ISSN: 2455 - 5630

International Journal of Scientific Research and Modern Education

Impact Factor 7.137, Special Issue, March 2020 – Conference Proceedings

International Conference on Rise of Disembedded Unilateral Economy: InnoVision in the Era of Deglobalization (KRUPACON 2019) On 8th & 9th November 2019 Organized By

Krupanidhi Group of Institutions, Bangalore, Karnataka

A STUDY ON CLOUD COMPUTING FOR CRYPTOGRAPHY AND STEGANOGRAPHY ALGORITHM

Jissy Thomas* & N. Anuradha**

* Krupanidhi Group of Institutions, Bangalore, Karnataka

** Krupanidhi Degree College, Bangalore, Karnataka

Cite This Article: Jissy Thomas & N. Anuradha, “A Study on Cloud Computing for Cryptography and Steganography Algorithm”, International Journal of Scientific Research and Modern Education, Special Issue, March, Page Number 16-19, 2020.

Abstract:

In the Internet of Things (IoT) and 5G technologies, the cloud computing grid is critical. It provides a platform for the dissemination of big amounts of information effectively. There are also some of authorities and economic institutions. Cloud computing use through government companies a records community communication. However, records management, protection, and privacy are all issues that should be addressed. To build a solid cloud community, privateness is a first-rate subject. Provider and cozy the community's crucial records in First, protection attacks on cloud computing are mentioned on this take a look at mentioned. Cryptography and other safety features are used to combat these attacks. Techniques of steganography are investigated, and a vital exam is executed completed. The open studies location is characterised via studies and vital evaluation, and it assists other researchers in contributing their have a look at in this topic.

Introduction:

A cloud is a completely unique form of network that can provide laptop offerings through sharing a pool of sources as opposed to relying on neighborhood servers or non-public devices. The cloud computing idea has acquired a number of guide because it promises good sized fee discounts and novel professional possibilities to users and carriers. IT agencies supply those computing resources, which are referred to as cloud resources, and that they price for them depending on standards such as consumption, fee, and versatility. End customers benefit from cloud computing in an expansion of methods, including the following:

- **Self Service Provision:** A person can calculate sources without regarding an administrator or different governing authority. Users contact a web-based gateway with a self-provider cloud to attraction or configure servers and control apps.
- **Elasticity:** Elastic computing is a cloud computing concept wherein pc property can be without problems scaled up and down through the cloud provider issuer. Users enjoy the scalability of the cloud platform. This reduces the want for massive cost-slicing in local corporations.
- **Migration Flexibility:** Businesses can circulate paintings from the cloud server to different levels for cost savings or to take advantage of new services as they end up available. If you require get admission to for your files and records when off-website online or at domestic, you may use any internet-enabled method to hook up with your digital office speedy and easily every time you need it.
- **Reliability:** Cloud computing allows statistics safety, statistics backup, disaster recovery, and organization balance by storing records in several redundant places at the cloud system.
- **Performance:** The maximum massive benefit of cloud computing services is their speed. Because the record is unfold throughout multiple statistics centers, it travels quickly and effectively. As a end result, software latency may be decreased.
- The cloud is classed into the subsequent types [11] based on the provider:
- **Public Cloud:** A public cloud is a third-birthday party cloud carrier provider that offers cloud offerings through the net. Users simply pay for the bandwidth or service they eat beneath this association. Public cloud companies include Amazon, Salesforce, and Microsoft.
- **Private Cloud:** This refers to a cloud network that is simplest utilized by a unmarried patron. That institution has get admission to the entire cloud source for its personal use. Despite its remote location, it isn't always shared with other users. Private clouds are frequently utilised by means of mid- to massive-sized businesses and government businesses where flexibility and safety are paramount.
- **Hybrid Cloud:** This is a hybrid cloud that combines public and personal cloud offerings. It offers users with more flexibility and statistics distribution options. The primary aim of a fusion cloud is to offer extra assets in times of excessive demand. Allow computation jobs to be transferred from a non-public cloud to a public cloud, for example.

Cloud Security Attacks:

In cloud computing, there are numerous safety threats, which includes [11].

- **Source Location:** Because the area of the assets for such services is unknown to end-customers, they inadvertently utilise the services that cloud resources supply. When objections stand up, this creates a difficult position. The records saved in cloud sources is encouraged no longer only by the policies of the source, but also via the laws of the countries in which the holder is living.
- **Multi-Tenancy Issue:** The problem provided with the aid of this problem is to defend person information from unauthorised get right of entry to through different users doing equal operations at the same servers.

- **Information Validation and Reliance:** Critical statistics is saved in a cloud agency; essential information may be altered without the approval of the holder. The holder then procedures the brand new information if you want to make selections. The maximum vital degree is to affirm the records, which must be carried out with fact.
- **System Monitoring:** As greater programs migrate to the cloud; customers are inquiring about cloud assets that could reveal their structures.

As a consequence of our observations, it is able to comprise sensitive information this is utilised by using the resources; sharing statistics with any of the clients is something that not all cloud carriers strive to do. A lot of communications between cloud assets and customers is vital to display such statistics (due to the fact it is a demand of the service settlement).

Cryptography and Steganography Overview:

Cloud security threats lower service fine and motive data leakage inside the community. Cryptography and steganography methods are hired to guard in opposition to those assaults. Cryptography is essentially hidden writing, while steganography, as visible in Figure 1a and 1b, is cover writing. The mystery facts and key are entering parameters to the encryption method in cryptography, and the end result is cypher facts, as shown in the diagram. The encryption algorithm is a feature of the important thing in cryptography. If a unmarried bit inside the key changes, the variety of bits within the cypher data modifications as nicely. In steganography, then again, cover media (including text, picture, video, and audio) and secret facts are fed into an embedding set of rules, which produces steganography media. The mystery facts are stored within the least widespread bit, ensuing in little fluctuation once facts have been hidden. The LSB approach is the most usually utilized in steganography.

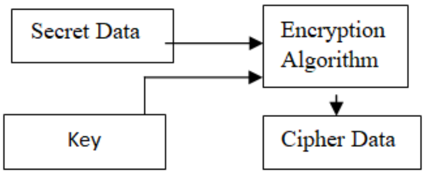

Figure 1a: Cryptography

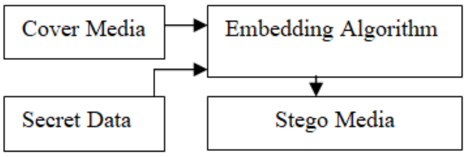

Figure 1b: Steganography

Table 1: Comparative Analysis between Cryptography and Steganography

Description	Cryptography	Steganography
Goal Achieved	Confidentiality	Imperceptibility
Carrier File	Plaintext	Image, Video, Audio, Plaintext
Key	Required	Optional
Output File	Cipher file	Stego file
Information Transparency	Visible	Non Visible
Security Level	Depend on key and encryption algorithm	Depend on Hiding Technique
Goal Failed	Plaintext Recovered	Communication Detected

The desk underneath depicts a contrast of cryptography and steganography, highlighting the several differences among the two. While a key's vital in cryptography, it is not required in steganography. Similarly, the desk depicts the numerous differences among them.

Related Works:

A number of research which have centered on safety parameters for cloud computing are mentioned on this phase. According to Akshita Bhandari, et al. [3,] a technique based on records hashed message authentication codes (HMAC) and index production turned into proposed for detecting errors and growing efficiency. They also looked at how well encryption methods executed in phrases of secrecy, integrity, and availability.

Ning Cao, et al. [4] endorsed making use of multi-keywords ranked search over encrypted cloud facts to explain and explain privateness problems (MRSE). The suggested method seemed towards ensuring privacy and performance. The preceding approach centered on a single keyword search or a Boolean key-word search, with the effects sorted. The creator proposed a method that would bring about much less calculating overhead.

Raj Kumar Chalse, et al. [5] centered at the protection inside the case of dependability, which is a vital excellent in cloud computing. To validate the accuracy of consumer facts in a cloud warehouse, the author developed a provable information possession technique that decreased information bite get right of entry to and computation quantity on the purchaser server.

Ranjit Kaur, et al. [7] used Novel Encryption strategies to raise attention approximately security. It locations regulations on unauthorised objects that allows you to control the consumer's facts and gives protection inside the face of numerous security flaws. The visualisation era become proposed via Ashalathar. et al. [2]. The attention became on maximising resource use and maintaining high flexibility. Because visualisation allows severa customers to percentage a unmarried physical server.

Mohammed A. Al Zain, et al. [1] presented a new Multi Clouds Database (MCDB) version, in addition to a triple modular redundancy (TMR) method, to improve the proposed cloud computing and growth safety. The most vital concern changed into information confidentiality, as well as records integrity and availability. Navia Jose, et al. [6] provide a way for building a cozy cloud computing environment using the Rivest Shamir Adleman (RSA) set of rules and MD5. The authors had been usually concerned with consumer authentication and information protection.

Randeep Kaur et al. [14] focused on cloud safety concerns. They proposed that two techniques be described: pixel key sample and picture steganography method. The most essential consideration was maintaining secrecy and honesty.

With one of these high degree of cloud computing worries, a organization determined to make a desire based totally on the blessings to hazard ratio. Because the approaches discussed above can encrypt the original records, information secrecy may be acquired.

Justin LeJeune et al. [8] set up a unique safety method for cloud file account recovery. The algorithm sutilised to comfy patron records through account security have been MIST and Malachi. The primary goal become to hold non-public records extra efficiently preserved, and it provided a unique method of safeguarding accounts in systematic logins.

Saakshi Narula, et al. [9] discussed cloud protection and defined how Amazon Web Services (AWS) cloud computing works. Organizations targeting unique regions at a time because it turned into difficult to offer overall performance to scattered customers. The authors have been in the main involved with maintaining user self belief and consider, in addition to preserving secrecy, integrity, and availability.

Sakinah Ali Pitchay, et al. [10] advanced an offer that used AES and RSA to encrypt facts on a USB device. All files are encrypted inside the cloud until the regular serial bus (USB) tool is plugged into the PC. In this approach, the machine detects the remoted key's USB port and utilises the documents transferred from the cloud.

Shipra Shukla et al. [12] created diverse stages of safety rules for cloud computing systems towards threats, hazard, and vulnerability. The author presented an object-oriented technological technique for imparting greater solid and truthful cloud surroundings. This method proved a success in resolving security and compliance worries as well as organisational challenges.

The work of Divya Prathana Timothy, et al. [13], provided safety for facts this is portable via the internet, ensuring that any invader cannot alter the facts earlier. The authors employ an aggregate of blowfish symmetric and RSA algorithms to provide a extra sincere, valuable, and safe environment for cloud computing. The use of the aforementioned method become able to decrease or get rid of information security and foremost cloud concerns.

This approach proved a success in resolving security and compliance issues in addition to organisational challenges. The paintings of Divya Prathana Timothy, et al. [13], offered protection for statistics that is transportable via the net, ensuring that any invader cannot regulate the statistics earlier. The authors appoint a aggregate of blowfish symmetric and RSA algorithms to offer a extra sincere, treasured, and secure environment for cloud computing. The use of the aforementioned technique was capable of lower or eliminate statistics security and principal cloud issues.

Critical Analysis:

In this element, Table 2 and Table 3 provide an essential evaluation of offerings and security algorithms based totally on the research.

Table 2: Evaluation of Cloud Computing Security Algorithms

Author	Confidentiality	Integrity	Availability	Trust	User Authentication
Akshita Bhandari et al.[3]	Yes	Yes	Yes	No	No
Navia Jose et al.[6]	No	No	No	No	Yes
Justin Le Jeune et al.[8]	No	Yes	No	No	No
Saakshi Narula et al.[9]	Yes	Yes	Yes	Yes	No
Divya Prathana Timothyet al.[13]	Yes	No	No	No	No
Randeep Kaur et al.[14]	Yes	Yes	No	No	No

According to Table 2, no approach that gives secrecy, integrity, authentication, or accept as true with has been suggested. The comparison of numerous cloud security settings is shown in this table.

Table 3: Critical Analysis of Cloud Computing Security Algorithms

Author	Technique Used	Parameters	Advantages	Challenges
Ning Cao et al.[4]	MRSE	Performance, system usability, and scalability are all important factors.	Less overhead on calculation	Control Search access is not within the possibility.
Navia Jose et al.[6]	Three layer architecture i.e. MD5 and RSA	Data Protection User Authentication.	Fast recovery of data	Separation of Sensitive Data and Access Control.
Justin LeJeune et al.[8]	MIST and Malachi	Integrity of data	Account Recovery and Protecting accounts for regular logins.	Zero Confirmation after submitting of three Q&A.
Shipra Shukla et al.[12]	Object Oriented Technique	Reliability and trustworthiness	Provide clients with maximum visibility into the security.	Operational and management security controls.
Divya Prathana Timothy et al.[13]	Blowfish And RSA and SHA-2	Authentication and data confidentiality	High security, proper Network access and Storage application	Key management becomes complicated and time consumption.
Randeep Kaur et al.[14]	Pixel Key Pattern and Steganography	Integrity and confidentiality.	Reduce default rate, Localization of points and Distinct reaction to an edge.	Ethical Challenge.

The vital exam in Table 3 well-known shows that symmetric and asymmetric encryption methods work collectively within the cloud to offer secrecy and authentication. In the table above, various cloud computing processes are in comparison, as well as various parameters for every technique.

Research Gaps:

Based on research and critical evaluation, sure research instructions have been diagnosed wherein more paintings can be done. Data is on the market remotely through cloud computing. As a result, the hackers placed malicious nodes within the network, inflicting the entire community to be affected. The authentication of nodes is a prime problem. For authentication, the writers Navia Jose et al. [6] utilised the RSA approach. When large prime numbers are utilised, the RSA method gives high protection, however it consumes quite a few sources and strength. One interesting topic is to investigate authentication algorithms that use less assets and convey less power. Cryptography techniques provide secrecy and authentication, consistent with the author Divya Prathana Timothy et al. [13]. Randeep Kaur, et al. [14], however, display that steganography strategies give information imperceptibility. Hybrid cryptography and steganography strategies, which enable multilayer security in cloud computing, are one open area.

Conclusion:

The Internet of Things and 5G technologies both use cloud computing. A lot of corporations provide remarkable offerings and pool their resources inside the cloud. For statistics switch, a large quantity of humans uses the cloud wirelessly. Because sensitive statistics is dispatched thru the internet, safety and privateness are most important issues. The first part of this text gives an define of a research in addition to a essential exam of cloud computing protection factors and techniques. To counter these assaults, the cryptography and steganography protection fields come into play, consistent with the studies. Furthermore, based on the observe, positive studies paths wherein extra work may be completed had been indicated.

Acknowledgement:

The authors express gratitude towards the assistance provided by The Management, Krupanidhi Group of Institutions (KGI) and Krupanidhi Research Incubation Centre, KGI in completing the research. We also thank our Research Mentors who guided us throughout the research and helped us in achieving the desired results.

References:

1. AlZain, M. A., Soh, Ben, & Pardede, Eric. (2012). A New Approach Using Redundancy Technique to Improve Security in Cloud Computing. (230-235). Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec).
2. Ashalatha, R. (2017). Network Virtualization System for Security in Cloud Computing. (346-350). 2017 11th International Conference on Intelligent Systems and Control (ISCO).
3. Bhandari, A., Gupta, Ashutosh, & Das, Debasis. (2016). A framework for Data Security and Storage in Cloud Computing. 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT).
4. Cao, N., Cong Wang, Ming Li, Kui Ren, & Wenjing Lou. (2015). Enhanced Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data. (s. 25). IEEE Transactions on Parallel and Distributed Systems.
5. Chalse, R., Selokar, Ashwin, & Katara, Arun. (2013). A New Technique of Data Integrity for Analysis of the Cloud Computing Security. (469-473). 2013 5th International Conference and Computational Intelligence and Communication Networks.
6. Jose, N., & A, C. K. (2013). Data Security Model Enhancement In Cloud Environment .IOSR Journal of Computer Engineering (IOSR-JCE), 01-06.
7. Kaur, R., & Singh, Raminder Pal. (2014). Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques Ranjit. (1227-1233). 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI).
8. Lejeune, J., Tunstall, Cara, Yang, Kuo Pao, & Alkadi, Ihssan. (2016). An algorithmic approach to improving cloud security: The MIST and Malachi algorithms. 2016 IEEE Aerospace Conference.
9. Narula, S., Jain, Arushi, & Prachi. (2015). Cloud Computing Security: Amazon Web Service. (501-505). 2015 Fifth International Conference on Advanced Computing & Communication Technologies.
10. Pitchay, S. A., Alhiagem, Wail Abdo Ali, Ridzuan, Farida, & Saudi, Madihah Mohd. (2016). A Proposed System Concept on Enhancing the Encryption and Decryption Method for Cloud Computing. (201-205). 2015 17th UK Sim-AMSS International Conference on Modelling and Simulation (UKSim).
11. Rong, C., Nguyen, Son T., &Jaatun, Martin Gilje. (2013). Beyond lightning: A survey on security challenges in cloud computing. Computers and Electrical Engineering, 47-54.
12. Shukla, S., & Singh, Rakesh Kumar. (2012). Security of Cloud Computing System using Object Oriented Technique. Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on.
13. Timothy, D. P. (tarih yok). A Hybrid Cryptography Algorithm for Cloud Computing Security. 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS).
14. Kaur, R., & Kaur, Jagroop. (2015). Cloud computing security issues and its solution: A review. (1198-1200). 2015 2nd International Conference on Computing for Sustainable Global Development (India Com).