International Journal of Scientific Modern Research and Technology
(Vol: 5, Issue: 1, Number: 13)
ISSN: 2582-8150

Security Consideration in Cloud using Cryptographic Policy with Instance-Based Encryption

Manish Kumar[1], Rajeev Raghuwanshi[2]
[1]Research Scholar, [2]Assistant Professor and Head
[1,2]Dept of CSE, MITS, Bhopal, India

Abstract- This work discusses the security of data in cloud computing. It is a study of data in the cloud and aspects related to it concerning security. The work will go into details of data protection methods and approaches used throughout the world to ensure maximum data protection by reducing risks and threats. Availability of data in the cloud is beneficial for many applications but it poses risks by exposing data to applications that might already have security loopholes in them. Similarly, the use of virtualization for cloud computing might risk data when a guest OS is run over a hypervisor without knowing the reliability of the guest OS which might have a security loophole in it. This task will also provide insight on data security aspects for Data-in-Transit and Data-at-Rest. The study is based on all the levels of SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). The growth of cloud computing is mainly hampered due to these security concerns and challenges. Proper security arrangements need to be placed before selecting the service provider for any cloud computing service and customers need to be very careful about understanding the risks of security breaches and challenges of using this new computing environment. The methodology is implemented on CloudSim 3.0.1 toolbox, which is configured in NetBeans 8.1. The outcome demonstrates that it gives improved execution contrasted with supplementary predictable security algorithm. Crypto operation time, key operation time, and total execution are reduced by 2.72%, 7.91% and 4.63% significantly.
Index Terms: Cloud Computing, SaaS, PaaS, IaaS, CloudSim, Netbeans, Data-in-Transit.

1. INTRODUCTION

Cloud computing is emerging as the best suited utility for organizations who dreamt for economic, feasible, flexible and scalable computing service for its day to day activities. The cloud computing offers network of centralized computing infrastructure which can be deployed very fast and can also be scalable as per user requirements with great efficiency and minimum burden of managing the system. With its un- precedence advantages, cloud computing enables a fundamental paradigm shift in how we deploy and deliver computing services. Users and organizations can avoid spending large amount of money and resources creating large capital outlays when purchasing and managing software and hardware, as well as dealing with the operational overhead therein.

In all types of computing systems and environments, it is matter of great concern that the data and applications remain secure and unauthorized access must be prevented to stop unwanted use of information but in cloud computing specific measures need to be taken and implemented to ensure data integrity, security, authentication and authorization. In comparison to the traditional computing environment, data, applications, resources and processes remain at some unknown remotely located position in a cloud computing environment. In cloud computing environment if any breach of data occurs then both the service provider and user are responsible and both are responsible to make cloud secure. In cloud computing mechanism of data storage, retrieval, security, process, application etc are to be kept hidden from the actual user who only sees the response of his request. All the parameters, processes, mechanisms, applications and resources which are meant to secure user interface with the cloud always remain hidden from him, which makes him more vigilant about the issues of data loss and security of his private information, which ultimately decreases the progress of cloud.

Any unwanted person can affect the user data, applications, data servers, hardware or software of the cloud infrastructure if proper security mechanisms are not placed at appropriate levels.

Cloud computing offers a big lot of resources, applications and facilities to the user which in general he cannot afford to have but at the same time service providers have to protect the cloud infrastructure by employing suitable security mechanisms. Cloud computing definitely provide a cost effective and beneficial service models for various users but in terms of security and issues related to privacy of data and user application usage profiles are still a big challenge to address and research. Performance of the cloud computing system is largely affected by these security issues. To ensure some level of security service providers are trying to provide some mechanism like virtualization, authentication mechanisms and cryptography techniques but these mechanisms have some chances to be affected also. While data, services, controls and web applications are made available to cloud system, their control is lost. Cloud computing environment is a shared facility for data access making security issue about data privacy, personal privacy, authentication, compliance, confidentiality, integrity, encryption, internet protocol where most of the IP services are un-trusted. In addition, Service Level Agreement (SLA) between user and service provider, third party management, risk of virtualization, non-availability of good standards, auditing process, law for compliance and regulations are other factors for security in cloud environment.

2. REALTED WORK

Cloud computing is one of the fastest emerging technologies in computing. There are many advantages as well few security issues in cloud computing. This paper explores the different data security issues in cloud computing in a multi-tenant environment and proposes methods to overcome the security issues. (P. Ravi Kumar, P. Herbert Raj, P. Jelciana; 2020)

Now customers can opt for software and information technology services according to his requirements and can get these services on a leased basis from the network service provider and this has the facility to scale its requirements to up or down. (Prof. Dr. Pradeep Kumar Sharma, Prof. Dr. Prem Shankar Kaushik, Prerna Agarwal;L 2019)

Along with the growing popularization of Cloud Computing. Cloud storage technology has been paid more and more attention as an emerging network storage technology which is extended and developed by cloud computing concepts.(Diao Zhe, Wang Qinghong, Su Naizheng and Zhang Yuhan; 2018)

"Cloud" is a common metaphor for an Internet accessible infrastructure (e.g., data storage and computing hardware) that is hidden from users. Cloud computing makes data truly mobile and a user can simply access a chosen cloud with any internet accessible device. In cloud computing, IT-related capabilities are provided as services, accessible without requiring detailed knowledge of the underlying technology.(Wang Qinghong, Su Naizheng; 2017)

Cloud computing turned into the most predominant innovation in recent years. This innovative technology provides services to the customers for software and hardware. One can state that distributed computing can blast the portable business. (Shazia Tabassam; 2016)

Off-site data storage is an application of cloud that relieves the customers from focusing on data storage system. However, outsourcing data to a third-party administrative control entails serious security concerns. Data leakage may occur due to attacks by other users and machines in the cloud. (Mazhar Ali, Saif U. R. Malik, Samee U. Khan; 2016)

Cloud computing is a model which provides on-demand delivery of Information Technology (IT) related capabilities or resources through the Internet to the outside world. Despite the advantages of cloud computing, the security of the data and resources is still doubtful which affect the cloud adoption. (Manpreet Kaur, Kiranbir Kaur; 2016)

3. METHODOLOGY

CP-IBE used to facilitate key management and cryptographic access control in an expressive and efficient way. An attribute descriptive string assigned to a user and each user may be tagged with multiple attributes under the construction of CP-IBE. Multiple users may share common attribute which allow sensors to specify a data access policy by composing

 ISSN: 2582-8150

multiple attribute through logical operators such as "AND", "OR".

The Algorithm of proposed methodology CPIBE (Cryptographic Policy with Instance Based Encryption) is as follows:

1. Setup: Defines the universal attribute set (U), computes the public key (PK) and master key (MK).
2. Encryption (PK, M, A): Takes input the public key PK, message M and an access structure. A built over the universal attribute set U. Gives as output the cipher text CT. Only users having a set of attributes corresponding to the access structure A can decrypt the cipher text (CT).
3. Key Generation (MK, S): Takes as input a master key MK and the user set of attributes S and generates the user's secret key SK.
4. Decryption (PK, CT, SK): Takes as input the public key PK, cipher text CT and a secret key SK. It returns a message M that is plain text of CT.

The flowchart of methodology is as follows

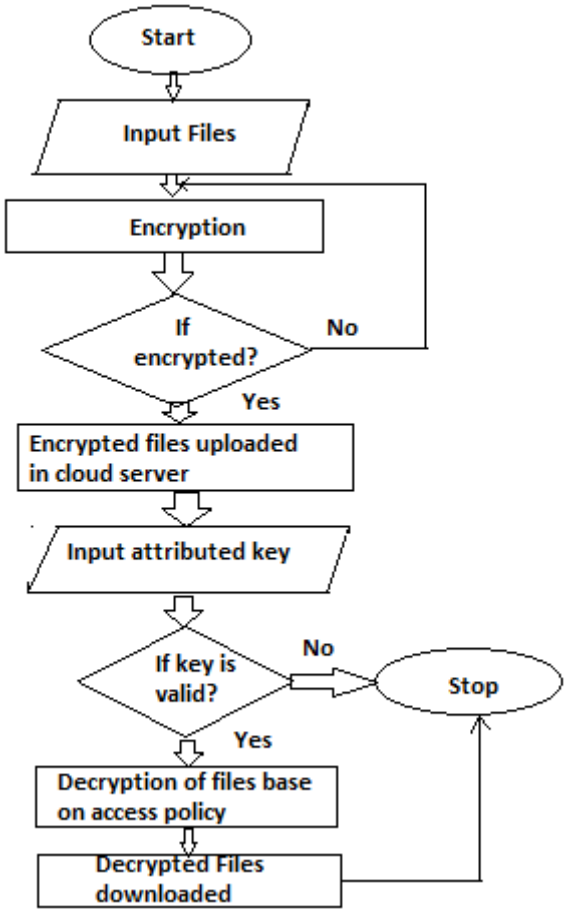

Figure 1: Flowchart of Methodology (CPIBE)

4. RESULTS AND ANALYSIS

We used Java for implementing a working prototype of CPIBE. The .Net cryptographic packages were used for the involved cryptographic operations. Large prime numbers were handled by using the cloud based cryptography classes. Policies were uploaded as a separate file to the cloud and the *KM*.

Table 1: Analysis of Key Establishment Time (in sec.)

File Size (in kb)	Upload		Download	
	DaSCE[6]	CPIBE (Proposed)	DaSCE[6]	CPIBE (Proposed)
0.01	0.1	0.074	0.97	0.068
1	0.098	0.068	0.99	0.072
10	0.09	0.062	0.97	0.071
100	0.15	0.84	0.95	0.78
1000	0.23	0.095	0.99	0.063
10000	0.28	0.098	0.98	0.059

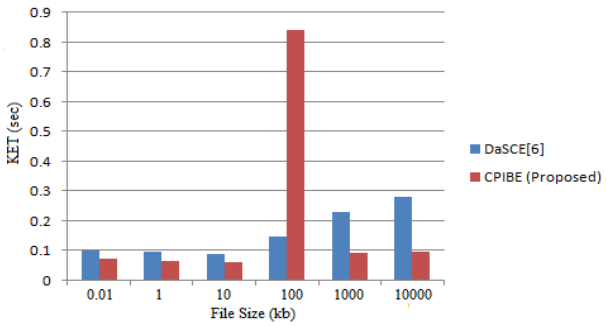

Figure 2: Comparison of Key Establishment Time (in sec.) in between of DaSCE[6] and CPIBE (Proposed) (upload case)

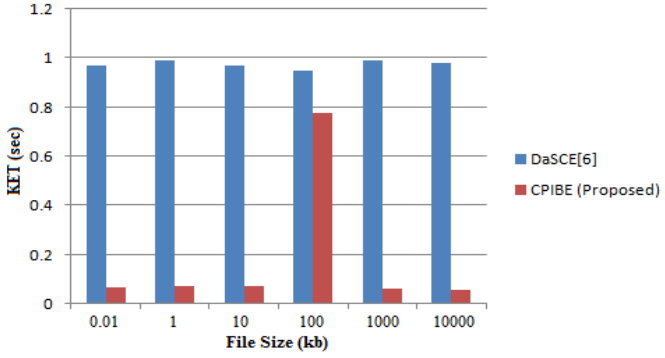

Figure 3: Comparison of Key Establishment Time (in sec.) in between of DaSCE[6] and CPIBE (Proposed) (download case)

 ISSN: 2582-8150

Table 2: Analysis of Crypto Operation Time (in sec.)

File Size (in kb)	Upload		Download	
	DaSCE[6]	CPIBE (Proposed)	DaSCE[6]	CPIBE (Proposed)
0.01	0.059	0.035	0.062	0.057
1	0.076	0.041	0.068	0.061
10	0.083	0.078	0.073	0.069
100	0.092	0.081	0.075	0.063
1000	0.14	0.094	0.187	0.096
10000	0.29	0.14	0.548	0.18

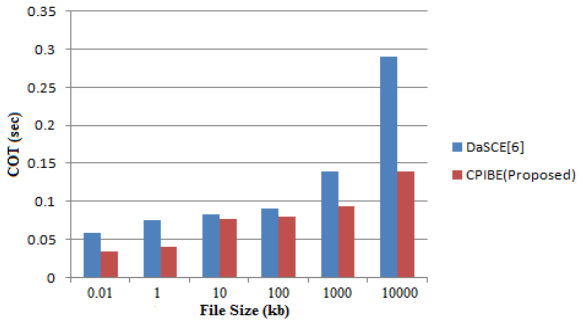

Figure 4: Comparison of Crypto Operation Time (in sec.) in between of DaSCE[6] and CPIBE (Proposed) (upload case)

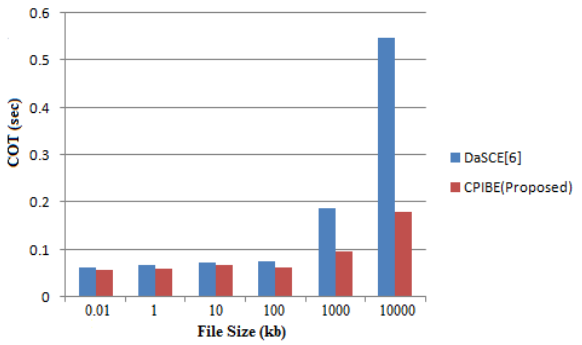

Figure 5: Comparison of Crypto Operation Time (in sec.) in between of DaSCE[6] and CPIBE (Proposed) (download case)

Table 3: Analysis of Key Transmission Time (in sec.)

File Size (in kb)	Upload		Download	
	DaSCE[6]	CPIBE (Proposed)	DaSCE[6]	CPIBE (Proposed)
0.01	0.093	0.067	0.091	0.077
1	0.094	0.071	0.092	0.079
10	0.091	0.069	0.089	0.082
100	0.092	0.071	0.094	0.084
1000	0.098	0.074	0.096	0.085
10000	0.089	0.076	0.093	0.081

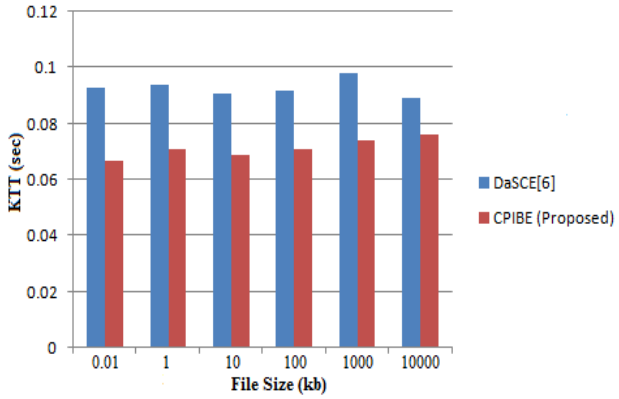

Figure 6: Comparison of Key Transmission Time (in sec.) in between of DaSCE[6] and CPIBE (Proposed) (upload case)

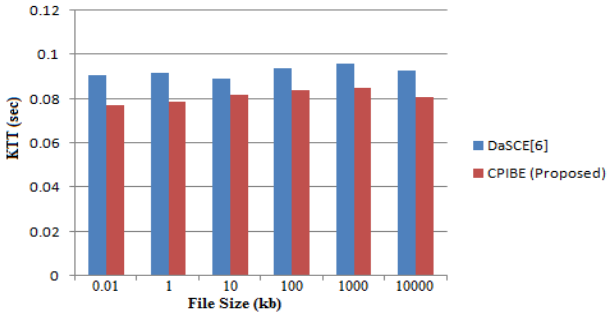

Figure 7: Comparison of Key Transmission Time (in sec.) in between of DaSCE[6] and CPIBE (Proposed) (download cas

Table 4: Analysis of File Transmission Time (in sec.)

File Size (in kb)	Upload		Download	
	DaSCE[6]	CPIBE (Proposed)	DaSCE[6]	CPIBE (Proposed)
0.01	0.24	0.18	0.018	0.007
1	0.48	0.36	0.059	0.019
10	0.53	0.39	0.185	0.091
100	0.82	0.57	0.97	0.14
1000	1.26	0.95	1.17	0.98
10000	9.83	6.79	27.3	18.38

 ISSN: 2582-8150

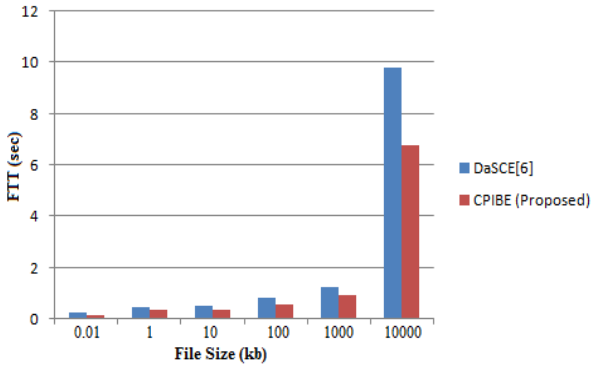

Figure 8: Comparison of File Transmission Time (in sec.) in between of DaSCE[6] and CPIBE (Proposed) (upload case)

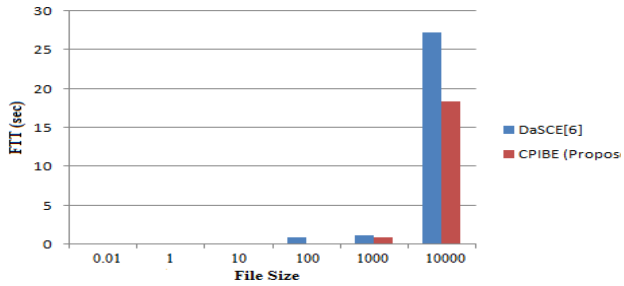

Figure 9: Comparison of File Transmission Time (in sec.) in between of DaSCE[6] and CPIBE (Proposed) (download case)

5. CONCLUSIONS AND FUTURE WORK

The main goal of this work was to analyze and evaluate the security techniques for data protection in the cloud computing. For that purpose we analyzed and evaluated the most important security techniques for data protection that are already accepted from the cloud computing providers. We classified them in four sections according to the security mechanisms that they provide: authentication, confidentiality, access control and authorization.

So, we successfully answered on the key questions in the cloud technology, or simply said should cloud computing be trusted in data protection. We can conclude that if all recommended measures are taken into account providing authentication, confidentiality, access control and authorization, then the cloud computing can be trusted in data protection.

We also focused on the security issues that should be taken into account in depth in order to have proper data security in the cloud. We recommended important security measures relating to data protection in the cloud that must be taken into account. We also proposed a lot of issues that should be considered in order to have improved data security in the cloud computing, like proper usage of administrative privileges, wireless access control of the data in systems that use wireless networks, data recovery and boundary defense in the cloud.

We proposed the CPIBE protocol, a cloud storage security system that provided key management, access control, and file assured deletion. Assured deletion was based on policies associated with the data file uploaded to cloud. On revocation of policies, access keys are deleted by the *KMs* that result in halting of the access to the data. There-fore, the files were logically deleted from the cloud. The key management was accomplished using (k, n) threshold secret sharing mechanism. We modeled and analyzed FADE. The analysis highlighted some issues in key management of FADE. CPIBE improved key management and authentication processes. The performance of the CPIBE was evaluated based on the time consumption during file upload and download. The results revealed that the CPIBE protocol can be practically used for clouds for security of outsourced data. The fact that the CPIBE does not require any protocol and implementation level changes at the cloud makes it highly practical methodology for cloud.

In future, the CPIBE methodology can be extended to secure group shared data and secure data forwarding. Cloud computing can become the frontrunner for a secure, flexible, scalable, cost effective, virtual and user friendly tool for information technology enabled services.

We recommended important security measures relating to data protection in the cloud that must be taken into account. We also proposed a lot of issues that should be considered in order to have improved data security in the cloud computing, like proper usage of administrative privileges, wireless access control of the data in systems that use wireless networks, data recovery and boundary defense in the cloud.

6. REFERENCES

[1] P. Ravi Kumar, P. Herbert Raj, P. Jelciana, “Exploring Data Security Issues and Solutions in

Cloud Computing", 6th International Conference on Smart Computing and Communications, ICSCC 2020, Kurukshetra, India.

[2] Prof. (Dr.) Pradeep Kumar Sharma, Prof. (Dr.) Prem Shankar Kaushik, Prerna Agarwal, "Issues And Challenges of Data Security In A Cloud Computing Environment", IEEE Conference on Cloud Computing, 2019.

[3] DIAO Zhe, WANG Qinghong, SU Naizheng and ZHANG Yuhan "Study on Data Security Policy Based On Cloud Storage", IEEE 3rd International Conference on Big Data Security on Cloud, 2018.

[4] WANG Qinghong, SU Naizheng, "High performance and security in cloud computing", Wiley Journal of Cloud Computing, 2017.

[5] Shazia Tabassam, "Security and Privacy Issues in Cloud Computing Environment", Journal of Information Technology & Software Engineering, 2016.

[6] Mazhar Ali, Saif U. R. Malik, Samee U. Khan, "DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party", IEEE Transactions on Cloud Computing, 2017.

[7] Manpreet Kaur, Kiranbir Kaur, "A Comparative Review on Data Security Challenges in Cloud Computing", International Research Journal of Engineering and Technology (IRJET) Volume: 03, Issue: 01, Jan-2016.

[8] B. Hari Krishna, Dr.S. Kiran, G. Murali, R. Pradeep Kumar Reddy, "Security Issues In Service Model Of Cloud Computing Environment", 2016 International Conference on Computational Science.

[9] Naresh vurukonda, B.Thirumala Rao, "A Study on Data Storage Security Issues in Cloud Computing", 2nd International Conference on Intelligent Computing, Communication & Convergence.

[10] Kire Jakimoski, "Security Techniques for Data Protection in Cloud Computing", International Journal of Grid and Distributed Computing Vol. 9, No. 1 (2016).

[11] Dr. K.B.Priya Iyer, Manisha R, Subhashree R,Vedhavalli K, "Analysis of Data Security in Cloud Computing", International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics, 2016.

[12] Ahmed Albugmi, Madini O. Alassafi, Robert Walters, Gary Wills, "Data Security in Cloud Computing", 5th International Conference on Future Generation CommunicationTechnology, 2016.

[13] Selvamani K, Jayanthi S, "A Review on Cloud Data Security and its Mitigation Techniques", International Conference on Intelligent Computing, Communication & Convergence, 2015.

[14] R. Velumadhava Rao, K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing", International Conference on Intelligent Computing, Communication & Convergence, 2015.

[15] Yunchuan Sun, Junsheng Zhang, Yongping Xiong and Guangyu Zhu, "Data Security and Privacy in Cloud Computing", International Journal of Distributed Sensor Networks, Volume 2014.