International Journal of Engineering & Technology, 7 (1.1) (2018) 64-70

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An enhanced security tree to secure cloud data

S. Renu[1*], S.H. Krishna Veni[2]

[1]Research Scholar, Dept. of CSE, Noorul Islam University, Tamil Nadu, India
[2] Assistant Professor, Dept. of IT, Noorul Islam University, Tamil Nadu, India
**Corresponding author E-mail: renus23@gmail.com*

Abstract

The Cloud computing services and security issues are growing exponentially with time. All the CSPs provide utmost security but the issues still exist. Number of technologies and methods are emerged and futile day by day. In order to overcome this situation, we have also proposed a data storage security system using a binary tree approach. Entire services of the binary tree are provided by a Trusted Third Party (TTP) .TTP is a government or reputed organization which facilitates to protect user data from unauthorized access and disclosure. The security services are designed and implemented by the TTP and are executed at the user side. Data classification, Data Encryption and Data Storage are the three vital stages of the security services. An automated file classifier classify unorganized files into four different categories such as Sensitive, Private, Protected and Public. Applied cryptographic techniques are used for data encryption. File splitting and multiple cloud storage techniques are used for data outsourcing which reduces security risks considerably. This technique offers file protection even when the CSPs compromise.

Keywords: *Trusted Third Party, Security Tree, Data Security, Data Classification, Data Storage.*

1. Introduction

The future of cloud gazes to the area of data storage management.. A reliable and secure data storage and management remould the face of cloud computing. Wiki describes "*Cloud computing security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.*"The security issues are increased rapidly along with the cloud services. Most of the Cloud service providers offer complete security to their product. But it is not up to the mark. We can concentrate on storage data security and its solutions [8]. Security and privacy are the major concerns of cloud storage. Some of the security threads are i)Loss of availability[4] ii) Loss and corruption of data [5][6] iii) Loss of privacy[9] iv) Vender lock-in[7] v) virtualization and accessibility vulnerability [10], data intrusion, service layer Agreements , data backup, legal issues, etc.

Through this security approach we have concentrated the protection of organizational data. Highly confidential organizational data is the input of our security system. Most of the company data are unorganized and mixed with non-confidential files. It is not possible to detect how many employees access or copies the data. It is noted that most of the data attacks are internal attacks. The possibilities of internal attacks are performed from either within the organization or within the outsourced storage device. It is not possible to develop a hardware or software for complete data security. Managing available security resources in an organized way is the only way to enable complete security. A security tree is designed to develop a complete security system.

2. Related works

C.Wanget.al[11][12] proposed a model ensuring data storage security in cloud computing analyze how the dynamic data storage with token precomputation is stored in the cloud and it provide information about effective storage mechanisms. Integrity is checking is used to detect and avoid misbehaving server data correction and error localization. Distributed system is employed to accomplish the data quality, availability, integrity of reliable storage services.

Hsiao.et.al[13] proposed a Secure Erasure Cod-Based Cloud Storage System with secure data forwarding model discussed the data storage using dynamic data operation. The distributed system is employed to carry out the forwarded data in cloud without retrieval, which ensure secure and robust data in cloud storage.

Q.Wang et.al[14] proposed Enabling public audit ability and Data Dynamics for storage security in cloud Computing model analyzed the data integrity in cloud storage devices. The intention is to get independent perspective and quality in service evaluating with third party auditor. The factors behind the data integrity are Dynamic data operation and public auditability. Storage model is developed to maintain multiple auditing tasks which improve efficiency.

S.K.Sood[15] propose a method a combined approach to ensure data security in cloud computing. The frame work has two phases, first phase deals with the process of transmitting and storing data securely into the cloud which include data classification, Index building and encryption uses Message Authentication Code (MAC).Second phase is index building and encryption where an index builder is used to create an index for searching over encrypted data.

C.Esposite .et.al[16] proposed a model regarding cloud based security and privacy in health networks. Latest and valuable tools

that help the organization and interconnection of health data have become a prerequisite for monitoring and preventing illness and also for distribution of medical knowledge. Currently, cloud-based solutions can carry joint data science platforms and send all types of processing operations throughout the network service chain. Here, the authors deal with healthcare-related data administration and exchange, and develop security and privacy necessities collectively with a novel micro services approach. This work shows how cloud computing can be accepted within healthcare models. The interoperability of traditional technologies improved the value of life and the competence of healthcare systems by creating it more personalized and centred on patients, together with reducing operational costs and medical errors. The authors analyzed and addressed the security and privacy issues, and develop a socially accepted health network service chain. They investigate the security and privacy necessities and allegations, and also studied existing systems, and in the end develop architecture of a secure manager for cloud-based healthcare-related data management and exchange.

H.Chen.et.al [17] develops a model which focuses Security-Sensitive Intermediate Data by using Selective Tasks Duplication in Cloud environments. With the extensive consumption of cloud computing in numerous business enterprises as well as science and engineering domains, high quality safety services are increasingly critical for giving out workflow applications with confidential transitional data. However, most accessible workflow scheduling methods ignores the security necessities of the intermediary data produced by workflows, and fail to notice the performance impact of encryption time of intermediary data on the start of successive workflow tasks. The inactive time slots on resources, resulting from data dependencies with workflow tasks, have not been sufficiently exploited to alleviate the impact of data encryption time on workflows' makes pans and financial cost. To focus these problems, this work presents an innovative task-scheduling structure for security sensitive workflows with three key characteristics. First, They offer a complete theoretical analyses on how selectively duplicating a task's antecedent tasks is helpful for preventing both the data transmission time and encryption time from waiting task's start time. Secondly, the workflow tasks' newest termination time, and prove that tasks have been completed before tasks' latest termination time by using cheapest resources to reduce financial cost without delaying tasks' descendant s' start time and workflows' makes pans. Finally, considering these analyses, they develop SOLID- a new scheduling approach with selective tasks duplication, which incorporate two important phases: 1) task scheduling with selectively duplicating antecedents tasks to inoperative time slots on resources; and 2) Transitional data encrypting by efficiently exploiting tasks' laxity time. The authors evaluate this work through exact performance assessment study using both arbitrarily generated workflows and some real-world workflow traces. The authors demanded that their work named SOLID, approach succeed over existing algorithms in terms of makes pan, financial costs and resource competence.

M.Kalhar et.al [18] make a review focusing cloud data auditing techniques. Huge quantities of data are accumulated with cloud service providers nowadays. Third-party auditors (TPAs), using cryptography, were frequently utilized to verify this data. But, most auditing systems haven't keep cloud user data from TPAs. An analysis of the state of the art and research in cloud data auditing methods emphasizes integrity and privacy challenges, solutions, and future research directions.

R.Barona and E.A Mary Anitha have proposed a system which discussed the severity of data breach challenges [19]. Cloud computing is an advance method which facilitates pay-per-use access to a gathering of shared resources for specific systems, servers, stockpiling, applications and administration, without physically receiving them. So it spares management expense and time for organizations. Many industries, for example, keeping money, social insurance and instruction are moving towards the cloud because of the efficiency of managements gave by the compensation per-use plan in view of the resources, for example, preparing influence utilized, storage capacity devoured, exchanges completed, information exchanged, or storage room possessed and so on. Cloud computing is a completely web based innovation where customer data is put away and reserved in the server farm of a cloud supplier like Amazon ,Google, Salesforce.com and Microsoft and so on. Constrained control over the data may obtain different security concerns and threats which include unreliable connectivity, data breach, inside attacks, sharing of resources, and data accessibility. A break of security may direct to the unintentional or illegal destruction, alteration, loss, personal data transmitted, unauthorized disclosure of, or access to, stored or otherwise processed. There are number of research challenges likewise there for embracing data breaches on cloud computing. This survey scans about cloud computing, various cloud models and primary security threats and data breach issues that are presents in the cloud computing framework. The authors investigates the remarkable research and difficulties that presents data breach in cloud computing and offers best practices to service providers and furthermore activities plan to influence cloud servers to enhance their key concern in this serious economic situation.

3. Proposed system

We have proposed a security tree for data security using Trusted Third Party (TTP). TTP is government or reputed organizations which ensure complete security at the entire cycle. TTP have develops, updates and audit security services for clients, but there is no direct contact with user data. An exciting feature of TTP is its binary tree structure. A binary tree which all the security features are represented by nodes.

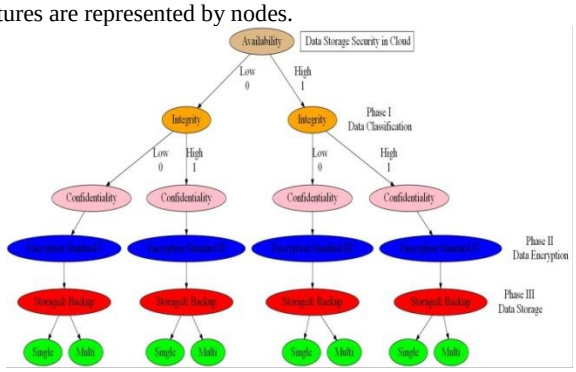

Fig. 1: Tree structured view of data security system

Figure1 shows a binary tree with three different Phases of services and shows a hierarchical relationship between them. Availability is the root nodes which categorize files into left and right sub trees having different security features. Each phase uses binary trees for the proper implementation. The three phases are Data classification, Data encryption and Data storage. Services of all the three stages are provided by TTP and are executed at the user side. Left sub-tree represent confidential data and right sub-tree shows non confidential data or public data. At the first phase a weighted CIA tree is used for data classification. This is performed inside the availability node. A weighted binary tree structure is also used for key generation in the second phase i.e., data encryption. A binary tree is used as a file organizer at the data storage phase. The security rating of each path is different.

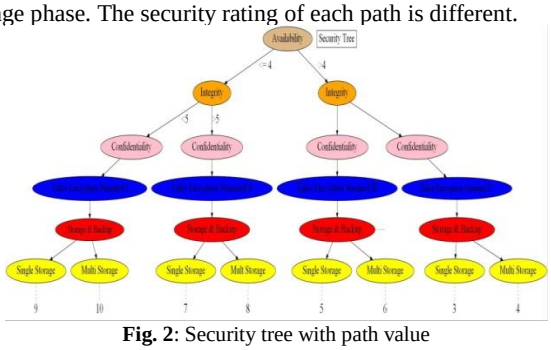

Fig. 2: Security tree with path value

Each path has path value depending on the security offered by the security tree. The path with higher value offers higher security and path with lower value offers lesser security.

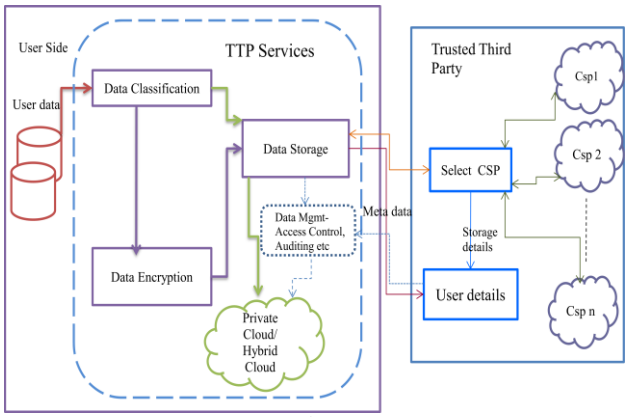

Fig. 3: Architectural view of data storage security system

The architectural diagram shows an overview of Trusted Third Party with its valuable services at the user side. The two main blocks represent the user side and the organizational (TTP) side. The dotted lines show the services provided by TTP at the user side.

3.1. Phase 1-data classification

Classification is executed at the root of the security tree. Data classification has major role in all the organizations. It is not necessary to employ all data in farthest security. Every nation has some standard laws and policies regarding data classification [1]. Categorize organizational data into some category either using organizational policies and procedures or national standards and laws. Unorganized files can be classified into sensitive, private, protected and public. Sensitive data are highly confidential and needs a higher level of protection. Private files are confidential but not higher than sensitive data. Protected file needs average level of security and public files have no security. An automatic data classification system can be used for file classification [2][3]. The user data will pass through an automatic data classification system and after classification the data can be categorized into sensitive, confidential, private and public. This categorization is based on level of confidentiality, integrity and availability. Input of the data classifier will be unstructured organizational data and output will be categorized data with security rating. The level of security rating is depended on the requirement of the user.

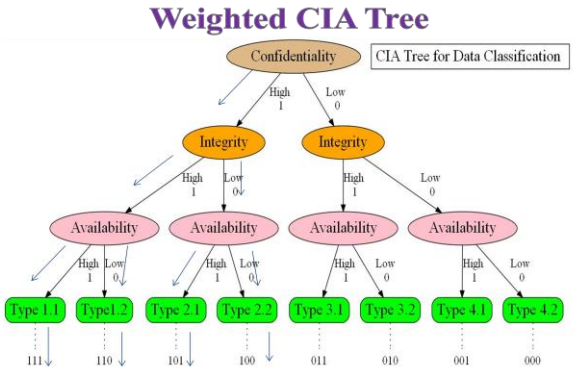

Fig. 4: CIA classification tree for file classification

A dictionary based string matching algorithm is carried out at the root of the weighted CIA tree[20]. Files can be classified based on its confidentiality. Dictionary based pattern or string matching algorithms are used for classification. The dictionary contains keywords or strings related to the sensitive or private and its corresponding security values. If the confidentiality is high, four different path having security values 111,110,101 and 100 are activated. If confidentially is low, right sub tree is activated having security values 011,010,001 and 000.

3.2. Phase 2-data encryption

Four different encryption schemes are used for encrypting at the second stage. Applied cryptographic methods are suited to this stage because four different encryption schemes are applicable here. More complex methods are needed at the left sub tree and less complex methods for right sub tree. It is necessary to grow and shrink the security aspects based on the requirement of the user. A combined feistal and substitution networks are used for encryption and decryption process. The chief characteristics of this network are that user can decide number of round functions and number of substitution matrices etc. Each round has two functions where we can use either same or different matrices. The data administrator has a facility to select appropriate functions from a list of available functions.
The modern cryptography techniques such as 3DES, AES etc can also be used. User has a facility to choose the encryption scheme based on the requirement and confidentiality of the data.

3.3. Phase 3-data storage

Data outsourcing is a major concern since CSPs started the outstanding facility storage as a service. The entire CSPs offers high security but security risks such as business continuity, data backup, legal issues, malicious insider, outsider attack etc are still remains. Storing files into multiple locations can reduce the risks. No need to store all files into multiple locations. It is better to use a file organizer to categorize files into single and multiple locations. File organizer is a node where all features are concentrated into single or multi storage locations. The file organizer is the parent nodes of leaf nodes, which is shown just above the leaf nodes. File having less availability is stored in single location and high availability stored in multiple locations. File splitting technique is used here. Two type of splitting is used before storage such as splitting before encryption and splitting after encryption. Encrypted file is divided and store into different location is the technique behind splitting after encryption. This is used in highly confidential data.

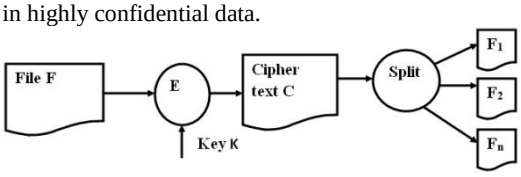

Fig. 5: File splitting after encryption

Confidential files are divided into number of small blocks and use different encryption techniques in each file piece are the technique behind splitting before encryption.

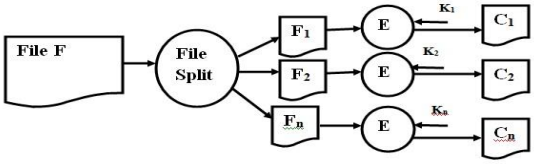

Fig. 6: File splitting before encryption

TTP offer different storage facilities such as internal storage and data outsourcing. Sometimes TTP can configure private clouds with storage facility and store encrypted data to the specified location. The special services such as data management, data auditing and access control will be performed by TTP if needed. TTP have details of the different prominent cloud service providers which support data storage. TTP select appropriate service provider based on the requirement of the user.
The three phases can work independently and user can select individual services directly. A sorted dictionary having keywords

of sensitive or protected file names with security value is the prerequisites of this model. Creating dictionary is risky and time consuming; only an expert having ample knowledge about both the domain is capable of preparing data dictionary. Any fault in the dictionary may affect the entire system.

4. Access control methods

Storage and access are the two faces of a single coin. User name and password of users who have permission to access confidential files are stored in advance.

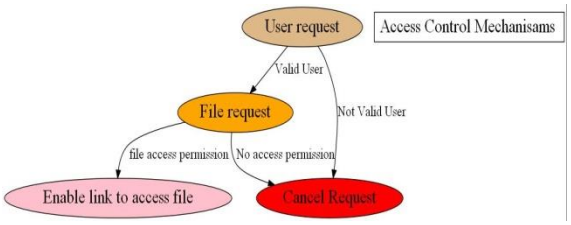

Fig. 7: Access control mechanisms

User send request contain user name and password to the data manager. If it is valid, check permission for accessing the requested file otherwise the request is automatically cancelled. If the user have permission to access the secret file, a link is enabled and direct user to the specified file.

5. Performance analysis

The tree structured security system offer high security based on their range. An accurate data dictionary will make a perfect file classification system. All stages except dictionary creation are automated so it reduces manual errors and time consumption. The access time of splitting files before and after encryption shows a time difference. Highly confidential static file is divided after encryption.

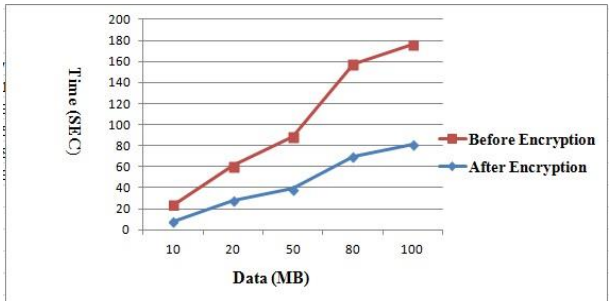

Fig. 8: Access time of files splitting before and after encryption

We can't access and use single file blocks, an authorized user can access complete data block and decrypt accordingly. The time consumption is more and security is high.

We can access and use each block separately. Each block is encrypted separately, so it consumes more time to decrypt each file blocks. The time consumption of accessing and using complete file is more compared to the accessing time of file blocks. The analysis shown that the accessing time of files splitting after encryption techniques take more time than the files splitting before encryption.

The keywords present in the dictionary for file classification at the first phase is encrypted and attached with the file blocks for file blocks identification. The dictionary is encrypted and kept at the user side. Each file piece has two or more key words for identification; these keywords are encrypted with a hash value and are attached with the file pieces. Users request a file using these keywords and the keywords are encrypted and compare with the dictionary values and direct users to the authorised cloud where the files stored. After a detailed analysis, it is observed that file searching using dictionary take less time compared to the system which is not using dictionary.

Security analysis

It is not possible to implement single system focusing whole vulnerabilities. Techniques are developed day by day to break the security. The security systems will be able to handle attacks and CSP flaws. Like, conventional systems proposed system also ensures double or triple authentication for access control and complex encryption techniques for confidentiality. However, we wouldn't avoid the chance of breaking the security. We have ensure security of confidential data if our proposed system compromise. The proposed system addressing some major threats such as Confidentiality, Integrity, Availability, Data loss, malicious user, data replication, financial loss and insider attacks.

The available storage options are Single CSP, Multi-cloud and Clouds Tree. The analysis shows security after the system compromise.

1. Single cloud

IF file F is stored in Single cloud THEN

i. data loss is high
ii. data replication is high
iii. confidentiality is low
iv. integrity is low
v. Availability is medium
vi. financial loss is medium
vii. insider attacks are high
viii. malicious users are high

Example: Consider a highly confidential file (F) of size 10GB is outsourced into single location (N)

Data loss, D_L = file size*number of locations (N)
= F*n =10*1= 10 GB

Data replication, D_R = file size (F) *number of locations (N)
= F*N
= 10* 1 =10 GB

Confidentiality

$$\frac{1}{\%\ of\ outsourced\ file\ *\ number\ of\ locations} * 100$$

$$\frac{1}{100 * 1} * 100$$

= .01*100 = 1%

Integrity $$\frac{1}{\%\ of\ outsourced\ file * number\ of\ locations} * 100$$

$$\frac{1}{100*1} * 100$$

= .01*100 = 1%

Availability = File size *N =10*1 = 10GB

Insider attack = % of outsourced File*number of locations
= 100*1 = 100%

Malicious users = % of outsourced File*number of locations
= 100*1 = 100%

2. Multi cloud

IF file F is stored in multi cloud THEN

i. data loss is very high
ii. data replication is very high
iii. confidentiality is very low
iv. integrity is very low
v. Availability is very high
vi. financial loss is very high
vii. insider attack is very high
viii. malicious user is very high

Example: Consider a highly confidential file (F) of size 10GB to be stored in a multi-cloud having 4 clouds. (F=10GB, N=4)

Data loss, D_L = file size*number of locations
= F*N =10*4= 40 GB

Data replication\CSP, D_R = File size(F)*number of locations (N)
= F*N
= 10* 4 =40 GB

Confidentiality = $$\frac{1}{\%\ of\ outsourced\ file * number\ of\ locations} * 100$$

$$\frac{1}{100*4} * 100$$

= 0.25%

Integrity $= \frac{1}{\%\ of\ outsourced\ file * number\ of\ locations} * 100$

$\frac{1}{100*4} * 100$

= 0.25%

Availability = F*N =10*4 = 40GB

Insider attack= % of outsourced File*number of locations

= 100*4 = 400%

Malicious user = % of outsourced File* number of locations

= 100*4 = 400%

3. Proposed System

IF file F is stored in proposed system THEN

i. data loss is low
ii. data replication is low
iii. confidentiality is high
iv. integrity is high
v. Availability is high
vi. financial loss is low
vii. insider attack is low
viii. malicious user is low

Example: Consider a highly confidential file (F) of size 10GB is to be stored in a clouds tree having 5 clouds.

Here, we split file into small block of size 2GB and stored each block into 3 different CSPs. None of the CSP owns a complete file. (F_1 = 2GB, Number of data blocks n=5, Number of Clouds N=3)

Data loss, D_L = file size*number of locations

= F_1*N =2*3*5= 30 GB

Data replication, D_R = file size (F) *number of locations (N)

= F*N = 2* 3*5 = 30GB

Confidentiality $= \frac{1}{\%\ of\ outsourced\ file * number\ of\ locations} * 100$

$\frac{1}{20*3} * 100 = 1.67\%$

Integrity = $\frac{1}{\%\ of\ outsourced\ file * number\ of\ locations} * 100$

$\frac{1}{20*3} * 100 = 1.67\%$

Availability = (F_1*n)*N = (2*3)*5 = 30GB

Insider attack = % of outsourced File*number of locations

= 20*3 = 60%

Malicious user = % of outsourced File *number of locations

= 20*3 = 60%

A file of size 50GB is tested with different methods with storage locations

Table 1: Case Study of Security Analysis

Data Blocks (GB)	No. of CSPs n=2	No. of CSPs n=3	No. of CSPs n=4
10	2.5	1.67	1.2
20	1.25	0.83	0.62
30	0.83	0.55	0.83
40	0.625	0.41	0.625

Rate of Confidentiality and Rate of Integrity are same

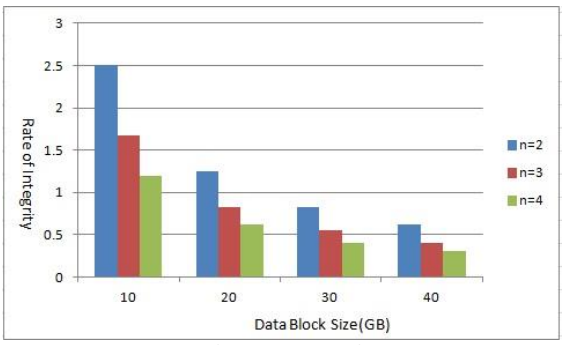

Fig. 9: Performance Rate of Integrity

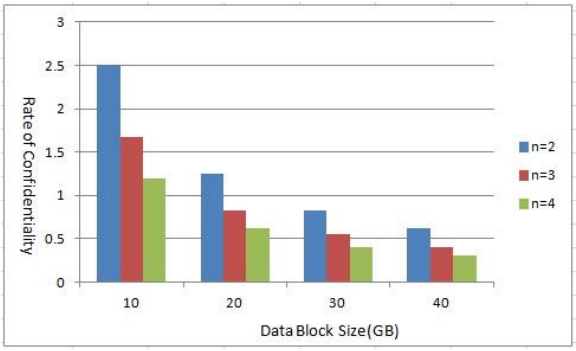

Fig. 10: Performance Rate of Confidentiality

This analysis shows that confidentiality and integrity are depended on the size of outsourced data and number of storage location. As the size of outsourced data increases, both confidentiality and integrity decreases gradually.

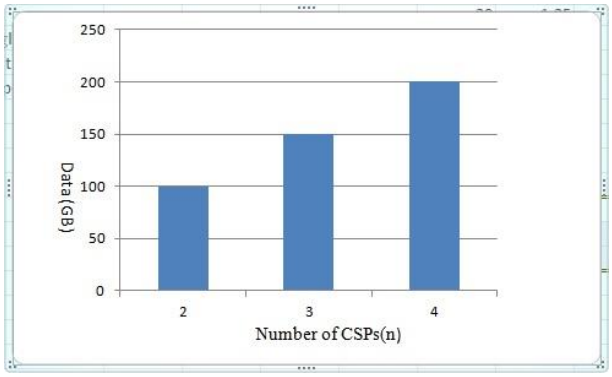

Fig. 11: Performance Rate of Availability

Availability is inversely proportional to Confidentiality and integrity. When availability increases confidentiality and integrity decreases gradually. The analysis shows that as the number of CSPs or storage locations increases; the availability also increases. The 50 GB data is replicated to 100 GB, 150 GB and 200 GB when we store it into 2, 3, 4 CSPs respectively.

6. Performance analysis with different security systems

Analyse our proposed security system with other two security models such as single cloud and multi cloud. Single cloud means storing user data into any one of the available Cloud Service Provider. Most of the data security system using in cloud environment is single cloud system. Multi cloud is otherwise called clouds-of cloud. It is an interconnection of number of CSPs, where each file is replicated to all the available CSPs.

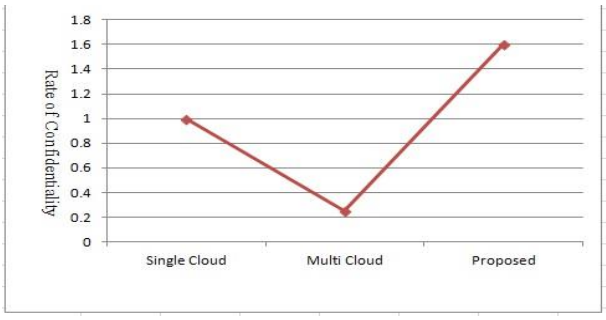

Fig. 12: Rate of confidentiality

The analytical study shows that proposed system offers high confidentiality compared to the other two systems.

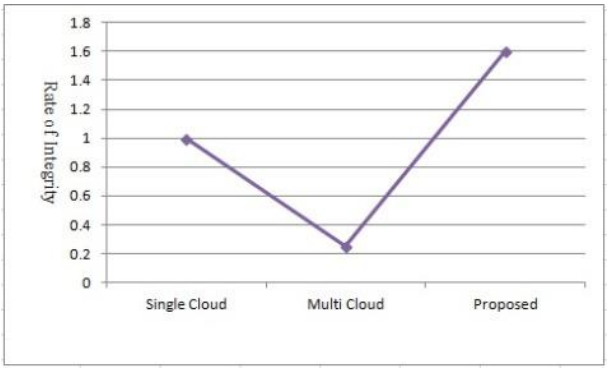

Fig. 13: Rate of integrity

Fig.13 shows that proposed system offers high integrity compared to the other two systems.

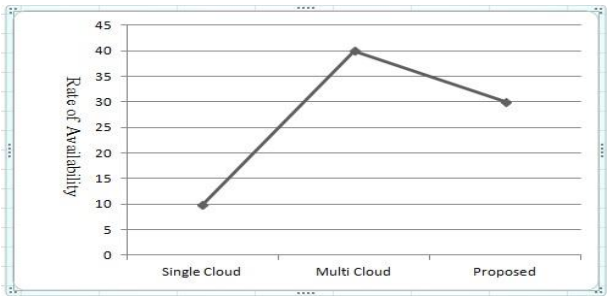

Fig. 14: Rate of availability

Fig.14 shows that the proposed system offers intermediate availability as compared to the other two systems.

7. Discussions

7.1. Raw-data outsourcing

Outsourcing raw data is a major concern which most of the organization faces. There is no possibility to outsource raw-data independently. Suitably encrypted data is outsources from the organization to cloud storages. Decryption also performed at the user side not at the network or the cloud storage space.

7.2. Protect necessary files only

We use an efficient data classification system to classify files into different classes. So it possible to apply high security techniques to highly confidential files and no security to public files.

7.3. Ensure business continuity

TTP promote multiple storage facilities to files having higher priority. A physical or technical disaster will not affect any changes in the smooth running of the organization.

7.4. Avoid unnecessary storage cost

Multi cloud or clouds of cloud replicate all files into number of CSPs; it leads to an unnecessary monetary loss. Here, we identify necessary files before outsourcing and store into two or more CSPs to ensure business continuity.

7.5. Security tuning

The term security tuning means that we can adjust the levels of security based on the significance of the files. No need to encrypt all files into same format. Sensitive files need more protection than protected files. We can apply more complex encryption techniques to more confidential files and less complex encryption to protected or public files.

8. Conclusion

A binary tree structured data security system offers complete security from data source to the CSP and back. This system offer a hierarchical relationship with the entire three phases with utmost security. A weighted CIA tree classifier classify unorganized data into four different category such as Sensitive, Private, Protected and Public. The security system offers different encryption standard depends on the confidentiality of the data. Applied cryptographic techniques are used to establish four different encryption standards. Symmetric encryption with enhanced substitution network is the key technique for applied cryptography. The confidential files are divided into number of small pieces and stored into multiple locations are the key concept behind this work. The data analysis shows that proposed system offers high security compared to the other existing security solutions. A whole system is control and cooperated by a trusted third party. Entire services are provided by TTP but are performed at the user side. The security system offers confidentiality, integrity and availability even if the security system compromise.

References

[1] The California State University (CSU) 8065.S02 Information Security Data Classification.
[2] Renu S, “A Novel Method to Classify Organizational Data Using CIA Tree approach”, *IEEE Explore*, pp.1-5, (2015).
[3] Renu S & Krishnaveni SH, “An Enhanced Automated Data Classification System Using Complex Network”, *IJCTA*, Vol.8, No5, pp. 2301-2306, (2015).
[4] A. Surendar and Usha Rani Nelakuditi, “Editorial - New Developments in Electronics, Cloud and IoT”, Electronic Government, An International Journal, Vol. 13, No. 4, 2017, ISSN online: 1740-7508 ISSN print: 1740-7494,pp -287-289
[5] Naone E, “Are we safeguarding social data? Technology”, *MIT Review*, (2009).
[6] Sarno D, *Microsoft says lost sidekick data will be restored to users*, Los Angeles Times, (2009).
[7] Abu-Libdeh H, Princehouse L & Weatherspoon H, “RACS: a case for cloud storage diversity”, *Proceedings of the 1st ACM symposium on Cloud computing*, pp. 229-240, (2010).
[8] Viega J, “Cloud computing and the common man”, *Computer*, Vol.42, pp.106-108, (2009).
[9] Cachin C, Keidar I & Shraer A, “Trusting the cloud”, *ACM SIGACT News*, Vol.40, pp.81-86, (2009).
[10] Wang C, Wang Q, Ren K & Lou W, “Ensuring data storage security in cloud computing”, *ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing*, pp.1-9, (2010).
[11] Wang C, Wang Q, Ren K, Cao N & Lou W, “Toward secure and dependable storage services in cloud computing”, *IEEE transactions on Services Computing*, Vol.5, No.2, pp.220-232, (2012).
[12] Wang C, Wang Q, Ren K & Lou W, “Ensuring Data Storage Security in Cloud Computing”, *Proc. 17th Int'l Workshop Quality of Service*, pp.1-9, (2009).
[13] Lin HY & Tzeng WG, “A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding”, *IEEE Transactions Parallel and Distributed Systems*, Vol.23, No.6, pp.995-1003, (2012).
[14] Wang Q, Wang C, Ren K, Lou W & Li J, “Enabling public auditability and data dynamics for storage security in cloud computing”, *IEEE transactions on parallel and distributed systems*, Vol.22, No.5, pp.847-859, (2011).
[15] Sood SK, “A combined approach to ensure data security in cloud computing”, *Journal of Network and Computer Applications*, Vol. 35, pp.1831–1838, (2012).
[16] Esposito C, Castiglione A, Tudorica CA & Pop F, “Security and Privacy for Cloud-Based Data Management in the Health Network Service Chain: A Microservice Approach”, *IEEE Communications Magazine*, Vol.55, No.9, pp.102-108, (2017).

[17] Chen H, Zhu X, Qiu D, Liu L & Du Z, "Scheduling for Workflows with Security-Sensitive Intermediate Data by Selective Tasks Duplication in Clouds", *IEEE transactions on Parallel and Distributed Systems*, Vol.28, No.9, pp:2674–2688, (2017).
[18] Kolhar M, Abu-Alhaj MM & El-atty SMA, "Cloud Data Auditing Techniques with a Focus on Privacy and Security", *IEEE Security & Privacy*, Vol.15, No.1, pp.42-51, (2017).
[19] Barona R & Mary Anitha EA, "A survey on data breach challenges in cloud security: Issues and threats", *International Conference Circuit, Power and Computing Technologies*, (2017).
[20] Renu S & Krishnaveni SH, An Enhanced CIA tree Using String Matching Algorithms, *IJAER*, Vol.12, No.16, pp-6123-6126, (2017).
[21] Surendar, A., Arun, M., Periasamy, P.S."Hardware based algorithms for bioinformatics applications - A survey",(2013) International Journal of Applied Engineering Research, 8 (6), pp. 745-754.
[22] B. Saichandana, G. Rachana sri, A. Surendar and B. Suniltej "controlling of wall lamp using arduino", International Journal of Pure and Applied Mathematics, Volume 116 No. 24 2017, 349-354, ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)