International Journal Of Computer Science And Applications Vol. 1, No. 3, December 2008
ISSN 0974-1003

Implementation Of MD5 Integrity Checking Mechanism For m-Commerce Transactions

Ganesan R
Research Scholar in Computer Science & Applications
PSG College of Arts & Science
Coimbatore 641 014,INDIA
emailnesan@yahoo.co.in

Gobi M
Research Scholar in Computer Science & Applications
PSG College of Arts & Science
Coimbatore 641 014, INDIA
mgobimail@yahoo.com

Dr VS Janakiraman
Professor & Head
Department of Computer Science
PSG College of Arts & Science
Coimbatore 641 014, INDIA

ABSTRACT
As technology migrates from e-commerce to m-commerce the issue of maintaining integrity of transactions takes a pivotal role. To implement m-commerce applications, Sun Java Wireless Toolkit is generally adopted. This is a state-of-the-art toolbox for developing wireless applications that are based on J2ME's Connected Limited Device Configuration (CLDC) and Mobile Information Device Profile (MIDP), and designed to run on cell phones, mainstream personal digital assistants, and other small mobile devices. In J2EE environment, the md5 implementation is available to ensure integrity. However, md5 implementation is not available in J2ME environment. With majority of applications moving to m-commerce environment, it becomes pertinent to develop and implement a class in Sun Java Wireless Toolkit that can ensure integrity of transactions. In this paper, we describe message digest class for the same, and present the technical details. This message digest has been implemented and tested on a Sun Java Wireless Toolkit 2.5.1 emulator. Using the Sun Java Wireless Toolkit, it is also possible to generate .jar files which can be uploaded to mobile devices.This implementation, in our view, finds wide applications in all m-commerce transactions where integrity of data is of prime importance.

General Terms
Security

Keywords
J2EE, J2ME, Sun Java Wireless Toolkit, MD5 Class

1 INTRODUCTION
The increasing uses of commerce applications have necessitated the need for maintaining integrity of transactions. To maintain integrity, J2EE (Java 2 Enterprise Edition) provides a class called MessageDigest. Details on how this class can be used can be had from [1].

The Sun Java Wireless Toolkit which is based on J2ME's Connected Limited Device Configuration (CLDC) and Mobile Information Device Profile (MIDP), do not have a class that can maintain integrity of transactions. In this paper we provide details on how such a class can be designed, developed and implemented in a J2ME environment. The paper is organized as follows.

In section 2, we present details on hashing and message digest. In section 3, we describe how this class can be designed. The implementation details are presented in section 4. Section 5 demonstrates how this class could be used to ensure integrity in m-commerce transactions. We also describe how .jar files can be created from the Sun Java Wireless Toolkit.

2 HASHING AND MESSAGE DIGEST
A hash function takes a message of any length as input and produces a fixed length string as output, sometimes termed a message digest. [2]

The characteristics of a good hash function are:

Should avoid collisions.

Should try to spread keys evenly in the array.

Should be easy to compute.

The two most-commonly used hash functions are MD5 and SHA-1 [3].

2.1 Basics of MD5
MD5 (**Message-Digest algorithm 5**), is an Internet standard (RFC1321) [4] and is one of the widely used cryptographic hash function with a 128-bit message digest. This has been employed in a wide variety of security applications.

The main MD5 algorithm operates on a 128-bit, divided into four 32-bit words. These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function, modular addition, and left rotation.

In this work, we have attempted to implement MD5 algorithm in Sun Java Wireless Toolkit. Since there is no in-built class for message-digest computation, we designed and implemented a class MD5 for the same.

ISSN 0974-1003

3 DESIGN OF MD5 CLASS IN MOBILES

The MD5Pack package which we designed and implemented in the Sun Java Wireless Toolkit contains the core message digest class called MD5cls class, which implements the functionality of MD5 algorithm. The MD5cls constructor accepts a string of any length and converts it into fixed length 128 bit message digest.

The main methods used in this class are initiate(), update(), final() and asHex(). The message digest result is the string type which contains the hexa-decimal value.

The following are the sequence of statements used to generate the message digest for the given string.

```
m.Init();                  //Init method is used to perform
                             initialization process.
m.Update(String);          //update method is used to
                             concatenate and update the
                             string which is passed.
m.asHex();                 // asHex method is used to return
                             the message digest as hexa-
                             decimalvalue; 'm' is the
                             MD5cls object.
```

This MD5cls class object is created and accessed from the MD5Demo class which extends the MIDlet class. This MD5Demo class is used to design the interface on mobile and is used to pass the string to main message digest class.

4 IMPLEMENTATION DETAILS

The Message Digest class that was developed, was implemented using Sun Java Wireless Toolkit 2.5.1 on Intel Pentium III Celeron Processor @ 933 MHz speed with 256 MB RAM. The details of the Sun Java Wireless Toolkit 2.5.1 can be had from [5] and the toolkit can be downloaded from [6].

5 DEMONSTRATION OF MD5 CLASS

Figures 1 to 7 demonstrates the implementation of message digest class.

5.1 .jar file creation

The Java™ Archive (JAR) file format enables one to bundle multiple files into a single archive file. Typically a JAR file contains various class files and auxiliary resources associated with the application. Details on what a Java Archive file is can be had from [7]. Sun Java Wireless Toolkit, provides necessary menus (project→ package → create package) for creation of .jar file and this .jar file can be transferred and executed in any mobile that supports Java.

6 CONCLUSION

In this paper, we have presented a method for designing and implementing MD5 algorithm in mobiles. The MD5 algorithm has been tested in the Sun Java Wireless Toolkit.
This implementation, in our view, finds wide applications in all m-commerce transactions where integrity of data is of prime importance.

ACKNOWLEDGEMENTS

The authors would like to place on record the constant support and encouragement the management of *PSG College of Arts & Science* is providing in carrying out this research work.

7 REFERENCES

[1] http://java.sun.com/j2se/1.4.2/docs/api/java/security/MessageDigest.html.

[2] Ilya Mironov , Hash functions: Theory, attacks, and applications, Microsoft Research, Silicon Valley Campus, November 14, 2005

[3] Federal Information Processing Standards Publication 180-2, Secure Hash Standard, 2002 August 1, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[4] http://www.scit.wlv.ac.uk/rfc/rfc13xx/RFC1321.html

[5] http://java.sun.com/javame/reference/apis.jsp

[6] http://java.sun.com/products/sjwtoolkit/download-2_5_1.html.

[7] http://java.sun.com/docs/books/tutorial/deployment/jar/

ISSN 0974-1003

Figure 1: Initial Screen

Figure 2: Sender Screen

Figure 3: MD generated by the sender

Figure 4: Receiver Screen

Figure 5: MD re-generated by the receiver

Figure 6: Integrity Check Passed

Figure 7: Integrity Check Failed