International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 2, February 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Data Sharing with Sensitive Information Hiding in Data Storage using Cloud Computing

Paruvathavarthini M[1], Prasuna K S[1], Sermakani. A. M[2]

[1]UG Scholar, [2]Associate Professor,

[1,2]Department of IT, S.A Engineering College, Chennai, Tamil Nadu, India

ABSTRACT

With cloud storage services, users can remotely store their data to the cloud and realize the data sharing with others. Remote data integrity auditing scheme is proposed to guarantee the integrity of the data stored in the cloud. In some common cloud storage systems such as the Electronic Health Records (EHRs) system, the cloud file might contain some sensitive information. The sensitive information should not be exposed to others when the cloud file is shared. Encrypting the whole shared file can realize the sensitive information hiding, but will make this shared file unable to be used by others. How to realize data sharing with sensitive information hiding in remote data integrity auditing still has not been explored up to now. In order to address this problem, we propose a remote data integrity auditing scheme that realizes data sharing with sensitive information hiding in this system.

***How to cite this paper*:** Paruvathavarthini M | Prasuna K S | Sermakani. A. M "Data Sharing with Sensitive Information Hiding in Data Storage using Cloud Computing" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-2, February 2020, pp.479-481, URL: www.ijtsrd.com/papers/ijtsrd30007.pdf

IJTSRD30007

INRODUCTION

In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file and transforms these data blocks' signatures into valid ones for the sanitized file. These signatures are used to verify the integrity of the sanitized file in the phase of integrity auditing. As a result, our scheme makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efficiently executed. Meanwhile, the proposed scheme is based on identity-based cryptography, which simplifies the complicated certificate management. The security analysis and the performance evaluation show that the proposed scheme is secure and efficient.

SCOPE OF THE PROJECT

In our scheme, the file stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. Besides, the remote data integrity auditing is still able to be efficiently executed.

RELATED WORKS-

- Firstly, this signature is constructed based on chameleon hashes. However, a lot of chameleon hashes exhibit the key exposure problem. To avoid this security problem, the signature requires strongly unforgeable chameleon hashes, which will inevitable incur huge computation overhead.
- Secondly, the signature does not support blockless verifiability. It means that the verifier has to download the entire data from the cloud to verify the integrity of data, which will incur huge communication overhead and excessive verification time in big data storage scenario.
- Thirdly, the signature used is based on the PKI, which suffers from the complicated certificate management.

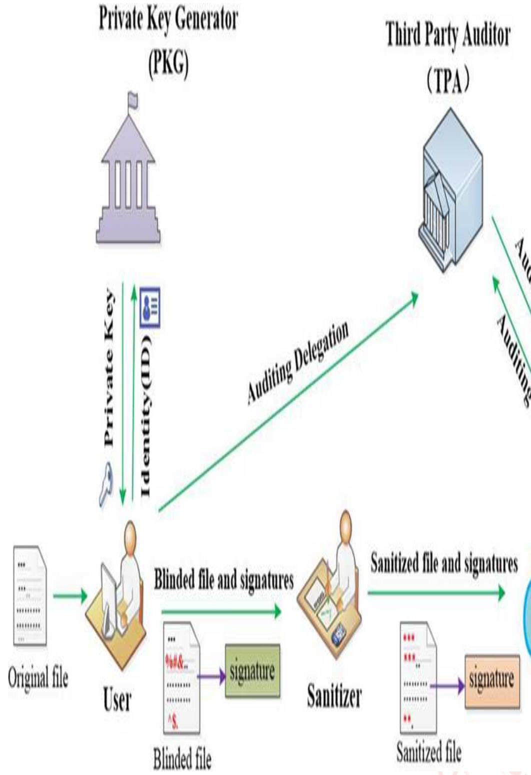
PROPOSED SYSTEM

We investigate how to achieve data sharing with sensitive information hiding in remote data integrity auditing, and propose a new concept called identity-based shared data integrity auditing with sensitive information hiding for secure cloud storage. In such a scheme, the sensitive information can be protected and the other information can be published. It makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is protected, while the remote data integrity auditing is still able to be efficiently executed.We design a practical identity-based shared data integrity auditing scheme with sensitive information hiding for secure cloud storage.

ADVANTAGES OF PROPSED SYSTEM

- However, all of existing remote data integrity auditing schemes cannot support data sharing with sensitive information hiding. Here , we explore how to achieve data sharing with sensitive information hiding in identity-based integrity auditing for secure cloud storage.
- Meanwhile, the proposed scheme is based on identity-based cryptography, which simplifies the complicated certificate management.
- The computation overhead can be reduced.

SYSTEM ARCHITECTURE



SCOPE OF THE SYSTEM

- The scope of the project covers in building a recommendation engine powered by novel machine learning algorithm for user criteria classification which is to reduce the time and space complexities.
- A Recommendation Engine.
- A Novel Machine Learning Algorithm for Classifying the user based criteria.
- Real world streaming user datasets.

IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system.

MODULE DESCRIPTION:

1. Initial Virtual Machine Information Module:
2. Virtual Machine Disk Space Details Module:
3. Server Level Information Module:
4. Network Path Tracing Module (Server level data info module):
5. Read/Write Status Module:
6. Application Log Events Visualization Module:
7. User Contexts Visualization Module:

Initial Virtual Machine Information Module:

The Initial Virtual Machine Information Module defines the network and traces the initial; machine information using the algorithm Data Stream Model and the k-ary Sketch Algorithm which is generable from a network, and produces a network N such that is generable from N and not from any other network.

Following items were visualized under this module:

A. Machine Name will be defined.
B. Server Name (instance Name) will be noted.
C. Edition Installed will be updated.
D. Product Build Information Level info will be shown.
E. SP Level & Collation Type will be fixed
F. Last Query/Server usage will be monitored

ALGORITHM USED

Path tracing is a graphical method of rendering traces of the data navigation happening in the network such that the global illumination is faithful to reality.

This algorithm is integrating over all accumulation of data arriving to a single point on the surface of an object. This accumulation is then reduced by an into sub paths based on the different access points in different intervals.

Following items were visualized under this module:

1. Number of TOTAL PACKET READS (In terms of bytes) since the last server was started
2. Latest packets read in a specific interval (Data read in bytes)
3. Number OF TOTAL WRITES ON THE PACKETS (In terms of bytes) since the last server starts
4. Latest packets write in a specific interval (Data read in bytes)
5. CONNECTION ESTABILISHED SINCE THE LASTER SERVER STARTS in a specific interval (Data read in bytes)

SYSTEM EVALUATION

As the number of security related events generated in modern networks is on the rise, the need for network security visualization systems is felt more than ever. In this paper, we have examined recent works in network security visualization from a use-case perspective. Five use-case classes, each representing a different application area, were defined and several recent works in each category were thoroughly described. We detailed the underlying data sources of network security visualization and gave a few examples of each category. Analysis of these systems motivated us to examine several issues and concerns surrounding this emerging field.

We elaborated on the advantages and shortcomings of all use-case classes and shed light on paths that researchers should focus toward. We aggregated the findings of our work into an informative table for future references. While the field of visualization is as wide as imagination allows, we hope that the analysis and taxonomy presented here will motivate better future work in this area

CONCLUSION

In future work, field. We elaborated on the advantages and shortcomings of all use-case classes and shed light on paths that researchers should focus toward. We aggregated the findings of our work into an informative table for future references. While the field of visualization is as wide as imagination allows, we hope that the analysis and taxonomy presented here will motivate better future work in this area.

REFERENCES

[1] C. Ware, Information Visualization: Perception for Design. Morgan Kaufmann Publishers, Inc., 2004.

[2] G. Conti, Security Data Visualization. No Starch Press, 2007.

[3] R. Marty, Applied Security Visualization. Addison-WesleProfessional, 2008.

[4] R. Erbacher, K. Walker, and D. Frincke, "Intrusion and Misuse Detection in Large-Scale Systems," IEEE Computer Graphics and Applications, vol. 22, no. 1, pp. 38-48, Jan./Feb. 2002.

[5] R. Erbacher, "Intrusion Behavior Detection through Visualization," Proc. IEEE Int'l Conf. Systems, Man and Cybernetics, pp. 2507- 2513, 2003.

[6] T. Takada and H. Koike, "Tudumi: Information Visualization System for Monitoring and Auditing Computer Logs," Proc. Sixth Int'l Conf. Information Visualisation, pp. 570-576, 2002.

[7] K. Lakkaraju, W. Yurcik, and A. Lee, "NVisionIP: Netflow Visualizations of System State for Security Situational Awareness," Proc. ACM Workshop Visualization and Data Mining for Computer Security, vol. 29, pp. 65-72, 2004.

[8] M. Arlitt and T. Jin, Workload Characterization of the 1998 World Cup Web Site, Hewlett-Packard Labs Rep. HPL-99–35R1, Sep. 1999.

[9] L. Bertini, J. C. B. Leite, and D. Moss, "Power optimization for dynamic configuration in heterogeneous web server clusters," J. Syst. Softw., vol. 83, no. 4, pp. 585–598, Apr. 2010.

[10] S. Bilgin and M. Azizoglu, _ "Operation assignment and capacity allocation problem in automated manufacturing systems," J. Com-put. Ind. Eng., vol. 56, no. 2, pp. 662–676, Mar. 2009.

[11] S. H. Bokhari, "Partitioning problems in parallel, pipeline, and distributed computing," IEEE Trans. Comput., vol. 37, no. 1, pp. 48–57, Jan. 1988.

[12] S. Bouchenak, N. De Palma, D. Hagimont, S. Krakowiak, and C. Taton, "Autonomic management of internet services: Experience with self-optimization," in Proc. Int. Conf. Autonomic Comput., Jun. 2006, pp. 309–310.

[13] G. Brown, R. Dell, and K. Wood, "Optimization and persistence," Interfaces, vol. 27, pp. 15–37, 1997.

[14] V. Cardellini, E. Casalicchio, F. Lo Presti, and L. Silvestri, "SLA-Aware resource management for application service providers in the cloud," in Proc. 1st Int. Symp. Netw. Cloud Comput. Appl., Toulouse, France, Nov. 2011, pp. 20–27.

[15] D. Carrera, "Adaptive Execution Environments for Application Servers," Ph.D. dissertation, Tech Univ. Catalonia, Barcelona, Spain, 2008.

[16] S. Chaisiri, L. Bu-Sung, and D. Niyato, "Optimal virtual machine placement across multiple cloud providers," in Proc. IEEE Asia-Pacific Services Comput. Conf., Dec. 2009, pp. 103–110.

[17] S. Chao, J. W. Chinneck, and R. A. Goubran, "Assigning service requests in voice-over-internet gateway multiprocessors," Com-put. Oper. Res., vol. 31, pp. 2419–2437, 2004.

[18] E. G Coffman, M. R. Garey, and D. S. Johnson, "An application of bin-packing to multiprocessor scheduling," SIAM J. Comput., vol. 7, pp. 1–17, Feb. 1978.