Survey On Cloud Security And Algorithms

Dr.K.Karuppasamy[1] Ms.F.Margret Sharmila[2] Tharani .T[3]

[1] *Professor,Computer Science and Engineering. RVS College of Engineering and Technology Coimbatore, India*

[2] *Assistant Professor,Computer Science and Engineering. SNS College of Engineering Coimbatore, India*

Abstract — Cloud computing is that the the next generation's computing infrastructure that is well known and Cloud computing offers some benefits by permitting users to use infrastructure, platforms, and softwares provided by cloud suppliers at low value .additionally, Cloud computing enable users to elastically utilize resources in AN on demand fashion.The Objective of the work is to understand the security threats and the appropriate security techniques used in the cloud computing. The security challenges and the counter measures in the cloud computing were also identified .The survey with many security experts on cloud computing is made and satisfactory number of challenges and mitigation techniques are used at the present stage.

Keywords — *Infrastructure, Software, Algorithmic Program, Data Encryption and Secure Key*

I. INTRODUCTION

A cloud computing could be a giant scale distributed network system enforced supported variety of servers Cloud is a computing model that derived as services over the Internet of both the applications, the hardware and system software in the datacenters that provide the services. Cloud Computing is used for deployment of applications on Internet. Cloud applications use large data centers and effective servers to host web applications and services.There has been a rapid progress in Cloud Computing for the past few years . Cloud Computing delivers a resources like computational power, computational platforms, storage and applications to users through the internet. Some of the providers in the current market are Amazon, Google, IBM, Microsoft, Salesforce, etc..,the protection of the data of various users is mandatory. we have described the two main states that hold your data is out in the Cloud: when the data is in transit and when the data is at rest.

II. IMPORTANT SECURITY ISSUES IN THE CLOUD

The virtualization and Cloud Computing delivers wide range of dynamic resources, the security concern is generally perceived as the huge issue in the Cloud and that can be resist themselves by adopting the technology of Cloud Computing. Some of the security issues in the Cloud are discussed below:

Integrity: Integrity helps the data held in a system is a proper representation and not been modified by an authorized person. When any application is running on a server, backup routine is configured the data loss is noted. Normally, in any portable media the data will backup on a regular basis which will then be supported in an off-site location .

Availability: Availability ensures that malicious action will not occur in data resources. It is the simple idea that when a user tries to access the data, it is available to be accessed.

Confidentiality: Confidentiality is that data cannot be accessed to unauthorized persons. Confidentiality loss occurs when data can be viewed or read by any individuals who are unauthorized to access it. Loss of confidentiality can occur physically or electronically. Physical confidential loss takes place through social engineering. Electronic confidentiality loss takes place when the clients and servers aren‟t encrypting their communications

III. SECURITY ALGORITHMS

The algorithmic program for public-key cryptography, involves a public key and a non-public key's RSA. The general public key are often legendary to everybody and is employed for encrypting messages. Messages encrypted with the general public key will solely be decrypted exploitation the personal key. User information embody encoding before storage, user authentication procedures before storage or retrieval, and building secure channels for information transmission.

:

MD5

Message-Digest algorithmic program 5, a wide used cryptanalytic hash operate with a 128-bit hash price, processes a variable-length message into a fixedlength output of 128 bits. The input message is uneven into chunks of 512-bit blocks . the message is soft so its length is divisible by 512.

AES

In cryptography, the Advanced encoding commonplace (AES) could be a symmetric-key encoding commonplace. Every of those ciphers encompasses a 128-bit block size, with key sizes of 128, 192 and 256 bits, severally AES algorithmic program ensures that the hash code is encrypted during a extremely secure manner. AES encompasses a mounted block size of 128 bits and uses a key size of 128

AES is quicker and a lot of economical parallel algorithms. once the transmission of knowledge is taken into account there's insignificant distinction in performance of various parallel key schemes. This give high security over open network however key transfer is the major issue in parallel algorithms. Based on the text files used and therefore the experimental result it absolutely was concluded that DES formula consumes least cryptography time and AES formula has least memory usage whereas cryptography time distinction is incredibly minor just in case of AES formula and DES formula, however RSA cryptography algorithms consume a big quantity of computing resources like hardware time, memory, and battery power.

Comparison of secret key and public key based mostly DES and RSA algorithms, it clears that RSA solves drawback|the matter} of the key agreement and key exchange problem generated on the Q.T. key cryptography. however it doesn't solve all the safety infrastructure .So DES is employed. RSA and DES take issue from one another in sure options. RSA have several flaws in its style thus not most well-liked for the industrial use. once the tiny values of p & letter of the alphabet area unit elect for the planning of key then the cryptography method becomes too weak and one will be ready to decipher the info by victimization random applied math and facet channel attacks. On the opposite hand if massive p & letter of the alphabet lengths area unit elect then it consumes longer and therefore the performance gets degraded compared with DES.

According to analysis done and literature survey it will be found that AES formula is most effective in terms of speed, time, outturn and avalanche result. Key Management in the cloud computing is a simple way to protect the data, The encryption algorithm is public, information transfer in this algorithm is secure as the key is secret.

IV. PROPOSED SYSTEM

Cloud is a computing model that refers to both the applications derived as services over the Internet, the hardware and system software in the datacenters that provide those services. Some of the security issues in cloud are Integrity, Availability, and Confidentiality. Few of the popular security techniques that are identified are Identity based authentication, Service Level Agreement (SLA), Third party auditor, Message authentication codes, Role based access control mechanism, Time bound ticket based authentication scheme. The impact of these security techniques include on Confidentiality, Integrity, Availability and security.

The aim of research work is to protect the confidential information between a browser and a web server during the exchange of sensitive information. Proper encryption of data and encryption of transmission is necessary. In existing research the encryption tool is used for data protection.

The proposed approach makes use of SSL and VPN security techniques to protect the sensitive information. Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted links between a server and a client typically a web server (website) and a browser; or a mail server and a mail client. It allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. To establish this secure connection, the browser and the server need an SSL Certificate. Virtual Private Network (VPN) a virtual private network is a secure tunnel between two or more computers on the internet, allowing them to access each other as if on a local network. In the past, VPNs were mainly used by companies to securely link remote branches together or connect roaming employees to the office network, but in the proposed approach it is used protecting them from attacks when they connect to public wireless networks.

V. CONCLUSION

Cloud Computing is world rising, next generation technology . it's varied benefits however some challenges area unit still existing during this technology. Security is that the most difficult issue during this technology. The cryptography algorithms and therefore the security issue is mentioned which deals with benefits and drawbacks of those algorithms. The aim of analysis work is to safeguard the information between a browser and an internet server throughout the exchange of sensitive information.

REFERENCES

[1] Priyanka Arora, Arun Singh, Himanshu Tyagi ―Analysis of performance by using security algorithm on cloud network‖ in international conference on Emerging trends in engineering and management (ICETM2012), 23-24 june, 2012.

[2] ―"Swamp Computing" a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25.

[3] ""Thunderclouds: Managing SOA-Cloud Risk", Philip Wik". Service Technology Magazine. 2011-10.

[4] Winkler, Vic. "Cloud Computing: Virtual Cloud Security Concerns". Technet Magazine, Microsoft. Retrieved 12 February 2012.

[5] Hickey, Kathleen. "Dark Cloud: Study finds security risks in virtualization". Government Security News. Retrieved 12 February 2012.

[6] Winkler, Vic (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics. Waltham, MA USA: Elsevier. pp. 59. ISBN Securing the Cloud Cloud Computer Security Techniques and Tactics.

[7] "4 Cloud Computing Security Policies You Must Know". CloudComputingSec. 2011. Retrieved 2011-12-13.

[8] "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02. Retrieved 2010-01-25.

[9] "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. 2011. Retrieved 2011-05

[10] "Cloud Security Front and Center". Forrester Research. 2009-11-18. Retrieved 2010-01-25.

[11] M. Sudha , Dr.Bandaru Rama Krishna Rao , M. Monica ―A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment in International Journal of Computer Applications (0975 – 8887) Volume 12– No.8,December 2010

[12] Ms.F.Margret Sharmila on Book Nest an Android Application in Seventh Sense Research Group pp.102-104, ISSN: 2348-8387 on April 2016