International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

"Algebraic Coding Techniques to the Aid of Information Security in Achieving Reliable Internet Banking"

Shefali Kapoor[1], Dr. G.V.Ramaraju[2]

[1] Research Scholar, Department of Mathematics, Lingaya's University, Faridabad, 121002,(India)

[2]Pro Vice Chancellor (R&D), Lingaya's University, Faridabad,121002, (India)

ABSTRACT

For banks, Reliable information is critical and hence Information Security is a vital area of concern. The objective of this paper is to demonstrate the application of "Algebraic Coding Techniques" in aiding & StrengtheningInformation Security in achieving Reliable Internet Banking.

For this, first we study the processes& measures as prescribed by the RBI in its guidelines in respect of Information Security related to Internet Banking, ascertain whether there are any gaps in Information Security and then proceed

to discuss the various Algebraic Coding techniques which can be deployed to aid &strengthen the Information Security for achieving Reliable Internet Banking.

Keywords : Information Security, Internet Banking, Spyware, Malware, Two Factor Authentication, Session time-out, Second Channel Notification, Error Coding, Simple Parity Check, Two Dimensional Parity Check, checksum, Cyclic Redundancy check, Hamming Codes.

I. INTRODUCTION

Reliable information is at the heart of risk management processes in a bank. Inadequate data quality is likely to induce errors in decision making. Data quality requires building processes,procedures and disciplines for managing information and ensuring its integrity, accuracy, completeness and timeliness. The fundamental attributes supporting data quality should include accuracy, reliability for information security.

1 INFORMATION SECURITY: AUTHENTICATION PRACTICES AND OTHER SECURITY MEASURES FOR INTERNET BANKING

RBI Guidelines[1]specifically lay down that banks should implement two-factor authentication for fund transfers through internet banking, to counter check cyber attacks and their potential consequences. Properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents and are more difficult to compromise.

The principal objectives of two-factor authentication are:

(i) To protect the confidentiality of customer account data and transaction details.

(ii) To enhance confidence in internet banking by combating various cyber attack mechanisms like Phishing, keylogging, spyware/malware and other internet based frauds targeted at banks and their customers.

Further, RBI Guidelines also prescribe that for carrying out critical transactions like fund transfers, the banks, at the least, need to implement two-factorAuthentication:

(i) First Factor : through user id/password combination and

(ii) Second factor: through a digital signature or OTP/dynamic access code through various modes like SMS over mobile phones.

RBI Guidelines also require that to enhance online processing security, confirmatory second channel procedures (like telephony, SMS, email etc) should be applied in respect of transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits.

Second channel notification / confirmation: The bank should notify the customer, through a second channel, of all payment or fund transfer transactions above a specified value determined by the customer.

Session time-out: An online session should be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.

II. GAPS IN CYBER SECURITY: RBI ASSESSMENT REVEALS GAPS IN CYBER SECURITY OF INDIAN BANKS

According to the RBI [2],the assessment of gaps in bank's cyber security preparedness reveals that barring a few banks the gaps are significant, more so in respect of public sector banks. This warrants immediate and continued attention of the boards and senior management of banks, said Deputy Governor SS Mundra, at a recent seminar on 'Financial Crimes Management' organized by CAFRAL (Centre for Advanced Financial Research and Learning).

In this regards, the Deputy Governor emphasised that it is important that the CISO (Chief Information Security Officer) is sufficiently senior in hierarchy; understands technology well; appreciates the security aspects of all the technologies adopted by the bank; is responsive; and is sufficiently enabled to stall launch of unsecured products, whenever necessary.

The Deputy Governor noted that the scare that was created during a recent ATM/Debit card incident where Information Security was breached clearly indicates that cyber security requires top attention by the boards.

III. INDIA'S LARGEST BANKING SECURITY BREACH

In October 2016, India's Largest Banking Security Breach was reported in which security of 3.2 million cards was compromised resulting in fraudulent withdrawal of Rs.1.3 Crore. [3]

The enormity of the security breach led to PM Office intervention.

Hitachi Payment Services admitted its systems were breached, based on a report by security audit from SISA Information Security, which determined that the breach happened between May 21,2016 and July 11, 2016. [4]

The Payments security specialist firm SISA, in its final audit report on the compromise of 3.2 million debit cards during October last year, has confirmed that the breach happened in Hitachi ATM payment network. The report also confirmed that the security breach remained undetected during the aforesaid compromised period. [5]

IV. MODUS OPERANDI OF HACKERS OF HITACHI SYSTEM

The hackers created a "dummy code book" within the Hitachi system – capturing all possible four digit numbers from 0000 to 9999, to steal the PIN's (Personal Identification Numbers) of customers as and when they used their cards to withdraw money from ATM's of a private bank in India. [6]

In view of above, it is apparent that the Information Security of Indian Banks needs to be strengthened for achieving Reliable Internet Banking with particular focus on detection of errors & their correction so that the losses arising therefrom are prevented and minimized.

We observe that there are various techniques of "Mathematical Algebraic Coding" focussed on Error Detection & Correctionwhich can be put to use to Strengthen Information Security in Internet Banking, which we now discuss in the ensuing paras.

V. TECHNIQUES OF ALGEBRAIC CODING FOCUSSED ON ERROR DETECTION & CORRECTION FOR STRENGTHENING INFORMATION SECURITY IN INTERNET BANKING

In Internet Banking, the message signal to be transmitted is in digital form. To strengthen Information Security in Internet Banking, there is a need for not only detecting the errors but also have a suitable mechanism that can correct the errors detected. The overall purpose of a digital communication system is to transmit the message or sequences of symbols coming out of a source to a destination point at as high a rate and accuracy as possible. Source and the destination point are physically separated in space and a communication channel connects the source to the destination point.

Now We demonstrate how the techniques of "Mathematical Algebraic Coding" for detecting and correcting errors, are applied for ensuring that information transferred is error free & reliable thereby aiding & strengthening the Information Security of the Indian Banking Sector.

VI. STRATEGIES OF ALGEBRAIC CODING FOR DEALING WITH ERRORS

These are two basic strategies for dealing with errors.

One way is to include enough redundant information (extra bits are introduced into the data stream at the transmitter on a regular and logical basis) along with each block of data sent to enable the receiver to deduce what the transmitted character must have been.

The other way is to include only enough redundancy to allow the receiver to deduce that error has occurred but not which error has occurred and receiver asks for a retransmission.

The former strategy uses Error – Correcting code and latter uses Error – Detecting code.

VII. HOW ERRORS ARE RECOGNISED& CORRECTED

Even if we know what type of errors can occurs, we can't simply recognize them without analysis.

We can do this simply by comparing this copy received with another copy of intended transmission. In this mechanism the source data block is sent twice.

The receiver compares them with the help of a comparator and if those two blocks differ, a request for re-transmission is made. To achieve forward error correction, these sets of the same data block are sent and majority decision selects the correct block.

VIII. ERROR CODING

Error coding uses mathematical formulas to encode data bits at the source into longer bit words for transmission. The "Code word" can then be decoded at the destination to retrieve the information. The extra bits in the code word provide redundancy that, according to the coding scheme, used will allow the destination to use the decoding process to determine if the communication medium introduced errors and in some cases correct them so that the data need not be retransmitted. [7]

Faster processors and better communications technology make more complex coding schemes, with better error detecting and correcting capabilities, possible for smaller embedded systems, allowing for more robust communications. However, trade-offs between bandwidth and coding overhead coding complexity and allowable coding delay between transmissions must be considered for each application.

XI. TECHNIQUES OF ALGEBRAIC CODING FOR ERROR DETECTION

Basic approach used for error detection is the use of redundancy, where additional bits are added to facilitate detection and correction of error. Techniques of error detecting are as follows:

(i) One Dimensional Parity Check orSimple Parity Check

(ii) Two Dimensional Parity Check

(iii) Checksum

(iv) Cyclic Redundancy Check

9.1 One Dimensional Parity Check or Simple Parity Check

The most common and least expensive mechanism for error-detection is the simple parity check. In this technique, a redundant bit called parity bit, is appended to every data unit so that the number of in the unit (including the parity becomes even).

Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of 1 is added to the block if it contains an odd number of 1'ss is (on bits) and 0 is added if it contains an even number of 1's. At the receiving end the parity bit is computed from the received data bits and company with the received parity bit. This scheme makes the total number of 1's even, that is why it is called even parity checking.

It is also possible to use odd parity checking, where the number of 1's should be odd. [8]

9.2 Two Dimensional Parity Check

Performance can be improved by using two - dimensional parity check, which organizes the block of bits in the form of a table. Parity check bits are calculated for each row, which is equivalent to a simple parity check bit.

Parity check bits are also calculated for all columns then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.

Two Dimension parity checking increases the likelihood of detecting burst errors. 2-D parity check of n bits can detect a burst error of n bits. A burst error of more than n bits is also detected by 2-D Parity check with a high probability.

9.3 Checksum

In checksum error detection scheme, the data is decided into 'k segments' each of 'm bits'. In the sender's end, the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.

The checksum segment is sent along with the data segments. At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum complemented. If the result is zero, the receiveddata is accepted, otherwise discarded.The checksum detects all errors involving an odd number of bits. It also detects most errors involving even number of bits. [9]

9.4 Cyclic Redundancy Checks (CRC)

This cyclic Redundancy check is the most powerful and easy to implement technique. Unlike checksum scheme, which is based on addition, CRC is based on binary division. In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number. At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted. A remainder indicates that the data unit has been damaged in transit and therefore must be rejected. The generalized technique can be explained as follows.

If a k bit message is to be transmitted, the transmitter generates an r-bit sequence, known as Frame Check Sequence (FCS) so that the (k + r) bits are actually being transmitted. Now this r-bit FCS is generated by dividing the original number, appended by r zeros, by a predetermined number. This numbers, which is (r + 1) bit in length, can also be considered as the coefficients of a polynomial, called Generator Polynomial. The remainder of this division process generates the r-bit FCS. On receiving the packet, the receiver divides the (k + r) bit frame by the same predetermined number and if it produces no remainder, it can be assumed that no error has occured during the transmission. [10, 11]

The transmitter can generate the CRC by using a feedback shift register circuit. The same circuit can also be used at the receiving end to check whether any error has occurred. All the values can be expressed as polynomial of a dummy variable X. For example, for P = 11001 the corresponding polynomial is $X^4 + X^3 + 1$.

A polynomial is selected to have at least the following properties:

(i) It should not be divisible by X.

(ii) It should not be divisible by (X+1)

The first condition guarantees that all burst errors of a length equal to the degree of polynomial are detected.

The second condition guarantees that all burst errors affecting an odd number of bits are detected.

C RC process can be expressed as:

$X^n M(X) / P(X) = Q(X) + R(X) / P(X)$

Commonly used divisor polynomials are:

(i) CRC – 16 = $X^{16} + X^{15} + X^2 + 1$

(ii) CRC – CCITT= $X^{16} + X^{12} + X^5 + 1$

(iii) CRC - 32 = $X^{32} + X^{26} + X^{23} + 1\ X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + 1$

CRC is a very effective error detection technique. If the divisor is chosen according to the previously mentioned rules, its performance can be summarized as follows.

(i) CRC can detect all single – bit errors

(ii) CRC on detect all double – bit errors

(iii) CRC can detect all burst errors of less than the degree of the polynomial.

(iv) CRC detect most of the larger burst errors with a high probability.

X. TECHNIQUES OF ALGEBRAIC CODING FOR ERROR CORRECTION:

UNDERSTANDING ERROR CORRECTION

Concept of error – correction can be easily understood by examining the simplest case of single - bit errors. As we have already seen that a single-bit error can be detected by addition of a parity bit (VRC) with the data which needed to be sent. A single additional bit can detect error, but it is not sufficient enough to correct that error too.

In theory it is possible to correct any number of errors atomically. Errors correcting code are more sophisticated than error detecting code and require more redundant bits. The number of bits required to correct multiple bit or burst error is so high that in most of the cases it is inefficient to do so. For this reason, most error correction is limited to one, two or at the most three bit errors.

For correcting an error one has to know the exact position of error, i.e. exactly which bit is in error (to locate the invalid bits). For example to correct a single bit error in an ASCII character, the error correction must determine which one of the seven bit is in error. To this, we have to add some additional redundant bits. [12]

To calculate the numbers of redundant bits (r) required to correct ‘d’ data bits, let us find out the relationship between the two , so we have (d + r) as the total number of bets, which are to be transmitted, then r must be able to indicate at least (d+ r +1) different values. Of these, one value means error and remaining (d+ r) values indicates error location of error in each of (d+ r) locations. So, (d+ r+1) states must be distinguishable by r bits and r bits can indicates 2^r states. Hence, 2^r must be greater than (d+ r +1).

i.e. $2^r \geq d+ r + 1$

The value of r must be determined by putting in the value of d in the relation. For example, if d is 7, then the smallest value of r that satisfies the above relation is 4. So the total bits, which are to be transmitted is 11 bits (d+ r = 7+4 =11).

XI. USE OF "HAMMING CODE" TECHNIQUE OF ALGEBRAIC CODING FOR ERROR CORRECTION

We can manipulate the bits to discover which bit is in error. A technique developed by R.W. Hamming provides or practical solution. The solution or coding scheme he developed is commonly known as Hamming Code. Hamming Code can be applied to data units of any length and used the relationship between the data bits and redundant bits and redundant bits as discussed.

11.1 How Hamming Code is used for Error Correction

Methodology for error detection by using Hamming Code is as follows:

(i) To each group of m information bits k parity are added to form (m+k) bit code as shown in figure given above.

(ii) Location of each of the (m+k) digits is assigned a decimal value.

(iii) The k parity bits are placed in positions 1,2,…….2^{k-1} positions . k parity checks are performed on selected digits of each code word.

(iv) At the receiving end the parity bits are recalculated. The decimal value of the k parity bits provides the bit-position in error, if any.

XII. CONCLUSION

Thus we can conclude that though in recent times the use of Internet Banking in the Indian Banking Sector has gathered momentum with number of transactions through Internet Banking increasing multi fold times both in Public Sector & Private Sector Banks, the Information Security remains an area of concern which needs to be strengthened to ensure Reliability of Internet Banking.

We have also demonstrated how the various Techniques of Algebraic Coding for Error Detection and Correction can be deployed for strengthening Information Security for achieving Reliable Internet Banking in the Indian Banking Sector.

REFERENCES

[1] Guidelines of the Reserve Bank of India on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, June 2, 2016.

[2] Business Line Bureau, "Big Gaps in cyber security preparedness in banks", pp. 10, february 3, 2017

[3] Business Standard, LeLeAbhijit, AnandNupur, DhasmanaIndivjal, "PMO Lens on Debit Card Security Breach Probe" , pp. 3, October 22, 2016.

[4] Business Standard, RoyAnup, "Breach in our system led to card fraud: Hitachi" , pp.4, february 10, 2017.

[5] The Economic Times, Bhakta Pratik, "Virus that infected Debit Cards was on Hitachi Network", pp. 13, february 10, 2017.

[6] The Economic Times, GhoshSugata, "Hitachi Hackers cashed in on security gaps", pp. 1, february 23, 2017.

[7] Sharma K.K., "Elements of Data Communication", Katson Books, 2011.

[8] HaykinsSimon , "Digital Communications" , Mc Master University, Wiley 2012.

[9] Sharma Sanjay, "Digital Communicatons", Katson Books, 2015.

[10] Haykins Simons, "Communication Systems" Mc Master University, Wiley 2012

[11] VermaBrijesh , "Digital and Analog Communications", Nokia Siemens Networks India, 2012.

[12] Sharma K.K , "Digital &Analog Communication" , Katson Books, 2012.