Pawan Kumar et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 4, Issue 4, December 2017, pp. 470-472

Security and Privacy Issues In Cloud Computing

Pawan Kumar

Assistant Professor, BMIET, Sonipat

Abstract: **Cloud Computing Approach has been wide used currently days. It's gaining several momentums lately. Cloud Computing model has been utilized by most of the world leader in IT business like Google, Microsoft, Amazon, Apple etc. the price reduction in it's been achieved by offloading of knowledge and computations the Cloud Computing. Notwithstanding Cloud Computing is associate economic model and is wide used model in recent days, several area unit still not fascinated by exploitation this model because of many security, privacy and trust problems. In the beginning, organizations would expire instrumentation (hardware associated/or software) and manage it themselves however in fashionable days several organizations like better to expire services from an IT service supplier. This is often typically mentioned as 'cloud'. The initial reaction of the protection community to the protection problems with cloud computing was that these can be resolved exploitation existing techniques transmitted from standard IT systems or perhaps distributed systems that area unit the ancestors of cloud computing environments. Sadly, this approach doesn't work, owing to the size and therefore the design of the cloud computing model. Hence, a requirement to re-consider security, privacy and trust considerations within the context of the cloud computing paradigm arises.**

Keywords: Cloud, Cloud Computing, Security, Privacy, Trust, Security Algorithms, DES, AES, Blowfish, RSA, Homomorphic algorithm.

I. SECURITY IN CLOUD ENVIRONMENT

The cloud service provider should make sure that they get the protection aspects right, for they are those who can shoulder the responsibility if things fail. The cloud offers many advantages like quick readying, pay-for-use, lower prices, quantify ability, speedy provisioning, speedy snap, omnipresent network access, larger resiliency, hypervisor protection against network attacks, inexpensive disaster recovery and knowledge storage solutions, on-demand security controls, real time detection of system change of state and speedy re-constitution of services. Whereas the cloud offers these benefits, till a number of the risks are higher understood, several of the main players are going to be tempted to carry back [1].

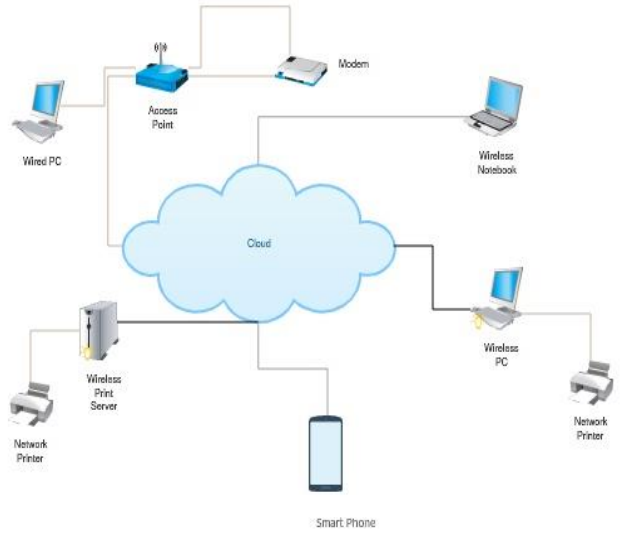

Figure1.1 : Cloud Computing

The advantages of victimisation cloud computing square measure giving infinite computing resources, low cost, security controls, hypervisor protection, speedy snap, high measurability and fault tolerant services with high performance. Several corporations like Microsoft, Google, Amazon, IBM, etc. developed the cloud computing systems and supply an oversized quantity of consumers by enhancing their services [2].

The increment within the adoption of cloud computing and therefore the market maturity is growing steady as a result of the service suppliers make sure the advanced security level, compliance and regulative. Partially this growth, the cloud services can deliver the hyperbolic flexibility and price savings [3]. In cloud computing, 2 main parties area unit concerned in cloud computing systems: the service supplier and therefore the service subscribers as individual or enterprise. every enterprise has its own sensitive knowledge that require to be terribly secured and guarded from unauthorized access and management[4].

The cloud supplier ought to give secure cloud surroundings to confirm user's privacy. Privacy refers to users' right to manage revealing of their personal knowledge [5]. There are many of security issues for cloud computing, because it is enclosed by various technologies additionally of 'networks databases', 'working structures', 'virtualization resource booking', 'trade organization', 'stack changing', 'concurrence management', and 'memory organization' [6].

II. SECURITY ALGORITHMS

Generally cloud computing has many customers like normal users, world and enterprises UN agency have totally different motivations to manoeuvre to cloud. If cloud purchasers square measure world, security impact on performance of computing and for them cloud suppliers got to realize the way to mix security and performance. For enterprises most vital drawback is additionally security however with totally different vision.

Data Encryption Standard (DES)

Data Encryption commonplace was developed in 1977. It absolutely was the primary secret writing commonplace to be suggested by government agency. DES is sixty four bits key size with sixty four bits block size. Since that point, several attacks and strategies have witnessed weaknesses of DES that created it associate insecure block cipher.[7]

Advanced Encryption Standard (AES)

AES may be a symmetric-key block cipher printed by the National Institute of Standards and Technology (NIST). Most adopted isosceles secret writing is AES. It operates computation on bytes rather than bits, treats 128 bits of plaintext block as sixteen bytes. These sixteen bytes area unit organized in four columns and 4 rows for process as a matrix. It operates on entire information block by mistreatment substitutions and permutations. The key size used for associate degree AES cipher specifies the quantity of transformation rounds employed in the secret writing method.[7]

Blowfish Algorithm

This was developed in 1993. it's one in all the foremost common public algorithms provided by Bruce Schneier. Blowfish could be a variable length key, 64-bit block cipher. No attack is thought to achieve success against this varied experiments and analysis. Analysis proved the prevalence of Blowfish formula over different algorithms in terms of the time interval. Blowfish is that the higher than different algorithms in outturn and power consumption.[9]

Rivest-Shamir-Adleman (RSA)

RSA may be a public key cipher developed by Rivest, Shamir and Adlemen in 1977. it's most well liked uneven key cryptanalytic rule. This rule uses numerous knowledge block size and numerous size keys. it's uneven keys for each coding and cryptography. It uses 2 prime numbers to get the general public and personal keys. These two completely different keys are used for coding and cryptography purpose. RSA these days is employed in many code product and might be used for key exchange, digital signatures, or coding of little blocks of information. This rule is especially used for secure communication associated authentication upon an open line [10].

Homomorphic Algorithm

It is associate degree coding algorithmic program that give exceptional computation facility over encrypted information (cipher text) and come back encrypted result. This algorithmic program will solve several problems associated with security and confidentiality problems during this algorithmic program coding and decipherment happening in consumer website and supplier site operates upon encrypted information. this could solve threat whereas transferring information between consumer and repair supplier, it hide plaintext from service supplier, supplier operates upon cipher text solely [11].

III. LITERATURE SURVEY

It was mentioned therein AES is quicker and additional economical interchangeable algorithms. Once the transmission of knowledge is taken into account there's insignificant distinction in performance of various interchangeable key schemes. This gives high security over open network however key transfer is that the major issue in interchangeable algorithms [7].

Seth et al (2017) aimed to study several key concepts, namely Cloud characteristics, delivery models, deployment models, and security issues. The document also discusses the work done on Cloud security and privacy issues [8].

DES algorithmic program consumes least secret writing time and AES algorithmic program has least memory usage whereas secret writing time distinction is incredibly minor just in case of AES algorithmic program and DES algorithmic program, however RSA secret writing algorithms consume a big quantity of computing resources like electronic equipment time, memory, and battery power [8]. Comparison of secret key and public key primarily based DES and blowfish algorithms clears that blowfish solves downside of the key agreement and key exchange problem generated on the cryptography. However it doesn't solve all the protection infrastructure .So DES is employed. Blowfish and DES dissent from one another in sure options. Blowfish have several flaws in its design so not most popular for the business use. Once the tiny values are chosen for the coming up with of key then the cryptography method becomes too weak and one is ready to decode the information by exploitation random applied math and aspect channel attacks. On the opposite hand if giant lengths are chosen then it consumes longer and also the performance gets degraded compared with DES [9]. Survey it is found that AES algorithm is best in terms of speed, time, turnout and avalanche result. the safety provided by these algorithms is increased any, if over one rule is applied to knowledge supported the text files used and therefore the experimental result it had been terminated that AES rule consumes least secret writing and RSA consume longest secret writing time. we have a tendency to conjointly discovered that decoding of AES rule is best than different algorithms. From the simulation result, we have a tendency to evaluate that AES rule is far higher than DES and RSA rule [10]. Homomorphic encryption affords identical level of privacy as the other encryption, whereas conjointly giving operations to be performed on knowledge while not the necessity to examine

the particular data. Complete privacy between consumer and server would be doable with none belittled practicality. Such systems can be applied to almost something that needs computation, like ballot, banking, cloud computing, and lots of others [11]. Homomorphic encryption could be a new construct of security that permits providing results of calculations on encrypted information while not knowing the information on that the calculation was applied, with respect of the information confidentiality. Security of cloud computing supported absolutely Homomorphic encoding could be a new idea of security that is change to supply the results of calculations on encrypted information while not knowing the raw entries on that the calculation was applied respecting the confidentiality of information [11].

IV. CONCLUSION

Cloud Computing is world rising, next generation technology within the field of data technology. it's various benefits however some challenges area unit still existing during this technology.

Security is that the most difficult issue during this technology. During this paper we've mentioned numerous encryption algorithms to beat this security issue, deals with benefits and drawbacks of these algorithms. Here we tend to conclude that homomorphic formula is that the most fitted formula in cloud computing atmosphere to secure their valuable information in associate open network.

The flexibility of homomorphic formula to perform operations on encrypted information permits high security than alternative algorithms akin to DES, AES, RSA, and Blowfish. Future work is to implement hardware or software package technique with homomorphic formula to produce protection on cloud from any style of security attack.

V. REFERENCES

[1] Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I (2009)

[2] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," Proc. 6th Int. Conf. Semant. Knowl. Grid, pp. 105–112, 2010.

[3] P. Wilson, "Positive perspectives on cloud security," Inf. Secur. Tech. Rep., vol. 16, no. 3–4, pp. 97–101, 2011

[4] ABDUL NASIR KHAN, M.L. MAT KIAH, SAMEE U. KHAN & MADANI, S. A. (2013) Towards secure mobile cloud computing: A survey. Future Generation Computer Systems, 29, 1278-1299

[5] ENISA, "Cloud Computing – Benefits, risks and recommendations for information security" (2009).

[6] Ferretti L, Colajanni M, Marchetti M (2014) Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases. IEEE Trans Parallel Distrib Syst 25: 437-446.

[7] Kefa Rabah , 2005. Theory and Implementation of Data Encryption Standard: A Review. Information Technology Journal, 4: 307-325.

[8] Seth B., Dalal S. (2018) Analytical Assessment of Security Mechanisms of Cloud Environment. In: Saeed K., Chaki N., Pati B., Bakshi S., Mohapatra D. (eds) Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol 563. Springer, Singapore DOI https://doi.org/10.1007/978-981-10-6872-0_20

[9] Rijndael.Advanced Encryption Standard (AES). FIPS. November 23, 2001.

[10] Tingyuan Nie, Teng Zhang, "A study of DES and Blowfish encryption algorithm", *Tencon 2009–2009 IEEE Region 10 Conference. IEEE*, 2009.

[11] Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[12] Yi, Xun, Paulet, Russell, Bertino, Elisa "Homomorphic Encryption and Applications" Pages 27-46, ISBN 978-3-319-12229-8 Springer International Publishing

