms of security. In this article, security challenges were divided into traditional security issues that are applicable to cloud environments and new cloud-specific security issues. According to them, the security of cloud environments is mostly unexamined whereas they propose an encryption solution for private and secure data storage in public clouds. Furthermore, they stated that circumstances might require plaintext data transfer. In this case, they recommended a sort of a contract to prevent untrustworthy provider to misuse clients' data. Despite it is unclear how customers can track and monitor these obligations plus what defines an untrustworthy provider. Nevertheless, Tao et. al., [21] introduced a cryptographic mechanism which can handle plaintext activities as well one year before.

Xiao & Xiao [9] obtained existing privacy and security concerns in cloud computing. Subsequently, they identified five major related attributes: availability, integrity, confidentiality, privacy-preservability and accountability. Furthermore, they demonstrated threat models, vulnerabilities, established defence strategies the relations among those found attributes. The focus is on attacks like denial-of-service (DOS) to endanger the availability whereby they investigate such threats more in detail than Fernandes et. al., [1]. In essence, the outcome was that an improved level of privacy and accountability possibly impede each other. Notwithstanding, the question is if accountability can be counted as a security issue or if it is more a management concern regarding cloud adoption.

Hashizume et. al., [4] reviewed cloud environment, security issues in terms of new technologies for example virtualisation and Web 2.0. Beyond they identified major threats and vulnerabilities plus relating them to likely solutions. As a result, this paper presented various security concerns itemised towards the cloud

service models. Particularly, virtualisation and virtual networks are pointed out. Additionally, they distinguished between vulnerabilities and threats by highlighting their interference. Though, this paper is limited by the restriction to only three relations of vulnerabilities and threats. Hence, the significance of the obtained findings is questionable.

Fernandes et. al., [1] examined and classified key cloud security topics such as attack, threats and vulnerabilities in recent academic and industry publications. Besides, multiple indicated cloud security issues concerning data, storage, infrastructure, virtualisation and access, they highlighted cybercrime as one more today's major challenge. As cybercriminals keep up with emerging technologies, attacks become more sophisticated because data stored in public clouds are targets with huge potential benefits. This circumstance is aggravated by the diversity of offered cloud solutions, which are expected to be streamlined in the near future. The newly stated dimension of cybercrime in this paper is food for thoughts, however, cybercrime is used as a wide undefined term. To further obtain more meaningful findings, cybercrime needs to be defined and likely targets, as well as the motivation of cybercriminals, investigated.

Ali et. al., [8] conducted a detailed survey of cloud computing security challenges extended by a brief overview of mobile cloud computing vulnerabilities. Furthermore, they presented recent solutions to encounter the revealed issues. The security concerns were categorised into three major groups: challenges at communication level, challenges at architectural level and challenges at contractual and legal levels. As a result, this paper highlights that cloud security concerns resulting from the characteristic of multi-tenancy are major factors hampering organisations of cloud computing adoption similar to Rong et. al., [11]. Especially lacking isolation within the virtualisation technology entails new, unique security challenges. This survey extends and deepens the statements of Hashizume et. al., [4]. In addition, the distribution of technical capabilities around the globe exacerbates access control and identity management as well as legal, governmental issues. The limitations of this survey are the primary consideration of security concerns detected at provider sites without the authority of clients to interfere.

Choubey & Namdeo [22] performed a study on various solutions to provide data privacy and security in cloud environments. Moreover, they seize the in detail mentioned ABE encryption method from Ali et. al., [8]. The results of this research were that cloud data privacy is until now not fully achieved owing to the complexity of cloud environments and data privacy preservation methods alike. Known and established Internet technology approaches can only be partially adopted. Thus, they are going to introduce a fast and industry-adjustable encryption-based solution in the near future.

Singh et. al., [3] published a comprehensive overview of current security challenges in cloud computing with the focus on private and public clouds. Beyond, they stated considerable requirements for improved security management, plus the suggestion of a 3-tier security architecture. The three levels of this model are oriented towards the main layers in cloud service models. The suggested application level focuses on SaaS, the service middleware level on PaaS and the infrastructure level on IaaS. Basically, the application level makes use of encryption, the service middleware level consists of secure data transfer protocols, and the infrastructure level emphasises on virtual private networks (VPNs). However, this approach lacks encountering other security issues like availability, backup and recovery as well as virtualisation.

Zafar et. al., [12] investigated cloud storage security challenges, including outsourced data integrity schemes. Moreover, they examined likely security attacks and possible related mitigations regarding existing data integrity strategies. The findings were that previously envisaged schemes are not appropriate for all types of environments and data in terms of cloud computing security. Additionally, performance and design challenges were identified. Nonetheless, the consideration of re-outsourcing of data at provider sites was neglected.

5. CONCLUSION

The new cloud computing trend offers many new benefits in a dynamically changing business world. To keep up the competition, organisations seriously have to consider the adoption of cloud solutions. However, the outsourcing of business processes, services and sensitive data comes with newly emerged and slightly different security challenges than known from other solutions provided over the Internet.

This review showed the variety of available cloud models and solutions, whereas streamlining those by the industry will facilitate a better comprehension of security challenges as well as quicker adoption and further research on these topics. Additionally, this paper presented a consistent overview of current technical and non-technical cloud security issues. The findings foster the understanding of the various concerns and ease further research on more industry-related challenges. Revealed from previous related works, further research questions are; what can clients do to protect themselves by adoption cloud solutions as most articles only focused on the provider sites. However, this paper is limited by neglecting legal and governmental factors. Nevertheless, the survey illustrates the need of consistent cloud security standards enforced by both governmental and non-governmental institutions. This approach can force and ensure providers to observe certain rules, up-to-date technology and mechanisms.

REFERENCES

[1] 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.

[2] S. Sharma, S. Soni, and S. Sengar, "Security in cloud computing," in *National Conference on Security Issues in Network Technologies*, 2012.

[3] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications,* Vol. 75, pp. 200-222, 2016.

[4] 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.

[5] M. Sajid and Z. Raza, "Cloud computing: Issues & challenges," in *International Conference on Cloud, Big Data and Trust*, 2013, pp. 13-15.

[6] B. H. Krishna, S. Kiran, G. Murali, and R. P. K. Reddy, "Security Issues in Service Model of Cloud Computing Environment," *Procedia Computer Science,* Vol. 87, pp. 246-251, 2016.

[7] P. Mell and T. Grance, "The NIST definition of cloud computing [Recommendations of the National Institute of Standards and Technology-Special Publication 800-145]," *Washington DC: NIST. Recuperado de http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf* 2011.

[8] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information Sciences,* Vol. 305, pp. 357-383, 2015.

[9] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Communications Surveys & Tutorials,* Vol. 15, pp. 843-859, 2013.

[10] A. Jula, E. Sundararajan, and Z. Othman, "Cloud computing service composition: A systematic literature review," *Expert Systems with Applications,* Vol. 41, pp. 3809-3824, 2014.

[11] 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.

[12] F. Zafar, A. Khan, S. U. R. Malik, M. Ahmed, A. Anjum, M. I. Khan, *et. al.*, "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends," *Computers & Security,* Vol. 65, pp. 29-49, 2017.

[13] P. Costa, M. Migliavacca, P. Pietzuch, and A. L. Wolf, "NaaS: Network-as-a-Service in the Cloud," in *Presented as part of the 2nd USENIX Workshop on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services*, 2012.

[14] F. Gessert, F. Bücklers, and N. Ritter, "Orestes: A scalable Database-as-a-Service architecture for low latency," in *Data Engineering Workshops (ICDEW), 2014 IEEE 30th International Conference on*, 2014, pp. 215-222.

[15] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski*, et. al.*, "A view of cloud computing," *Communications of the ACM,* Vol. 53, pp. 50-58, 2010.

[16] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation computer systems,* Vol. 28, pp. 583-592, 2012.

[17] S. Reeja, "Role based access control mechanism in cloud computing using co–operative secondary authorization recycling method," *International Journal of Emerging Technology and Advanced Engineering,* Vol. 2, pp. 25-34, 2012.

[18] M. Hange, "Security Recommendations for Cloud Computing Providers," *Federal Office for Information Security,* 2011.

[19] W.-J. Chen, J. Chan, O. Mueller, M. Singh, and T. Väättänen, *DB2 Virtualization*: IBM Redbooks, 2009.

[20] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, 2012, pp. 647-651.

[21] L. Tao, Y. Xiaojun, and W. Jianmin, "Protecting data confidentiality in cloud systems," in *Proceedings of the Fourth Asia-Pacific Symposium on Internetware*, 2012, p. 18.

[22] S. D. Choubey and M. K. Namdeo, "Study of data security and privacy preserving solutions in cloud computing," in *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*, 2015, pp. 1101-1106.