A SECURED DATA TRANSMISSION IN A CLOUD ENVIRONMENT USING ENHANCED CODE CERTIFICATION AND AUTHENTICATION TECHNIQUE

Vijyendra Karpatne[1], Dr.E.J.Thomson Fredrik [2]

ABSTRACT

Every organization wants to safeguard its data when it travels within cloud. In the existing approaches, issues related to cloud storage and specific data protection techniques have not been addressed particularly to protect the data or email information within cloud. Hence the trust is significantly reduced, when any organization gets service from Cloud Service Provider (CSP). In order to overcome the above-mentioned issues, this paper, discusses code verification technique, implementation of DPaaS, RAM Virtualization and Algorithm to secure the emails within cloud. In case of private cloud, the data stored by the user is accessible only to the data owner. Data security across all the cloud types is dependent on the security measures instituted by the service provider. The service provider may provide resources in the form of Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), but concerns about security which have been raised. This paper analyses various challenges in Cloud storage security. Virtualizing RAM technique and server-side flash memory are proposed to overcome the challenges of cloud storage security. The proposed cloud based email Security as a Service (SecaaS) has unique capabilities which can really secure the emails which are travelling along in cloud environment.

Key words: CSP, SaaS, IaaS, DPaaS, SecaaS, RAM

I. INTRODUCTION

The important belief of cloud computing is based on the chief idea of congregated organization and collective resources. Improving the efficiency of the shared resources is one of the targets of cloud computing. Cloud computing architecture offers three types of computing clouds public, private and hybrid. Therefore, when resources are shared with the consumers, there is no control over the cloud. Private clouds are owned by individual companies which control the cloud resources. Hybrid clouds are a combination of public and private systems. But the companies which provide service often dictate the offered cloud services and controls. Data security across all the cloud types is dependent on the security measures instituted by the service provider. The service provider may provide resources in the form of Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS), but concerns about security which have been raised.

This paper analyses various challenges in Cloud storage security. Virtualizing RAM technique and server-side flash memory are proposed to overcome the challenges of cloud storage security. The proposed

[1]Research Scholar, Department of Computer Science,Karpagam Academy of Higher Education E-mail: karpatne3@gmail.com

[2]Associate Professor, Dept. of CS, CA & IT, Karpagam Academy of Higher Education E-mail: thomson500@gmail.com

Virtualizing RAM technique will help to improve the performance of a large amount of memory in cloud storage. The results of implementing Virtualizing RAM technique and server-side flash memory shows that data security of cloud storage is enhanced and cloud storage memory is used efficiently.Email plays a dynamic role in business communication among parties. The email facility can be used with different types of software clients and almost on all web browser. Safeguarding email in cloud is equal to safeguarding email in the organizations or enterprise. Cloud based email Security as a Service (SecaaS) has unique capabilities which can really secure the emails which are travelling along in cloud environment. Cloud based service providers must ensure the security and authenticity of the email message

2. LITRATURE REVIEW

The objective of this section gives a brief summary of the available review articles corresponding to cloud security. The review articles and surveys studied in this section do not particularly highlight cloud security, more than the principal necessities which will simplify it. The work about cloud security is relatively new and quickly increases the reputation of the cloud in addition to the developing necessities to share information among people. Tarunpreet Bhatia and A. K. Verma, 2017, analyzed various biometric, cryptographic and multifactor lightweight solutions for data security in cloud and conducted a survey. Reddy and Balaraju, 2018, did a comparative study on third party auditor to provide integrity and security in cloud computing. It was ensured that the reliable data storage systems were providing computing resources as a service. Ramalakshmi.S and Rexy J 2017, proposed the cloud data classification which was done automatically by applying proper algorithms and data was encrypted based on the classification. Their proposed method reduced the processing power, memory usage and the time consumed of cloud computing.

Valentina el al 2018, illustrated a security SLA-based monitoring approach and outlined the problems related to monitoring security in the cloud. Real cases were provided related to offering services protection against Denial of Service (DoS) attacks.

Shabeera et al. 2017, discussed the problems about virtual machines allocation in cloud-based platforms. They proposed the technique to resolve the data transfer delay between virtual machines. Chien et al. 2018, proposed a new cell programming method to improve the chip performance in cloud-based platform. The proposed method also helped to reduce the bit error rate.

Akashdeep and Sam 2017, examined the kinds of threats for cloud-based email systems and the solutions for those threats. Mitigation of risks in cloud-based email required service providers and corporate users to adopt a universal approach. This approach ensured security especially when the application services were used over insecure Internet connection. Mohamed et al. 2018, proposed a security service model which allowed cloud users to monitor and protect their cloud-based emails and other information by deploying this proposed security mechanism in the cloud environment.

3. Secure Data Transmission in CLOUD Using Code Certification and Authentication Technique

3.1. EXISTING WORK

At times the user can set privacy settings, so that only

authorized user can access the data. In case of private cloud, the data stored by the user is accessible only to the data owner. In the case of data storage, security and privacy issues are possible. In order to secure and protect data, various techniques and methodologies were used. The existing work never describes the use of code verification and using of code certificate, in order to perform secure and trusted sharing of data transmission.

3.2. THE PROPOSED WORK

The proposed work, mainly focuses to protect the information at transportation and data in use by incorporating the code certification and authentication methodology. The code certification is a methodology to cover the vulnerable information from the users. In the cloud surroundings, this method works for the data in such a way that it ensures the reliability and belief in the cloud surroundings. The policies of the code certification and the authentication technique for information at transportation and data in assist help to improve the overall security cloud surroundings.

3.3. CODE CERTIFICATE AND AUTHENTICATION PROCEDURE IN THE PROPOSED TECHNIQUE

The pad bit generator is creating the padding bits and it is known as random bits. Whenever a novel user accesses the private cloud, a series of pad bits by the side of with the reference index is created. The pad bit series are only recognized by the data holder. The data which is recorded in private cloud are encrypted with the assistance of secure key generator before being stored. Along with the encryption method, these pad bits are included in the data are stored in the private cloud. The accumulation or elimination of pad bits is taken care by Account Centre. The account center credit value can be updated for every transaction, by the side of with the pad bits. Suppose the transaction process is efficiently completed, the positive credit value is updated, and suppose the transaction is a failure, negative credit value is updated.

There are two parts in Secure Key Centre. One is secure key generator and key index. The encryption key is created by the secure key generator which is used for encrypting the information to be stored in the private cloud. Every secure key/encryption key has a suitable key index. While the data is to be stored in cloud, they are encrypted with the assistance of secure key generator for code certificate and authentication process. The encrypted data by the side of the pad bits is transferred to the private network. While the data is to be retrieved, the pad bits are eliminated and after that it is decrypted with the assistance of decryption key. This process of eliminating pad bits and decrypting the data is referred to as data preprocessing. System architecture of implemented model is shown in Figure 1.

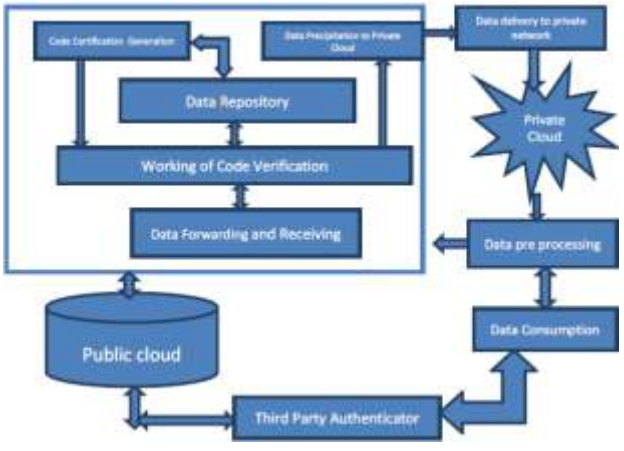

FIGURE 1.SYSTEM ARCHITECTURE OF IMPLEMENTED MODEL

The pad bit generation algorithm is used to create the

padding bits. At this point, the OAEP algorithm with the RSA is used to create the pad bits. The pad bits are created randomly and it is highly complex to calculate the pad bits, owing to its randomness. If the entire normal text is retrieved by deriving the accurate cryptographic hash bits or the complete text is lost, it will use a rule of All-or-nothing. This rule makes this algorithm highly efficient and more secure. The sum of the pad bits to the stored data in the private network is completed with respect to ensure the high security and privacy. As the pad bits are called by the user, and also the pad bit series is created randomly, the probabilities for affecting or eliminating or hacking the data is very low, while it is differentiated to the conventional encryption methodologies. Security is high, data integrity and accessibility are made potential and the real data is returned to the data owner.

The third-party authentication is a component where the third-party authenticator gets the track of all the activities carried out in the private and public network. The authenticator monitors all the activities and blocks the unwanted activities carried out in the network. The third-party auditor is also responsible for generating the key and sending it to the original user.

These calculations are done in the cloud simulation environments whose values are then differentiated with the previous system calculation values. The complete details of the performance calculations and their differentiation are provided in the following sections. The differentiation is made between the proposed Secured TPA, code certification and authentication,and the previous Authentication Codes and encryption methods.

4. Enhancing Security of Data in Cloud Environment Using Data Protection As a Service (DPaaS)

4.1. EXISTING WORK

Cloud computing architecture offers three types of computing clouds public, private and hybrid. Depending on the type, the security threats and risks vary. The company or service provider owns the public cloud. Therefore, when resources are shared with the consumers, there is no control over the cloud. Private clouds are owned by individual companies which control the cloud resources. Hybrid clouds are a combination of public and private systems. But the service providing companies often dictate the offered cloud services and controls. Data security across all the cloud types is dependent on the security measures instituted by the service provider but the application of DPaaS was never experimented as a data centric approach to safeguard cloud data.

4.2. PROPOSED WORK

Despite the popularity of Cloud computing, it has many challenges. Teething problems are highlighted in major cloud development applications in providing cloud services. Security of the clients' data should be a joint venture of organizations, institutions, companies, agencies, and governments to eliminate the cyber security threats which results in cyber terrorism activities, Accountability is provided because it offers auditing and logging. Maintenance issues are directly addressed by DPaaS, development as well. In the existing environment, providers should offer this DPaaS.

The challenges in the proposed approach aim at handling threats to the data transmission and privacy

concerns are recorded in different system components. The first drawback associated with the existing structure is a strain on the resources particularly from the software developers, whose attention and concentration goes into developing multiple codes to suit different environments in the cloud (Ryan, 2013). In case of DPaaS applications approach, Cloud application developers may concentrate only on the business logic.

The success of a DPaaS is pegged on the ability of the computing world to work together in a comprehensive manner. The approach's service may be a culmination of efforts from all players in the sector as opposed not to share the resources and having the investors continuously reproduce the works undertaken by other experts (Ertaul, Singhal, &Saldamli, 2010). The security concept leans on the adoption of an open source methodology, although concerns about such an approach may be expected. The industry demands increased collaboration between security agents, firms, and institutions in developing a comprehensive plan against attacks to data and privacy, and in the age of the cloud, such an opportunity exists, embodied by sharing technologies and developments on improving security.

4.3. ALGORITHM

The cipher text classes are created according to the data size. In this method, before determining the number of cipher text classes, the communication will be initialized between the user and the server. After the data has been sent, data is transmitted to the server and the server response the user about the cipher text classes. This will be determined based on the number of specific classes. Assume E is the given service in excess of a finite field, process P is added itself N times creates the identity; NP=id, where the notation nQ for integer and point means the n-fold addition of Q with itself. The original message is denoted as m as a point of the service, Se. the data protection service problems are based on this execution and it is inverted all the way through the formula,

Algorithm for DPaaS in cloud environment

1. Input as the information or data gathered for transmission in cloud
2. send the data to the S //S=Server, =Person
3. Server gives the data to SeCC
4. S sends the to the
5. gets the NK,SK, MS from HIA //NK=Normal key, SK=Semi-functional key, MS=Master secret key and HIA=Health Insurance Authority
6. // encrypts the HD
7. //=Normal cipher text for health data, HD=Health data
8. //= Semi-cipher text for health data, i=index\
9. //KS=Particular set of cipher text classes, S=Set of cipher text classes
10. encrypt the data and stored in cloud storage
11. // organizations decrypt the data
12. //AK=Aggregated key
13. Organization decrypt the data and provide return information (example Medical prescription say MP.)
14. //=Normal cipher text for Medical prescriptions,

MP= Medical prescriptions

15. //= Semi-cipher text for Medical prescriptions

16. Organizations encrypt the data and stored in cloud storage

17. // decrypt the data (Data are secured with DPaaS with greater value)

18. get the medical prescriptions. (All information protected with better security)

Algorithm describes the DPaaS technique. In this algorithm, data in cloud are transmitted and stored in the cloud storage. In the encrypted format the information is stored. For the encryption process, the dual encryption method is used with cipher text classes. The particular cipher text ids are aggregated, generate the aggregated key and send to the organization. The organization accesses and decrypts the data and using aggregated key. The organization provides the required information by attaching to the message, in the encrypted format by using the same as the dual encryption method with cipher text classes. Then the recipient decrypts the data using the aggregated key. Finally, the person gets the response back with the greater data security.

5. The Cloud Storage Security Using Virtualizing RAM and Server-side Flash Memory

5.1. EXISTING WORK

Despite many advances made to the cloud environment, Data storage in Cloud Computing continuously faces information security issues. These challenges, though few and concentrated, impact the growth of cloud computing in the business industry as many strive to hold onto their data in house for as long as possible. The security issues in storage are marked as one of the biggest challenge because movement of data without any loss or attack is never simple in cloud. We do not have evidence ofRAM Virtualization technique with Flash memory implementation to improve the performance of a large amount of memory in cloud storage. In the existing scenario, RAM Virtualization was not used in cloud to make the cloud storage efficient but that technique was used in cloud for other purpose.

5.2. THE PROPOSED WORK

Historical data plays an important role in cloud computing environment, where it needs to be handled carefully. However, the nature of cloud resources becomes volatile to handle the sensitive information where there is high possibility of data corruption. Thus, selection of good cloud storage resources becomes the importance factor in order to store the health care data or any other personal data in a sensitive way. There are various requirements are considered for storing and retrieving the cloud data with more performance improvement. The requirements are considered in terms of both cloud user satisfaction level and cloud resource reputation.

5.2.1. CUSTOMER'S VIRTUAL STORAGE REQUIREMENT IN CLOUD

Due to the improvement of public cloud contributions for the cloud customers, it is complicated to decide whether the contributor can satisfy the cloud storage virtual peripheral requirements. In cloud environments, the storage services are given by the cloud contributor have numerous cost and performance stages. For that reason, the clients face complications to choose the best

service provider for their needs. The computing services such as Assurance of storage Service, Usability, Security and Privacy and Accountability are calculated to grade the cloud services. By using this assessment, the clients discriminate the cloud storage services.

5.3. OPTIMAL CLOUD VIRTUAL STORAGE SERVICE SELECTION BASED ON SCORE VALUE

In this segment, the virtual machine is denoted as V and the group of physical nodes is denoted as H. The process from V to H is represented as M (M: V H). The summary holds the data grouped from the client's clues and client requests. The client is motivating the combined with VM provision which makes the consumption patterns. The VM importance to resources of the physical node is compared with the patterns.

To discover the adjacent-optimal VM-to-host association, this technique doubles the summary evaluation and production from the process. This process can be located into two types:

1) Soft Constraints: The satisfaction level of constraints that is appropriate to the class contributes to the entire superiority of the produced profile.

2) Hard constraints: Postulations located in this collection have to be satisfied to their complete degree.

Algorithm : Scheduling Cloud Services based on Customer Hints and storage desires

Input: Set of VM and Set of physical nodes, client Constraints

Output: Optimal selection of profiles

1. Organize the and physical nodes set referred as
2. Client server needs and clues are specified as input
3. // client clues
4. // Mtraf= smallest amount traffic in the physical network
5. // SupportVM= Reserve single hosting node for a specific VM
6. // client storage needs
7. // Computation of Average response time
8. // Where = time surrounded by the client I requested for IaaS service, n= Total number of requests
9. // Computation of flexibility
10. // Computation of Energy efficiency
11. // Computation of reliability
12. // anywhere n_failure=Number of clients who capable failure in a time interval, n= Number of customers, = promised mean time to failure
13. // Computation of Stability
14. // Where = Computation unit, = experiential average performance, = promised values in the SLA, T=Service Time, n= Total number of customers
15. //Computation of Availability
16. // Computation of Usability
17. Client constraints= client clues + client storage needs
18. Combine client constraints and VM specifications
19. Generate a deployment pattern
20. //CC=client Constraints, =Set of the entire clues , = Set of storage needs, and w individual weights
21. // counterpart the VM needs to physical node resources

22. The whole constraint is defined by utility function
23. F: [0, 1] // Where represented set of the entire deployment profiles
24. //Score Measurement
25. // Where is set of the complete constraints and w is the weights of individual
26. // Choose the Best profile
27. Based on the score value the optimal profile is selected
28. If(Score () Score (
29. Return best profile for RAM virtualization & Flash memory for data storage in cloud.

6. Overcoming Email Security Issues in Cloud Using SecaaS

6.1 EXISTING WORK

Email plays a dynamic role in business communication among parties. Customers, organization staff and service providers can interact with one another effectively via email. The data can be transferred very easily between senders and receivers over the Internet. The email message can be stored, received, replied to or forwarded as per the user's choice. Safeguarding email in cloud is equal to safeguarding email in the organizations or enterprise. Cloud based email Security as a Service (SecaaS) was never implemented in such a way to really secure the emails which are travelling in cloud environment.

6.2 THE PROPOSED WORK

In case of the email security in cloud, lot of issues and challenges arise. Sometimes it is really difficult to overcome, as daily a new malware attack on email is invented. The email is the only medium where the malware attack can be made very easily and in cloud where millions and millions of emails flow on a daily basis. It is very easy to add a malicious email links to the original email and deliver them to the recipients.

6.3 PROPOSED ALGORITHM FOR SecaaS FOR EMAIL SECURITY

In the proposed solution, a feature on the AES encryption algorithm is added. This is considered as one of the most secure algorithms for email security. The algorithm is applied to encrypt data in fixed size block at a time. The key bit encrypts or decrypt block in 128 bits. At every round plain texts are converted into cipher texts. The proposed solution offers the security using SecaaS because it allows 192-bit encryption and decryption. A total of 12 rounds get completed for converting the plain text into cipher text. Only 10 rounds of conversion are possible in the existing algorithm. In the proposed solution, the key size is too large hence it automatically more secure. Moreover, it is never slower than another encryption algorithm. This solution provides more flexibility to choose key process and encryption process. This can be used without many restrictions. The following algorithm states the steps for encryption and decryption.

The encryption algorithm involves the following steps:

Step 1 - Originate the set of round keys on cipher key.

Step 2 - Get block data and initialize the array. The block data is the plaintext.

Step 3 - Add the initial round key in the starting of array.

Step 4 - Perform 10 rounds of manipulation and perform Sub byte, shift row, mix column and round key stages.

Step 5 - Perform 11th round of manipulation separately.

Step 6 - Perform 12th round of manipulation to handle 192-bit. This round has manipulation slightly different from other rounds. This will be considered as the FINAL round.

Step 7 - Get the Cipher text as a final array state.

The decryption process to get the plaintext from the cipher text involves the reverse process which we followed in encryption process above.

The decryption algorithm involves the below steps

Step1 - Perform initial decryption stages
Inverse_round, Inverse_shift, and Inverse_subbyte

Step 2 - Perform ten full decryption stages
Inverse_round,
Inverse_MixCols,Inverse_shift, and
Inverse_subbyte

Step 3 - Perform 11th round separately.

Step 4 - Perform Final 12th decryption round

Step 5 - Obtain plain text.

The proposed approach incorporates using all available methods of email security, protection, email message encryption, logging, handling malicious links and early malware attacks.

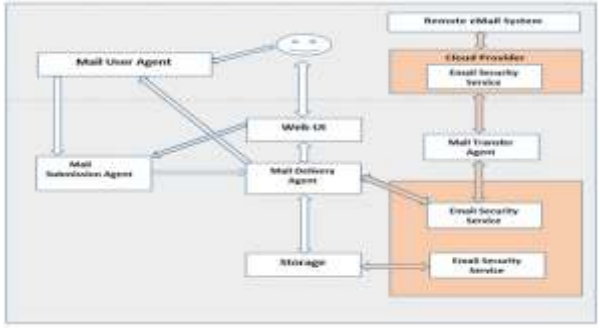

FIGURE 2. EMAIL SECURITY WITHSecaaSIN CLOUD COMPUTING

The Figure 2, demonstrates that the security control policies are applied on the email message in cloud. Answerability is provided since it offers email security measures, logging and auditing. As SecaaS is implemented using data centric approach, email messages will be scanned right from the beginning. SecaaS gives more importance to email messages. This data centric approach will also help to detect the new and real-time attacks on the email message as it exchanges the information from MTA (Mail Transfer Agent). This approach of SecaaS enables the system to have information exchange from the remote email system for deliveries.

8. CONCLUSION

In this paper, various methodologies have been proposed to ensure the secured and trust aware cloud environment where the user's stored contents are secured from malicious access and also protected from third-party clients to find ownership details of the particular contents. This environment is more suitable for the Health care environment where patient's information is stored in the private cloud storage from which it is proved that the proposed method leads to provide better result. In the first work, it is shown that the use of code certificate in this system architecture ensures secure and trusted transmission of data between public and private cloud based on code verification. The code generator generates the code certificates where a random set of numbers is generated. The code certificate must match with the code index table with which the verification process is performed. The user can only generate the code certificates corresponding to the data accessed which ensures data integrity. The second work proposes a new method called Data Protection as a Service,(DPaaS)

that provides efficient security of data in cloud environment. In the third work, RAM Virtualization and memory flash technique has been adopted to provide extensive security of data storage in cloud environment. Companies desire a technology that is flexible, adaptable, and evolving with an exit door available should a better technology solution be developed. The usage of virtualizing RAM technique and server-side flash memory in cloud computing storage enhances that data security of cloud storage and improves the efficient usage of cloud storage memory.In the fourth work, cloud based email security has been adopted. The proposed SecaaS explanation combines integration and security in a solitary dais. SecaaS delivers the model for integration of security services into cloud computing infrastructure. SecaaS overcomes the several issues with the email security in cloud by providing security features such as strong encryption, logging, theft detection, malware filter and early malware detection on email messages. The authentication framework in cloud network will be improved further in the future work for increasing the privacy of personal data. We plan to implement an advanced biometric security scanning in securing the data stored in the cloud.

REFERENCES

[1] Akashdeep Bhardwaj and Sam Goundar "Security challenges for cloud-based email infrastructure" Network Security, Vol. 2017, Issue 11, pp. 8-15, November 2017.

[2] Chien-Chung Ho, Yu-Ming Chang, Yuan-Hao Chang and Tei-Wei Kuo, "An SLC-Like Programming Scheme for MLC Flash Memory" ACM Transactions on Storage, Vol.14, No.1 pp.1-26 · March 2018.

[3] Mohamed Hawedi, ChamseddineTalhi and HanifaBoucheneb "Security as a Service for Public Cloud Tenants" Procedia Computer Science Journal, Vol. 130,No. 18, pp. 1025-1030, 2018.

[4] Ramalakshmi S, Rexy,J.,Enhancing Cloud Security with Automatic Data Classification and Appropriate Encryption Algorithms, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 1, pp.1027-1032,January 2017.

[5] Reddy Shirisha K, Dr.M.Balaraju "Third Party Auditor To Provide Integrity And Security In Cloud Computing", Materials Today, A-Peer-reviewed scientific Journal,Vol. 5, Issue 1, No. 1, pp. 557-564,2018.

[6] Shabeera T P,SDMadhu Kumar and Priya Chandran, "Curtailing job completion time in MapReduce clouds through improved Virtual Machine allocation", International Journal ofComputers & Electrical Engineering, Vol. 58, pp. 190-202, February 2017.

[7] Tarunpreet Bhatia,A. K. Verma, "Data security in mobile cloud computing paradigm", The Journal of Supercomputing , Vol. 73, Issue 6, pp. 2558-2631, ISSN: 0920-8542 10.1007/s11227-016-1945-y, June 2017.

[8] Valentina Casola, Alessandra De Benedictis, Massimiliano Rak and Umberto Villano, "Monitoring Data Security in the Cloud: A Security SLA-Based Approach", Handbook - Security and Resilience in Intelligent Data-Centric Systems and Communication Networks, 1st Edition, Author- Massimo Ficco, pp. 235-259, 2018.