WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Data Integrity Attacks in Cloud Computing: A Review of Identifying and Protecting Techniques

***Durga Venkata Sowmya Kaja[1], Yasmin Fatima[2] and Akalanka B. Mailewa[3, *]***

[1]Department of Information Systems, St. Cloud State University, St. Cloud, Minnesota, USA
*durgavenkata.kaja@go.stcloudstate.edu*

[2]Department of Information Systems, St. Cloud State University, St. Cloud, Minnesota, USA
*yfatima@go.stcloudstate.edu*

[3]Department of Computer Science and Information Technology, St.Cloud State University,St. Cloud, Minnesota, USA
*amailewa@stcloudstate.edu*

DOI: https://doi.org/10.55248/gengpi.2022.3.2.8

A B S T R A C T

Cloud computing is growing tremendously in recent years. Many organizations are switching their traditional computing model to a cloud based because of its low cost and pay-as-you-go manner. Although Cloud Service Provider (CSP) ensures that the data stored in their remote cloud server will be intact and secure. But there are many data integrity issues exist that needed to be addressed. In Cloud environment, lack of data integrity is a major concern. In this paper, we have surveyed several past studies which identifies the issues related to the cloud data storage security such as data theft, unavailability, and data breach of cloud server data. We have also provided a detailed analysis of types of data integrity attacks and their mitigation techniques.

Keywords: Data Integrity,Cloud Computing, IDS/IPS,Attack, Security, Vulnerabilities

## 1. Introduction (Cloud Computing, Data Integrity)

With the advancement of technology in the past several years, cloud computing has changed the working procedure of organizations by transferring their workload off premises. Cloud computing provides cost-effective and flexible delivery of IT services and resources including database, bandwidth, software, servers, storage, networking, etc. over the internet [1] [2].

Today this new technology is very popular that academic researchers and industries are taking interest in it [3]. Managing private data center or having large secondary storage is out of budget for many organizations. Cloud storage is the best option for such organizations because of its flexible service model [2]. There are 3 Cloud storage model are offered as shown in the figure 1:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

* *Corresponding Author: Akalanka B. Mailewa*
E-mail address: amailewa@stcloudstate.edu

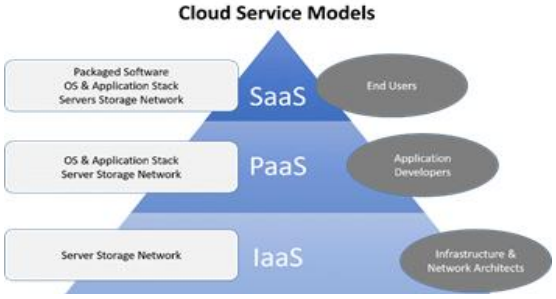


Figure 1. Cloud Service Models [4]

Despite the numerous Cloud computing benefits [5], it comes with several technical and security obstacles such as data integrity, confidentiality, and privacy. Once the user or organization store their data or information to the cloud storage, they lost the control of their confidential data [6]. The cloud service provider (CSP) must assure its customers that their data is kept safe from alteration and corruption by using different mechanisms [7]. The cloud service provider (CSP) is accountable and restricted by the Service Level Agreement (SLA) to guarantee the information security but it does not ensure the 100% data integrity.

There are multiple data integrity issues that can embarrass cloud service provider and becomes user's nightmare. For example, information can be manipulated intentionally or accidently with malicious activity, one can take advantage of any vulnerability exist in shared multi-tenant model and damage other user's data, data backup failure, data leakage etc. [2].


Figure 2. Importance of Data Integrity [2]

The International Data Corporation (IDC) survey showed that in cloud computing security is the biggest challenge [8]. There is a critical need to address data integrity verification and privacy preserving issues in cloud environment [9], [10], [5]. In this survey paper, we first discuss the previous research work that has been done on data integrity issues in cloud computing. Later, we will discuss in detail about the possible data integrity attack in cloud computing and mechanisms used to detect and prevent them.

## 2. Background and Related Work

### 2.1. Related Work

NareshVurukonda and B.Thirumala Rao [11] have done a research to identify the cloud security issues like data storage, access control and identity management. They have also suggested few solutions to the issues [12]. Ayesha Malik and Muhammad MohsinNazir [13] have defined a security architecture for cloud service providers to protect user's confidential and sensitive information. They have also described in their research different cloud service models and their characteristics, etc. [12]. Yunchuan Sun, Junsheng Zhang, YongpingXiong, and Guangyu Zhu [14] have studied different security solutions for data protection and storage security in cloud computing. They have done an important research analysis of existing mechanisms used for information security [12]. Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos [15] have reviewed several security problems of cloud computing. Their research included the recent cloud security solutions and mechanisms used for cloud security issues [12]. Sultan Aldossary and William Allen [16] have studied the issues of cloud data storage and its solutions. The research consists of issues of data integrity, confidentiality, availability, and virtualization. They have also listed several threats on cloud computing [12].

### 2.2.Background

US Government data breach in 2020, a serious data breach has been occurred to the US federal, state government which effected 1000's of organizations globally. This is considered as a major cyber-attack for the US government. The attackers attacked on VMware, Microsoft, and supply chain attack on SolarWinds's Orion Software. Which is a Microsoft windows application [17]. This is one of the most common software used in the government and industry. Another such a critical incidence is the Capital One attack in 2019 March 22 and 23 [18], a sever data breach have been occurred where more

than 100 million customers from 2005 till 2019, data got hacked and an immediate warning message have be send to all the users a head by informing that hacker had broken into the servers. Finally, they have detected the breach in June.

## 3. Cloud Data Storage Challenges & Issues

The main disadvantage of cloud computing is that once the data is stored on the cloud storage, the user lost the control over it. Instead cloud service providers (CSPs) hold complete control over the information stored in the cloud data centers. The CSP can modify, destroy, or copy data without the knowledge of the user. Due to lack of control over stored sensitive data, this leads to biggest concerns of data integrity issues. Although cloud computing is lower in cost and require less resource management, but still, it has severe data security, privacy, and integrity threats. Due to multi-tenancy architecture, the resource which assigned to one user can be assigned to the other user sooner or later. A malicious user can exploit a vulnerability in resource pooling system and uses malicious code to recover previous user's confidential data. Improper sanitization of the disk may lead to risk the stored data in multi-tenant cloud.Accidental or intentional data backup disasters can result in unavailability of the data. Security mechanisms should be used prevent tampering of data and unauthorized access to the cloud environment [11].

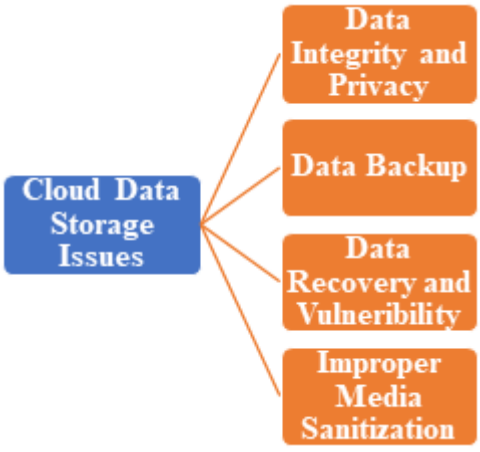


Figure 3. Cloud Data Storage Issues [11]

Today, some organizations are offering competitive rates, quick and secure IT solutions to stay in the race. If companies keep their data on their own servers, it costs them a lot for maintenance, security, employment, and space, etc. After years of research, IT companies has found a solution, to keep the company's data at a lower cost, accessible and available to everyone over the network using cloud computing [19] [7]. Below we have discussed few advantages and challengesof cloud computing:

1. **Cost Effective**
   By using Pay-as you go Cloud model reduces the maintenance cost, personal training cost, security cost, operational cost, and software licensing cost.

2. **Time and Flexibility**
   Using cloud storage, you can easily access data from anywhere any time through internet. This can make people work on the same project at the same time globally. No time is needed to spend in management and maintenance.

3. **Compatibility**
   Cloud makes it feasible compatibility documents and between different operating systems.

4. **Back-up and Restore Data**
   It is easy to restore and backup from the cloud once the information is stored in the cloud. Like the benefits mentioned above, cloud computing has also several disadvantages, discussed below:

5. **Internet Connectivity**
   Even if the cloud service provider is offering the best quality cloud service to its customer, if the internet connection is down, one cannot access the data until it is back on. The longer the internet connection is lost, the more cost the customer must face.

6. **Data Integrity**
   It is the biggest concern for customers, which their data is nor corrupted, altered or deleted intentionally or accidently.

7. **Data Confidentiality and Privacy**
   It is important to keep the confidential and personal data of the customer safe. But once the data is stored in the external servers, its customer's main concern that who can access that data?

8. **Data Location**
In cloud computing the cloud server's Physical location, where of the data is stored is unknown. These details are not transparent to the customer. The servers might be in different country [7].

## 4. Types of Data Integrity Attacks

This section introduces some data integrity attacks related to the cloud computing.

1. **Unauthorized Access**
In this attack the user will not be able to Access their files or data and the data will be modified without any control. This can happen wither from inside or outside of the organization of the security in cloud [20]. This is the most serious attack once this is happened, then the data breach will happen by using the old equipment and reusing the drivers [2].

2. **Data Lock-in**
In the cloud there is no rule or conditions on how the data is stored which depends on the Cloud Storage Provider (CSP) [20]. Usually, the data will be scattered across the server and systems. The corporations are not supposed to move from one provider to another prover as this man leas to loss of the user's data and cause problems from the front side. The servers of the CSP also should be stable if not there is a chance of data loss [2].

3. **Security Against Internal and External Attacks**
The risk of attack will be increased when the user leaves the system without logging it off. Some other person might open the system and do some malicious work which might expose to internal and external attacks [20]. The user's data will be insecure on the CSP end. In addition to this always encrypting data will protect the data confidentiality [2].

4. **SQL Injection Attack**
This is one of the most used and common web-based attack. This needs a web application that uses a database. When the SQL query is generated on the web application and this is sent to the database and the query is executed on the database then the relevant data is returned to the application. This is what generally happens. This attack happens when the malicious string or data is passed through the query, and does something on the system which is not ideally supposed to do so [21].

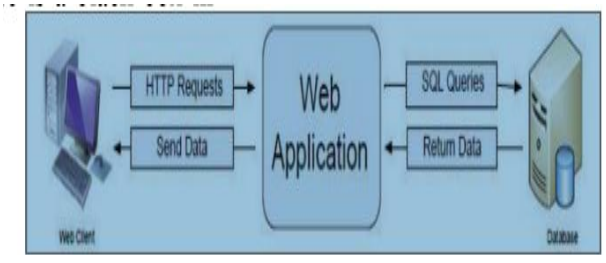


Figure 4. SQL injection attack process [22]

5. **Man in the Middle Attack (MiMA)**
The insufficient encryptions can make users vulnerable to man in the middle attack which is an indirect one [6]. TLS a cryptographic protocol allows a client server application [23] in order to prevent eavesdropping from any sensitive information that is happening on HTTPS which makes use of TLS. If a person access to the unknown network and do his work in HTTPs, the attacker who is acting as a middleman, will then take advantage by grabbing all the sensitive data through HTTPS packets. Few variations of MiMA are as follows:
   - Wrapping Attack
     The attacker tries to copy the credentials of the user by SOAP messages [24] where it is set as a mediator between the server and the browser.
   - Flooding Attack
     Here a continuous flow of requests is been passed through the servers where the employee will not be able to focus on the problem and sometimes this will lead to the system crash.
   - Internet Attack
     This deals with the data theft which is carried out through the SOAP messages encryption. When the internet LAN/WAN gets attack all the systems which are connected to that LAN/WAN will be attacked. Here the transparency will be affected.
   - SSL (Secure Socket Layer) Attack
     This is the defense tool which is kept in between the server and the user where the attacker can easily rob the information and it is categorized into various forms.

6. **DDOS Attack**
This causes huge damage to the resources and access the data of the user. "When there is a flood of requests passed through the system and HTTP is facing a serious threat to the resource centers" [25]. This is the most serious attack on today's Internet cloud environment. This attack cannot be solved completely as there are no sufficient resources in the client server [26]. But there are some mitigation techniques where the risk can be reduced.

7. **Authentication Attacks**
Few authentication attacks:
   - Replay Attack

This attack happens when an unknown person had a look on the data traffics, he then sends the communication data to its place, as an original sender. To prevent this attack, we need to implement the timestamps and sequence numbers [27].

- Brute Force Attack or Dictionary Attack
  This is the basic attack where the attacker will try all the combinations of the password to access the data of the users. The more length of the password the more time it will take for the user to hack/attack to guess the correct one [28].
- Phishing Attack
  This is about on how the attacker tries all the possible ways of attacking the victim by finding all the combinations of the code and passwords. The more complex the code is, the more time will be taken for the attacker to find it out [29].

8. **Tag forgery Attack**
   This attack takes place if the untrusted seller who cheats on their customers by showing a wrong barcode. If the customer scans this one on their devices, there he gets to access all the sensitive data which leads to the possible risks to cheating and privacy leakage [30].

9. **Timeliness Attack**
   When a project is given in a company, it does have deadline/time limit. If the team is very active and completes the work before the deadline will they be able to submit to the manager? If this attack occurs, the system will not be able to submit the project to their manager before the deal line. This will lead to some problems [30].

10. **Roll back Attack**
    This attack always takes place when the during the update process. If the system is updated with some new software's, still the provider provides the oldest software. This will lead to the data loss and crashes. Sometimes this will also lead to the loss of company's reputation. Roll back also occurs without proper deleting of the user's old data and updating the system with the new version [30].

11. **Byzantine Attack**
    In this attack takes place in the various parts of the cloud computing by stopping or crashing the systems. This will happen when the request is not passed through the system correctly [30].

12. **Domain Name System (DNS) Attack**
    DNS will resolve the domain names to IP addresses which works as a phone number. It is a query response protocol. This attack happens when your system gets attacked with some malicious software, here is the explanation of that. When you type www.google.com in your search bar, this link is translated into an IP address and sends query to a server. So, what every you give in the address bar, you will not be able to see the desired one instead some other website will be opened. Whenever the unknow webpage opens, the attacker will be easily able to access the personal information used in the servers [31].

13. **Sniffer Attacks**
    When a person clicks some SOAP messages or links on the browser, then this attack will be happening. Once the clicked link is activated; program will capture the flow of packets in the network and gets access to the personal data of the users like passwords, bank account details etc. which is not encrypted [32] [21].

## 5. Mechanisms Used for Detecting & Preventing Data Integrity Attacks on Cloud Environment

As discussed above, there are numerous threats and vulnerabilities exists, which can exploit the data integrity of data stored in the Cloud storage. An attacker can be anyone from owner to the malicious user or untrusted third party to the CSP. There are several mechanism and schemes have been proposed for protecting the data possession and the data integrity in the Cloud computing environment. Below are few mechanisms and schemes we have surveyed from past researches [30].

1. **Mitigation of Tag Forgery and Data Leakage Attack**
   If the CSP attempts to cheat the user by using fraudulent data tags, the user might now know and get victimized. To prevent this attack, there is a scheme proposed by Yun Zhu et.al [33] known as Cooperative Provable Data Possession (CPCP) which is used in combination of two other techniques (Homomorphic Verifiable Response and Hash Index Hierarchy), which provides transparent verification of data and strong security. Before the customer forwards the information to the CSP, the customer creates a challenge tag and then forward it to Cloud Service Provider later. They Challenge the Cloud Service Provider by validating the integrity of data with the help of Trusted Third Party (TTP) [30].

2. **Mitigation of Replay and Timeliness Attack**
   To prevent the data integrity from replay and timeliness attack, Jun Feng el .al [34] has proposed a Non-Repudiation (NR) protocol. By using this protocol user can abort an execution when the other party does not respond. The evidences from data Originator and the data Recipient are encrypted using the receiver public key by the sender. Then a sequence number and a random number is also added to the sender's signature, which is increased in each process to avoid the replay attack. Additionally, timestamp [34] is also added to this protocol, to prevent from timeliness attack, where the process ends after the time limit [30].

3. **Mitigation of Roll-Back Attack**
   In this proposed scheme, the roll back attack in the cloud environment is protected by implementing Merkle Hash Tree Method [35] [36]. In this method the data block tag and its counter value are get updated, whenever a new data is updated. If an attacker wants to modify the data, the counter value will also change. Data integrity can be verified using this method [34].

4. **Mitigation of Byzantine Failure and Malicious Data Attack**
   A cryptosystem HAIL(High Availability and Integrity Layer) Protocol is proposed by Browers el.al [37]. This protocol ensures that user data is stored intact and retrievable securely from servers. To provide redundancies and make sure that the data is available if the server is misbehaving, Erasure correcting code is used for file distribution. This prevents the Byzantine attacks and malicious data attack [30].

**5. Protecting Data Integrity Using Encryption**

Data encryption is considered a better solution to protect the data in the cloud environment. Data should be encrypted before storing it to the cloud server, this will make the data unusable. Hash value of the data should also be calculated before storing it to the cloud server. This will ensure that data has not been modified [38].

**6. Provable Data Possession (PDP) Technique**

PDP technique uses the challenge response protocol to verify the integrity of the data stored on the cloud server. In this technique, symmetric encryption, MAC, or any other encryption is used. The file is filled with meta data before storing or sending it to the cloud server. Once the file is sent to the Cloud Service Provider, the user still saves the metadata of the file to verify its integrity. The user then deletes the local copy of file. The user then verifies the proof of server's possession of the file using challenge response protocol [7]. It has two stages: Set-up Stage and Challenge Stage.

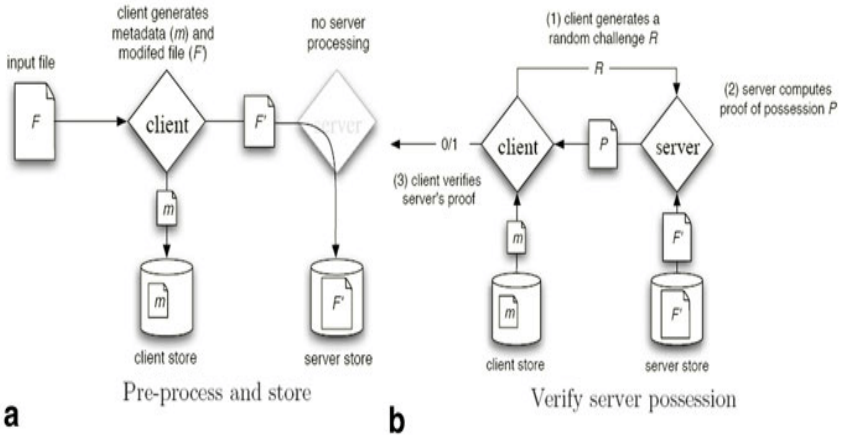


Figure 7. PDP – Setup Stage and Challenge Stage Process [32]

**7. Proofs of Retrievability (POR) Technique**

Proof of Retrievability (POR) technique is used to validate the data remotely, which is stored on the Cloud Service Provider, using the authentication key. In this method data is not needed to be retrieved from the CSP and user also does not store the original copy of the file locally. User stores his file to the CSP along with the authentication key. User can then verifies the integrity of the data using that authentication key, without retrieving back the file from the CSP [7] [[39][40].

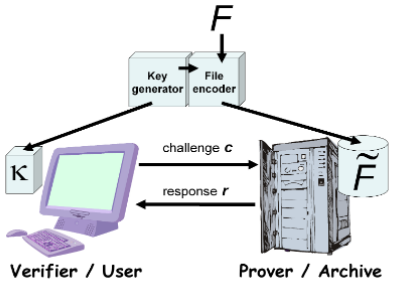


Figure 8. POR – Data Verification Process [40]

## 6. Results

This sections shows the summary of most common data integrityattacks in cloud computing with some preventions techniques suggested by some other authors in various deferent research articles and conference preceding as solutions to those attacks as this article described in previous sections.

Table 1. Summary of Existing Attacks and its Solutions

| S.No | Problem Type | Available Solutions |
|---|---|---|
| 1 | Data Leakage | UserRank method |
| 2 | Denial of Service(DoS) | Encryption,SSL, identity-based encryption, Homomorphic encryption ,Multilevel algorithm, Signature based detection, deep packet inspection |
| 3 | XML Attack | Filter based Approach |
| 4 | Spoofing | Strong Authentication |

| | | |
|---|---|---|
| 5 | Hypervisor–Layer Attack | hardware token |
| 6 | Repudiation | Audit logging, Digital Signature |
| 7 | Data Isolation Failure | Multi-tenant data isolation,<br>Sharing Middleware Scheme |
| 8 | Data Tampering | Hashing/ Digital Signature |
| 9 | DE Duplication Attack | Multilevel Authentication |
| 10 | Intrusion Detection | Anomaly Detection System<br>Statistical Anomaly Detection Systems Data Mining Based Anomaly Detection Systems, Machine Learning Based Anomaly Detection Systems, Adaptive Anomaly Detection Systems |
| 11 | CAPTCHA Breaking | Text Based Captcha ,Audio Captcha ,Puzzle Based Captcha ,Image Based Captcha |
| 12 | Flooding Attack | Digital signatures, Authentication Technology |
| 13 | SQL Injection Attacks | parameterized statements |
| 14 | Cross Site Scripting Attacks | XSS Prevention Rules |
| 15 | Man in the Middle Attack | Strict SSL |
| 16 | Sniffer Attacks | SSH, IPsec |
| 17 | Hopping attacks Cookie Poisoning | Encryption keys |
| 18 | Cross vm side channel attack | XML signatures, Elgamal Encryption |

## 7. Conclusion

In this article we have discussed about few attacks which can be detected by the cloud service provider. A brief note on cloud computing and data integrity including the concepts of introduction to cloud computing and data integrity. This has been discussed with respect to the related work done by the other authors. Many IT companies started adopting to the cloud computing technologies like AWS, Microsoft Azure. Cloud computing is a storage in cloud where every user and employee data is stored. A cloud secure Provider is responsible to ensure the security of the companies' data, where they can store data in various formats and ways. Cloud store is cheaper and faster than data centers. Data Confidentiality and data integrity is the major concern of cloud computing. few mechanisms were discussed for the mitigating the risks to prevent data loss. As a conclusion, the cloud computing need to be designed very sensitively and should think in all aspects of security to make data secure. Data integrity is the wide-open issue in cloud computing and a good opportunity for the research work.

## REFERENCES


[1] S. Nepal, S. Chen, J. Yao, and D. Thilakanathan, "DIaaS: Data Integrity as a Service in the Cloud," in 2011 IEEE 4th International Conference on Cloud Computing, Jul. 2011, pp. 308–315, doi: 10.1109/CLOUD.2011.35.

[2] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Vulnerability prioritization, root cause analysis, and mitigation of secure data analytic framework implemented with mongodb on singularity linux containers." In Proceedings of the 2020 the 4th International Conference on Compute and Data Analysis, pp. 58-66. 2020.

[3] Mailewa, Akalanka, and Jayantha Herath. "Operating systems learning environment with VMware." In The Midwest Instruction and Computing Symposium. Retrieved from http://www. micsymposium. org/mics2014/ProceedingsMICS_2014/mics2014_submission_14. pdf. 2014.

[4] "Types of Cloud Services. Cloud computing has three most common… | by IDM | Medium." https://medium.com/@IDMdatasecurity/types-of-cloud-services-b54e5b574f6 (accessed Feb. 05, 2021).

[5] M. F. Al-Jaberi and A. Zainal, "Data integrity and privacy model in cloud computing," in 2014 International Symposium on Biometrics and Security Technologies (ISBAST), Aug. 2014, pp. 280–284, doi: 10.1109/ISBAST.2014.7013135.

[6] Y. Chen, L. Li, and Z. Chen, "An Approach to Verifying Data Integrity for Cloud Storage," in 2017 13th International Conference on Computational Intelligence and Security (CIS), Dec. 2017, pp. 582–585, doi: 10.1109/CIS.2017.00135.

[7] K. N. Sevis and E. Seker, "Survey on Data Integrity in Cloud," in 2016 IEEE 3rd International Conference on
Cyber Security and Cloud Computing (CSCloud), Jun. 2016, pp. 167–171, doi: 10.1109/CSCloud.2016.35.

[8] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 42–57, Jan. 2013, doi: 10.1016/j.jnca.2012.05.003.

[9] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Dynamic & portable vulnerability assessment testbed with Linux containers to ensure the security of MongoDB in Singularity LXCs." In Companion Conference of the Supercomputing-2018 (SC18). 2018.

[10]Akintaro, Mojolaoluwa, Teddy Pare, and Akalanka Mailewa Dissanayaka. "Darknet and black market activities against the cybersecurity: a survey." In The Midwest Instruction and Computing Symposium.(MICS), North Dakota State University, Fargo, ND. 2019.

[11]N. vurukonda and B. T. Rao, "A Study on Data Storage Security Issues in Cloud Computing," Procedia Comput. Sci., vol. 92, pp. 128–135, Jan. 2016, doi: 10.1016/j.procs.2016.07.335.

[12]S. Rajeswari and R. Kalaiselvi, "Survey of data and storage security in cloud computing," in 2017 IEEE International Conference on Circuits and Systems (ICCS), Dec. 2017, pp. 76–81, doi: 10.1109/ICCS1.2017.8325966.

[13]A. Malik and M. M. Nazir, “2012). Security Framework for Cloud Computing Environment: A Review.”
[14]Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, “Data Security and Privacy in Cloud Computing,” Int. J. Distrib. Sens. Netw., vol. 10, no. 7, p. 190903, Jul. 2014, doi: 10.1155/2014/190903.
[15]M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” Inf. Sci., vol. 305, pp. 357–383, Jun. 2015, doi: 10.1016/j.ins.2015.01.025.
[16]S. Aldossary and W. Allen, “Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions,” Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 4, 2016, doi: 10.14569/IJACSA.2016.070464.
[17]“2020 United States federal government data breach,” Wikipedia. Feb. 02, 2021, Accessed: Feb. 05, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=2020_United_States_federal_government_data_breach&oldid=1004415192.
[18]“List of data breaches,” Wikipedia. Jan. 18, 2021, Accessed: Feb. 07, 2021. [Online]. Available: https://en.wikipedia.org/w/index.php?title=List_of_data_breaches&oldid=1001210845.
[19] Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Security assurance of MongoDB in singularity LXCs: an elastic and convenient testbed using Linux containers to explore vulnerabilities." Cluster Computing 23, no. 3 (2020): 1955-1971.
[20]A. Jyoti, M. Shrimali, S. Tiwari, and H. P. Singh, “Cloud computing using load balancing and service broker policy for IT service: a taxonomy and survey,” J. Ambient Intell. Humaniz. Comput., vol. 11, no. 11, pp. 4785–4814, Nov. 2020, doi: 10.1007/s12652-020-01747-z.
[21]S. Sudalai and S. S., “A Survey on Cloud Security Issues and Challenges with Possible MeasuresA Survey on Cloud Security Issues and Challenges with Possible Measures,” Apr. 2016.
[22]B. Shunmugapriya and D. B. Paramasivan, “Protection Against SQL Injection Attack in Cloud Computing,” Int. J. Eng. Res. Technol., vol. 9, no. 2, Feb. 2020, doi: http://dx.doi.org/10.17577/IJERTV9IS020273.
[23]H. Mohapatra, “Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System,” Int. J. Emerg. Trends Eng. Res., vol. 8, no. 5, pp. 1503–1510, May 2020, doi: 10.30534/ijeter/2020/05852020.
[24]C. Bagyalakshmi and E. Samundeeswari, “DDoS Attack Classification on Cloud Environment Using Machine Learning Techniques with Different Feature Selection Methods,” Int. J. Adv. Trends Comput. Sci. Eng., vol. 9, pp. 7301–7308, Nov. 2020, doi: 10.30534/ijatcse/2020/60952020.
[25]G. Somani, M. S. Gaur, and D. Sanghi, “DDoS Protection and Security Assurance in Cloud,” in Guide to Security Assurance for Cloud Computing, S. Y. Zhu, R. Hill, and M. Trovati, Eds. Cham: Springer International Publishing, 2015, pp. 171–191.
[26]Mazi, Hilary, FokaNgniteyoArsene, and Akalanka Mailewa Dissanayaka. "The influence of black market activities through dark web on the economy: a survey." In The Midwest Instruction and Computing Symposium.(MICS), Milwaukee School of Engineering and Northwestern Mutual, Milwaukee, Wisconsin. 2020.
[27] Lai, Cheng-I., Alberto Abad, Korin Richmond, Junichi Yamagishi, NajimDehak, and Simon King. "Attentive filtering networks for audio replay attack detection." In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6316-6320. IEEE, 2019.
[28]Shetty, Roshan Ramprasad, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. "Secure NoSQL based medical data processing and retrieval: the exposome project." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 99-105. 2017.
[29] Mailewa Dissanayaka, Akalanka, Roshan Ramprasad Shetty, Samip Kothari, Susan Mengel, Lisa Gittner, and Ravi Vadapalli. "A review of MongoDB and singularity container security in regards to hipaa regulations." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 91-97. 2017.
[30]“Survey on various data integrity attacks in cloud environment and the solutions - IEEE Conference Publication.” https://ieeexplore.ieee.org/abstract/document/6528889 (accessed Feb. 05, 2021).
[31]Thapa, Suman, and Akalanka Mailewa. "The Role of Intrusion Detection/Prevention Systems in Modern Computer Networks: A Review." In Conference: Midwest Instruction and Computing Symposium (MICS), vol. 53, pp. 1-14. 2020.
[32]S. Sudalai and S. S., A Survey on Cloud Security Issues and Challenges with Possible MeasuresA Survey on Cloud Security Issues and Challenges with Possible Measures. 2016.
[33]Y. Zhu, H. Hu, G. Ahn, and M. Yu, “Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231–2244, Dec. 2012, doi: 10.1109/TPDS.2012.66.
[34]J. Feng, Y. Chen, W. Ku, and P. Liu, “Analysis of Integrity Vulnerabilities and a Non-repudiation Protocol for Cloud Data Storage Platforms,” in 2010 39th International Conference on Parallel Processing Workshops, Sep. 2010, pp. 251–258, doi: 10.1109/ICPPW.2010.42.
[35]J. Feng, Y. Chen, D. H. Summerville, and K. Hwang, “Fair Non-repudiation Framework for Cloud Storage: Part II,” in Cloud Computing for Enterprise Architectures, Z. Mahmood and R. Hill, Eds. London: Springer, 2011, pp. 283–300.
[36]J. Feng, Y. Chen, D. Summerville, W. Ku, and Z. Su, “Enhancing cloud storage security against roll-back attacks with a new fair multi-party non-repudiation protocol,” in 2011 IEEE Consumer Communications and Networking Conference (CCNC), Jan. 2011, pp. 521–522, doi: 10.1109/CCNC.2011.5766528.
[37]H. Lin and W. Tzeng, “A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 995–1003, Jun. 2012, doi: 10.1109/TPDS.2011.252.
[38]R. V. Rao and K. Selvamani, “Data Security Challenges and Its Solutions in Cloud Computing,” Procedia Comput. Sci., vol. 48, pp. 204–209, Jan. 2015, doi: 10.1016/j.procs.2015.04.171.
[39]M. S. Giri, B. Gaur, and D. Tomar, A Survey on Data Integrity Techniques in Cloud Computing.
[40] Mailewa, Akalanka, Jayantha Herath, and SusanthaHerath. "A survey of effective and efficient software testing." In The Midwest Instruction and Computing Symposium.(MICS), Grand Forks, ND. 2015.
[41]A. Juels and B. S. Kaliski, “Pors: proofs of retrievability for large files,” in Proceedings of the 14th ACM conference on Computer and communications security, New York, NY, USA, Oct. 2007, pp. 584–597, doi: 10.1145/1315245.1315317.