BE-MCSDMA : BI-LEVEL ENCRYPTED MULTI CLOUD SECURE DATA MANAGEMENT ARCHITECTURE

DAMISETTI VEERABHADRARAO[1] , G APPARAO [2] ,ANURADHA S [3]

[1]Assistant Professor, GITAM University, Department of CSE, GST, India

[2]Professor, GITAM University, Department of CSE, GST, India

[3] Assistant Professor. GITAM University, Department of CSE, GST, India

E-mail: [1]vdamiset@gitam.edu, [2]agiduturi@gitam.edu. [3]asesetti@gitam.edu

ABSTRACT

During this information age, every sector is generating massive data on daily basis and this data is to be stored so that the storage entities possess vital characteristics such as availability, integrity, authenticity, and offering secure, confidential, simple, and fast retrieval. Right from the file systems, the storage architecture evolved to today's hybrid cloud and maybe tomorrow's quantum cloud to meet the prevailing customized requirements. Cloud computing is a legendary technology that is necessary for all business segments in terms of efficient data storage needs. It is more beneficial to those organizations which cannot afford much on the computing infrastructure to avail of various major cloud services like IaaS, PaaS, SaaS, and other supplementary ones. Cloud technology has drastically modulated the service and industrial sectors to an extent that cyber attackers are relying much more to capitalize on even miniature leaks despite the exhaustive security measures. The technology took its shape in offering various types like Public, Private, Hybrid, Multi and Multi-Hybrid clouds. Every technology is a threat prone not leaving cloud-related as an exception. Due to Covid 19 pandemic, the Health segment is revolutionized in which enormous data is generated worldwide. Not only in the health domain but also in various sectors the data is generated at a rapid speed. Whichever the industry, the data is to be immensely protected. In this research fragment, we are intended to design novel security architecture for a multi-cloud environment applied to Electronic Health Records (EHR) and analyze it's working.

Keywords: *Multi Cloud Security, Cloud Security In Health Sector, Multi Cloud Computing, E-Health Cloud Security*

1. INTRODUCTION

The advent of Cloud computing eased the storage solutions more to the point offering computational efficiency. The cloud infrastructural solutions extend tremendous support to small, medium and large scale organizations. However the security ailments shall not leave any technological prospects. Security is like a race between offensive and defensive potential. Although cloud technology seems to be promising, security violations are unavoidable.

Health care domain is accelerating above and beyond is sensitive. The data generated from time to time in the form of EHRs, laboratory tests information, medical scan images, and pharmaceutical data is very massive and requires enormous storage. The sources of information of health care data are as given in the figure 1. Of course the cloud and big data services are addressing the problem. Observing the dark side of the technology there are numerous developments which aid in compromising the security. In this context the need of security solutions is inevitable. It is never ending process that protective solutions for the abhorrent security issues are to be developed. Data ownership is more related to data privacy rather than data security. Privacy could be claimed as a moral right for individuals and groups when using information systems, whereas computer security is not a moral right in itself.

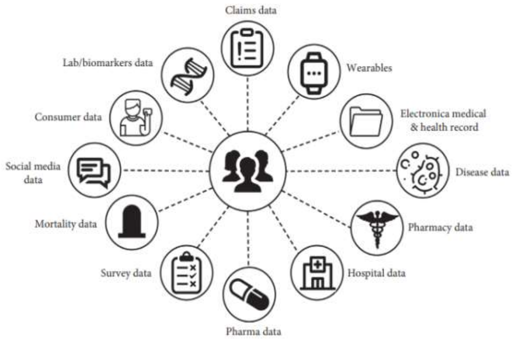


Fig 1: Health care data sources of information [23]

80% of company management “fear security threats and loss of control of data and systems”. Single cloud services are subjected to outage wherein the shift towards inter clouds or multi cloud is the current trend. The businesses trust that it is an effective solution to move to multi cloud due to the reason that they get relaxed from vendor lock in problems and also the security concerns. In this scenario agile solutions are need of the hour towards which we made our effort in designing a competent solution in which the data is divided and bi-level encrypted/decrypted with proficient algorithms before getting uploaded/retrieved to or from multiple clouds. In the subsequent section we reviewed the literature of various researchers followed by the discussions of proposed solution which covers architecture, algorithms and performance analysis in the next section. The conclusions are given in the final section.

2. BACKGROUND RESEARCH

Several researchers proposed their solutions among which few are reviewed and highlighted their work. In **[1] Yazan Al-Issa et.al.** discussed the need of storing the e-health data stating the benefits and limitations of e-health cloud [15[[16]. They also mentioned the security threats for such e cloud solutions and mitigation mechanisms. A couple of standards defined in the security and privacy perspective of EHRs include ISO/TS 18308 standard [13], International Medical Informatics Association (IMIA) [14].

N. Velmurugan et.al. in [2] & [3] mentioned the concept of Confidentiality, Protection and Privacy of Data (CPPD) giving a detailed analysis of few algorithms and the level of security of cloud environment. They proposed an exclusive mechanism in the form of an algorithm in the multi cloud architecture so as to improve CPPD.

Adoption of cloud technologies by enterprises had been accelerated due to the distinctive benefits offered to various domains. Health care industry is one among them which avails the technological advantages. It was addressed by **Tatiana Ermakova et.al.** in **[4].** They presented a novel solution to provide security to store the health care data into multi-cloud. In their solution they health records were fragmented and moved to various clouds. The prime features of their proposed solution is Shamir’s secret sharing scheme and Rabin’s algorithm which performed well by creating a low overhead. They performed various case studies and satisfied the security and privacy concerns to most extent which were mentioned in [17] [18] [19] [20] [21] [22].

The security and privacy confronts hamper the cloud adoption at a large scale towards which **Benjamin Fabian et.al.** in **[5]** had given a novel solution for inter organizational data sharing. Attribute based encryption was used as a part of their multi cloud architecture which resulted in reducing the adversaries of different cloud providers. They demonstrated the practical viability and performance of their implementation in the form of several experiments.

Poor architectures results in impeding the cloud security. It was indicated in **[6]** by **Henry Edet et.al.** through their mapping study conducted. In their study it was identified that 73 percent of literature revealed that efficient frameworks and architectures lead to prevent the security and data privacy breaches in cloud computing [24] [25]. They aimed at designing a universal multi cloud security after studying few frameworks viz., Risk Assessment Framework designed by European Network and Information Security Agency (ENISA)[26], NIST reference architecture[27] and others.

Medical record databases, power system historical information and financial data are some examples of critical data which certainly needs the cloud assistance which provides reliability and security to a large extent. In **[7], Alysson Bessani et.al.** presented DEPSKY, a system aiming at improving the availability, integrity and confidentiality of data uploaded onto diverse clouds which form cloud-of-clouds. They used four commercial clouds and deployed using PlanetLab. DEPSKY provides all the necessary features of cloud security at an optimal cost. They combined Byzantine quorum systems protocols in attaining the optimality.

In [8] Kevin D. Bowers et.al. introduced a distributed Cryptographic multi cloud security system HAIL (High-Availability and Integrity Layer) which is robust. HAIL is a remote file integrity checking protocol which offers the vital features of multiserver application of Proof of Reliability protocols. HAIL exhibited better performance when compared to the existing solutions.

Haider Ali Khan Khattak et.al. in **[9]** identified that Single cloud seems to be more vulnerable in terms of security and hence it is less popular in healthcare. Then a move towards multi–cloud which is also said as “cloud–of–clouds” was made. They provided insights of security aspects in single–cloud as well multi–cloud apart from the security recommendations for healthcare systems.

Hybrid and Secure Data Sharing Architecture (HSDSA), an innovative and effective architecture was proposed by **Tayssir Ismail et.al.** in **[10]**, which bridges the patient and e-health system requirements. HSDSA is a privacy preserving framework concerned with security, privacy, and integrity of healthcare data in multi cloud architecture. In their approach RSA was used to encrypt the medical records. Shamir’s secret sharing approach had been adopted for distribution of shares to different cloud service providers. In the retrieval phase, they used Schnorr algorithm and for key management Diffie-Hellman algorithm was used. Due to the vital features in their approach, the patient acquires total control over the generation and management of the keys.

The model in **[11]** proposed by **Leila Megouache et.al.** provide authentication and data integrity in a distributed and interoperable cloud environment. Their approach comprises three steps, establishing a private virtual network to secure the data in transit; followed by an authentication method based on encryption and finally a mechanism to compute the integrity of data which was distributed on to various clouds. The data is fragmented to minimize the risk of vulnerability. Their simulation model reduced the number of intrusions.

In **[12], Jens-Matthias Bohli et.al.** surveyed various research articles on the security merits with respect to multiple distinct clouds. A variety of architectures have been introduced and discussed depending on the security and privacy aspects. They analyzed four multi cloud approaches in terms of legal compliance, guaranteed security, fragile spots and feasibility.

Observations from the above literature:

Having gone through the mentioned related research work and other research articles, it is understood that multi cloud architecture has significance in providing cloud services to the health care domain users. Although the infrastructure seems to be substantial, the security features may decline the prospect of multi cloud system. To empower the multi cloud system certain security models have to be incorporated. Several researchers worked in this direction and proposed distinguished approaches among which HAIL, HSDSA and others have been noteworthy. All the approaches are identified implementing single encryption mechanism. Hence the implementation of encryption at two levels is introduced which happens before and after dividing the data. Due to this double encryption mechanism the security gets enhanced. In some articles the data is categorized and depending on the type of data it has been uploaded to cloud. In our approach which ever data is to be uploaded, it shall be fragmented into equivalent parts and then uploaded to the clouds. Moreover the idea is to implement both symmetric and asymmetric encryption mechanisms due to which the data is securely covered under holistic approach.

3. PROPOSED WORK (MULTI CLOUD SECURITY MODEL)

3.1 Architecture

Our architecture encompasses bi level encryption/decryption design in which at the first level the data is processed using public encryption mechanism and at the second level private encryption procedures are used.

The data which is to be uploaded by the user firstly gets encrypted with RSA algorithm, further divided into three chunks. Each data chunk gets uploaded to separate cloud post encryption using DES, AES and BlowFish respectively. Receiving the user request, the data retrieval process is initiated by generating three keys for decrypting the stored data in three clouds. The decrypted chunks from the clouds get merged on which decryption is applied at the next level from which the original data file is obtained. The overall architecture could be observed from figure 2.

3.2 Upload And Retrieval Process

Our cloud security architecture which stores data into multiple clouds comprises various modules. The upload and retrieval processes are as shown in figures 3 and 4 respectively. Following are the algorithms for both the processes.

Algorithm_Upload data:

```
Step 1: User selects the data
Step 2: Generate $RSA_U$(Public key) & $RSA_R$(Private key)
Step 3: $RED \leftarrow RSA_U(data)$
Step 4: $REDC_t \leftarrow DDM(RED)_t$ $(t=1,2,3)$
Step 5: Generate $K_1$, K2, K3
Step 6: Obtain D, T, IP
Step 7: Initialize V
Step 8: $DES_{K_{C1}} \leftarrow K_1 \oplus D \oplus T$
Step 9: $AES_{K_{C2}} \leftarrow SHA_{256}(K_2 \oplus V)$
Step 10: $BLFI_{K_{C3}} \leftarrow K_3 \oplus IP$
Step 11: $DEDC_1 \leftarrow E_{DES_{K_{C1}}}(REDC_1)$
Step 12: $DEDC_2 \leftarrow E_{AES_{K_{C2}}}(REDC_2)$
Step 13: $DEDC_3 \leftarrow E_{BLFI_{K_{C3}}}(REDC_3)$
Step 14: Upload $DEDC_t$ to $Cloud_t$ (t=1,2,3)
```

Algorithm_Retrieve data:

```
Step 1: Patient requests the data
Step 2: Get $DES_{K_{C1}}$, $AES_{K_{C2}}$, $BLFI_{K_{C3}}$
Step 3: $DDC_1 \leftarrow D_{DES_{K_{C1}}}(DEDC_1)$
Step 4: $DDC_2 \leftarrow D_{AES_{K_{C2}}}(DEDC_2)$
Step 5: $DDC_3 \leftarrow D_{BLFI_{K_{C3}}}(DEDC_3)$
Step 6: $MD \leftarrow DMM(DDC_1, DDC_2, DDC_3)$
Step 7: $data \leftarrow RSA_R(MD)$
```

3.3 Encryption And Decryption Processes

The encryption process is done in two phases; one being the Asymmetric encryption and the other being Symmetric encryption. We used RSA algorithm towards public encryption mechanism while in the private encryption phase three algorithms viz., Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blow Fish (BlFi) for each cloud respectively are used. As we are proposing our model for security for EHRs, we felt the need of incorporating asymmetric encryption i.e., through RSA algorithm. During the first phase there is a need of a public-private key pair which is generated through a key generation process and during the second phase three keys one for each algorithm are generated.

The key generated for DES encryption is of 56 bits and for AES it is 256 bits; besides BLFI algorithm is operated with the key size in multiples of 32 bits. The encryption and decryption elements are represented in table 1.

Table 1: Encryption and Decryption representation

Encryption elements	Decryption elements
$RED = RSA_U(data)$ $REDC_1 = DDM(RED)_1$ $REDC_2 = DDM(RED)_2$ $REDC_3 = DDM(RED)_3$ $DEDC_1 = E_{DES_{K_{C1}}}(REDC_1)$ $DEDC_2 = E_{AES_{K_{C2}}}(REDC_2)$ $DEDC_3 = E_{BLFI_{K_{C3}}}(REDC_3)$	$DDC_1 = D_{DES_{K_{C1}}}(DEDC_1)$ $DDC_2 = D_{AES_{K_{C2}}}(DEDC_2)$ $DDC_3 = D_{BLFI_{K_{C3}}}(DEDC_3)$ $MD = DMM(DDC_1, DDC_2, DDC_3)$ $data = RSA_R(MD)$

RED – RSA Encrypted Data, REDC – RSA Encrypted Data Chunk
DEDC – Double Encrypted Data Chunk, DDM – Data Division Module
U – Public key representation, R – Private key representation
DDC – Decrypted Data Chunk, MD – Merged Data, DMM – Data Merge Module

3.4 Data Division And Merge Modules

This is one among the strengths of our architecture. Rather than uploading the data to single cloud, it is uploaded into multiple clouds. The data shall be divided into multiple parts and then processed. As we are using three clouds we divided the data into three parts and uploaded each to one cloud. Similarly after decryption, the data chunks are merged so as to provide it to the RSA decryption. Here the division of data is done in equal proportions. However the research is open on how the data could be partitioned. Usually the EHR data will be in the form of either alphanumeric, a document, or an image. We performed the experimentation on all three types of data.

3.5 Key Management Module

The vital part of offering efficient security lies in strong encryption and decryption procedures as well the keys. Our key management module consists of two phases namely Key generation and key distribution. In our architecture we followed an effective mechanism towards key generation and it is as follows.

As our current context is providing security for Electronic health records of patients, the data is uploaded to cloud/s either by the health care unit or by the patient. In case the health care unit uploads the data, for RSA we need public key and it could be from the user details. Connectively the private key of the particular user will be with the user him/her self with which the data could be retrieved.

Alternatively if the patient uploads/retrieves the data then the public and private keys are available with him/her. In our experiment we demonstrated with two random generated keys considering one as public key and the other as private key for RSA Encryption and Decryption procedures.

At the next level i.e., private encryption/decryption processes, there is a need of three keys for the three algorithms. Since we are implementing symmetric process, the same key is used for encryption as well as decryption.

In our experiment three keys K_1 of length 56 bits, K_2 of length 256 bits and K_3 of length n*32 bits are randomly generated after which three dynamic values are used for final key generation.

$$DES_{K_{C1}} = K_1 \oplus D \oplus T$$

$$AES_{K_{C2}} = SHA_{256}(K_2 \oplus V)$$

$$BLFI_{K_{C3}} = K_3 \oplus IP$$

K_1 = Randomly generated Key of size 56 bits
D = Date in the form DD-MM-YYYY = 8*7 bits = 56 bits
T = Time in the form HH-MM-MSEC = 8*7 bits = 56 bits
Hence $DES_{K_{C1}}$ is of size 56 bits

K_2 = Randomly generated Key of size 56 bits
V = A fixed value of size 256 bits
$AES_{K_{C2}}$ is of size 256 bits which is obtained by applying SHA on $K_2 \oplus V$

K_3 = Randomly generated Key of size in multiples of 32 bits
IP = IP address of size either 32 bits or 128 bits.

4. ANALYSIS OF THE PROPOSED ARCHITECTURE

We developed the proposed simulated architectural solution using Java on the Intel i3-3220 @ 3.30GHz machine. Our proposed solution involves efficient architectural design.

Due to the public key encryption there is no need to share the key with other parties. It is enough for the EHR holder to share the public key. The bi-level encryption adds high security to the data due to the reason that, an attacker needs to crack 4 keys and break four algorithms.

The advantage with this mechanism is that the data is partitioned and uploaded to three clouds which enhance the security. The probability of security improvement is represented in table 2.

Table 2: Security probabilities of various architectures

Probability of Security	**Architecture**
$Pr(Sec_{data}) \propto Pr(Sec_{C}) + Pr(Sec_{EA})$	Single cloud – Single encryption algorithm
$Pr(Sec_{data}) \propto Pr(Sec_{C1})+Pr(Sec_{C2})+\dots\dots\dots +Pr(Sec_{Cn})+Pr(Sec_{EA})$	Multiple cloud – Single encryption algorithm
$Pr(Sec_{data}) \propto Pr(Sec_{C1})+Pr(Sec_{C2})+\dots\dots\dots +Pr(Sec_{Cn})+Pr(Sec_{EA1}) +Pr(Sec_{EA2}) +\dots\dots +Pr(Sec_{EAn})$	Multiple cloud – Multiple encryption algorithms$^{\#}$

# - In our proposed architecture the number of clouds and Encryption algorithms are 3 and 4 respectively.

$Pr(Sec_{data})$ represents Probability of data being secure
$Pr(Sec_{C})$ is the Probability of security provided by the cloud C.
$Pr(Sec_{Cn})$ is the Probability of security provided by the cloud Cn.
$Pr(Sec_{EA})$ is the Probability of security provided by the Encryption algorithm EA.
$Pr(Sec_{EAn})$ is the Probability of security provided by the Encryption algorithm EAn.

The key computation for the three algorithms is done very elegantly which further boosts the security of architecture.

i) DES algorithm is operated with the key generated using 3 components, a random number, date and time (time stamp) which are dynamic in nature.

ii) A 256 bit key which is the hash code generated by applying Secure Hash Algorithm (SHA-256) on the XOR value of a random number and a fixed value, is supplied for AES.

iii) The Blow Fish algorithm is supplied a key generated using two components i.e., a variable size random number in multiples of 4 Bytes and IP address of the machine from where the document is being uploaded. The IP address is dynamic in nature having size of either 32 (IPV4) or 128 (IPV6) bits. The 'n' number of 4 Byte parts of random value will be XORed with one another and produces 32 bit value say K3. If the IP address is of size 32 bit it is directly XORed with K3. Alternatively if the size of IP address is 128 bits the four number of 4 Byte parts of 128 bit are XORed with one another producing 32 bit value after which it will be XORed with K3.

Due to the dynamic nature of components considered in key generation, the probability of security with Encryption algorithms shall be high.

Performing brute force attack may be quite difficult since the number of exhaustive keys required is $2^{(56+256+32)}$ along with the RSA private key.

The advantages of our proposed architecture are remarkable but it places overhead of data division and merge, multiple encryptions and data upload to multiple clouds.

The time consumption of various modules with respect to the simulations carried out are depicted in figures 5 & 6 respectively. However the performance in terms of time consumption when implemented with the actual clouds shall depend on various factors like the internet speed, cloud support and others.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. CONCLUSION:

Multi cloud is a major research area in which the security concerns are very much imperative. In our article we proposed a multi cloud security architecture which is a bi level design implementation. The architecture constitutes upload and retrieval of Electronic health data of patients on to multiple clouds by partitioning the data into chunks encrypted with multiple algorithms at two levels. The simulation carried out demonstrates the implementation of architecture with the time consumption details. Nevertheless the performance of practical implementation is influenced by various factors. Our solution seems to be promising in terms of security because of the features two-level encryption; dynamic, simple and robust key generation process; data fragmentation and reassembly; multiple encryption algorithms and multiple clouds. The security performance is analyzed on a theoretical basis leaving the cryptanalysis part for the future research. Also few aspects such as data partitioning algorithms, Number of clouds to be considered, Key distribution mechanism, Trust factor computation may be considered for research in future.

REFERENCES

[1] Yazan Al-Issa, Mohammad Ashraf Ottom, Ahmed Tamrawi, "eHealth Cloud Security Challenges: A Survey", Journal of Healthcare Engineering, vol. 2019, Article ID 7516035, 15 pages, 2019. https://doi.org/ 10.1155/2019/7516035

[2] N. Velmurugan and S. Godfrey Winster, “An Invincible Rudimentary Architecture for Data Security in Cloud Environment Using Multi Cloud”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-11, September 2019

[3] N. Velmurugan and S. Godfrey Winster, “An Inimitable Mechanism and Architecture for Security in Cloud using Multi Cloud”, International Journal of Recent Technology and Engineering (IJRTE), Volume-8 Issue-5, January 2020

[4] T. Ermakova and B. Fabian, "Secret Sharing for Health Data in Multi-provider Clouds," 2013 IEEE 15th Conference on Business Informatics, 2013, pp. 93-100, doi: 10.1109/CBI.2013.22.

[5] B. Fabian, et al., Collaborative and secure sharing of healthcare data in multi-clouds, Information Systems (2014), http://dx.doi.org/10.1016/j.is.2014.05.004i

[6] Henry Edet. 2021. A Reference Architecture for Validating Security Across Multi-Cloud Computing Systems. In Evaluation and Assessment in Software Engineering (EASE 2021), June 21–23, 2021, Trondheim, Norway. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3463274.3463345

[7] Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando André, and Paulo Sousa. 2013. DepSky: Dependable and Secure Storage in a Cloud-of-Clouds. <i>ACM Trans. Storage</i> 9, 4, Article 12 (November 2013), 33 pages. DOI:https://doi.org/10.1145/2535929

[8] Kevin D. Bowers, Ari Juels, and Alina Oprea. 2009. HAIL: a high-availability and integrity layer for cloud storage. In <i>Proceedings of the 16th ACM conference on Computer and communications security</i> (<i>CCS '09</i>). Association for Computing Machinery, New York, NY, USA, 187–198. DOI:https://doi.org/10.1145/1653662.1653686

[9] H. A. K. Khattak, H. Abbass, A. Naeem, K. Saleem and W. Iqbal, "Security concerns of cloud-based healthcare systems: A perspective of moving from single-cloud to a multi-cloud infrastructure," 2015 17th International Conference on E-health Networking, Application & Services (HealthCom), 2015, pp. 61-67, doi: 10.1109/HealthCom.2015.7454474.

[10] Ismail, Tayssir & Touati, Haifa & Hajlaoui, Nasreddine & Hassen, Hamdi. (2020). Hybrid and Secure E-Health Data Sharing Architecture in Multi-Clouds Environment. 249-258. 10.1007/978-3-030-51517-1_21.

[11] Megouache, Leila & Zitouni, Abdelhafid & Djoudi, Mahieddine. (2020). Ensuring user authentication and data integrity in multi-cloud environment. Human-centric Computing and Information Sciences. 10. 10.1186/s13673-020-00224-y.

[12] J. Bohli, N. Gruschka, M. Jensen, L. L. Iacono and N. Marnau, "Security and Privacy-Enhancing Multicloud Architectures," in IEEE Transactions on

Dependable and Secure Computing, vol. 10, no. 4, pp. 212-224, July-Aug. 2013, doi: 10.1109/TDSC.2013.6.

[13] ANSI, TS. 18308 Health Informatics-Requirements for an Electronic Health Record Architecture, ISO, Geneva, Switzerland, 2003.

[14] US Department of Health & Human Services (HHS), Health Information Privacy, US Department of Health & Human Services (HHS), Washington, DC, USA, 2005.

[15] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, “e-health cloud: opportunities and challenges,” Future Internet, vol. 4, no. 3, pp. 621–645, 2012.

[16] N. Dong, H. Jonker, and J. Pang, “Challenges in eHealth: from enabling to enforcing privacy,” in Foundations of Health Informatics Engineering and Systems. FHIES 2011. Lecture Notes in Computer Science, Z. Liu and A. Wassyng, Eds., pp. 195–206, Springer, 2011.

[17] L. Chen and D.B. Hoang, Novel Data Protection Model in Healthcare Cloud. IEEE International Conference on High Performance Computing and Communications, 2011.

[18] T.-S. Chen, C.-H. Liu, T.-L. Chen, C.-S. Chen, J.-G. Bau, and T.-C. Lin, Secure Dynamic Access Control Scheme of PHR in Cloud Computing. Journal of Medical Systems, 36, 4005–4020, 2012a.

[19] Y.-Y. Chen, J.-C. Lu, and J.-K. Jan, A Secure EHR System Based on Hybrid Clouds. Journal of Medical Systems, 36, 3375–3384, 2012b.

[20] M. Deng, M. Petkovié, M. Nalin, and I. Baroni, A Home Healthcare System in the Cloud - Addressing Security and Privacy Challenges, in Proceedings of the IEEE 4th International Conference on Cloud Computing, 2011.

[21] Z.-R. Li, E.-C. Chang, K.-H. Huang, and F. Lai, A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform. 15th IEEE International Symposium on Consumer Electronics, 2011a.

[22] M. Li, S. Yu, Y. Zheng, K Ren, and W. Lou, Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption. IEEE Transactions on Parallel and Distributed Systems, 2012.

[23] Privacy Analytics Inc., Patient-Level Data, Privacy Analytics Inc., Ottawa, Canada, 2017.

[24] Ivor D Addo, Sheikh I Ahamed, and William C Chu. 2014. A reference architecture for high-availability automatic failover between PaaS cloud providers. In 2014 International Conference on Trustworthy Systems and their Applications. IEEE, 14–21.

[25] Alexander Oppermann, Marko Esche, Florian Thiel, and Jean-Pierre Seifert. 2018. Secure Cloud Computing: Risk Analysis for Secure Cloud Reference Architecture in Legal Metrology. In 2018 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 593–602.

[26] Vladimir Sklyar and Vyacheslav Kharchenko. 2019. ENISA documents in cybersecurity assurance for industry 4.0: IIoT threats and attacks scenarios. In 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Vol. 2. IEEE, 1046–1049.

[27] Wayne Jansen and Timothy Grance. 2011. Draft NIST special publication guidelines on security and privacy in public Cloud computing. Computer Security, Jan (2011)

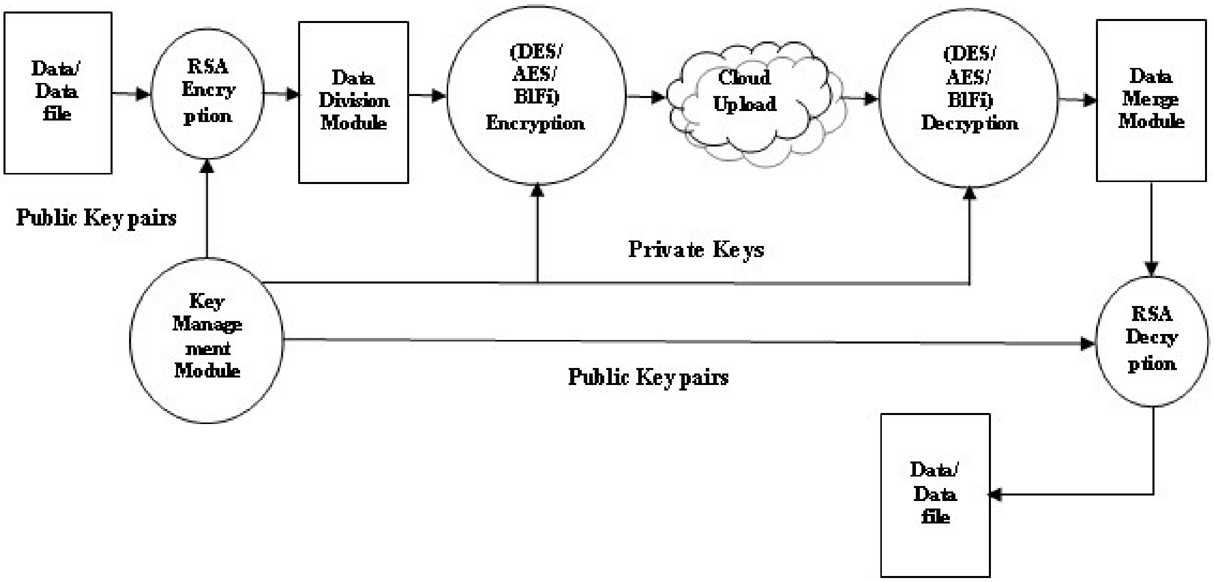


Fig 2: Proposed Architecture of Multi cloud Security

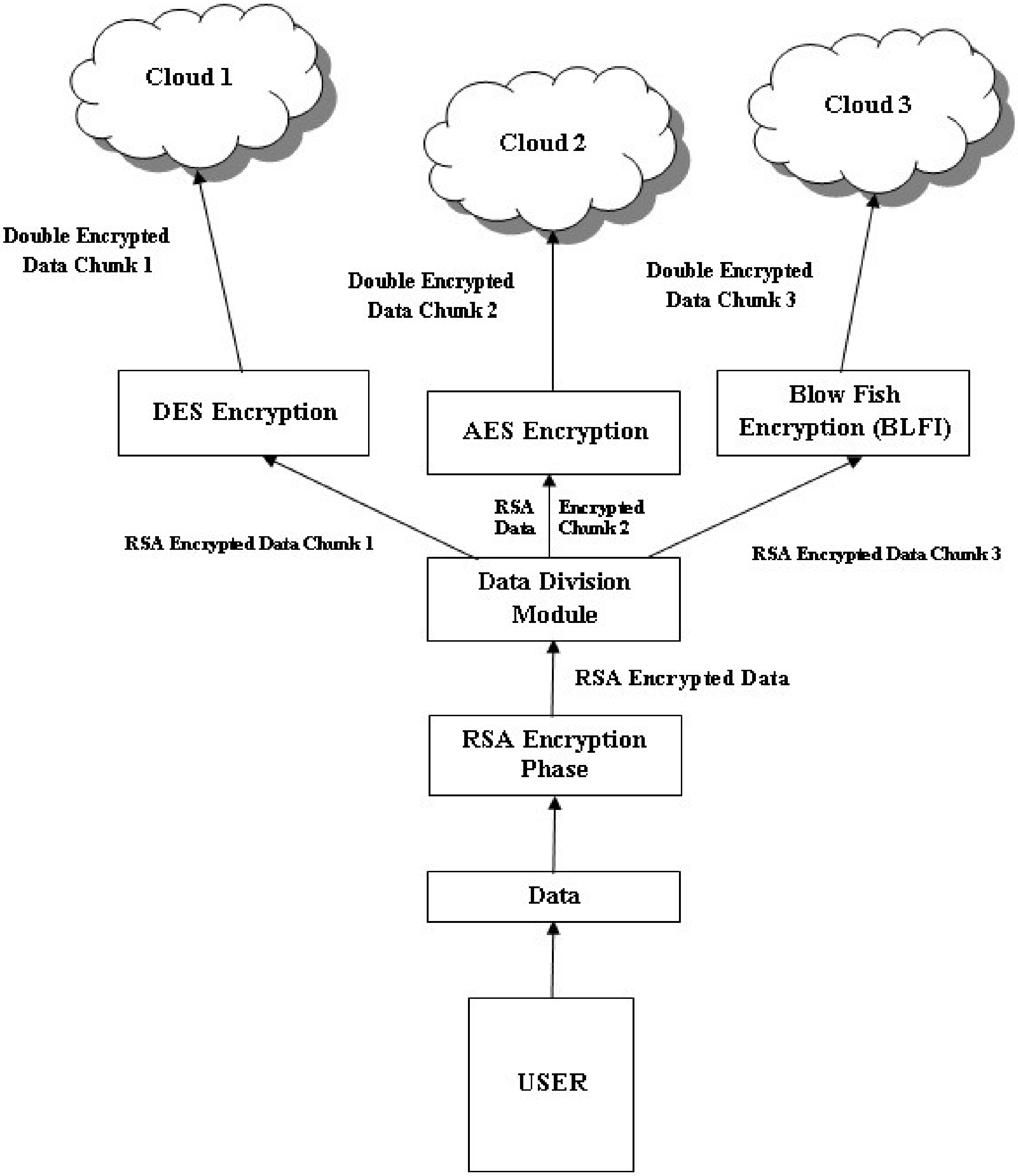

Cloud 1
Cloud 2
Cloud 3
Double Encrypted Data Chunk 1
Double Encrypted Data Chunk 2
Double Encrypted Data Chunk 3
DES Encryption
AES Encryption
Blow Fish Encryption (BLFI)
RSA Encrypted Data Chunk 1
RSA Data
Encrypted Chunk 2
RSA Encrypted Data Chunk 3
Data Division Module
RSA Encrypted Data
RSA Encryption Phase
Data
USER

Fig 3: Data upload Process

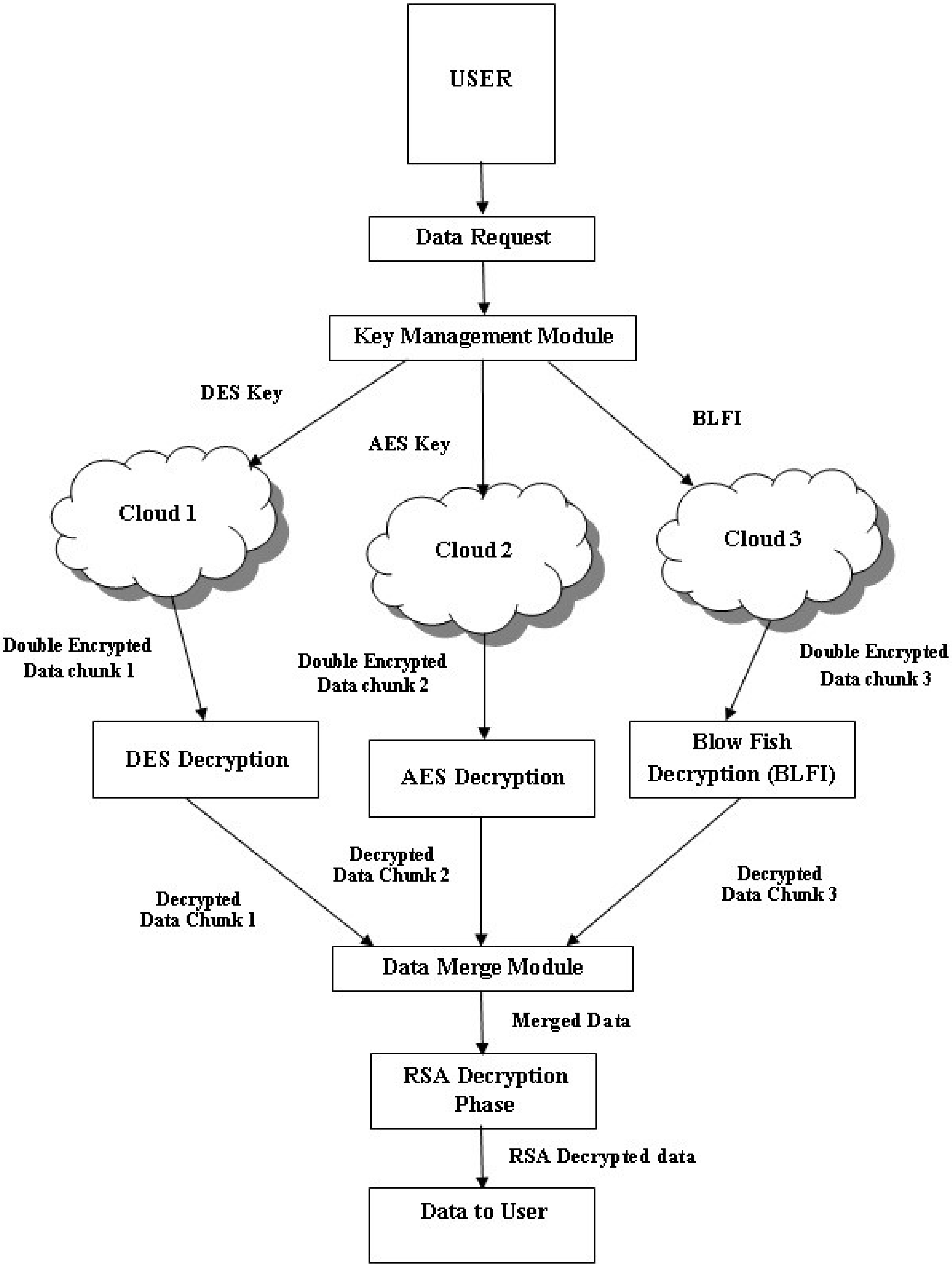
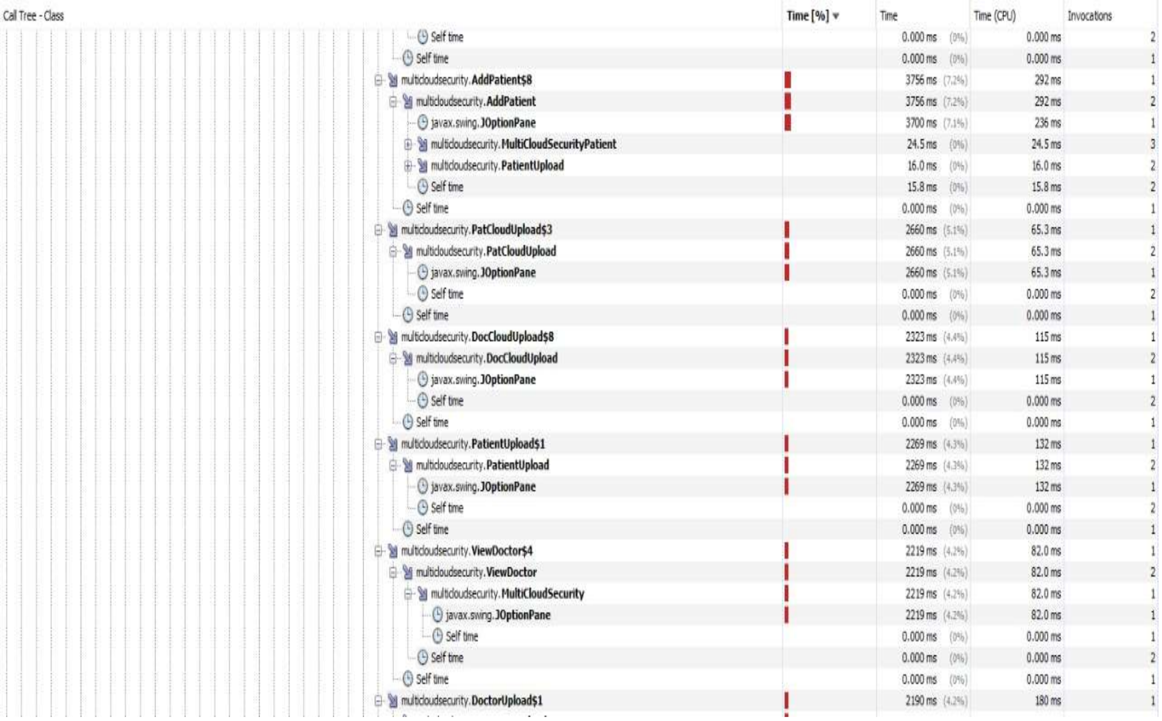
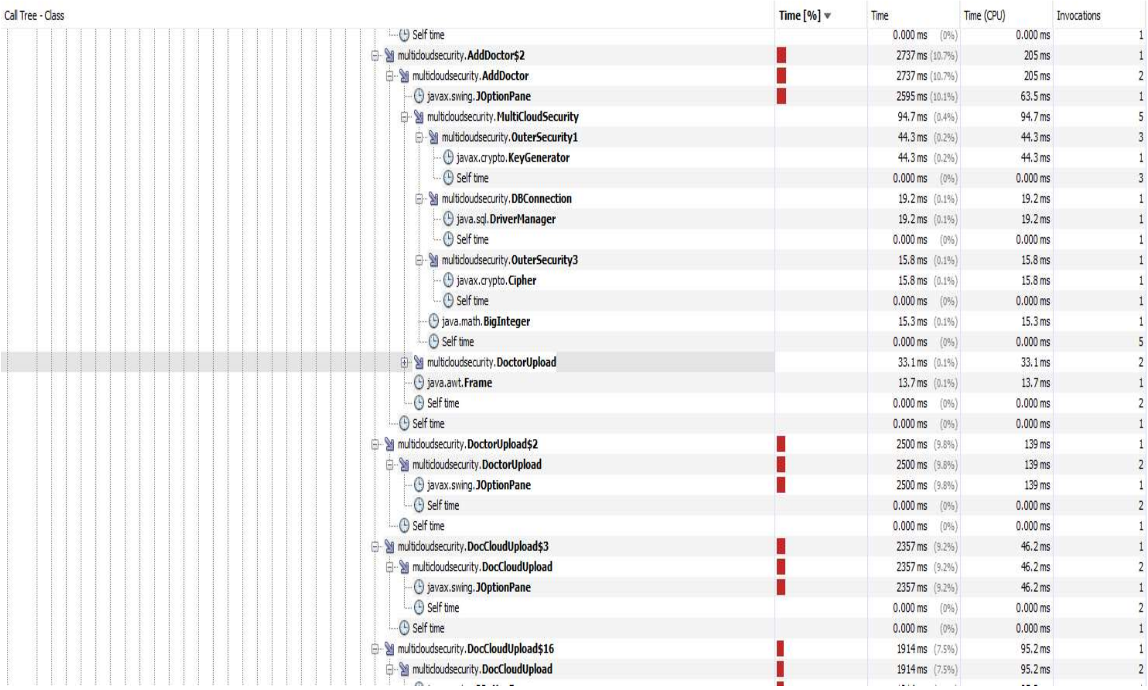


Fig 4: Data Retrieval Process



Call Tree - Class	Time [%] ▾	Time	Time (CPU)	Invocations
Self time		0.000 ms (0%)	0.000 ms	2
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.AddPatient$8	▮	3756 ms (7.2%)	292 ms	1
multicloudsecurity.AddPatient	▮	3756 ms (7.2%)	292 ms	2
javax.swing.JOptionPane	▮	3700 ms (7.1%)	236 ms	1
multicloudsecurity.MultiCloudSecurityPatient		24.5 ms (0%)	24.5 ms	3
multicloudsecurity.PatientUpload		16.0 ms (0%)	16.0 ms	2
Self time		15.8 ms (0%)	15.8 ms	2
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.PatCloudUpload$3	▮	2660 ms (5.1%)	65.3 ms	1
multicloudsecurity.PatCloudUpload	▮	2660 ms (5.1%)	65.3 ms	2
javax.swing.JOptionPane	▮	2660 ms (5.1%)	65.3 ms	1
Self time		0.000 ms (0%)	0.000 ms	2
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.DocCloudUpload$8	▮	2323 ms (4.4%)	115 ms	1
multicloudsecurity.DocCloudUpload	▮	2323 ms (4.4%)	115 ms	2
javax.swing.JOptionPane	▮	2323 ms (4.4%)	115 ms	1
Self time		0.000 ms (0%)	0.000 ms	2
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.PatientUpload$1	▮	2269 ms (4.3%)	132 ms	1
multicloudsecurity.PatientUpload	▮	2269 ms (4.3%)	132 ms	2
javax.swing.JOptionPane	▮	2269 ms (4.3%)	132 ms	1
Self time		0.000 ms (0%)	0.000 ms	2
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.ViewDoctor$4	▮	2219 ms (4.2%)	82.0 ms	1
multicloudsecurity.ViewDoctor	▮	2219 ms (4.2%)	82.0 ms	2
multicloudsecurity.MultiCloudSecurity	▮	2219 ms (4.2%)	82.0 ms	1
javax.swing.JOptionPane	▮	2219 ms (4.2%)	82.0 ms	1
Self time		0.000 ms (0%)	0.000 ms	1
Self time		0.000 ms (0%)	0.000 ms	2
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.DoctorUpload$1	▮	2190 ms (4.2%)	180 ms	1

Fig 5: CPU Time consumption



Call Tree - Class	Time [%] ▾	Time	Time (CPU)	Invocations
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.AddDoctor$2	▮	2737 ms (10.7%)	205 ms	1
multicloudsecurity.AddDoctor	▮	2737 ms (10.7%)	205 ms	2
javax.swing.JOptionPane	▮	2595 ms (10.1%)	63.5 ms	1
multicloudsecurity.MultiCloudSecurity		94.7 ms (0.4%)	94.7 ms	5
multicloudsecurity.OuterSecurity1		44.3 ms (0.2%)	44.3 ms	3
javax.crypto.KeyGenerator		44.3 ms (0.2%)	44.3 ms	1
Self time		0.000 ms (0%)	0.000 ms	3
multicloudsecurity.DBConnection		19.2 ms (0.1%)	19.2 ms	1
java.sql.DriverManager		19.2 ms (0.1%)	19.2 ms	1
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.OuterSecurity3		15.8 ms (0.1%)	15.8 ms	1
javax.crypto.Cipher		15.8 ms (0.1%)	15.8 ms	1
Self time		0.000 ms (0%)	0.000 ms	1
java.math.BigInteger		15.3 ms (0.1%)	15.3 ms	1
Self time		0.000 ms (0%)	0.000 ms	5
multicloudsecurity.DoctorUpload		33.1 ms (0.1%)	33.1 ms	2
java.awt.Frame		13.7 ms (0.1%)	13.7 ms	1
Self time		0.000 ms (0%)	0.000 ms	2
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.DoctorUpload$2	▮	2500 ms (9.8%)	139 ms	1
multicloudsecurity.DoctorUpload	▮	2500 ms (9.8%)	139 ms	2
javax.swing.JOptionPane	▮	2500 ms (9.8%)	139 ms	1
Self time		0.000 ms (0%)	0.000 ms	2
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.DocCloudUpload$3	▮	2357 ms (9.2%)	46.2 ms	1
multicloudsecurity.DocCloudUpload	▮	2357 ms (9.2%)	46.2 ms	2
javax.swing.JOptionPane	▮	2357 ms (9.2%)	46.2 ms	1
Self time		0.000 ms (0%)	0.000 ms	2
Self time		0.000 ms (0%)	0.000 ms	1
multicloudsecurity.DocCloudUpload$16	▮	1914 ms (7.5%)	95.2 ms	1
multicloudsecurity.DocCloudUpload	▮	1914 ms (7.5%)	95.2 ms	2

Fig 6 : CPU Time consumption