IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96137

DATA SECURITY MODEL FOR CLOUD COMPUTING

SUMUKHA M[1], C S SWETHA[2]

Student, Department of MCA, Bangalore Institute of Technology, Bangalore, India[1]

Asst.Prof, Department of MCA, Bangalore Institute of Technology, Bangalore, India[2]

Abstract Popular Cloud-based cloud services may have inconsistent concerning data management. Companies utilise the cloud. Moving cloud apps and databases may disturb big data management. Safe. Cloud isn't local. Cloud services may access customer applications and data, undermining security. Cloud clients employ similar security architecture. Cloud encryption is advanced. Cloud services stink. Discusses V-CRT security. This helped cloud computing. 3rd cloud security reduces concerns. Uniqueness is dangerous. Cloud computing saves remotely. Cloud data and applications are insecure. Cloud services provide clients with standardised security. The cloud encrypts data. Cloud services may fail. V-CRT protects cloud data. This prevented a cloud computing downside. Cloud services minimise data misuse.

Keywords: Include at least 4 keywords or phrases.

I. INTRODUCTION

"Computer networks are in their infancy," remarked Leonard Kleinfeld, an ARPANET scientist. Like electric and telephone utilities, computer utilities may become prevalent in the US soon. "On-demand computer services would be available, as in the present world. One of the earliest computer industry concepts in the 21st century. A change in the computer industry led to the creation of computing utilities. Due to this trend, the entire industry must shift. Only when consumers use computer services do they pay suppliers. This solution doesn't need costly equipment or a complicated network. All users can utilise offered services. "Cloud computing" has replaced the term "utility computing" "Cloud" lets users access software development applications from wherever, at any time. Associated with cloud computing demand, Google, Microsoft, Internet!, and IBM are creating data centres quickly. Cloud services include architecture, platform, and software. Pay-as-you-go if you would not want a monthly subscription.IaaS, Ppp, and SaaS are offered commercially (SaaS). A new research predicts cloud computing may transform the IT industry. Result: cloud computing. SaaS is interesting.

Cloud computing should drive the next phase of data centre design so consumers may deploy programmes economically worldwide. Cloud computing lets users install applications anywhere. New Internet services need less equipment and people. Insufficient. Business expansion is an option. Cloud reduces setup time for hardware and software. IT may prioritise initiatives. Future-focused IT enterprises may exist. Businesses may enhance services. Market analysts think cloud computing has huge promise. Indeed, Gartner predicted 50 billion. A wide variety of applications employ Amazon Web Services' cloud-based computer systems. Linking buyers and sellers speeds up transactions. Pay-as-you-go "cloud computing" Users may request data, programs, and other mutual aid across a network. The cloud provides high software products [12,19]. Before employing cloud services, customers must move data to a data centre (CSP). Traditional Web servers ran on laptops and Desktops. Cloud computing was lacking. Server load slows page delivery. Popular websites or online programmes might overload a web server with queries. Low demand idled substantial capacity. Cloud-hosted workloads are more powerful. If the site suddenly became popular, more machines may be asked to produce pages and more money may be paid to compensate for the increased usage. The amount owed lowers as the item's popularity declines.This is partly attributable to cloud computing's pay-as-you-go model.

II. RELATED WORKS

When critical data is kept in the cloud, providers can't eliminate insider attacks. This risks consumers. If cloud service providers don't trust their customers, data might leak. Basic encryption can't handle complicated demands like searching, updating data concurrently, and fine-grained network access. Encryption can't meet these constraints. We'll look at past publications seeing how cloud computing impacts data confidentiality.Encryption safeguards data. Rivest devised homomorphic encryption. Algebraic procedures on encrypted text enable compatibility without decryption. This solution protects cloud data and processes.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96137

Gentry's advice to use "completely homomorphic" [1] encryption influenced this idea. Homomorphic encryption software has improved. These calculations are costly. Homomorphic encryption is useless.

Diffie-Hellman [2,12]. They're incompatible.[3] Ssl, triple des, and a software program are used in hybrid encryption [3]. To achieve this goal, combine each approach's merits. RSA and triple des encrypt data. RSA can safeguard a communication channel, but 3DES is preferable for large data

blocks. Next, we'll explore both ciphering methods. Researchers are looking for non-cloud uses for limited homomorphic encryption in the presence of homomorphic encryption. Homomorphic encryption is compatible with the cloud. This may be due to cloud settings. Decrypting data is a frequent approach. Population-accessible [5] is indeed an article on the TSFS method. This encryption technology is easily recognisable to customers because of its acronym. Processing and computing are proportional to key access. If there are many keys, this might be problematic. In-memory database encryption protects critical cloud data. This need spawned this technology. This is why this technology was invented (IMDE). Encryption can secure memory-resident data. [6] A third party ensures consumers and data owners have equal access to stored data. Consumers require services. to decrypt the owner's encrypted data, the synchronizer The synchronizer may understand shared data with this key. With this functionality, data may be synchronized. A synchronizer must secure secret keys and any shared data it include. Need a synchronizer. Extra connection with a central time-synchronization device slows this procedure. With this strategy, there are additional concerns. Encryption and communication limitations among nodes and the synchronizer may help.[7] Huang and Tso introduced asymmetric encryption for online cloud storage. Asymmetric encryption is only allowed if specific conditions are satisfied. Encryption's commutative nature allows the public secret and private key to be used in any sequence. This method employs several encryption-decryption cycles, thus it doesn't care how keys are utilised. Re-encryption may also be employed. To offer the same level of protection as two, the cryptosystem data is encrypted again. This stage is accomplished since it satisfies strategy needs. A mixed technique [18] may protect data privacy and authenticity. This method combines shared keys and authentication to provide maximum data security. Strict crucial and authentication may safeguard users' and cloud providers' connections. The Public - key technique [17] can protect key distribution between customers and cloud providers. You have many options; don't limit yourself. First-layer data security requires one-time password or two-factor verification, both three-layer components. A rapid decryption follows a second encrypted stage to secure the user's data. When deletion is validated, it's challenging to restore erased data. Users will never reclaim their info. Multiple copies of cloud data are kept due to concerns about security and retrieval speed. This must be addressed. When a user deletes data, all copies must be erased simultaneously. Certain data recovery techniques may restore customers' hard drives. These are for sale. Protecting deleted client data so only cloud service providers may access it is a smart idea. Before saving data, encrypt cloud storage. No one can access or use the data. The data can't be retrieved

III. METHODOLOGY

Cloud computing has a major downside since cloud service companies might misuse data in their datacentres. This path is risky. This must be handled before going to the cloud. client. No one solution can solve the situation right now. Concerns about cloud technology will persist until cloud service providers can't access data. OTP's inefficiency for cloud computing is due to its several uses. OpenNebula configures the cloud. RSA and 3DES employ random number generation for public-key encryption. These solutions are used for authentication in a multi-level hierarchy sequence to maintain data privacy and security. Authentication went well. This demonstrates that the techniques are applied in order. This technique uses open-source Java and other technologies. This technique is used throughout. Cloud service providers utilise these technologies because they're compatible with cloud computing. V-key GRT's distribution system uses Kerberos for authentication. Security and efficiency are best with key distribution. This plan succeeds because it uses techniques.

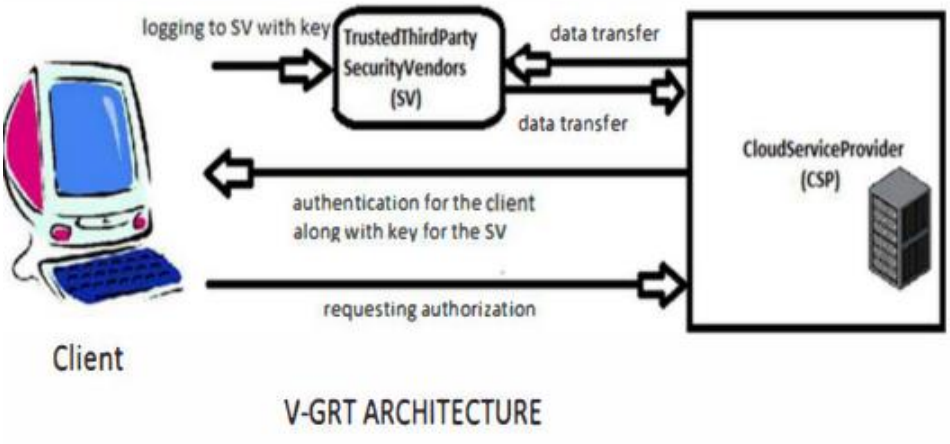
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96137

IV. MODELING



V-GRT ARCHITECTURE

V. RESULTS AND DISCUSSION

In this section, we'll compare our proposed machine capabilities to those of the other relevant standards. Using a Windows 10 64-bit PC powered by an Intel Core i3-5100 CPU with 520GB of internal hard drive space, we ran each algorithm [1]. Backend SQL Statements are used to build the application's front end. Backend JavaScript. Both of these approaches are employed in the project's creation. As for the software, it's being built with NetBeans 8.2 and MySQL 5. The system's performance graph had been loaded from Google and displayed using bar charts. Another advantage of this graph is that it shows how quickly the system as a whole respond when new applications are installed. Since the user's private key must be determined for each and every one of an identity's traits, the time it takes to complete the key extraction method rises proportionately. The time it takes to generate a file's hash code has been determined. One megabyte (MB) of data can be stored for each attribute, with a total of ten attributes per set. Each attribute can be stored in its own file. A cloud storage provider's uploading speed is influenced by the computer's internet connection speed.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96137

VI. CONCLUSION

Cloud security and privacy are crucial. Every cloud service undermines privacy and security. This allows cloud users to store private data. User must grasp credited information. Cloud users require assurance. Users may encrypt various data using the Encryption Algorithm's adaptability. The user may sequence any techniques. User determines how provider utilises encrypted data. Random numbers are used regardless of user preference. Even without encryption and other security measures, the user is secure. Decoding sequence will be saved in a database for safety. Multiple encryption layers impede request processing. Long process. This problem may be overlooked if just a small quantity of data, such passwords, is protected. Fewer details are required. The security company's multilayered hybrid encryption may increase protection.

REFERENCES

[1]. C. Gentry, "A fully homomorphic encryption scheme [Ph.D. thesis]", International Journal of Distributed Sensor Networks, Stanford University, 2009.
[2]. D. Boneh, "The decision Diffie-Hellman problem", Algorithmic NumberTheory. 2008.
[3]. A. Kaur and M. Bhardwaj, "Hybrid encryption for cloud database security", Journal of Engineering Science Technology, 2010.
[4]. R. Arora, A. Parashar, and C. C. T. Transforming, "Secure user data in cloud computing using encryption algorithms", International Journal of Engineering Research and Applications, June 2013. [5]. D. Manivannan and R. Sujarani, "Light weight and secure database encryption using tsfs algorithm", Proceedings of the International Conference on Computing Communication and Networking Technologies ICCCNT '10.
[6]. F. Pagano and D. Pagano, "Using in-memory encrypted databases on the cloud", Proceedings of the 1 st IEEE International Workshop on Securing Services on the Cloud (TWSSC '11).
[7]. K.Huang and R. Tso, "A commutative encryption scheme based on ElGamal encryption", Proceedings of the 3rd International Conference on Information Security and Intelligent Control (ISIC '12), August 2012.
[8]. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacypreserving multi-keyword ranked search over encrypted cloud data", IEEE Transactions on Parallel and Distributed Systems, 2012.
[9]. M. A. AlZain, B. Soh, and E. Pardede, "Mcdb: using multiclouds to ensure security in cloud computing", Proceedings of the IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC '11).
[10]. C. P. Ram and G. Sreenivaasan, "Security as a service (sass): securing user data by coprocessor and distributing the data". Proceedings of the 2nd International Conference on Trendz in Information Sciences and Computing, (TISC '10).
[11]. M. Asad Arfeen, K. Pawlikowski, and A. Willig, "A framework for resource allocation strategies in cloud computing environmen", Proceedings of the 14th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW'II).
[12]. P. Victer Paul, D. Rajaguru, N. Saravanan, R. Baskaran and P. Dhavachelvan, "Efficient service cache management in mobile P2P networks", Future Generation Computer Systems, Elsevier, Volume 29, Issue 6, August 2013, Pages 1505-1521.
[13]. E. M.Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing" , Proceedings of the 8th International Conference on Informatics and Systems (INFOS '12).
[14]. S. Biedermann and S. Katzenbeisser, "POSTER: event-based isolation of critical data in the cloud", Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, 2012.
[15]. C. Delettre, K. Boudaoud, and M. Riveill, "Cloud computing, security and data concealmen", Proceedings of the 16th IEEE Symposium on Computers and Communications (lSCC '11).
[16]. Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "Fade: secure overlay cloud storage with file assured deletion", Security and Privacy in Communication Networks, 2011.
[17]. P. Victer Paul, N. Saravanan, S.K.V. Jayakumar, P. Dhavachelvan and R. Baskaran, "QoS enhancements for global replication management in peer to peer networks", Future Generation Computer Systems, Elsevier, Volume 28, Issue 3, March 2012, Pages 573-582.
[18]. A. Rao, "Centralized database security in cloud", International Journal of Advanced Research in Computer and Communication Engineering, 2011
[19]. P. Victer Paul, T. Vengattaraman, P. Dhavachelvan, "Improving efficiency of Peer Network Applications by formulating Distributed Spanning Tree", Third International Conference on

