Providing Secure Session through Encryption of Logs for Financial Services

D.S.S. Veeresh[1], Kanugula Kalyaan[2]

[1]Associate Professor, Department of CSE, Gurunanak Institutions, Ibrahimpatnam, Hyderabad, India
[2]B. Tech Student, Department of CSE, Gurunanak Institutions, Ibrahimpatnam, Hyderabad, India

---***---

Abstract - *Now a days security is very important especially in financial and banking sectors. The log files in financial sectors often contain sensitive information, confidentiality and privacy of log records which are equally important. The first thing an attacker often does is to damage log files or interrupt the logging services. It is very important to provide a logging in a secure manner and that the records should be protected for a predetermined amount of time. Integrity of the files and that of the logging process need to be ensured at all times. We address security and integrity issues not only just during the log generation phase, but also during other stages in the log management process. However, deploying a secure logging infrastructure involves substantial capital expenses that many organizations may find overwhelming. In this paper, we identify the challenges for a secure data-based log management service for an organization and propose a framework for doing the same within the viable cost saving measure.*

Key Words: Security, Privacy, Logging Services, Integrity, Data-base Management.

1. INTRODUCTION

A LOG is a record of events occurring within an organization's system or network. Logging is important because log data can be used to troubleshoot problems, fine tune system performance, identify policy violations, investigate malicious activities, and even record user activities. Since log files contain record of most system events including user activities, they become an important target for malicious attackers. An attacker, breaking into a system, typically would try not to leave traces of his or her activities behind. Consequently, the first thing an attacker often does is to damage log files or interrupt the logging services. Furthermore, the sensitive information contained in log files often directly contributes to confidentiality breaches. The emerging paradigm of data-base computing promises a low cost opportunity for organizations to store and manage log records in a proper manner. Organizations can outsource the long-term storage requirements of log files to the data-base. The data-base provider can be honest but curious. This means that it can try not only to get confidential information directly from log records, but also link log record related activities to their sources. No existing protocol addresses all the challenges that arise when log storage and maintenance is pushed to the data-base.

2. EXISTING SYSTEM

Log files contain record of most system events including user activities; they become an important target for malicious attackers. An attacker, breaking into a system, typically would try not to leave traces of his or her activities behind. Consequently, the first thing an attacker often does is to damage log files or interrupt the logging services. It is very important to provide a logging in a secure manner and that the log records are adequately protected for a predetermined amount of time.

3. PROPOSED SYSTEM

In this paper, we propose a comprehensive solution for storing and maintaining log records in a server operating in a data-base-based environment. We address security and integrity issues not only just during the log generation phase, but also during other stages in the log management process, including log collection, transmission, storage, and retrieval. This successfully prevents the data-base provider or any other observer from correlating requests for log data with the requester or generator. Finally, we develop a proof-of-concept prototype to demonstrate the feasibility of our approach and discuss some early experiences with it. To the best of our knowledge, ours is the first work to provide a complete solution to the data-base based secure log management problem.

4. SYSTEM ARCHITECTURE

The users or nodes involved in our papers are Sender, Intermediate and Receiver. In order to send file, the sender has to find out the list of nodes which are connected with the sender. From that available list he can choose receiver. Then the sender has to analyze the performance of each and every node which is connected with the sender. The performance analysis list will return the priority based result so that sender can choose the intermediate to send the file. The Intermediate will receive the file from sender then it will analyze the performance so that it can send data to another inter4.1mediate or receiver. In the receiver side, the receiver has to select the file path to receive the file from sender or intermediate. Then the receiver can view the file received file.

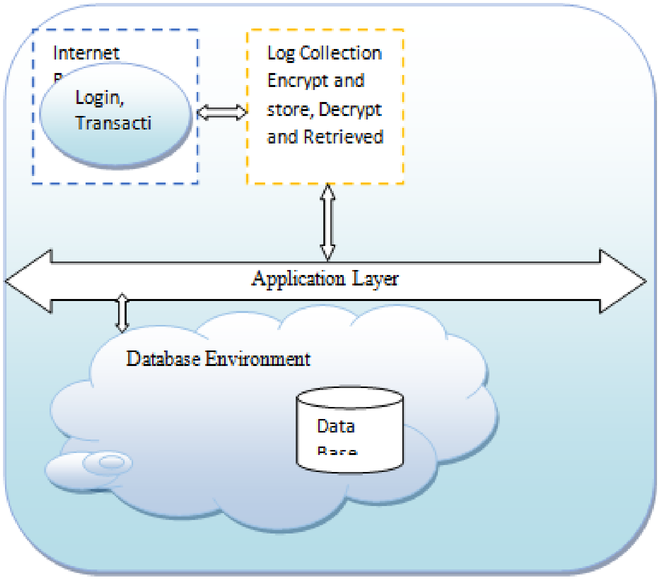
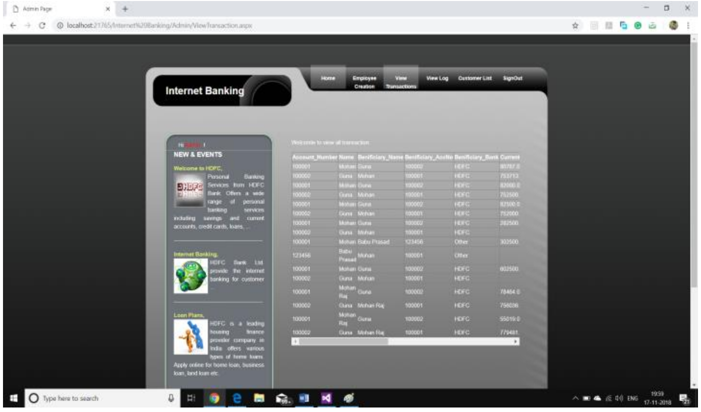


Fig-1: System Architecture

5. IMPLEMENTATION

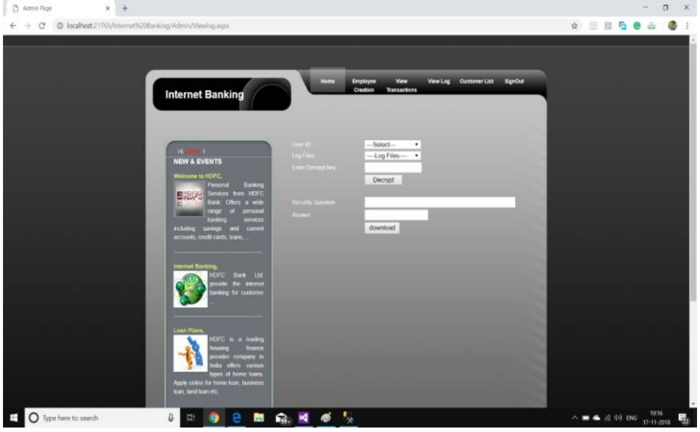


Welcome to view all transaction

Account_Number	Name	Benficiary_Name	Benficiary_AccNo	Benficiary_Bank	Current
100001	Mohan	Guna	100002	HDFC	80787.0
100002	Guna	Mohan	100001	HDFC	753713
100001	Mohan	Guna	100002	HDFC	82000.0
100002	Guna	Mohan	100001	HDFC	752500
100001	Mohan	Guna	100002	HDFC	82500.0
100002	Guna	Mohan	100001	HDFC	752000
100001	Mohan	Guna	100002	HDFC	282500
100002	Guna	Mohan	100001	HDFC	
100001	Mohan	Babu Prasad	123456	Other	302500
123456	Babu Prasad	Mohan	100001	Other	
100001	Mohan	Guna	100002	HDFC	802500
100002	Guna	Mohan	100001	HDFC	
100001	Mohan Raj	Guna	100002	HDFC	78464.0
100002	Guna	Mohan Raj	100001	HDFC	756036
100001	Mohan Raj	Guna	100002	HDFC	55019.0
100002	Guna	Mohan Raj	100001	HDFC	779481

Fig 2.1 Transaction Page

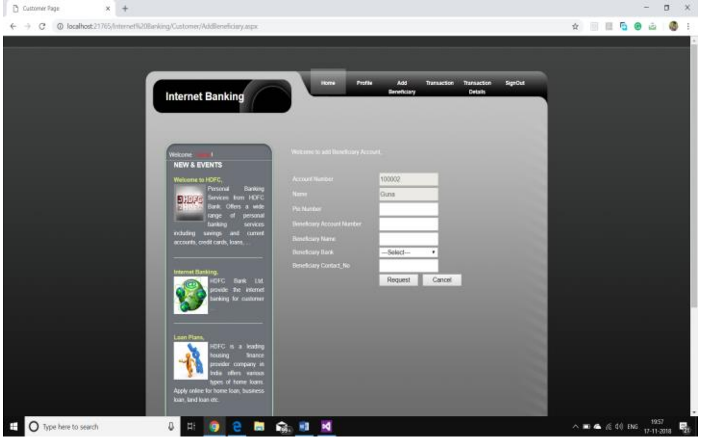
Description: A employee can track the transactions of the users of their bank



User ID ---Select---
Log Files ----Log Files----
Enter Decrypt key
Decrypt
Security Question
Answer
download

Fig 2.2 Log Management Page

Description: Admin only can access the log files using the decrypt key.

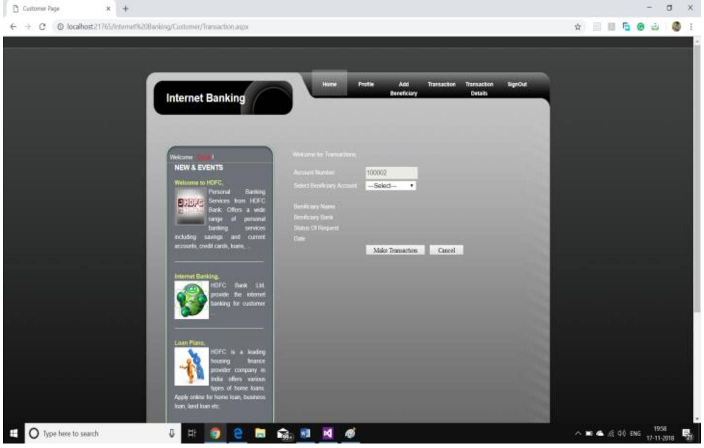


Welcome to add Beneficiary Account.

Account Number 100002
Name Guna
Pin Number
Beneficiary Account Number
Beneficiary Name
Beneficiary Bank ---Select---
Beneficiary Contact_No
Request Cancel

Fig 2.3 Beneficiary Page

Description: In this page a user can add benefaction to their account.



Welcome for Transactions,

Account Number 100002
Select Benificiary Account ---Select---
Benificiary Name
Benificiary Bank
Status Of Request
Date
Make Transaction Cancel

Fig 2.4 Funds Transaction Page

Description: In this a user can make transaction to others

6. CONCLUSION

Maintaining logs securely over long periods of time is difficult and expensive in terms of the resources needed. The emerging paradigm of data-base computing promises a more economical alternative.

7. FUTURE ENHAMCEMENT

In the future, we can refine the log client implementation so that it is tightly integrated with the OS to replace current log process. In addition, to address privacy concerns current implementation allows access to log records that are indirectly identified by upload-tag values.

REFERENCES

1) K. Kent and M. Souppaya. (1992). Guide to Computer Security Log Management, NIST Special Publication 800-92

2) PCI Security Standards Council. (2006, Sep.) Payment Card Industry (PCI) Data Security Standard—Security Audit Procedures Version 1.1

3) M. Bellare and B. S. Yee, "Forward integrity for secure audit logs," Dept. Computer. Science., Univ. California, San Diego, Tech. Rep., Nov. 1997.

4) D. Ma and G. Tsudik, "A new approach to secure logging," ACM Trans. Storage, vol. no. 1, pp. 2:1–2:21

5) B. Schneier and J. Kelsey, "Security audit logs to support computer forensics," ACM Trans. Inform. Syst. Security, vol. 2, no. 2, pp. 159–176

6) D. Dolev and A. Yao, "On the security of public key protocols," IEEE Trans. Inform. Theory, vol. 29, no. 2, pp. 198–208

7) D. L. Wells, J. A. Blakeley, and C. W. Thompson, "Architecture of an open object oriented database management system," IEEE Computer., vol. 25, no. 10, pp. 74–82

8) J. E. Holt, "Logcrypt: Forward security and public verification for secure audit logs," In Proc. 4th Australasian Inform. Security Workshop, 2006, pp. 203–211

9) K. Nørv°ag, O. Sandst°a, and K. Bratbergsengen, "Concurrency control in distributed object oriented database systems," in Proc. 1st East-Eur. Symp. Adv. Databases Inform. Syst