International Journal of Control Theory and Applications

ISSN : 0974–5572

Volume 9 • Number 40 • 2016

Encrypted Message Processing using Java

Rajarshi Bhowmick[a] and K.Navin[a]

[a]Assistant Professor(O.G), Dept. of Information technology, SRM University

E-mail: Rajarshibhowmick007@gmail.com, k.navin@ktr.srmuniv.ac.in

Abstract: Information security is one of the most important subjects of major information system (MIS). This paper is about the use of a message encryption project based on Microsoft Active Pages (ASP) that encourages MIS students to develop some of the technical aspects of information security in some depth. This project prepared for a valuable pedagogical tool. Students, who having only limited programming and database experience benefited significantly from this paper.

1. INTRODUCTION

Computer network becomes a very important part of the business world and in our daily life. Information security should be taught not only to the computer science students. The business students and the common people should be taught. Hands-on projects, which are technical but easy to implement, can help increase the interest the MIS students explore the technical concepts in information security. On this basis, the authors assigned to the students a project to develop a Web application providing message encryption and decryption. This project is for them to implement, as it requires basic java programming skills and having some knowledge in database and having interest in information security

1.1. What is Message Processing

When we are establishing an agent that will be exchanging messages, it's very important to think about how message processing will integrate and works with the rest of the objects making up the agent.

1.2. Isolate communications

This helps us free to prepare the bulk of the classes making up the application around application problems related to the communication scheme you happen to be using. Likewise, the communications subsystem can be prepared and updated by own, based on the communication needs of the whole system.

1.3. Provide a structured way to link messages

You need a well-defined way for receiving messages to trigger method calls on application objects, and for object methods to make messages to remote agents to system requests.

These may seems conflicting the important requirements. But we'll see that they can be satisfied to one another by a single message-processing method.

1.4. Asynchronous vs. Synchronous Message

A important question in preparing a message-processing system is whether it needs to be asynchronous or not. In chess example, the player agents can process messages synchronously. Since they'll be shaking hand throughout the game. That is, one player sends a move to the other player. the second player applies the move to weighs its options. He sends its countermove to the first player. In this example, there isn't anything else a player needs to do while choosing its move or waiting for the other player to send its move, so there's no need for the ability to receive and process messages asynchronously.

Messages normally trigger some significant processing by an third party service provider, which can be carried on while waiting for another new messages. Agents in a message processing application will usually be better off if they can send and receive the messages asynchronously from any other work they may need to do. This "work" might be in response to the messages, or might be independent of the message passing and it is an ongoing process. If we were implementing a sophisticated network game than our simple chess system, each player may have plenty of work to do and sending and receiving messages. There might be user input for dealing with, multiple remote players to synchronize with the graphical displays for updating, and complicated internal models to keep straight. To keep everything running smoothly message I/O will probably be highly necessary. So our message-passing project should support it.

1.5. Problem Statement

1. The main problem is the security issue.
2. If one person can able get some other person's id and password he or she can see all the important message of the person.so we need more security.

1.6. Basic Message Processor

Based on our earlier discussion of a message processing project, the class which is implemented of a message object. It has a message identifier and a list of arguments which are all presented as strings. The Basic Message having public methods to query its identifier (messageId()) and its arguments (argList()). It also having an abstract Do() method.It will be implemented in subclasses of Basic Message to perform as per requirement by the message. It is in the Do() method implementations that we have to define our message protocol. We should link our message-passing scheme to the application objects in the system which we useing. For each message in our protocol, a subclass of Basic Message we have to defined to interpret the message arguments and do as per users requirement for that type of message.

For the message communication over a connection we have to use the Basic MgsHandler. This class handles messages which is termed as string*tokens* .The full message is simply a series of tokens followed by an "end- of-message" indicator like we can use flag. The first token which identifies the message, and the rest are arguments to the message. The readMsg() method on BasicMsgHandler is used for reading the identifier of message of the incoming message first. Then it calls buildMessage() for constructing the message object which iscorresponded to the message type. The buildMessage() method is abstract in BasicMsgHandler. It is implemented by subclasses for matching the message protocol which should be used.

1.7. Encryption and Decryption of Text String using Java

Encryption : Encryption is the process of encoding a message in such a way that only user can see while sending the message only which is entirely new in message processing system. Encryption denies the intelligible content to a would-be interceptor. In our encryption scheme, the sent message referred as plaintext. Then it is encrypted using an encryption algorithm to generate ciphertext that can only be readable if decrypted. For the technical reasons, an encryption scheme usually uses a random encryption key generated by the algorithm. But, for a well-designed encryption scheme computational resources and skills are mostly required. A user can see decrypt the message also with the help of users account password which user has given at time of sign up.

1.8. Use of Encryption

Firstly encryption is used for military work and govt purpose for secret communication. In military they have to communicate secretly if hacker can hack their message they can make harm to the whole country. But now a day hacking become a very harmful activity to common people also. Hacker used to get valuable information and with that they are doing wrong things. So encryption became very essential wherever any kind data being shared. Example: mobile , message processing, Bluetooth, wireless microphone, wireless intercom etc.

2. DECRYPTION

Decryption is the process to encoded encrypted text or other data and converting it back into normal text that user can read and understand. This term is used to describe a method of un-encrypting the data manually using the proper codes or keys.

The use of data encryption is to make it difficult for someone to steal the information. If this messages need to be viewable, that time it require decryption. When the decryption passcode or key is not available, special software may be needed to decrypt the data with the help of algorithms to make the decryption and make the data readable.

2.1. How it works

Here we have showed how to encrypt and decrypt text string using Java. The Encryption and Decryption is based on a key/password that's why it is referred as Password Based Encryption(PBE).

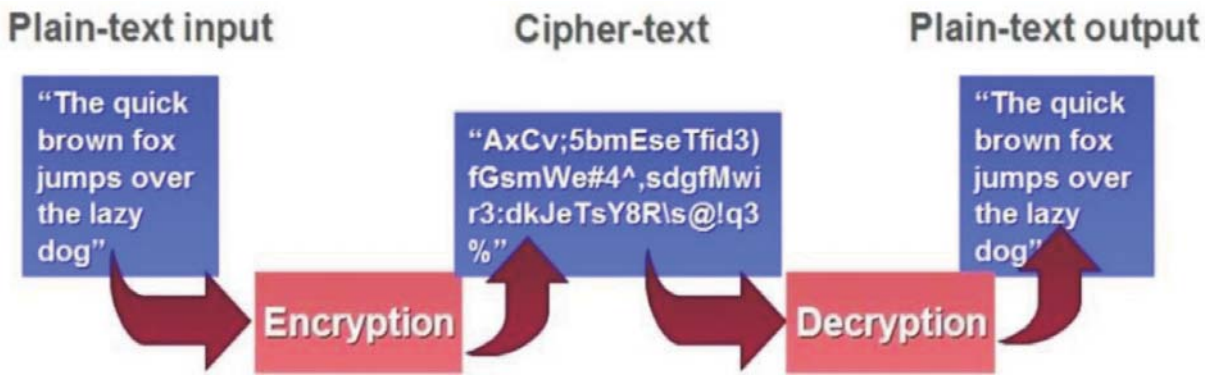

Figure 1

Here we are showing how the encryption works. First, we are getting input as simple text message from the registered user. Then it is encrypted into ciphertext from the plain text message which is stored in the database. In our message processing project user can see the encrypted message also while sending the message and can also see decrypted message.

2.2. Message Sending Process

HTTP is the easiest process to send data from one application to another. Java has its own method calls for submitting HTTP requests. This means that HTTP is a very good choice to send SMS text messages to registered id. If we have to operate an SMS gateway in our system, for example the Oracle SMS Gateway, we can pass SMS messages to it using DO GET or DO POST method calls using servlet. We can use this mobile phone to send and receive your messages. It can also possible to send the messages through the Internet to an SMS service provider. Here in our message processing project users must register first for communicating each other. Because here user can send normal text message to the registered user only. After sending the message , the message is being encrypted and stored into data base and receiver when logs in he or she can get the received messages from the sender.

2.3. Message storing process

Storing messages at a very fast rate is much needed for an message processing application. After doing a lot of research I finally used for storing and retrieving messages in ORACEL tables. We don't need any kind of sorting and retrieving is very fast even if you have only one server with good configuration.

In this project I will be using oracle as my database management system. But this same design can be implemented using any SQL, No-SQL or any other kind of database management system.

Demo_message table: In this table we store all the messages between all users. The userid column has identifier appended with the message number between those two users. userid column is the primary key. Therefore it will have unique values and is indexed.

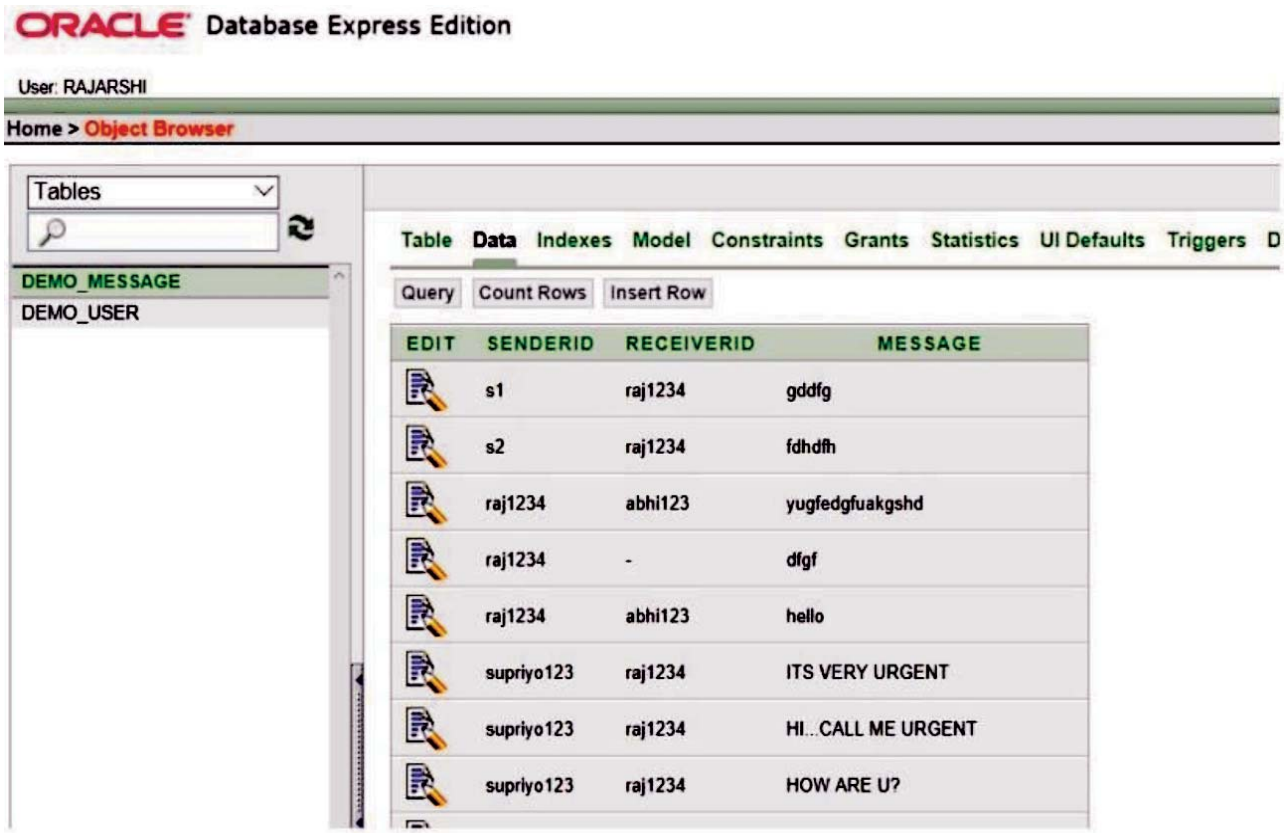

Figure 2

DEMO_USER : In this table, we are storing user's information, like user id, password, date of birth, pan no., Aadhar no. etc. The data is storing in database directly from the sign-up page when use is giving registering for the message processing process.

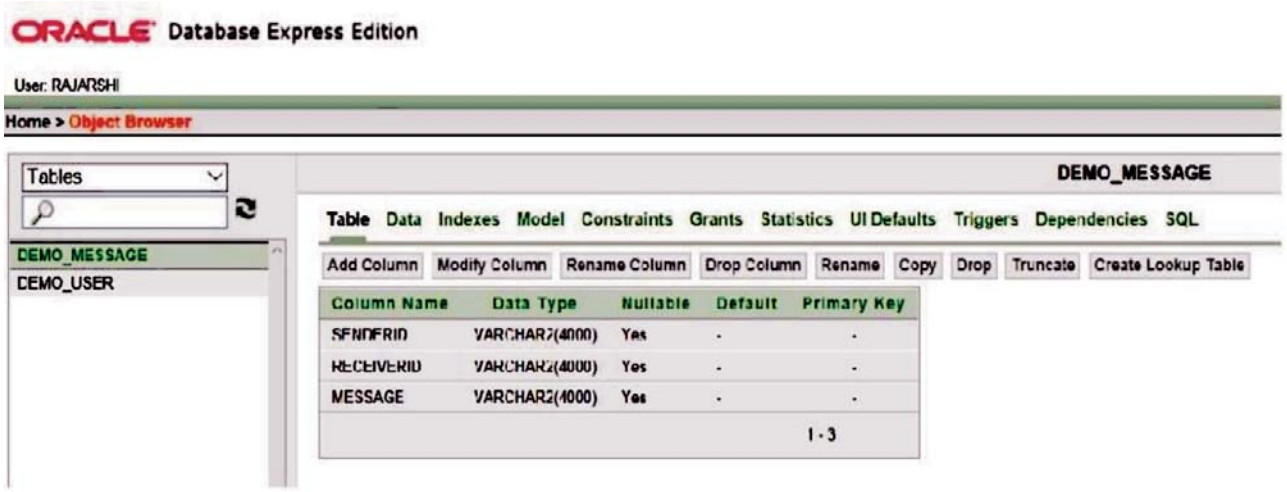

Figure 3

2.4. Message security

In any kind of messaging application, the most import issue is security. User may share their important details here. Hacker can easily hack their detail and make harm to the user. Normally in any kind of message processing schema, one time security checking is used. Here I tried two times security checking process. Here we are checking the password validation while login process and another one while opening the message we are asking randomly asking date of birth or pan no. or Aadhar no. so that any hacker if gets any user's id and password although the hacker can able open the user's important message. In this way I have tried my message processing schema to more secure.

2.5. Pros and cons of the existing system

This proposed system aims to fill this gap by providing an advanced level of file protection. RSA is known to be the strongest publicly available encryption method. This algorithm works with both private key and public key. The only way of decrypting the files which are encrypted with the public key is to use the private key. Users' file will be encrypted right before the upload process to the cloud Server. Only the encrypted file will be uploaded to the Server. Normally in a message processing schema there is no own security technique. They are using device security or other applications to secure the messages and the user's information. But in our message processing project user have to register 1^{st}, then he or she will get secure log in id and password. With the help of the id and password only they can get into the project. After that when user want to see the messages in inbox for each message the system will ask user to enter random attributes which is related to the logged in users, like pan no., Aadhar no., phone no., date of birth. Now comes to the important part of the project, we all know whenever we are sending messages to any one in any kind of message processing system we know the messages will be encrypted but we can't see the encrypted message. But here can see the encrypted message also while sending the message to other registered user, also they can see the decryption process also to get back the original message.

REFERENCES

[1] Fatima Zohra ENNAJI Abdelaziz EL FAZZIKl Mohamed SADGAL Computer Systems Engineering Laboratory (LISI) Faculty of Sciences - UCAM Marrakech, Morocco Social Intelligence Framework: Extracting and Analysing Opinions for Social CRM DjamalBENSLIALilVE Informatics Laboratory in Image and Information SystemsClaude Bernard University Lyon I, France

[2] "Twitter41. " [Online]. Available: http://twitter4j.orgi

[3] S. Asur and B. Huberman, "Predicting the future with social media," in Agent Technology (Tn-IAT), 2010 IEEE .. , 2010, pp. 492-499

[4] Y. M. Li, H. M. Chen, J. H. Liou, and L. F. Lin, "Creating social intelligence for product portfolio design," Decls. Support Syst., vol. 66, pp. 123-134,2014.

[5] Zhiheng Huang EECS DepartmentUniversity of Californiaat BerkeleyCA 94720-1776, USAzhiheng@cs.berkeley.edu, Marcus Thint Intelligent Systems Research Center British Telecom Group Chief Technology Officemarcus.2.thint@bt.comZengchang Qin EECS DepartmentUniversity of Californiaat BerkeleyCA 94720-1776, USAzqin@cs.berkeley.eduQuestion Classification using Head Words and their Hypernyms.

[6] Collins, M. 1999. Head-Driven Statistical Models for Natural Language Parsing. *PhD thesis*, University of Pennsylvania.

[7] Berger, A. L., V. J. D. Pietra, and S. A. D. Pietra. 1996. A Maximum Entropy Approach to Natural Language Processing. Computational Linguistics, 22(1):39–71.