Security and Privacy Issues in Cloud Computing

Bayan A. Alenizi1, Mamoona Humayun2, NZ Jhanjhi3

1College of Computer and Information Sciences, Jouf University, Sakakah, Saudi Arabia
2Department of Information systems, College of Computer and Information Sciences, Jouf University, Sakakah, Saudi Arabia
3School of Computer Science and Engineering (SCE), Taylor’s University, Malaysia

Corresponding author: Mamoona Humayun (mahumayun@ju.edu.sa)

Abstract

The idea of Cloud Computing (CC) provides dynamically scalable services that are delivered over the Internet as a service. The key driver of the cloud is economic benefits, as it aims to minimize capital expenditure as well as operating expenditure. There are still some problems to be overcome in order for this to become reality. One of the important issue is security and privacy concerns, which has been addressed by many researchers but still the problem persist. Security assurance is an important driver for cloud adoption and for increasing cloud deployment. To provide a detailed overview of existing cloud security challenges and mitigation strategies, this paper provides a comprehensive survey of underlying cloud security and privacy issues and concerns along with countermeasures. Further; as a contribution in research, we have provided a framework to address the security and privacy concerns in CC. Proposed framework uses hybrid authentication mechanism for the security of CC. The study provides a deeper insight to the researchers and practitioners about CC and underlying security and privacy concerns along with countermeasures and a novel solution.

Keywords: Cloud computing, Security issues, Privacy, Framework, Survey, Countermeasures

Introduction

CC is an important instrument that reflects the digital computing paradigm and business models for both software and hardware resources. Its economic advantage is that it provides an efficient way to minimize operating expenditures and capital expenditure. Despite CC is providing solutions to the most problem faced by individuals and organizations, it has exposed many businesses to security and privacy threats and issues [1, 2]. Various researches have been done on privacy and security in CC. Arjun et al in paper [3] stated that security issues are based on the cloud provider, service user, and instance. Another researcher in paper [4] argued that security issues are based on the delivery model, PaaS, IaaS, and SaaS. There exist four cloud deployment models namely: public cloud, private cloud, hybrid cloud, and community cloud and each has its own security and privacy concerns. To provide an overview of cloud security and privacy attacks, we briefly elaborate some key attacks and challenges faced in CC for better understandability of the area under study

Accounts hijack: In this type of attack, hackers attacks a CSP web service or application by installing their malicious software [5].

CC abuse: Cloud security architecture considers it most serious attack because attackers attacks on CC power [6].

Channel attacks: Such attacks interrupt the availability of services and disrupts privacy of data in IaaS layer of cloud [7].

XSS Attacks: In this kind of attack, Java script language is used and it is usually found in web application [8].
Malware attack: As the name suggests, hackers attack cloud systems by injecting malwares in this type of attack category [9].

DOS attack: Service availability is denied when requested by the user. E.g., Error 404 is considered as DOS attack [10].

Man in the middle attacks: This attack is usually performed on the secure connection between user and CSP without the knowledge of the attacker [11].

Metadata attack: In such attack, a shared metadata document between CSP and user is attacked by the attacker with the intention to alter the details of metadata [12].

Insider attack: An attack would be insider attack when employees access services from CSP without the proper knowledge of security concerns [13].

SQL Injection attacks: SQL statements are used to deactivate the security of the web application [14].

Shared network attack: When multiple users share the same CC infrastructure, there is a strong chance of data breaches. Furthermore, if there is any security concern in to customer’s infrastructure, it will be considered as threat to the cloud [15].

Sniffer attacks: When unencrypted data is transferred then attacker can attack the network by using any application, or a device by sniffing network traffic [16].

Virtual machine (VM) attack: A rapidly increasing shared VM technology can be attacked because of existing vulnerabilities [17].

Anonymous risk: When cloud services are provided without considering any security and privacy protocols, data breaches can happen easily [18].

Zombie attacks: This attack occurs at the virtual machine or hypervisor layer. Due to this attack, provided services slows down and fake accounts appears [16].

Besides above mentioned attacks, CC is also facing lot of challenges. Some common challenges faced by CC are as follows:

Network access: It is typically considered a big challenge by cloud service providers because attackers can take control of networks and data breaches usually occur because of it [19].

Security Management among CSPs: In cloud data management, maintaining and managing security specifications and complying with SLA is indeed a huge challenge. In order to meet the security criteria, CSPs can cooperate with each other [20].

Accounting: In order to achieve better network management, it is a challenging task for CSPs to estimate and analyse networks before deployment [21].

Shared Access: A challenge for service providers is to give access to the users. CSPs and consumers are responsible for taking measures to increase cloud security. There are still no effective solutions available e.g. in private cloud, users should be able to access the resources in a traditional way. So, the resources can be easily shared among the users depending on their needs [12].

Heterogeneous issue: Multiple technologies are used by the CSPs to deliver a large amount of services due to which heterogeneity occurs [3].

Security policies: Cloud infrastructure requires a strong security framework and guidelines to be applied [22].

Information loss: Losing gadgets or computers, such as phones or laptops, may allow an intruder to access personal information through theft [23].

Web browser security: Web browsers are not secure for using banking solutions. Such information can be hacked [24].
Figure 1: Common security challenges of CC

Figure 1 provides a broad picture of key challenges faced by CC. The remaining part of the paper is organized as follows: Section 2 discusses literature review and relevant findings related to CC. Section 3 discusses existing cryptographic solutions for CC. In section 4, we proposed a conceptual framework to fix the challenges of CC. Section 5 analyse the proposed framework. Finally section 6 conclude the paper by providing directions for future research. Table 1 provides the list of acronyms and abbreviations used in this study for better understanding of the readers.

| Acronyms | Abbreviations |
|----------|---------------|
| CC       | Cloud computing |
| CSP      | Cloud service provider |
| XSS      | Cross site scripting |
| DoS      | Denial of service |
| SQL      | Structured query language |
| AES      | Advanced encryption standard |
| DES      | Data encryption standard |
| SLA      | Service level agreement |
| RSA      | Rivest, Shamir, and Adleman |
| DH       | Diffie-Hellman |
| ECE      | Elliptic curve encryption |
| SHA      | Secure Hash Algorithms |
| IaaS     | Infrastructure as a service |
| PaaS     | Platform as a service |
| SaaS     | Software as a service |
| ABE      | Attribute based encryption |
| IBE      | Identity based encryption |
| NIST     | National Institute of Standards and Technology |

Literature review

In this section, we will discuss some latest researches to provide the current-state-of-the-art regarding security concerns in CC based on key CC parameters which include availability, security, privacy, confidentiality and integrity.
This study aims to address some key security dimensions including data availability, confidentiality, and integrity. It also highlights some common security threats such as hijacking, denial of service, loss of control, invalid storage, and data boundaries. Researchers stated that to maintain the user confidentiality information, one has to avoid sharing or using the system with an unknown service provider or any public user. Information seizes to be confidential only when the user shares its credentials with the service provider or any other user. Increased data storage in the system may lead to overloading and thus cause to system failure that will ultimately leads to loss of integrity. Loss of control happens due to the client's information being owned by the provider and there always exist the risk of manipulation. Lack of storage to store data enforce clients to pay for secondary storage, that create the issue of privacy.

Similarly, in another study, the essential factors of CC were discussed with main focus on security and privacy concerns. Service provider and vendors requests for service competency and user's security information. Issues arising in security management are reliability, privacy, access to data control, and legal problems. To manage privacy, the provider has considered encryption of data. However, the cloud service provider can experience insider or outsider attack compromising data security, confidentiality and integrity. To overcome these problems, CSPs have to take proper measures such as identity management and access control.

Paper addresses the problems of consumer safety, attention is also given to the competitiveness of the proposed system. The authors propose that the client should get nothing into the database, and the server should not collect any information about the biometric relation. The property-based encryption method was proposed for the identification of sophisticated sharing of data. The fine-scale, high data consumer performance, and standard privacy of cloud data sharing still remain unclear.

A study state that various security models have been suggested for enhanced security, there is still no universal solution for coping with both safety and privacy issues. CC poses various threats to privacy and security; namely loss of data and accessibility, account hijacking, user, and service provider problems. Further, it emphasize that safety systems should be paid more attention. Besides, the technique for the classification of knowledge to be followed depends on whether you need to defend yourself from outsider attackers or even insiders. Current ways of dealing with insiders safely rely on protocols for location abnormality.

According to security and privacy are the critical challenges of the computing application. This paper identifies several aspects of protection, including confidentiality, availability, and honesty. It also debates on protection and privacy issues. According to this paper, data encryption is the safest possible way to maintain confidentiality. However, essential control is a severe problem of encryption. The data owners can not presume to handle keys. Key management is expected from cloud service providers, and this is not a good option. The object of data integrity is to protect data from unlawful users being altered or deleted. In centralized structures, data confidentiality can be easily achieved. If unauthorized users deduce something from the cloud data, the privacy of the data is impaired. Misuse of data and the prevention of attacks are the most significant privacy risks to cloud storage. The attacker aim to misuse and destroy cloud data and will try to access it using the hash code. This causes the confidential data to be leaked. Different cloud services providers, including Microsoft Azure, Google Web Services, etc. provide cost-effective cloud access. They offer consumer and customer services on demand that pays what they get but security, privacy, and data protection are still significant concerns. It involves the production and distribution of replicas of shares among different providers of resources. For encrypting the shares, the AES algorithm is employed. The scheme and AES algorithms created shares are known as encapsulated shares. The technique is proposed to improve safety and reduce fraud. The technology offered is used to address the complex maintenance issue.

According to static data protection guarantees the safety of static information on the cloud storage system, while dynamic storage security guarantees integrity and trust during the transmission of data. Encryption is an efficient tool for data security protection. Data encoding is necessary when translating the original data or plaintext file using specific algorithms in unreadable code strings, commonly referred
to as ciphertext. In such case, if anyone intercepts the faded code, they cannot use the faded code to get the original information and ensure that it is confidentially preserved.

In paper [31], entity connections between cloud entities/players are highlighted for revealing protection areas in each cloud layer. This research work promotes the concept of compliance or corrective measures based on a security incident source or origin. This is an example of the unique security concerns of the public cloud. The facility is managed by a service provider where consumers access resources from an unreliable network. Public clouds are deemed financially viable. Special security issues unique to hybrid clouds in which the company and a third-party control and own a model infrastructures. Another simple opportunity is the potential to make any cloud agency more accountable by easily defining a source or origin of a safety incident, including enforcing disciplinary or remedial steps.

Paper [32] discuss a data-centric way for enhancing security, it provides a Computing Trust principle that offers trusted third-party technology to protect cloud providers' virtual machines. This idea gives the user many tools to track and analyse the data in a controlled way safely. It is evident that a partially trusted or trusted brand of cloud provides strong privacy, but the insecure server can depict clients with protected data. Still, it could be possible to exploit a legitimate user pattern in the same period as an untrusted cloud provider and provides a Computing Trust principle that offers trusted third-party technology to protect cloud providers' virtual machines. This idea gives the user many tools to track and analyse the data in a controlled way safely. It has been noted that the data provider establishes only the protection set by third parties. The big concern is that the user or the third party does not manage the solutions outside the user's domain. The danger is that any unknown persons will gain access to and exploit the data.

To resolve security concerns, researchers of paper [33] claims that there is need to define a range of attributes representing many aspects of cloud security and privacy. They analyse the availability of resources for cloud data retrieval and security in a disaster event and they further measure the robustness of the VM Manager (VMM) mechanism for safe operation. They encompass measurements, networking, and storage to identify protection against unauthorized usage by scrambling the content on its way from the user to the cloud, so that it is read-only by someone with a coding key to unscramble. Paper [34] discuss the CC Challenges in healthcare domain. According to this research, the present trend towards the design of cloud-hosted applications follows Microservices' approach, which splits the whole application into several logic and execution units and distributes application data between them for better protection and confidentiality. The use of microservices to architecture cloud service-oriented software adds to the imagined scenario's security and privacy problems due to the well-known issue of the shaking trend in the literature.

An excellent hybrid-CC environment focused on the interactive health care system framework has been suggested by [35]. A peer-to-peer cloud system is divided into small blocks that are reliable and enhance data security storage. Presence of big data analytics that analyse data efficiently and offer the client needed results. Their approach assesses the design of an installed layered cloud and proposes a way to handle data storage. Consider potential threats and put countermeasures in place to protect the system and improve patient information privacy. Data storage is carried out separately, and storage facilities are connected by a series of operations to assign space and facilitate data requests, resulting in low chances of data loss.

The above discussion shows that cryptographic solutions provide a common way to secure CC environment. Cloud cryptography uses encryption methods to protect data that is used or stored in the cloud. It helps users to access shared cloud resources easily and safely, as all information hosted by cloud providers is secured by encryption. In section below, we provide existing cryptographic solutions and then based on these solutions we will provide a framework that will address the security and privacy concerns of CC.

**Cryptographic Solutions**
Since there is no confirm solution exist for data confidentiality and protection, organizations usually fear about the loss of data in the cloud. Logically, certain ways of enhancing data storage and privacy may be enforced by SLA. Here, we are going to explore in detail some countermeasures relating to data protection and security. There are several cryptographic solutions currently available that are used to overcome security and privacy attacks. Some solutions are already discussed but further detail is added in this section.

**Symmetric-key Encryption:**

The use of Symmetric-key encryption is an easy and fast method of encrypting data in CC. Special key for data encryption and data decryption is used in this technique, and this key should be exchanged before data transfer between users. Common methodologies for symmetric encryption are AES and DES [36].

1) **Data Encryption Standard (DES)**

One of the most effective technique that utilizes fewer physical resources. A higher level of data security can also be provided by adding another cipher key to this technique.

2) **Advanced Encryption Standard (AES)**

This approach is used for block data encryption. Currently, there are several reliable AES based low cost solutions available that use less computational power

**Asymmetric-key encryption:**

AES is more secure and effective encryption technique, but it is slow and normally requires huge ciphers with complexed algorithms. RSA and DH are most common types of Asymmetric-key encryption [36].

1) **Rivest, Shamir, and Adleman (RSA)**

It is one of the practical solutions, developed before 2000. In this techniques, key-size requires to be same as of modulus and it is built on prime factors so, larger keys are used for better security.

2) **Diffie-Hellman key**

The purpose of this technique is to share keys over unsecure channel and 2048 bits are required for encrypted exchange.

3) **Elliptic curve encryption (ECE)**

ECE is a famous scheme because it requires less computational power and it was developed by Koblitz et al [37]

The Asymmetric encryption algorithms is considered effective in case of security but complex implementations are required by using backend mathematical operational developments.

**Secure Hash Algorithms**

SHA is widely used technique for securing and authenticating data. In this method, values are created using hash functions. These values are further used to verify the reliability and integrity of data. The most common application for this type of algorithm is the digital document. Many secure hash algorithms are currently presented. Among all the available SHA hash functions, SHA2 and SHA3 are mostly used and reliable algorithms. SHA 2 comprises of six hash functions with various bit combinations using 224, 56, 384, or 512.It is not easy to implement this function. An advanced hash function that substituted the SHA 1 and SHA2 is SHA-3, but it is also complex to implement [38].

**Advanced Cryptographic Solutions**
Many other cryptographic solutions are available for securing data. These solutions offer different cryptographic features. Some of the common encryption solutions are Homomorphic encryption, ABE, IBE, Multi-party secure computation, verifiable computation. Other than that, NIST has published a Format Preserving Encryption standard in 2016 which is useful for big data and complex application [39].

**Proposed conceptual framework for CC security and privacy issues:**

Security and privacy are the main issues of CC and to resolve these issues complex computational algorithms are implemented. Such algorithms gradually decrease the cloud performance, so, it is better to use more than one server for enhancing security features. Multiple servers can be used separately for authentication and encryption purposes. Web-based applications are usually protected from bot attacks by using CAPTCHA and multi-factor authentication. Two factor authentication technique is already used in CC systems. AES and RSA can be used together as a hybrid technique to enhance data security. In such technique, AES can encrypt and decrypt the data whereas the RSA can be used to encrypt and decrypts the symmetric key of AES. So, in this paper we have presented a conceptual framework that provides security and privacy model and using this framework, confidentiality, authentication, and integrity can be achieved as shown in figure 2.

![Proposed framework for addressing security and privacy concerns in CC](image)

**Figure 2: Proposed framework for addressing security and privacy concerns in CC**

Suitable security approaches are crucial for defining appropriate framework. Numerous techniques are already implemented to overcome the security and privacy issues. Such techniques include user and password authentication, verification, cryptography, and CAPTCHA etc. Many researchers have provided detailed frameworks to implement these solutions. Consequently, success of CC security totally depends on implementing appropriate methods.

In our framework, there are two servers; one for authentication and the other one for cryptography operation. In this way, the performance and speed will remain intact and time consumption to complete process will be improved as shown in our proposed framework. When the client wants to upload the
data on the cloud, data verification request will be sent to the server 1 and server 1 will verify the request in order to avoid zombie attack so that real client could upload his data safely. Server 1 uses two approaches to avoid zombie and bot attacks. First approach is to verify the client’s identity using TFA and the second approach is to use CAPTCHA. Server 2 manages the encryption of data by using AES and RSA techniques. The user also creates encrypted data keys using SHA-256. That encrypted data will be stored on the cloud. In order to regain the uploaded cloud data, the same authentication process will be followed again which are use of TFA and CAPTCHA. After getting access to the data, the client again creates the key using SHA-256, and compares keys. Data will be accepted in case of similar keys. To decrypt the data, RSA approach will be applied to the AES key and then original data will be accessed.

Proposed framework is safe to use because it gives security against dictionary attack, brute-force, key logger and replay attacks by using CAPTCHA, TFA. Using two servers will resolve issues like security and server speed. Server performance will also be better. The other proposed systems face main challenges like resource allocations, time issue and security. The only solution is to use more than one server so that resources can be utilized effectively. In this way, availability, integrity and confidentiality will be achieved easily.

Discussion

There is no doubt in the efficiency and performance of CC services and application. This field is used to improve applications and services in numerous organizations. Storing data on the cloud is easy to access for users but at the same time, it creates issues like confidentiality, integrity and availability. Our proposed conceptual framework uses simple yet effective techniques to enhance security and privacy. Suggested techniques will prevent attacks and will provide security. In the proposed scheme, two factor authentication mechanism is used that protects the data from security breaches. Combining two security techniques namely RSA and AES enhances security and privacy. This framework can be further strengthened by using optimization techniques. Some commonly used techniques for optimization purposes are pollination technique, Bat method, Honey bee, Cuckoo search, Particle swarm and Flower algorithm. Further, CMA-ES is commonly used for resource allocation that provides effective solution for optimization. The main feature is to search cipher for symmetric encryption. CMA-ES is capable to generate multiple cipher texts by modifying the key [40, 41]. As a result, this proves that optimization can easily enhance the performance and security. Lastly, optimization techniques are suggested for resource allocation, CMA-ES is a good example for optimization technique. To conclude the analysis of the proposed framework, our work uses multiple encryption techniques so that integrity, confidentiality and availability can be attained. The security and privacy are the major concerns in Cloud for cloud operations, as well as for the different applications which run with the cloud [42-43]. These issues deemed the performance of the Cloud and applications supported by them. The researchers presented several approaches related to load balancing [44], lightweight, etc. to indirectly support to the security issues.

Conclusion and future work

Cloud computing is the distribution of computing services over the Internet ("the cloud"), including servers, storage, databases, networking, applications, analytics and intelligence, to provide quicker innovation, versatile resources and economies of scale. Lot of organizations are shifted to clouds and remaining are thinking about it. However; some of the key challenges faced by cloud computing is that of privacy and security. Confidentiality, availability and integrity are also important for maintaining security and privacy of data. This paper provides a comprehensive survey to provide the state-of-the-art knowledge about CC privacy and security concerns, key attacks targeting clouds and challenges faced by CC. Further, it discuss commonly used cryptographic techniques. Based on all this, a hybrid
framework is proposed for the privacy and security of CC. In future, we are planning to apply this framework on a real CC environment.

References

1. Mishra, S., S.K. Sharma, and M.A. Alowaidi, Analysis of security issues of cloud-based web applications. Journal of Ambient Intelligence and Humanized Computing, 2020: p. 1-12.
2. Mishra, Sambit Kumar, Sonali Mishra, Ahmed Alsayat, N. Z. Jhanjhi, Mamoon Humayun, Kashira Sagar Sahoo, and Ashish Kr Luhach. "Energy-Aware Task Allocation for Multi-Cloud Networks." IEEE Access (2020).
3. Arjun, U. and S. Vinay. A short review on data security and privacy issues in cloud computing, in 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC). 2016. IEEE.
4. Sun, X. Critical security issues in cloud computing: a survey. in 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity). 2018. IEEE.
5. Ali, Sadia, Yaser Hafeez, N. Z. Jhanjhi, Mamoon Humayun, Muhammad Imran, Anand Nayyar, Saurabh Singh, and In-Ho Ra. "Towards Pattern-Based Change Verification Framework for Cloud-Enabled Healthcare Component-Based." IEEE Access 8 (2020): 148007-148020.
6. Chatterjee, Moitrayee, Prerit Datta, Faranak Siami Namin, and Keith S. Jones. "Abuse of the Cloud as an Attack Platform." In 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1091-1092. IEEE, 2020.
7. Elangovan, R. and M. Prianga, Side Channel Attacks in Cloud Computing, in Cognitive Social Mining Applications in Data Analytics and Forensics. 2019, IGI Global. p. 77-98.
8. Ranjan, I. and R.B. Agnihotri. Ambiguity in cloud security with malware-injection attack. in 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA). 2019. IEEE.
9. Yadav, R.M., Effective analysis of malware detection in cloud computing. Computers & Security, 2019. 83: p. 14-21.
10. Chandel, S., G. Yang, and S. Chakravarty, AES–CP-IDABE: A Privacy Protection Framework against a DoS Attack in the Cloud Environment with the Access Control Mechanism. Information, 2020. 11(8): p. 372.
11. Rahman, G. and C.C. Wen, Man in the Middle Attack Prevention for edg-fog, mutual authentication scheme. International Journal of Recent Technology and Engineering (IJRTE), 2019, 8(2s2).
12. Alhenaki, Lubna, Alaa Alwatban, Bashar Alamri, and Noof Alarifi. "A survey on the security of cloud computing." In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-7. IEEE, 2019.
13. Zhan, Jing, Xudong Fan, Jin Han, Yaqi Gao, Xiaqing Xia, and Qian Zhang. "CIADL: cloud insider attack detector and locator on multi-tenant network isolation: an OpenStack case study." Journal of Ambient Intelligence and Humanized Computing (2019): 1-23.
14. Shunmugapriya, B. and B. Paramasivan, Protection Against SQL Injection Attack in Cloud Computing.
15. Zimba, A., H. Chen, and Z. Wang, Bayesian network based weighted APT attack paths modeling in cloud computing. Future Generation Computer Systems, 2019. 96: p. 525-537.
16. Fidele, K.A. and A. Hartanto. DoS Attack Prevention Using Rule-Based Sniffing Technique and Firewall in Cloud Computing, in E3S Web of Conferences. 2019. EDP Sciences.
17. Dong, Y. and Z. Lei, An access control model for preventing virtual machine hopping attack. Future Internet, 2019. 11(3): p. 82.
18. Almuairifi, S.J. and M. Alenezi, Anonymous Authentication for Privacy Preserving of Multimedia Data in the Cloud, in Handbook of Research on Multimedia Cyber Security. 2020, IGI Global. p. 48-72.
19. Neware, R. and A. Khan. Cloud Computing Digital Forensic challenges. in 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA). 2018. IEEE.
20. Arafat, M. Information security management system challenges within a cloud computing environment. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. 2018.

21. Hui, X., Challenges and Countermeasures of Management Accounting in the Era of Big Data. World Scientific Research Journal, 2019. 5(10): p. 115-121.

22. Mushtaq, Muhammad Faheem, Urooj Akram, Irfan Khan, Sundas Naqeeb Khan, Asim Shahzad, and Arif Ullah. "Cloud computing environment and security challenges: A review." International Journal of Advanced Computer Science and Applications 8, no. 10 (2017): 183-195.

23. Maithili, K., V. Vinothkumar, and P. Latha, Analyzing the security mechanisms to prevent unauthorized access in cloud and network security. Journal of Computational and Theoretical Nanoscience, 2018. 15(6-7): p. 2059-2063.

24. Alshammari, Abdulaziz, Sulaiman Alhaidari, Ali Alharbi, and Mohamed Zohdy. "Security threats and challenges in cloud computing." In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 46-51. IEEE, 2017.

25. Humayun, M., Role of Emerging IoT Big Data and Cloud Computing for Real Time Application. International Journal of Advanced Computer Science and Applications (IJACSA), 2020. 11(4).

26. Rao, B.T., A study on data storage security issues in cloud computing. Procedia Computer Science, 2016. 92: p. 128-135.

27. Deorankar, A. and K.T. Khobragade. A Review on Various Data Sharing Strategies for Privacy of Cloud Storage, in 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020. IEEE.

28. Kumari, Chandini, Gagandeep Singh, Gursharan Singh, and Ranbir Singh Batth. "Security Issues and Challenges in Cloud Computing: A Mirror Review." In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), pp. 701-706. IEEE, 2019.

29. Fatima, S. and S. Ahmad, An Exhaustive Review on Security Issues in Cloud Computing. KSII Transactions on Internet & Information Systems, 2019. 13(6).

30. Yang, P., N. Xiong, and J. Ren, Data Security and Privacy Protection for Cloud Storage: A Survey. IEEE Access, 2020. 8: p. 131723-131740.

31. Mthunzi, Siyakha N., Elhadj Benkhelifa, Tomasz Bosakowski, chirine Ghedira Guegan, and Mahmoud Barhamgi. "Cloud computing security taxonomy: From an atomistic to a holistic view." Future Generation Computer Systems 107 (2020): 620-644.

32. Arora, A.S., L. Raja, and B. Bahl. Data centric security approach: A way to achieve security & privacy in cloud computing, in Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT). 2018.

33. Barik, Rabindra K., Rakesh K. Lenka, K. Rahul Rao, and Devam Ghose. "Performance analysis of virtual machines and containers in cloud computing." In 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 1204-1210. IEEE, 2016.

34. Esposito, Christian, Aniello Castiglione, Constantin-Alexandru Tudorica, and Florin Pop. "Security and privacy for cloud-based data management in the health network service chain: a microservice approach." IEEE Communications Magazine 55, no. 9 (2017): 102-108.

35. Lo'ai, A.T. and G. Saldaamli, Reconsidering big data security and privacy in cloud and mobile cloud systems. Journal of King Saud University-Computer and Information Sciences, 2019.

36. Yassein, Muneer Bani, Shadi Aljawarneh, Ehtah Qawasneh, Wail Mardini, and Yaser Khamaysheh. "Comprehensive study of symmetric key and asymmetric key encryption algorithms." In 2017 international conference on engineering and technology (ICET), pp. 1-7. IEEE, 2017.

37. Lawal, O. M., O. R. Vincent, A. A. A. Agboola, and O. Folorunso. "An improved hybrid scheme for e-payment security using elliptic curve cryptography." International Journal of Information Technology (2020): 1-15.
38. Guesmi, Ramzi, Mohamed Amine Ben Farah, Abdennaceur Kachouri, and Mounir Samet. "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2." Nonlinear Dynamics 83, no. 3 (2016): 1123-1136.

39. Kuchta, Veronika, Gaurav Sharma, Rajeev Anand Sahu, and Olivier Markowitch. "Multi-party (leveled) homomorphic encryption on identity-based and attribute-based settings." In International Conference on Information Security and Cryptology, pp. 71-92. Springer, Cham, 2017.

40. Aruna, M. and K. Mohan, Secured cloud data migration technique by competent probabilistic public key encryption. China Communications, 2020. 17(5): p. 168-190.

41. Tamunobarfiri, A., S. Aghili, and S. Butakov, Data Security and Privacy Assurance Considerations in Cloud Computing for Health Insurance Providers. International Journal of Monitoring and Surveillance Technologies Research (IJMSTR), 2017. 5(4): p. 1-22.

42. Almusaylim, Z. A., & Jhanjhi, N. Z. (2020). Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. Wireless Personal Communications, 111(1), 541-564.

43. Z. A. Almusaylim, N. Zaman and L. T. Jung, "Proposing A Data Privacy Aware Protocol for Roadside Accident Video Reporting Service Using 5G In Vehicular Cloud Networks Environment," 2018 4th International Conference on Computer and Information Sciences (ICCOINS), Kuala Lumpur, 2018, pp. 1-5, doi: 10.1109/ICCOINS.2018.8510588.

44. D. A. Shafiq, N. Jhanjhi and A. Abdullah, "Proposing A Load Balancing Algorithm For The Optimization Of Cloud Computing Applications," 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), Karachi, Pakistan, 2019, pp. 1-6, doi: 10.1109/MACS48846.2019.9024785.

45. Natarajan, B., Obaidat, M.S., Sadoun, B., Manoharan, R., Ramachandran, S. and Velusamy, N., 2020. New Clustering-Based Semantic Service Selection and User Preferential Model. IEEE Systems Journal. DOI: 10.1109/JSYST.2020.3025407.

46. Nataraj, S.K., Al-Turjman, F., Adom, A.H., Sitharthan, R., Rajesh, M. and Kumar, R., 2020. Intelligent Robotic Chair with Thought Control and Communication Aid Using Higher Order Spectra Band Features. IEEE Sensors Journal, DOI: 10.1109/JSEN.2020.3020971.

47. Babu, R.G., Obaidat, M.S., Amudha, V., Manoharan, R. and Sitharthan, R., 2020. Comparative analysis of distributive linear and non-linear optimised spectrum sensing clustering techniques in cognitive radio network systems. IET Networks, DOI: 10.1049/iet-net.2020.0122.

48. Sitharthan, R., Yuvaraj, S., Padmanabhan, S., Holm-Nielsen, J.B., Sujith, M., Rajesh, M., Prabaharan, N. and Vengatesan, K., 2021. Piezoelectric energy harvester converting wind aerodynamic energy into electrical energy for microelectronic application. IET Renewable Power Generation, DOI: 10.1049/rgp.2.12119.

49. Sitharthan, R., Sujatha Krishnamoorthy, Padmanaban Sanjeevikumar, Jens Bo Holm-Nielsen, R. Raja Singh, and M. Rajesh. "Torque ripple minimization of PMSM using an adaptive Elman neural network-controlled feedback linearization-based direct torque control strategy." International Transactions on Electrical Energy Systems 31, no. 1 (2021): e12685. DOI: 10.1002/2050-7038.12685.