ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

E-SC: Collusion-Detection and Outsourcing of Sequence Comparison Algorithm and Finding the Cryptanalyst

Dr. D. Vinodha, K. Prabhakaran, B. Raghul, A. Sakthi Vinayagar

Department of Computer Science and Engineering S. A Engineering College, Chennai, Tamil nadu, India

ABSTRACT: Today data sharing and maintaining its security is major challenge. User in the data sharing system upload their file with the encryption using privatekey.Therearelotsofchallenges like data stolen, confidentialityfordataowner to share their data on servers or cloud. There are different solutions to solve these problems. These techniquesareverymuchcriticaltohandlekeyshared by the data owner.

I.INTRODUCTION

Definition –Cryptanalyst
A cryptanalyst is a person who understands how to decipher secret codes and write codes that cannot be cracked by hackers. They assess and decode the secret messages and coding systems for government agencies, police agencies, and the military. These individuals also protect the privacy of organizations by supervising the online security of data systems.

Cryptanalysis means decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerability and break information security systems.

Types of Security attacks-
1)Active Attack
2)Passive Attack
Active Attack:
A performance attack is a network exploitation in which a target hacker aims to change target data or modify it.

1) Denial of service (DoS)
A security phenomenon that blocks legal users from accessing particular computer systems, devices, services or other ID resources

2) Session replay
After a user steals an incorrect session ID, the session again violates the impersonation of an authorized user to perform fraudulent transactions / transactions.

3) Masquerade
A masquerade assault appears to be an admissible user in order to get an accessibility approach or get more rights

Passive Attack:
Passive attack is a network attack in which the ports and systems are monitored and sometimes scanned for vulnerabilities. The purpose of the attack is to gain information of the target with any modification of information at the target.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

1) Repudiation

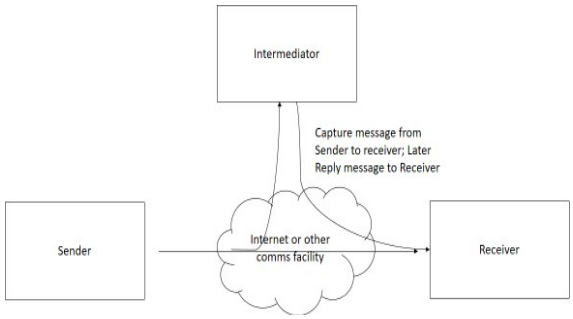
Repudiation is a rejection of something that happens. Regular monitoring and logging of user activities When an application or system restrictions do not follow, the denial strikes, allowing for malicious handling or new actions.

2) Replay

A replay attack (also known as the background attack) is a form of network attack, in which a valid data exchange becomes worse or fraudulent or delayed or delayed.

The Primary sequence comparison algorithms are deployed as a universal outsourcing service on public clouds. But at the same time, its security and privacy issues are increasingly emerging. The outsourced data stored as plaintext could easily be exposed to malicious external intruders and internal attackers in the CSP, and the individual private information carried by character sequences (e.g., personal identification, financial transaction records,genetic markers for some diseases, information that is used to identify paternity or maternity, etc.) could more or less be disclosed or abused. Therefore, secure outsourcing is designed to protect the privacy of character sequences, and toensurethatthescheduledcomputingrequests arenormally performed on the cloud servers.

For this purpose, we present a scheme called Encrypted Sequence Comparison based on a single-server model.Somenovelsaltedhashandencryptiontechniquesare employed to allow public clouds to perform sequence comparisons directly on the character sequences outsourced as ciphertext. Overall, E-SC achieves a user-controlled reliable storage and a collusion-resistant outsourcing service, which plays an important role in the trade-off between security and execution performance. Our scheme is easy in deployment, efficient in processing and controllable in overhead.



II.MODULE DESCRIPTION

A) Login Module

When users access the system through Portal Direct Entry, they are considered guests until they log in. The Login Module is a portal module that allows users to type a user name and password to log in. This module can be placed on any module tab to allow users to log in to the system.

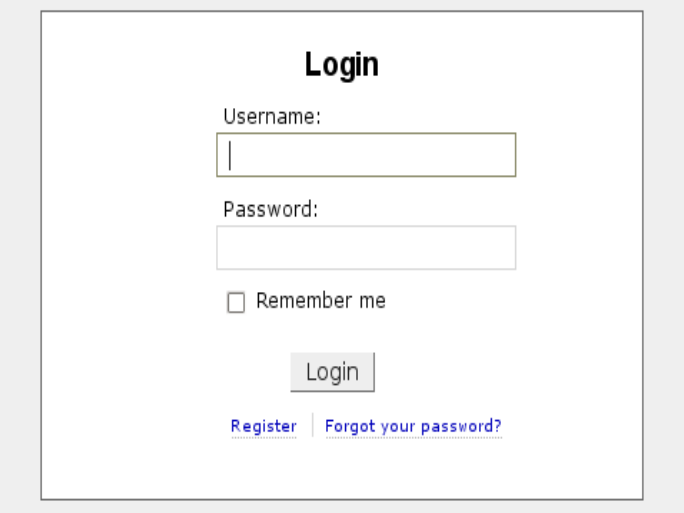
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019



Alternatively referred to as a logon is a set of evidence used to gain access to the area where appropriate authorization is required. Computers, networks and bulletin boards, and other services and devices are used to access and control.

B) RegistrationModule

Registration is the main set of any data management system. The patient's Medical Registration Management System begins to register the patient. OpenMRS is a customizable and advanced solution for Medicare Management which requires a customer patient registration method.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

C) Collusion Detection Module

In This Module, Receiver can find collusion occurring or not using calculating a distance.Collusion detection module will finds whether the data is compromised or not. This module will enhances the user compatibility and develops users knowledge about their data. It will response only data is hacked or not to the user. It won't show who has stolen or hacked their data. Conflict detection The intersection of two or more items is a computational problem. While conflicting detection is often used in video games and is associated with other physical simulations, it is in robotics applications. This method uses mathematical representation technique for checking their data.

D) Third Party Detection Module

In This Module, receiver can also find third-parties. Third party refers to another company makingsoftware for the original vendors product.

Third-party libraries are widely used in Android applications to ease development and enhance functionalities. However, the incorporated libraries also bring new security & privacy issues to the host application, and blur the accounting between application code and library code. Under this situation, a precise and reliable library detector is highly desirable. In fact, library code may be customized by developers during integration and dead library code may be eliminated by code obfuscators during application build process. Theseareallthesomeoftheadvantagesofthetechnique "THIRD PARTYDETECTION'This methodology is widely used from all of them to secure their data confidentially. Here we also use the AES Algorithm with the combination of SHA. AES standsfortheAdvancedEncryptionStandard.Thisis used for Encrypting the messages from both the end users

III. PROPOSED SYSTEM

We propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user. Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function. Our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. We provide security analysis to prove the security of our scheme.

Advantages:

- Power Means of Persuasion andcontrol
- MoreReliable
- It's more secure andefficient.
- Dataconfidentiality

IV. CONCLUSION

Throughtheabovesummary,duetotheproblemsabout the collusion attacks that are widespread in the secure outsourcing of sequence comparison algorithms, this paper proposed the E-SC based on a single-server model.IndividualprivatedataareoutsourcedtotheCSP in the encrypted form, which can preserve the data privacy of end users and support the effective computation of cipher text values. By designing an additive order preserving encryption algorithm as well as a salted hash algorithm, some functional modules of padding, partition, and expansion are deployed. The maneuverability of character sequences and the search ability of cost matrices are totally preserved without requiring the public cloud to modify its outsourcing architecture. In this way, the encrypted sequence

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

comparison can be operated directly by a single server. The real practical E-SC finds out a good balance between security and execution performance. The results of outsourcing computations are accurate, while thetimeandspaceoverheadarereasonable.**"THUSIT SHOWS HOW WE CAN DETECT THE CRYPTANALYSIST AND HOW WE CAN GET BACK THE DATA FROMTHEM".**

REFERENCES

1. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 2018, pp.68–73.
2. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 2018, pp. 271–350.
3. K. Elissa, "Title of paper if known," unpublished.
4. R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.
5. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 2018[Digests 9th Annual Conf. Magnetics Japan, p. 301, [2018].
6. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 2018
7. Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing ServicesDebiao He, Neeraj Kumar, Muhammad Khurram Khan, Lina Wang, Jian Shen IEEE Systems Journal 2018
8. Securing Fog Computing for Internet of Things Applications: Challenges and SolutionsJianbing Ni, Kuan Zhang, Xiaodong Lin, Xuemin Sherman Shen IEEE Communications Surveys & Tutorials 2018
9. X. Wang, Q. Wu, and Y. Zhang. (Aug. 2018). ''T-DB: Toward fully functional transparent encrypted databases in DBaaS framework.'' [Online].
10. B. Lang, J. Wang, and Y. Liu, ''Achieving flexible and self-contained data protection in cloud computing,'' IEEE Access, vol. 5, pp. 1510–1523, Feb. 2018.
11. D. Yorukoglu, Y. W. Yu, J. Peng, and B. Berger, ''Compressive mapping for next-generation sequencing,'' Nature Biotechnol., vol. 34, no. 4, pp. 374–376, Apr. 2018.
12. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, ''New algorithms for secure outsourcing of modular exponentiations,'' IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2386–2396, Sep. 2018.
13. Y. Feng, H. Ma, X. Chen, and H. Zhu, ''Secure and verifiable outsourcing of sequence comparisons,'' in Proc. Int. Conf. Inf. Commun. Technol. (ICT-EurAsia), Yogyakarta, Indonesia, 2018, pp. 243–252.
14. T. F. Smith and M. S. Waterman, ''Identification of common molecular subsequences,'' J. Molecular Biol., vol. 147, no. 1, pp. 195–197, Mar. 2018
15. B. Lang, J. Wang, and Y. Liu, ''Achieving flexible and self-contained data protection in cloud
16. computing, IEEE Access, vol. 5, pp. 1510–1523, Collusion-Secure Fingerprinting for Digital DataDan Boneh, James Shaw IEEE Trans. Information
17. B. Berger, J. Peng, and M. Singh, ''Computational solutions for omics data,'' Nature Rev. Genet., vol. 14, no. 5, pp. 333–346, May 2018
18. F sequence comparisons,'' Intell. Autom. Soft Comput., vol. 21, no. 1, pp. 51–63, Jan. 2018.
19. M. Lesk, Introduction to Bioinformatics. Oxford, U.K.: Oxford Univ. Press, 2014, pp. 175–221.
20. X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, ''Verifiable computation over large database with incremental updates,'' IEEE Trans. Comput., vol. 65, no. 10, pp. 3184–3195, Oct. 2018