International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7460
***Article Received**: 19 May 2023 **Revised:** 18 July 2023 **Accepted:** 04 August 2023*

Assessment of Security Trepidation in Cloud Applications with Enhanced Encryption Algorithms

Thotakuri Srilekha[1], Vijay Bhanu S[2], Niranjan P[3]
[1]Research Scholar, Dept. of Computer Science & Engg., Annamalai University
srilekha.522@gmail.com
[2]Research Supervisor, Dept. of Computer Science & Engg., Annamalai University
Svbhanu22@gmail.com
[3] Research Co-Supervisor, Dept. of Computer Science & Engg., Annamalai University
pnr.cse@kitsw.ac.in

Abstract— To alleviate crank in routine process in IT related work environment we are maintaining information's in cloud storage even though we affected by pandemic and other natural disaster still can able to access data by avoiding degrade in target process. Members who posses account in cloud no need to have separate high end configuration devices because even less configured devices could connect to cloud and make use of all services using virtual machine. Applications belong to cloud storage intimidated in the aspect of safety. This paper reviews the various security related issues and its causes along with latest cloud security attacks. We discussed about different technology to protect information resides in cloud and analyzed different enhanced algorithm for encryption for securing the data in cloud due to surge use of devices interacting cloud services.

Keywords- Cloud Applications; Cloud Encryption; Cloud Security; Cloud Tool

I. INTRODUCTION

With the remarkable development of distributed computing, cloud specialist organizations will offer exceptional organization IT administrations and an ever-increasing number of nearby administrations are being moved to cloud stages. Cloud storage became unavoidable now a day due to the nature of holding others data and providing the same whenever they required. Be that as it may, the complexity of the cloud foundation is becoming progressively because of the remarkable ascent in cloud size and cloud clients, causing more potential assault vectors and gadget weaknesses [1].

They are raising another worldview of administrations as web innovation and huge information distributed computing extend. The expanding number of online exercises can be interconnected through these new administrations. The Internet of Things (IoT) is progressively developing the capacities of the cloud, as per a Cisco review. The three essential conveyance models, after a few preliminaries, are IaaS, PaaS, and SaaS. There are as yet many assistance models accessible as per their arrangement and administration giving capacities, which have prompted the advancement and conveyance models for Anything-as-a-Service [2,3].

To accomplish multi-tenure, the cloud utilizes a virtual world. Computerized machines contain bugs that represent an express danger to cloud suppliers' security and protection. On the web and information movement across the Internet is another component in cloud administrations. The Application Program Interface (API) program and the organization channel contain numerous security weaknesses. Through utilizing the multi-tenure idea, cloud administrations are circulated and divided between various clients [4].

Listening in and satirizing are two sorts of assault that are ordinarily completed on the organization layer. A listening in assault explicitly targets decoded information by getting little information taking parcels. A ridiculing assault is an antagonistic activity that, by making bogus information or ID, professes to be a genuine communicator. A few examinations have as of late endeavored to bring down the danger of listen [5].

Numerous runs of the mill digital assaults are single-run and programmed, with the objective of separating networks, for example, PC infections. As an outcome, the likelihood of achievement of these digital assaults is lower and the danger of location is higher. Adept for information burglary, then again, is time-consistent and profoundly energetic, and normally completed by very much financed aggressors, endeavoring to clandestinely take important information from the objective CSS throughout a significant stretch of time without being identified [6].

A. Cloud Services

Recent days cloud is extending its support towards several industries like information technology, medication

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7460
***Article Received**: 19 May 2023 **Revised:** 18 July 2023 **Accepted:** 04 August 2023*

related services, automobile and other industries to keep their unassailable data in the covered places. The vulnerability is a chance when they reside their information in cloud and retrieving these data from storage. Cloud security threats are possible in limited services to specific industry (private cloud), services to anyone as free public cloud, extended private cloud (Community cloud) and combination of above stated types of cloud (Hybrid cloud). Apart from threatens of security in the above mentioned categories of model we still facing protection problem in security of a code set, the structure of cloud, holding capacity, connection. In the similar fashion we discussed issues of security in reputation, trust lacking, client monitor problem, and authentication in forthcoming chapter [7].

The cloud is extensively used by many organizations and at the same time it is affected by numerous attacks which glitches the strong reflection in security. The security concepts must consider for same tuned with enhancement related to scalability, login credentials', Available information, load balance mechanism and trustable management of resources [8].

II. ANALYSIS

The current action revealed in review trails with recorded assault designs is adjusted by Misuse Detection strategies. Information is acquired from various sources, for example, reports of organization traffic. Prior to moving it to the Detection Engine, the crude information got is first preprocessed and changed into a valuable organization. A choice model that decides if to move the information or produce an alarm dependent on some realized action is executed by the Detection Engine. To recognize the malware recognition parts running on the observed PC, progressed malware programs are keen. They attempt to impair the security instrument or bargain it suddenly and completely on the gadget [9].

It tends to the various security challenges when planning the climate for distributed computing. The order tends to an installed security issue in which virtual machine property represents a few security issues, for example, misconfiguration of Cross-VM assault, and single point disappointment in programmability. In addition, this section additionally centers on the subject of the application stage. The utility help depends on online administrations and applications. In programming frameworks, there are a few lines of code and a few dialects are being made to build an interface that can bring about numerous security weaknesses [10,11].

Server farm innovation requires various frameworks and modules that are regularly comprised of one another. There are both physical and virtualized IT administrations in the server farm. Equipment frameworks comprise of actual IT devices, including organizing frameworks, home registering, workers and hardware. The virtualized IT asset exists over the virtualization layer that the virtualization stage runs and oversees. The essential rules for diminishing the negligible, working and venture expenses of the cloud are particularity and normalization [12].

A gathering of exercises to check whether an individual or a gathering of clients approaches a PC object, for example, an application or a gadget, is the standard of personality the board. Fundamental errands incorporate ID, confirmation, and approval during the check cycle. It has a cover with the entrance control's administration. Character insurance and access control, nonetheless, have diverse central focuses. Personality the executives generally centers on verification, while access control manages approval [13].

The above recuperation work is asset concentrated, and security assets should be set up to achieve this recuperation work, including cash and work. Then again, the cloud safeguard's security assets are regularly insignificant. Accordingly, the cloud safeguard should deal with his security assets productively so when confronting an APT, he can react in a convenient way. Improvement in existing methodology is mandatory in terms of encryption process. [14-15].

A. Recent Threats in Cloud

The Figure 1 represents the cam4 leaks in capacity of server and the same depicted in graph representation to denote issue in the cloud and same to be resolved in strong concrete mechanism [16].

The above figure 1 graph represented the issues of leakage of records in server based system. We have reviewed certain recent incident happened in cloud breaches for references and these incidents forced us to strengthen mechanism to prevent security concern. In the above graph x axis denoted with country name and y axis representing the value of attacks in volume of records with respect to security concern. We observed the security breakages value in peak towards valley and insist us to install better cloud solution software which has strong encryption algorithm and it's essential up gradation. The table 1 given below indicates three major breaches in the world [17-20].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7460
***Article Received**: 19 May 2023 **Revised:** 18 July 2023 **Accepted:** 04 August 2023*

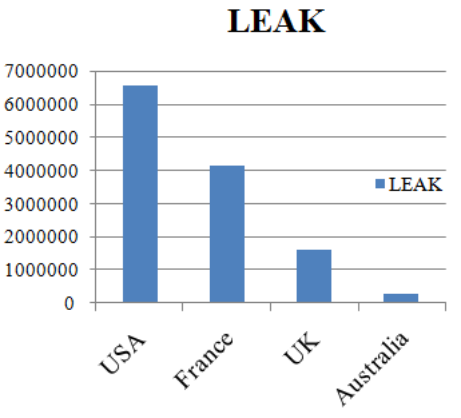

Figure 1. Server Record Leaks

The intention behind the above tabular information insisted to have a great extent of protection against data kept in the internet cloud and necessity to learn software's in the market. We have reviewed few latest tools against malicious action and identification when the data in and out to cloud. Table 3 shown to represent the available software for cloud security, purpose, vulnerability [21].

Table 1: Recent Breaches in Cloud [22-26]

Name	Reason	Lose	Inference
Marriot	Credential Stuffing	Personal Information (Gender, DoB, Linked Account)	Strengthen Employee data access
Slickwraps	Vulnerable remote code execution	Access to customer photos, Billing Shipping address, admin details	Strong audit required for independent security
Antheus Technology	No password protection, Human Error	Exposed 16GB data,81.5 million records, admin login	Strengthen password security

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

III. ENCRYPTION ALGORITHM

To secure users data confidential and integrity when the services retained in cloud existing AES algorithm is not sufficient due to more number of gadgets participation in service. New Enhancement of AES used to protect confidential messages of cloud and concrete setup given to data stored in remote premises. When plain text sizes increased from 16 to 128 bytes the encryption time average calculated and the same taken for evaluating improved Advance Encryption standard. The result shown minor reduction in time process and improved AES used for energy consumption reduction, delay in network dependency and security enhancement [27-29].

Lightweight cryptographic algorithm used for securing data in cloud and its uses block cipher which contains 128 bit and for encryption process they used 128 bit key to resolve complexity while converting plain to cipher change process. To increase complexity they have derived the concept from feistel and architecture of SP taken for attaining above purpose. New methodology is compared with current methodology like DES, blowfish and others by considering the size of block, key, mathematical steps and power. They proved this technique is more suitable for strong level of security and improving security in the process of encryption along with reverse strategy [30-32].

To improve security in terms of small level to sophisticated stage firms combined with blowfish encryption and homographic strategy is used. Homographic used in layer one for getting input text and layer 2 contains blowfish to obtain outcome of encryption process. No decryption involved in homographic without key of private details. Both changes from plain to cipher and reverse are happening in blowfish and dedicated key was used for the purpose of key. The privacy of cloud and security strongly addressed with blowfish. Combination of two different algorithms can be used to give best security in the cloud data and its equivalent services [33-37].

Table 2: Comparison of Encryption Algorithms

Name of the Encryption Algorithm	Size of Key(bits)	Size of block	Security concern
DES	64	64	Yes
AES	128,192,256	128	Yes
BlowFish	32-448	64	Yes

Multi level algorithm of encryption used to eliminate anti-patterns for strengthening security of application joined in the current cloud setup. Here blowfish combined with advanced encryption standard to provide security in cloud services. Multilevel approach considering input as cipher which is retrieved with the coordination of database and the data is being encrypted by AES to obtain primary level of encryption. Further outcome is linked with blowfish implementation to generate next subsequent level of decryption process. So that stringent force of protection can be amendment in the process. Finally generation of file and its access made. Table 2 denotes the comparison of various encryption algorithms and the outcome relevant to interoperable nature and security concern. Major algorithms we considered here are AES, DES and BlowFish [38-40].

.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7460
***Article Received**: 19 May 2023 **Revised:** 18 July 2023 **Accepted:** 04 August 2023*

IV. CLOUD SECURITY TOOLS

The main topic from introduction to above discussion of encryption algorithm usages in cloud implies that we need to have gated protection against cloud storages and its plenty of applications. To consider the intension behind leakages in cloud we have reviewed numerous tools prescribed in Table 3 which implemented by various algorithm of encryption for safeguarding the data according intrusion detection procedure. Each tool are analyzed its prime purpose and the kind of intrusion can be predicted during surveillance of monitoring process. These tools can be in the form of physical components and set of code incorporated with famous cryptographic algorithm.

Table 3: Software Tool for cloud security

Tool Name	Purpose	Vulnerabilities
ACUNETIX	Cloud Web Applications	SQL injection and Cross site scripting
AIRCRACK-NG	IaaS models	Malicious Activity
CAIN & ABEL	Password Recovery, Analyzing encrypted Protocols	Man – in – Middle Attacks, Routing protocols authentication monitoring
ETTERCAP	IP based scanning, MAC based scanning, Functionality ARP	Network analysis protection
JOHN THE RIPPER	Password Testing	Hash Identification
METASPLOIT	IP Address	IP Verification
NMAP	Cloud network scanning	Congestion and Latency
WIRESHARK	Monitoring Cloud	Packet analyzing between cloud providers

From Table 1 and Table 3 we inferred with the importance of software to safeguard leasing data which are maintained in data centre in order to prevent individual organizations and their business at most protection from credential losses.

V. CONCLUSION

Security is a key component to be consider in any kind of emerging applications which indeed a crucial attention towards prevent from the same. IT industries rely on cloud related technology since numerous supports is being given by this technology. The end user of the cloud services is utilizing infrastructure, information and set of code as a service. Many algorithm-based mechanisms are available to protect the data in cloud but still drastic breaches are possible in security. The strong tool is required and the same should be upgraded frequently depends upon new innovations and current problems. Encryption algorithm emphasize security interrelated issues to shield the essential information retained by providers of cloud. Advancement in these algorithms still upgraded since several intruders can disclose information for their manipulation or yield defame to cloud providers. Thus, we have summarized few improved encryption algorithms and its highlights even more number of devices are being attached to cloud.

REFERENCES

[1] Suthir S and Janakiraman S, “SNT Algorithm and DCS Protocols coalesced a Contemporary Hasty File Sharing with Network Coding Influence”, Journal of Engineering Research, Vol. 6, Issue 3, pp.54-69, 2018.

[2] Prabhu et.al., “Privacy preserving steganography based biometric authentication system for cloud computing environment”, Measurement: Sensors Journal, Vol 24, Dec 2022, https://doi.org/10.1016/j.measen.2022.100511

[3] Thyagarajan C, et.al., “A Typical Analysis and Survey on Healthcare Cyber Security” in Int. Journal of Scientific and Technology Research, Vol.9, Issue.3, pp.3267-3270, 2020, ISSN: 2277-8616

[4] Saurabh Singh, Young-Sik Jeong, Jong Hyuk Park, A survey on cloud computing security: Issues, threats, and solutions, Journal of Network and Computer Applications, Volume 75,2016,Pages 200-222,ISSN 1084-8045,https://doi.org/10.1016/j.jnca.2016.09.002.

[5] Subashini, and Veeraruna Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of network and computer applications, Vol. 34, Issue 1, pp. 1-11, 2011.

[6] Ashish Singh, Kakali Chatterjee, Cloud security issues and challenges: A survey, Journal of Network and Computer Applications,Volume 79,2017,Pages 88-115,ISSN 1084-8045.

[7] Krishnamurthy A, Kumar B,” The Repaschine: A Robot to Analyze and Repair Roads Using Cutting-Edge Technologies, EAI/Springer Innovations in Communication and Computing, pp. 249–254, 2021, https://doi.org/10.1007/978-3-030-49795-8_24

[8] P. Li and X. Yang, "On Dynamic Recovery of Cloud Storage System Under Advanced Persistent Threats," in IEEE Access, vol. 7, pp. 103556-103569, 2019, doi: 10.1109/ACCESS.2019.2932020.

[9] Vijayaraj, N., Arunagiri, S. Demultiplexer design using photonic crystal ring resonator with high quality factor and less footprint for DWDM application. Opt Quant Electron 54, 465 (2022). https://doi.org/10.1007/s11082-022-03817-2

[10] Nivethitha, et.al., “Conceptual approach on smart car parking system for industry 4.0 internet of things assisted networks”, in Measurement: Sensors, Volume 24, December 2022, https://doi.org/10.1016/j.measen.2022.100474

[11] Prabhu D, et.al., “Design of Multiple Share Creation with Optimal Signcryption based Secure Biometric Authentication System for Cloud Environment”,International Journal of Computers and Applns., 2022, 44(11), pp. 1047–1055, https://doi.org/10.1080/1206212X.2022.2103890

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7460
***Article Received**: 19 May 2023 **Revised:** 18 July 2023 **Accepted:** 04 August 2023*

[12] Y. Liu, Y. Zhang, J. Ling, and Z. Liu, ''Secure and fine-grained access control one-health care records in mobile cloud computing, ''FutureGener. Comput. Syst., vol. 78, pp. 1020–1026, Jan. 2018.

[13] Vijayalakshmi C, et.al., "A survey on solving dilemmas of adapting blockchain in different applications" 1st International Conference on Recent Advances in Manufacturing Engineering Research, ICRAMER 2021, AIP Conference Proceedings, 2460, 070011 (2022); https://doi.org/10.1063/5.0095701

[14] Nivethitha.V, M.Bhavithra – "Real Time Sectionalization of Enhanced Sharpness Video using FPGA" in Elysium Journal of Engineering Research and Management, Volume 3, Issue 4, Page No. 23 - 26, August-2016. ISSN: 2347-4408.

[15] Zhang, Y., Juels, A., Reiter, M.K., Ristenpart, T., 2012. Cross-vm side channels and their use to extract private keys. In: Proceedings of the ACM conference on Computer and communications security. ACM, pp. 305–316.

[16] Sangeetha SKB, Vanithadevi V, Rathika SKB (2018) Enhancing cloud security through efficient fragment-based encryption. Int J Pure Appl Math 118(18):2425–2436

[17] Dr. Ramalingam Sugumar and K. Arul Marie Joycee, "FEDSACE: a framework for enhanced user data security algorithms in cloud computing environment," International Journal on Future Revolution in Computer Science & Communication Engineering, vol. 4, no. 3, 2018.

[18] Li Wei, Machine Learning in Fraudulent E-commerce Review Detection , Machine Learning Applications Conference Proceedings, Vol 2 2022.

[19] Nivethitha V, Sivasubramanian A "Intensification and Interpretation of Performance in 5G adopting Millimeter Wave: A Survey & Future Research Direction", International Arab Journal of Information Technology, Volume 20, Issue Number 4, July 2023.

[20] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, ''Cloud-trust—A security assessment model for infrastructure as a service cloud,'' IEEE Trans. Cloud Comput., vol. 5, no. 3, pp. 523–536, Jul./Sep. 2017.

[21] H. A. Al Essa and A. S. Ashoor, "Enhancing performance of AES algorithm using concurrency and multithreading," ARPN Journal of Engineering and Applied Sciences, vol. 14, no. 11, 2019.

[22] Suthir S, Janakiraman S, Srividya M and Anusha N, "A contemporary network security technique using smokescreen SSL in huddle network server", 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), 2016, pp 673-676. https://doi.org/10.1109/AEEICB.2016.7538376

[23] Suthir S and Janakiraman S, "A Contemporary hasty file sharing system in network", 2018, http://hdl.handle.net/10603/231589

[24] C Jayashri, et.al. July-2017. "Big Data Transfers through Dynamic and Load Balanced Flow on Cloud Networks", in IEEE Xplore, ISBN: 978-1-5090-5434-3. DOI: 10.1109/AEEICB.2016.7538376

[25] Suthir S & Dr.S.Janakiraman, 2013. "Contemporary and efficient shared area network in Peer-to-Peer Communication", in IEEE Xplore, ISBN: 978--14673-2758-9. DOI: 10.1109/ICRCC.2012.6450544

[26] B. Allen, J. Bresnahan, L. Childers, I. Foster, G. Kandaswamy, R. Kettimuthu, J.Kordas, M. Link, S. Martin, K. Pickett, and S. Tuecke, "Software as a service for data scientists," Commun. ACM, vol. 55, no. 2, pp. 81–88, 2012.

[27] Suthir S & Dr.S.Janakiraman, May-2017. "A Survey of Fast File Sharing System in Network" in International Journal of Engineering Development and Research, Vol. 5, Issue: 2, May 2017, pp. 1298-1304, ISSN: 2321-9939, https://zenodo.org/record/583721

[28] Ijaz Ahmad Awan, Muhammad Shiraz, Muhammad Usman Hashmi, Qaisar Shaheen, Rizwan Akhtar, Allah Ditta, "Secure Framework Enhancing AES Algorithm in Cloud Computing", Security and Communication Networks, vol. 2020, Article ID 8863345, 16 pages, 2020. https://doi.org/10.1155/2020/8863345

[29] G.S. Mahmood, J. H. Dong, and B. A. rahman Jaleel, "Achieving an effective, confidentiality and integrity of data in cloud computing," International Journal of Network Security, vol. 21, no. 2, pp. 326–332, 2019.

[30] Li Wei, Machine Learning in Fraudulent E-commerce Review Detection , Machine Learning Applications Conference Proceedings, Vol 2 2022.

[31] A. Firman, A. N. Hidayanto, and P. Harjanto, "Critical components of security framework for cloud computing community: a systematic literature review," International Journal of Pure and Applied Mathematics, vol. 118, no. 18, pp. 3345–3358, 2018.

[32] Fursan Thabit, Associted Prof. Sharaf Alhomdy, Abdulrazzaq H.A. Al-Ahdal, Prof. Jagtap, A New Lightweight Cryptographic Algorithm for Enhancing Data Security In Cloud Computing,Global Transitions Proceedings,2021,ISSN 2666-285X, https://doi.org/10.1016/j.gltp.2021.01.013.

[33] Prof. Virendra Umale. (2020). Design and Analysis of Low Power Dual Edge Triggered Mechanism Flip-Flop Employing Power Gating Methodology. International Journal of New Practices in Management and Engineering, 6(01), 26 - 31. https://doi.org/10.17762/ijnpme.v6i01.53

[34] A. H. A. Al-ahdal, NLBSIT : "A New Lightweight Block Cipher Design for Securing Data in IoT" International Journal of Computer Sciences and Engineering Open Access NLBSIT : A New Lightweight Block Cipher Design for Securing Data in IoT Devices, November, 2020.

[35] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," The Journal of Supercomputing, vol.75, no.10, pp.6663–6682, 2019.

[36] Sajay, K.R., Babu, S.S. & Vijayalakshmi, Y. Enhancing the security of cloud data using hybrid encryption algorithm. J Ambient Intell Human Comput (2019). https://doi.org/10.1007/s12652-019-01403-1

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7460
***Article Received**: 19 May 2023 **Revised:** 18 July 2023 **Accepted:** 04 August 2023*

[37] Z.Z.Cao et.al Joint Static and Dynamic Traffic Scheduling in Data Center Networks. in Proceedings of IEEE INFOCOM 2014, pp.2445-2553.

[38] Xinyi Huang, Shaohua Tang, Jin Li, Xiaofeng Chen, Yang Xiang, Senior Member, IEEE, Mohammad Mehedi Hassan, Member, IEEE, and Abdulhameed Alelaiwi, Member, IEEE "Secure Distributed De Duplication Systems with Improved Reliability" IEEE Transac. on computers, vol. 64, no. 12, December 2015.

[39] Lin Xiang, Xiaohu Ge, Senior Member, IEEE, Cheng-Xiang Wang, Senior Member, IEEE, Frank Y. Li, Senior Member, IEEE, and Frank Reichert, "Energy Efficiency of Cellular Networks Oriented on Spatial Distributions of Traffic Load and Power Consumption" IEEE Trans. wireless communications, vol. 12, no. 3, March 2013.

[40] Utkarsh Gupta1 and Mrs. Shivani Saluja and Mrs. Twinkle Tiwari, Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms, International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, March 2018, pp. 55-61.

[41] Frank Muller, Thijs Veugen, Robbert de Haan, Ronald Cramer "A Framework for Secure Computations with Two Non-Colluding Servers and Multiple Clients, Applied to Recommendations", IEEE transact. on info. Forensics, vol. 10, no. 3, March 2015.

[42] Elumalaivasan et.al.," CBIR- Retreival of Images using Median Vector Algorithm", International Conference on Green Computing, Communication and Conservation of Energy, ICGCE 2013, Proceeding of IEEE XPlore, pp. 1–5, 2013, https://doi.org/10.1109/ICGCE.2013.6823389

[43] Taha Junaid, et.al., "A comparative analysis of transformer-based models for figurative language classification", Computers and Electrical Engineering, vol. 101, July 2022, https://doi.org/10.1016/j.compeleceng.2022.108051