IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Improved Payroll Service with Hybrid Security Algorithm

Sujith K G[1], S. Kuzhalvaimozhi[2]

M.Tech Student, Department of PG Studies, National Institute of Engineering, Mysore, India[1]

Associate Professor, Information Science & Engineering, National Institute of Engineering, Mysore, India[2]

Abstract: Payroll services in banks are major sources of their revenue. Almost all the banks have moved to Core Banking and are offering payroll services to corporates. Corporates are utilising this service to a very great extend because of the advantages they offer to them. But now a days the scenario has changed. Wage related information is expected to be kept as a secret and hence the topic of concern is how effectively the payroll software maintain secrecy and ensure data integrity while preserving a secure channel for information interchange. This paper provides a hybrid algorithm for improving the payroll processing in banks which employ branch banking.

Keywords: Payroll Service, Hybrid cryptography, AES, MD5

I. INTRODUCTION

Payroll processing is one of the most important services rendered by banks to Corporates. For rendering this service banks use payroll processing softwares which are one of the most sophisticated softwares in industry. Such softwares generally provide services like data processing, monitoring, reconciliation etc. Nowadays since almost everyone is having Internet access the threats arising from Internet are also rising. This has affected many softwares and many industries and banking is one of the most affected ones.

Different software vendors are adopted different ways to combat the security scenario. The requirements from corporate customers have also changed a lot pertaining to the changes in the information security scenario. This has put the banks in pressure to come up with modified algorithms in the payroll processing softwares to meet the requirements from the corporate customers. Considering banks with employee branch banking most of the times customers bring salary information directly to branches in non-secure manners. They usually bring data in plain text format and in conventional data storage devices. Since every bank has moved to core banking software, the data brought by the customers in there custom format, need to be converted to a format which can be recognised by the core banking software.

Conversion usually happens manually and hence is prone to errors. During the conversion process data may change and this causes errors in payroll processing.Hence the situation no demands and improved payroll processing software which is capable enough to close the gaps in conventional softwares and also provide features like additional security, data integrity check, non-repudiation, monitoring etc. This paper presence an improved architecture making use of hybrid cryptographic and hashing techniques. That software using this improved architecture combines the advantages of PKI encryption and hashing the provider threat and fraud free payroll processing environment.

II. HARDWARE/SOFTWARE REQUIREMENTS

This section provides the hardware and software requirements in coming up with an improved payroll processing software.

A. Hardware Requirements

Hardware	Regular
System architecture	Intel, AMD
Memory	256 MB
Disk	1.5 GB
Processor	Pentium 2 (min)

B. Software Requirements

Software	Regular	Provider
Operating System	Windows 7 (min)	Microsoft
Java (JDK)	1.7	Oracle
Oracle	11g	Oracle
Gpg4win	2.3.0	Gpg4win
Java API for file transfer protocol	3.3	Apache

III.LITERATURE SURVEY

Combining encryption and hashing provides a unique algorithm which is flexible and scalable enough to suit increasing demands in vulnerability. Encryption and decryption and provide cryptographic security while verification of data integrity is possible with hashing.Encryption techniques provide origin authenticity by using shared secret key. Advanced Encryption System (AES) is the specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). Hash function is an important

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

technique for implementing information integrity. In this paper MD5 hash function is used. The main problem is the creation of forged hash value by intruder. The technique of combining encryption algorithm with hash function is given so that both data integrity and confidentiality can be realised while transmitting message between sender and receiver [1]. Storing data in secure manner is another challenge for softwares dealing with critical data. Usage of hybrid encryption and hashing techniques have proven to be a good tool to have secure data storage. Implementation of such hybrid algorithm has been made possible using open source Java language and NetBeans ID[2].

IV. RELATED WORK

A. System Architecture

Fig 1 shows the system architecture of the software presented in this paper. From the paper it is clear that the architecture makes use of two servers, one hosted in the Internet and another hosted in the intranet. Data transfer across Internet and intranet makes use of secured file transfer protocol (SFTP) which is a file transfer protocol with SSH as its base. SSH authentication is required for a user to use SFTP and perform data transfer. This ensures that only authorised personnel accesses the system and transfer data through the system. Out of the two servers used in the architecture, the one hosted in Internet provides a Web login to customers to access the software and to feed in the payroll information. This server itself is responsible for encrypting the data, feed in by the customer, before transferring the same through the Internet to the branch server. Hence this part of the architecture ensures that the data that comes in is always ciphertext and it's always through a consistent medium and in consistent format.

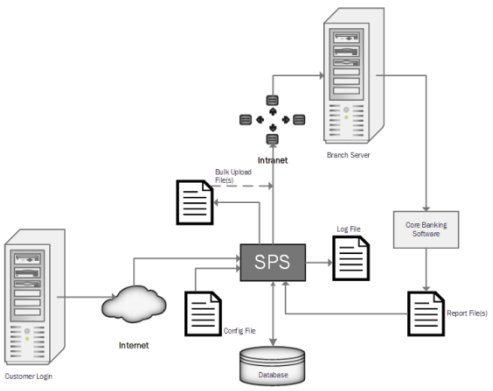

Fig. 1. System Architecture

B. Database and Files

The Database used in this system architecture is a relational database. Compared to any other databases relational databases provide much more scalability and operability. The tables are designed in such a way that they are in third normal form and consume very less space. The Entity relationship between the tables are established keeping in mind the monitoring and reports generation feature of the software. Apart from the relational database, several flat files are also part of the architecture. These flat files play a major role measuring the health of the system and for debugging in case of any errors. The configuration file contains information necessary to setup the software in any new environment. For any changes in the parameters, only the configuration file will undergo change. The log files are essential in case of any software, and are one of the most space consuming files. Recording of all the events happening inside the software is as important as the software itself. In case of a malfunctioning the increase in the logs would help the debugger to identify what went wrong. The bulk file is the interface between the payroll software and the core banking system. This file contains the payroll information in the format which the CBS understands. The report file generated from the CBS acts as a feedback for the payroll software to identify which all transactions went through successfully and which all failed. It is from this report file that the corresponding feedback is sent to the corporate customer.

C. Process Flow

Fig2shows the process followed the by the corporate customers in feeding content and initiating the payroll process. It is evident from the flow that it is mandatory for the customers to have pre-registered in the software along with their public digital certificate to enable signing and encryption.

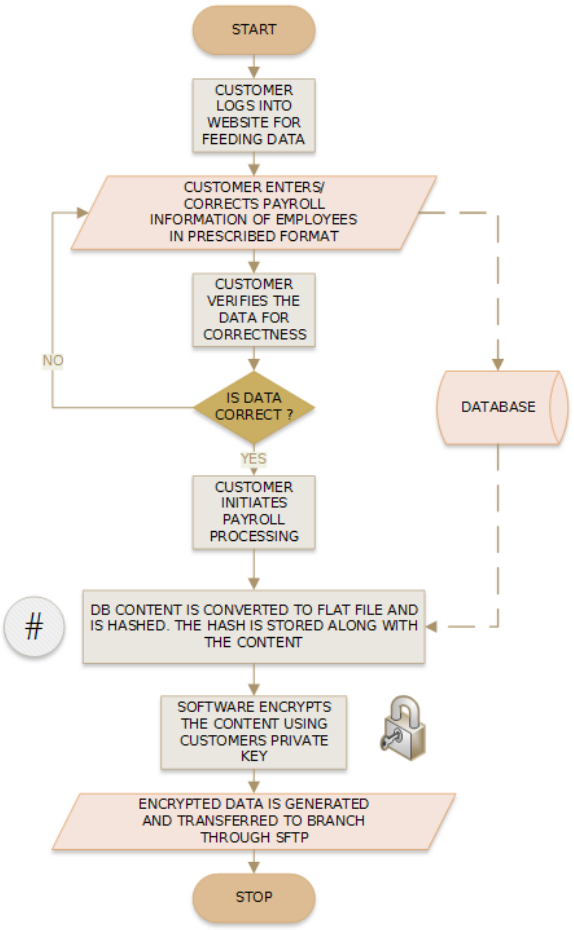

Fig. 2. Customer Process Flow

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

The combination of hashing and encryption improves the message authentication [1]. The use of digital certificate is mandatory for signing and encryption. The digital certificate of the customer needs to be registered in the software whichfollows the algorithm mentioned in [3].

Fig 3 provides the process flow followed in banks for processing in the incoming file. The file that is encrypted, first needs to be decrypted using the public key registered by the customers in the software. PKI encryption ensures non-repudiation of the file and also ensures from any third party from accessing the same which contains confidential data. Further, the hash is regenerated and verified for data integrity. If any error occurs during any of the above process, the flow terminates and an email intimation will be sent to customer. This is a mechanism for real time feedback.

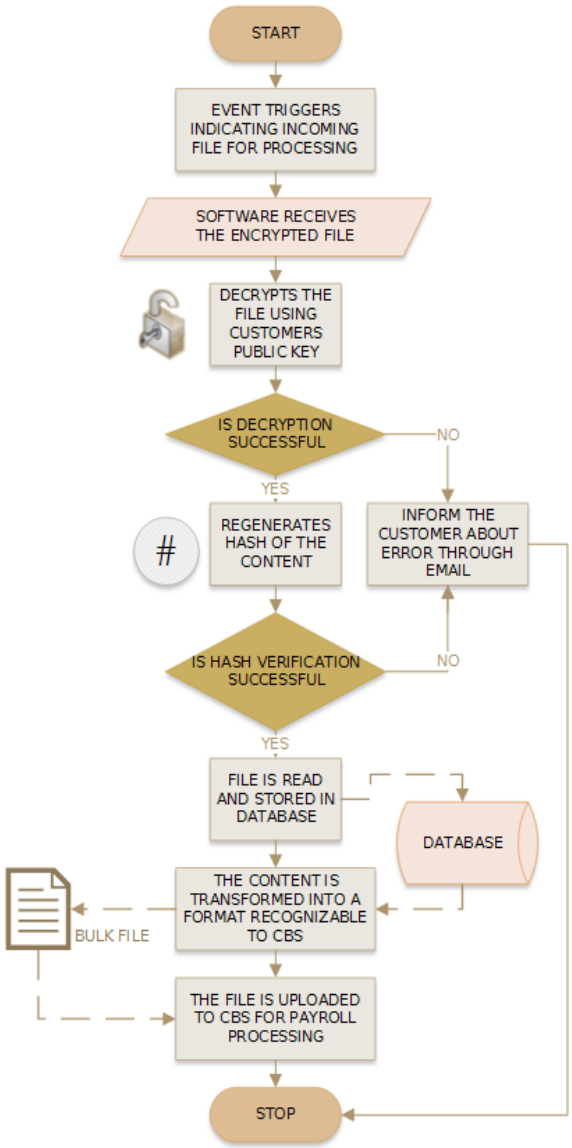

Fig. 3. Bank Process Flow

Upon completion of the processing by CBS, the report that get generated will be sent back to customers, in encrypted form, as feedback, thus ensuring end-to-end secure channel of communication.

V. CONCLUSION

Payroll services will continue to be one of the premium services provided by banks. To meet the changing demands of the corporate customers and scalable and robust system is necessary in banks. It software presented in this paper meets all the domains put forward by the current information scenario and will remain a scalable. Though customizations would be essential before configuring the software for any bank, the improved payroll software architecture provided here will act as a strong base on which the challenges of data security, data integrity, non-repudiation and monitoring can be overcome.

ACKNOWLEDGMENT

First and foremost we express our sincere gratitude to the almighty for the successful initiation, execution and completion of this paper. We would like to thank our colleagues in college sincere support, help and guidance. Our sincere thanks to one and all who may not find a mention but have always wished only success.

REFERENCES

[1] M.Meenakumari, G.Athisha, "Improving Message Authentication by Integrating Encryption with Hash function", International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering Vol. 2, Issue 1, January 2014

[2] J. Breckling, Ed., The Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[3] Rivest R.L., A. Shamir and L. Adleman, 1978. ?A method for obtaining Digital Signatures & Public key Cryptosystems? ,Communication ACM Vol.21, No.2, pp. 120-126

BIOGRAPHIES

Sujith K G is final year M.Tech Student of National Institute of Engineering, Mysore.He has received his B.Tech from Cochin University of Science and Technology (CUSAT). His interested subjects include Data Security and Automation using Artificial Intelligence.

S. Kuzhalvai Mozhi is Associate Professor in the Department of Information Science & Engineering. She has received her M.E. from PSG, Coimbatore and B.E. from Trichy. She is pursuing her Ph.D. Her teaching and research interests are in the field of Cryptography and Compiler.