IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115189

Cloud Storage Security Based on Dynamic key Generation Technique

Soundarya Sunil Tumsare[1], Lowlesh Nandkishor Yadav[2], Vijay M. Rakhade[3]

Student, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[1]

HOD, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[2]

Asst.Prof, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[3]

Abstract: Cloud computing is an emerging concept combining many fields of computing. The motive of mobile cloud computing is to deliver the services, software and processing capacity over the Internet so far to reduce the computation cost and increase the storage capacity. The goal of this paper is to implement a user authentication algorithm, which can be used in cloud storage to verify the authenticity of the user. In this paper we build a secure mobile cloud-based algorithm, where the user's mobile phone is used as an authentication device, presenting a onetime encrypted password for the user and password is decrypted using proposed algorithm in user's mobile application.

Keywords: IAAS, PAAS, SAAS, Virtual Machine, Cloud

INTRODUCTION

In current decade security and access control technique is big issue in cloud computing. Now a day's various researcher and scientist focus on cloud security issue. The cloud security issue damages the data and faced a problem of authorization and authentication. For the improvement of cloud data security various cryptography technique are used. Cloud Computing referred as the accessing and storing of data and provide services related to computing over the internet. The cloud is a very convenient place to store all of your most important files. It simply referred as it remote services on the internet manage and access data online rather than any local drives. The data can be anything like images, videos, audios, documents, files etc.

BACKGROUND RESEARCH

To interact with various services in the cloud and to store the data generated/processed by those services, several security capabilities are required.
Based on a core set of features in the three common cloud services

- Infrastructure as a Service (IaaS).
- Platform as a Service (PaaS).
- Software as a Service (SaaS).

According to our research they have analyzed that many of the papers focuses on the problem of better security issues for cloud environment with the key management concepts. Few review of summary described here and implicated with their respective author names and the rest of information will be further described in the references.

RELATED WORK

We used cyclic key shift technique for the generation and cloud Data Storage, with focus to provide confidentiality and integrity services and mechanism. More precisely, we have analysed each and every operational step of the model, to achieve the desired goals. We also have defined and elaborated a set of comparison and assessment criterion which are used for analysing, comparing and evaluating the proposed architecture with already available cloud storage service providers in order to identify their pros and cons. Technical security issues in Cloud Computing, however, these issues are more related with the problems of web services and web browser and not of Cloud Computing. Browser Security is also an important issue in Cloud Computing as in a cloud most of the computation is done on remote servers and the client PC is only used for I/O, and authorization of commands to cloud.

 This work is licensed under a Creative Commons Attribution 4.0 International License

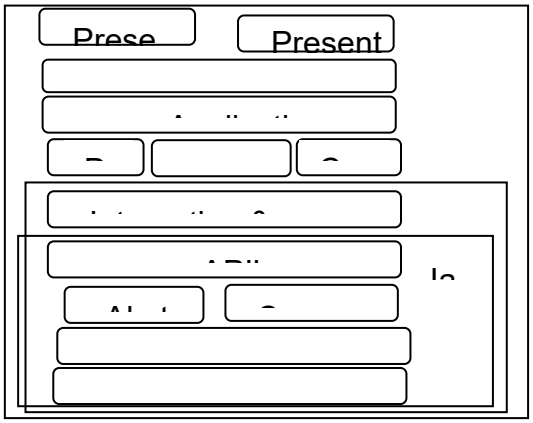
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

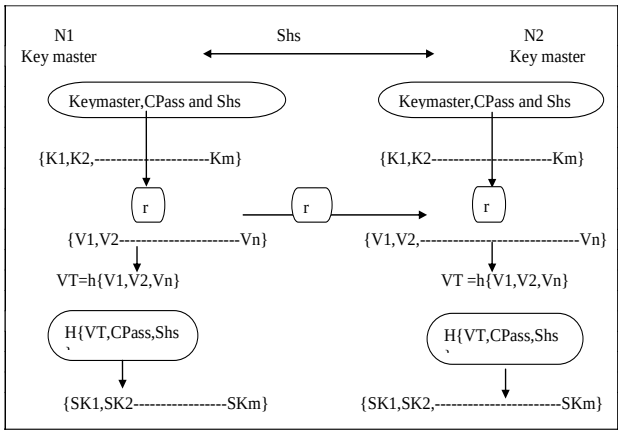
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115189

CLOUD REFERENCE MODEL (CLOUD SECURITY ALLIANCE)



SHOWS PROPOSED KEY GENERATION TECHNIQUE



PROPOSED METHOD

- {N1,IN.N2} The set of notation represent the value of user party, TPA and cloud server
- Sk = Session key.
- (Ki)s = secrete key.
- Cid = the common key unit.
- VT = represent value of group key, it equals h{V1,V2,V3}
- Token = a generated token for server and user
- (X) =message.
- h(X) = hashed message

CONCLUSION

Key generation and key management is a novel security paradigm where versatile provisioning of computational resources and services are facilitated. In contrast to numerous benefits offered by cloud viz. elasticity, scalability, reliability, sustainability, metering resources consumed, location independency etc. data security concerns are yet to be fully addressed before its wide adoption.

The analysis and evaluation have enabled us draw some conclusions. Majority of the already available models are mature enough, but, they do not provide flexible security options for encryption based on data sensitivity. Also, verifying the integrity of data on cloud requires some computation and communication cost, which needs to be reduced drastically, due to network traffic and slow internet connectivity.

REFERENCES

1. Rui Zhang, Ling Liu “Security Models and Requirements for Healthcare Application Clouds” 2010, Pp 1-8.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 5, May 2022

DOI: 10.17148/IJARCCE.2022.115189

2. Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono "On Technical Security Issues in Cloud Computing" International Conference on Cloud Computing, IEEE 2009. Pp 109-116.
3. Liang Yan, Chunming Rong, Gansen Zhao "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography" Springer, 2009. Pp 167-177.
4. S. Subashini, V. Kavith "A survey on security issues in service delivery models of cloud computing" Elsevier ltd. 2011, Pp 1-11.
5. Vinod Kumar, Lalita Devi "RSA Public Key Cryptography for Data Protection in Cloud Computing Environments" international journal of innovative research & development, 2014. Pp 326-329.
6. Dr. Sarbari Gupta"Securely management crypgraphic keys used within a cloud environment", 2012 NIST Cryptographic Key management workshop, Sept 2012.