ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

Enhanced Security Measures in Cloud Business Environment

Shanthosh Priyanka S [1], Preethi E[2], Prof Priya V[3]

School of Information Technology and Engineering, VIT University, Vellore, Tamilnadu, India[1, 2]

Assistant Professor, School of Information Technology and Engineering, VIT University, Vellore, Tamilnadu, India[3]

ABSTRACT: Distributed computing is the utilization of figuring assets (equipment and programming) that are conveyed as an administration over a system (regularly the Internet). The name originates from the utilization of a cloud-molded image as a deliberation for the complex foundation it contains in framework outlines. Distributed computing depends on remote [1] services with a client's information, programming and reckoning. Distributed computing gives three key services [2] Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Normally used business environment is very expensive and tough to use. Software and Hardware components required to run the applications are daunting. This business environment requires a huge team member to install, configure, access and maintain the entire processes and data's of the business environment. This business environment is not suitable for small and medium level environment. Next level of business process leads to better way. New process of environment is Cloud computing technologies. Though cloud computing has much more advantages, security is the threatening issue. This paper gives an enhanced security measures to overcome the security threats.

KEYWORDS: Encryption/Decryption, Infrastructure as a Service (IaaS), Platform as a Service, Software as a Service (SaaS), CRM (Customer Relationship Management).

I. INTRODUCTION

Undertakings normally store information in interior stockpiling and introduce firewalls to secure against gatecrashers to get to the information. They additionally institutionalize information access systems to anticipate insiders to uncover the data without authorization. In distributed computing, the information will be put away given by administration suppliers. Administration suppliers must have a reasonable approach to ensure their customers' information, particularly to keep the information from exposure by unapproved insiders. Putting away the information in encoded structure is a typical strategy for data protection assurance. In the event that a cloud framework is in charge of both undertakings on capacity and encryption/decoding of information, the framework executives might at the same time acquire scrambled information and unscrambling keys. This permits them to get to data without approval and consequently represents a danger to data security. This study proposes a plan of action for distributed computing focused around the idea of dividing the encryption and decoding administration from the stockpiling administration. Moreover, the gathering in charge of the information stockpiling framework should not store information in plaintext, and the gathering in charge of information encryption and encryption must erase all information upon the reckoning on encryption or unscrambling is finished. A CRM (Customer Relationship Management) administration is portrayed in this paper as a sample to outline the proposed plan of action.

II. RELATED WORK

Regular techniques for ensuring client information incorporate encryption preceding storage [9], client validation methodology before capacity or recovery, and building secure channels for information transmission. These insurance systems regularly oblige cryptography calculations and advanced mark strategies, as clarified underneath. Basic information encryption systems incorporate symmetric and topsy-turvy cryptography calculations. Symmetric cryptography is utilized within the U.s. Government Information Processing Standard's (FIPS) 46-3 Triple Data Encryption Algorithm (TDEA, otherwise called Triple-DES or 3des) or 197 Advanced Encryption Standard (AES) and others. This kind of encryption and unscrambling methodology utilizes a mystery key. Awry cryptography, then again,

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

utilizes two separate keys, an "open key" for encryption, and a "private key" for decoding. Cases incorporate RSA cryptography and Elliptic Curve Cryptography [11] (ECC). As a rule, symmetric cryptography is more effective, and is suitable for encoding expansive volumes of information. Deviated cryptography requires more processing time and is utilized for the unscrambling keys needed for symmetric cryptography. The utilization of passwords as a validation procedure is better known to general clients, yet messages sent by the client are powerless against surreptitious recording by programmers who can then utilize the information within the message to log into the administration as the client. In more exceptional verification frameworks, the framework side will produce an irregular number to send the client a test message, asking for the client to transmit a scrambled reaction message in answer to the test message, consequently validating that the client has the right encryption key. Without this key, the client won't be permitted access. At present test and reaction the customer's encoded key uses the customer's watchword to change over a determined quality and. In this program, every correspondence between the customer and server is remarkable, and a hacker [10] utilizing an old message would neglect to get to the framework. Furthermore, the One-Time Password (OTP) confirmation framework varies from most people groups' origination of a secret word. Most individuals comprehend a secret word to be a watchword picked by the client to be significant, and could be utilized over and over. The stress of Otp[12], however is the single-use nature of the watchword. In the wake of accepting validation from the client, the framework side must make a safe transmission channel to trade data with the client. The Secure Sockets Layer[13] (SSL) is a typical system for building secure channels, basically utilizing RSA encryption to transmit the mystery keys required for the both sides to encode and unscramble information transmitted between them. At the point when utilizing cryptographic innovation to ensure client information, the keys utilized for encryption and unscrambling of that information must be safely put away. Specifically, distributed computing administration suppliers must have particular systems for obliging interior framework administration staff to keep them from acquiring both encoded information and their decoding keys – this is discriminating to ensuring client information. Administrator approaches for securing client information must be obviously laid out in the Service Level Agreement (SLA) and must clarify how extraordinary benefit clients are kept from disgracefully getting to client information. Kandukuri, Paturi and Rakshit offer six suggestions for SLA substance, including

1) special benefit client information access must be controlled to forestall unapproved capacity or recovery,
2) cloud figuring administrations must conform to important laws,
3) user information must be legitimately put away and encoded,
4) a reset system must be given if there should arise an occurrence of administration disturbance or framework crash
5) service must be feasible and ensured against administration suspension because of progress or disintegration of the supplier and
6) If distributed computing administrations are utilized for unlawful purposes, the supplier must have the capacity to give records to support with examinations.

III. PROPOSED WORK

For distributed computing to spread, clients must have an abnormal state of trust in the strategies by which benefit suppliers ensure their information. This study proposes a Business Model for Cloud Computing [17] Based on a Separate Encryption and Decryption Service, accentuating that approval for the stockpiling and encryption/unscrambling of client data [7] must be vested with two distinctive administration suppliers. Moreover, the benefits of the Encryption/Decryption as Service supplier incorporates administration of the key needed for the encryption/unscrambling of client information, yet not the capacity of unscrambled or encoded client information. In this new plan of action, client information in the Storage Service System is all spared scrambled. Without the unscrambling key, there is no chance to get for the administration supplier to get to the client information. Inside the Encryption/Decryption Service System there is no put away client information, in this manner disposing of the likelihood that client information may be dishonourably revealed.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

IV. EXPERIMENTAL RESULTS

Undertakings generally store information in inside capacity and introduce firewalls to ensure against interlopers to get to the information. In distributed computing, the information will be put away given by capacity administration suppliers. Administration suppliers must have a feasible approach to secure their customers' information, particularly to keep the information from hole by unapproved insiders. On the off chance that a cloud framework is in charge of both assignments on capacity and encryption/decoding of information, the framework heads might all the while get encoded information and unscrambling keys. This permits them to get to data without approval and accordingly represents a danger to data protection.

USER CONTROL

This study proposes a Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service. The idea is focused around differentiating the stockpiling and encryption/unscrambling of client information. In this plan of action, Encryption/Decryption as a Service and Storage as a Service (Saas) are not given by a solitary administrator. What's more, the Saas supplier may not store decoded client information and, once the supplier of Encryption/Decryption as a Service has wrapped up the client information and gave it off to an application (e.g. a CRM framework), the encryption/decoding framework must erase all scrambled and unscrambled client information. The idea of partitioning power is frequently connected ready to go administration. Case in point, obligation regarding an organization's accounts is partitioned between the bookkeeper and clerk. Good to go operations, the bookkeeper is in charge of keeping records, while the clerk is in charge of making installments. By keeping these two capacities separate, the organization can keep the bookkeeper from distorting records and stealing corporate trusts. Authority reports much of the time need to be stamped with two seals (i.e., the corporate seal and the legitimate delegate's seal), therefore keeping a staff part from misapplying his position to issue fake records, and these seals are ordinarily endowed to two diverse individuals. These illustrations of the division of power are intended to maintain a strategic distance from a convergence of force which could raise operational dangers.

CRM MODULE

In a distributed the earth, the client ordinarily uses cloud administrations with particular capacities, e.g., Salesforce.com's CRM administration [14], SAP's ERP administrations [15], and so forth. Information produced while utilizing these administrations is then put away on storage spaces on the cloud administration. This study stresses the expansion of a free encryption/unscrambling cloud administration to this sort of plan of action, with the come about that two administration supplier's part obligation regarding information stockpiling and information encryption/decoding. To outline the idea of our proposed plan of action, Fig. 3 displays an illustration in which the client uses separate cloud administrations for CRM, stockpiling and encryption/unscrambling. As indicated by the client's requirements, CRM Cloud Services could be swapped for other capacity particular application administrations (e.g., ERP Cloud Services, Account Software Cloud Services, Investment Portfolio Selection and Financial Operations Cloud Services). Preceding the development of an accentuation on the autonomy of encryption/decoding administrations, CRM, ERP and other cloud administrations would at the same time give their clients stockpiling administrations. This study underlines that Encryption/Decryption Cloud Services must be given freely by a different separate provider.

ENCRYPTION/DECRYPTION OF SERVICE

This segment displays a CRM application benefit as an illustration of the new plan of action. After the client logs into the CRM framework, if the CRM Service System requires any customer data, it will execute a Data Retrieval Program. At the point when this information needs to be spared, it will execute a Data Storage Program. The Data Retrieval Program is outlined in Fig. 4 and is clarified underneath. At the point when a client needs to get to the CRM Cloud Service, he should first execute the Login Program as demonstrated in Step 1. This step can utilize current e-business or different administrations which have as of now safely confirmed the client's enrolment, for example, symmetric key-based test and answer login check, or through an One-Time Password. After the client's login has been effectively

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

checked, if the CRM Service System obliges customer data from the client, it sends a solicitation for data to the Storage Service System, as demonstrated in Step 2. In this step, the CRM Service System transmits the client ID to the Storage Service System where it hunt down the client's information. This information is scrambled thus, once discovered, a solicitation must be sent to the Encryption/Decryption Service System alongside the client ID. Step 3 demonstrates the Storage Service System executing the transmission of encoded customer information and the client ID to the Encryption/Decryption Service System. Since the Encryption/Decryption Service System can serve various clients and the encryption/decoding for each client's information obliges an alternate key, in this way each client's exceptional ID and keys [5] are put away together. Subsequently, in Step 4, the Encryption/Decryption Service System utilizes the got client ID to record the client's information unscrambling key, which is then utilized to unscramble the got information. Utilizing the right unscrambling key to decode the information is discriminating to restoring the information to its unique state.

ACCESS TO STORAGE SERVICE

After the Encryption/Decryption Service System has unscrambled the customer's information, in Step 5 the decoded customer information is given to the CRM Service System which then shows the customer information to the client in Step 6, finishing the Data Retrieval Program. Before sending the decoded customer information, the Encryption/Decryption Service System and the CRM Service System can secure a safe information transmission channel (e.g., a Secure Sockets Layer association) to safely transmit the unscrambled customer information. After the unscrambled customer information is sent, the Encryption/Decryption Service System is not permitted to hold the decoded information and any decoded information must be erased to keep the scrambled information and the unscrambling key from being put away in the same framework. This is a discriminating variable in guaranteeing the security of client information. The aforementioned Data Retrieval Program requires the coordinated effort of three distinctive cloud administration frameworks. Diverse routines for framework coordinated effort are now upheld by developed innovations, including two frameworks focused around Universal Description Discovery and Integration (UDDI), Web Service Description Language (WSDL), and Simple Object Access Protocol (SOAP) to utilize Web Services or transmit Extensible Mark-up Language (XML) designed information. Next, we depict the Data Storage Program, as indicated in Fig.3. This system additionally includes the cooperation of three cloud administration frameworks: CRM Service System, Encryption/Decryption Service System, and Storage Service System. Step 1 of Fig. 3 demonstrates the customer sending a Data Storage Request to the CRM Service System which then starts the Data Storage Program, asking for information encryption from the Encryption/Decryption Service System as demonstrated in Step 2. In Step 2, the CRM Service System and the Encryption/Decryption Service System make a protected information exchange channel to transmit the client ID and the information obliging capacity from the CRM Service System to the Encryption/Decryption Service System. As the encryption of information from diverse clients obliges distinctive keys, in Step3 the Encryption/Decryption Service System starts information encryption, which includes utilizing the got client ID to file the client's encryption key which is then used to scramble they got information. Emulating this present study's accentuation on the guideline of isolated power, once the customer information is encoded by the Encryption/Decryption Service System it must be exchanged to the Storage Service System where the client ID and scrambled information are put away together. Thusly, when the Encryption/Decryption Service System executes Step 4, it must exchange the client ID and scrambled customer information to the Storage Service System. Step 5 demonstrates the Storage Service System accepting the client ID matched with the information for capacity. In this plan of action, the accompanying the finishing of Step 4 at the Encryption/Decryption Service System, all decoded and unscrambled client information must be erased. Step 6, the last venture of the Data Storage Program [4], transmits a Data Storage Complete message from the Storage Service System to the CRM Service System, at which point the CRM Service System may affirm that the customer information has been put away. In the event that it doesn't get a Data Storage Complete message, it can re-launch the Data Storage Program or, after a given time of time, move ahead with outstanding circumstance taking care of. In the above illustration, the client's objective in logging into the CRM Service System is perhaps to keep up some piece of the customer information, consequently the framework outline must think seriously about information upkeep. Doable configuration techniques incorporate matching the scrambled customer information with the comparing client ID and customer ID, therefore taking into account the indexing of the client ID to get the relating customer information. At that point the customer ID might be utilized to list the customer information the client wishes to keep up. Considering the enormous measure of customer information, seek

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2014

effectiveness could be enhanced by joining the client ID and customer ID to structure a joined ID utilized for looking for a particular customer's information.

In the new plan of action, various cloud administration administrators together serve their customers through existing data innovations including different application frameworks, for example, ERP, bookkeeping programming, portfolio determination and monetary operations which may require the client ID to be consolidated with different Ids for indexing put away or recovered information. Also, the prior portrayal of the two frameworks can utilize Web Service related engineering to attain operational cooperative energies and information trade objectives. These innovations can consider open universal measures including the World Wide Web Consortium's (W3c) distributed Web Service, UDDI, WSDL and SOAP standard documentation.

V. CONCLUSION AND PROPOSED WORK

Encryption/Decryption Services" in distributed computing situations, clients of distributed computing administrations (e.g., CRM, ERP, and so on.) will utilize the administrations of no less than two distributed computing administration suppliers, so understandings between these administration suppliers are obliged to build a model for participation and division of obligations in giving a typical administration to customers. This study gives a draft of a multi-signatory Service Level Agreement[3] (SLA) in which the signatories can incorporate distributed computing rental clients, application administration suppliers, encryption/unscrambling administration suppliers, stockpiling administration suppliers, and so on., with substance including the rights and commitments in the middle of administrators furthermore incorporates information security strategies between every administrator and customers. The center idea of this study is predictable with division of administration power to decrease operational danger, accordingly maintaining a strategic distance from the danger of wrongful revelation of client information.

REFERENCES

[1] A. Weiss, “Computing in the clouds”, net Worker, vol. 11, no. 4, pp. 16-25, December 2007.
[2] C. S. Yeo, S. Venugopal, X. Chu, and R. Buyya, "Autonomic metered pricing for a utility computing service", Future Generation Computer Systems, vol. 26, issue 8, pp. 1368-1380, October 2010.
[3] B. R. Kandukuri, V, R. Paturi and A. Rakshit, “Cloud security issues,”in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.
[4] R. Sterritt, “Autonomic computing,” Innovations in Systems and Software Engineering, vol. 1, no. 1, Springer, pp. 79-88. 2005.
[5] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computer Systems, vol. 25, issue 6, pp. 599-616, June 2008.
[6] L. M. Vaquero,L. Rodero –Merino ,J. Caceres, and M. Lindner, “A breakin the clouds: towards a cloud definition,” ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50-55, January 2009.
[7] C. Weinhardt, A. Anandasivam, B. Blau, N. Borissov, T. Meinl, W.Michalk, and J. Stößer, “Cloud computing – a classification, business models, and research directions,” Business & Information Systems Engineering (BISE), vol. 1, no. 5, pp. 391-399, 2009.
[8] N. Hawthorn, “Finding security in the cloud,” Computer Fraud &Security, vol. 2009, issue 10, pp. 19-20, October 2009.
[9] A. Parakh and S. Kak, “Online data storage using implicit security” Information Sciences, vol. 179, issue 19, pp. 3323-3333 ,September2009.
[10] R Rivest , A. Shamir, and L. Adleman , “A method for obtaining digital signatures and public key cryptosystems”, Communications of the ACM, vol. 21, no. 2, pp.120-126, 1978.
[11] V. Miller, “Uses of elliptic curves in cryptography,” Advances in Cryptology - CRYPTO '85, Lecture Notes in Computer Science, pp.417-426, 1986.
[12] L. Lamport, “Password authentication with insecure communication, ”Communications of the ACM, vol. 24, no. 11, pp. 770-772, 1981.
[13] A. Elgohary, T. S. Sobh, and M. Zaki, “Design of an enhancement forSSL/TLS protocols,” Computers & Security, vol. 25, no. 4, pp. 297-306,June 2006.
[14] Salesforce.com, Inc., “Force.com platform,” Retrieved Dec. 2009, fromhttp://www.salesforce.com/tw/
[15] SAP AG., “SAP services: maximize your success,” Retrieved Jan. 2010,from http://www.sap.com/services/index.epx
[16] D. Benslimane, S. Dustdar, and A. Sheth, "Services mashups: the new generation of web applications". IEEE Internet Computing, vol. 12, no.5, pp. 13–15, 2008.
[17] A Business Model for Cloud Computing Based on separate Encryption and Decryption. 978-1-4244-9224-4/2011/IEEE, Jing-Jang Hwang and Hung-Kai Chuang, Yi-Chang Hsu and Chien-Hsing Wu
[18] http://www.php.net/
[19] http://www.wikipedia.org/
[20] [20] http://www.w3schools.com/