2019 International Conference on Mechatronics, Robotics and Systems Engineering (MoRSE)
4-6 December 2019, Bali, Indonesia

Security System ATM Machine with One-Time Passcode on M-Banking Application

Rendy Munadi
Electrical Enginering Faculty
Telkom University
Bandung, Indonesia
rendymunadi@telkomuniversity.ac.id

Arif Indra Irawan
Electrical Enginering Faculty
Telkom University
Bandung, Indonesia
arifirawan@telkomuniversity.ac.id

Yuman Fariz Romiadi
Electrical Enginering Faculty
Telkom University
Bandung, Indonesia
yumanfariz@gmail.com

***Abstract*— Automated Teller Machine (ATM) security system currently still uses magnetic cards and static PIN as its security system, which create many security holes. This security hole in many cases caused many bank customers to lose money mysteriously. In this paper a two-factor authentication system which uses ATM card and dynamic PIN is proposed to overcome this security hole. In this paper, a prototype of an ATM and m-banking application were built. The ATM prototype uses several components such as the Raspberry Pi 3B, smart card, smart card reader / writer, keypad number and LCD monitor. Dynamic PINs are generated using the CSPRNG-SHA1-MWC random number generator. In developing the prototypes, the framework used in this study is based on mobile applications and cloud computing. To evaluate the quality of the prototype, we performed qualitative and quantitative tests. Qualitatively we tested the prototype using a questionnaire using 165 sample respondents to provide an opinion about the safety and comfort of our prototype and quantitatively we measured the prototype to find out the level of randomness of the generated PIN and the QoS of the designed prototype.**

Keywords—ATM Security, Dynamic PIN, Management Security, Cyber Security

I. INTRODUCTION

According to *Lembaga Penjamin Simpanan* (LPS) in Indonesia, the use of saving services has increased every year which in July 2018 reached 262.058.775 accounts [1]. The increase in the number of accounts contributed to the level of use of ATM which is used to carry out savings and loans provided by banks. With such a large number of ATMs spread throughout Indonesia, banks are required to be able to serve the needs of customers for 24 hours by providing access to ATMs in various regions in Indonesia and can guarantee the security of customer transaction processes.

In Indonesia, especially in remote areas, ATMs are often without supervision. ATMs in remote areas are usually only secured by several CCTV. As a result, lately there are 33 customers who have lost more than 140 million rupiah. The alleged crime committed by the perpetrators is done by taking the victim's data by recording data that is on the magnetic tape located behind the ATM card or what we call skimming [2].

There is a lot of research discussing the improvement of security systems on ATMs, some of which have been the basis of the development of this research. As done by [3] fingerprint verification is purposed. This security system utilizes a proven fingerprint that has been unique, accurate, safe, easy, and convenient to use as identification when compared with other biometric systems this security system is much more efficient. Similar research was also carried out by [4] who used fingerprints on the thumb to authenticate the ATM.

However, the use of biometrics for ATM authentication cannot yet be carried out in Indonesia because biometric verification is not mandatory requirement for registration process. To be able to implement this, it is necessary to have a biometric data collection of all customers so that it requires a lot of cost and time. We introduced a system that can be used to strengthen a bank's security system without using biometric authentication. Our security system using an encrypted smart card as an access card and dynamic PIN in the form of One-Time Passcode (OTP). This OTP PIN can only be used once in the PIN authentication process

II. RELATED WORK

Security at ATMs has an important role in preventing attacks on bank customers, many researchers have conducted research on ATM security methods including those conducted by [5] wherein the applicant authenticates an ATM using one's face and body condition. This system was formed in addition to being used as an additional feature for customers who do not carry ATM cards. A security method using biometrics is also carried out by [6] where a biometric authentication system is proposed with the addition of an SMS-based OTP to secure one or more bank accounts owned by the customer.

ATM security methods do not always use biometrics only, as proposed by [7] where a two-steps verification is proposed, namely using an ATM card and ID number from a smart phone. Other research was also carried out by [8] where the authentication at the ATM was carried out using a unique PIN between banks and One Time Password (OTP).

Another system proposed in [9] where the detection of an attack is carried out by monitoring the bank customers' habits by using several input parameters such as ATM location, time of withdrawal, amount of money taken and the order of withdrawal. Research detecting money theft in the ATM by using customs is also done by [10] who uses static data from the process of making money carried out by bank customers.

III. SYSTEM DESIGN

This prototype system was created to increase security for customers when making transactions at ATMs. The type of PIN used is OTP, when every transaction PIN will always change and be sent via the mobile Banking. The OTP uses the random number generator (RNG) algorithm as the PIN that will be used. The internet functions as a communication medium that connects prototypes with end users. In addition, this system uses Amazon Web Services (AWS) services as the

978-1-7281-3984-5/19/$31.00 ©2019 IEEE

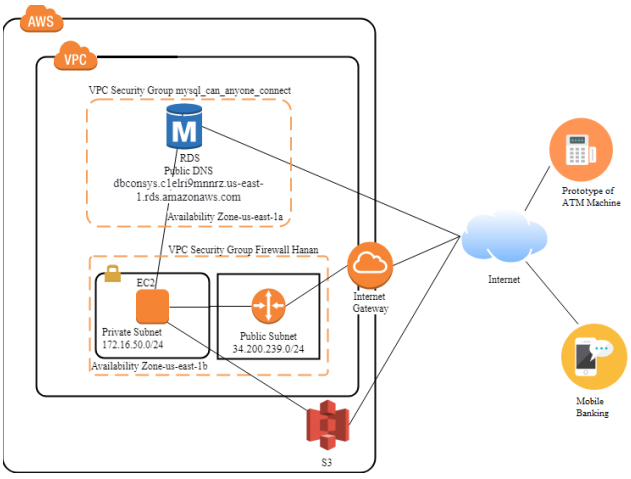

Fig. 1. The topology of system.

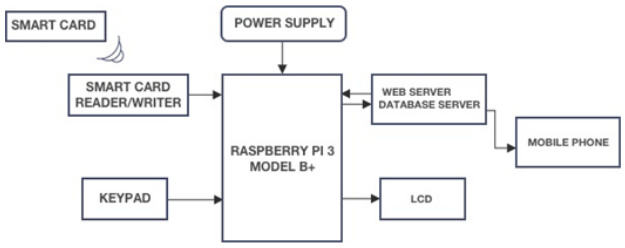

Fig. 2. Block diagram system.

database server and web server. As shown in Fig. 1, the prototype has three main parts: an ATM prototype used for the authentication process between smart cards and dynamic PIN, mobile application is used to receive dynamic PIN and AWS which acts as a backend server.

The transaction process using this prototype starts from the customer inserting a smart card as access to the ATM machine prototype. ATR ID data on the smart card will be read by an ATM prototype with a smart card reader / writer device, ATR ID data will be authenticated with customer data on the database server, the role of the database server here as a medium for storing customer data in real-time and online. The next stage is authentication based on dynamic PIN or we call One Time Passcode (OTP) PIN [11]. If the customer can go through both stages of the authentication, the customer can proceed with the transaction.

After the transaction process is complete, the OTP PIN will be generated again using the CSPRNG-SHA1-MWC algorithm. The OTP PIN that has been generated will be stored on the database server according to the account number of the customer who made the transaction process. The server will send information regarding the OTP PIN and customer balance. The customer will receive the OTP PIN information through the M-Banking prototype application, the OTP PIN received by the customer can be used for the next transaction process. Customers can also receive balance information by electronic mail or commonly known as email. Block diagram prototype system Fig. 2

A. ATM Machine Prototype System.

The ATM machine prototype will use OTP authentication sent via mobile banking. The cards used are smart cards that have encryption superior to magnetic cards, and customer data will be monitored on the database server. This smart card uses ATR as the customer's UID. This prototype makes a PIN that was initially static to be dynamic because customers will get a different PIN for each transaction. The prototype ATM machine uses Raspberry Pi 3 Model B as a data processor and will be integrated with the keypad number as OTP input into the system, smart card reader / writer to read smart card, Amazon Web Services as a web server and database server and LCD server with features touchscreen to display the main application.

Fig. 3 illustrates a block diagram of ATM machine, where the main processing component uses Raspberry Pi 3 model B+ which provide GUI interface that is used to make transactions. In main processing there are other features such as the random number generator system, customer authentication, and banking transaction which can be described as the use case in Fig. 4. The ATM machine use case consists of three actors namely admin, bank and ATM machines. Each actor describes the activity of the system. The customer actor can make transactions at ATM machines such as withdrawing money and checking customer balances. In addition, the rights possessed by the customer actor only obtain an OTP to authenticate the ATM machine. At the bank actors do the logging of all customers' activities. In the system also a blocking of the customer's account will occur if the customer has failed to enter the OTP 3 times a trial

B. Generating OTP PIN

In general, the authentication process at an ATM uses a PIN determined by the customer. In this study, a dynamic customer PIN is applied. Where the PIN will always change in every transaction process that is disposable or OTP. To generate OTP PIN using the application of Cryptographically

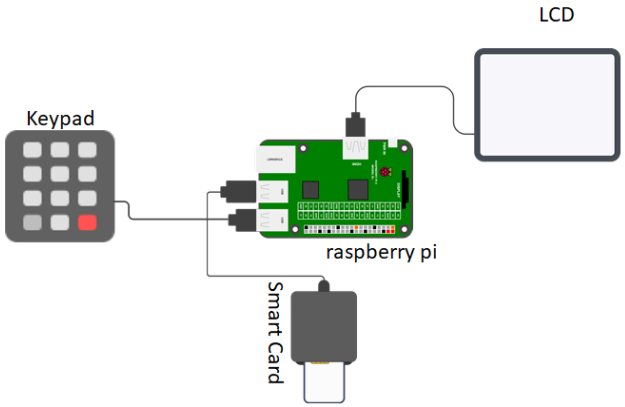

Fig. 3. Design prototype of atm machine.

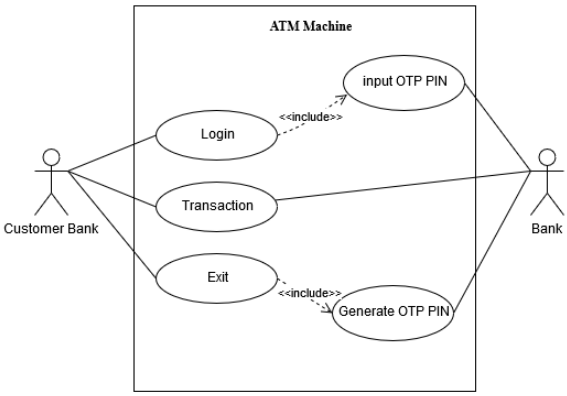

Fig. 4. Use case prototype of atm machine.

Secure Pseudorandom Number Generator (CSPRNG) SHA1 the MWC mathematical algorithm approach to the Java programming language. firstly, the generation of random numbers using the SHA1 cryptographic algorithm with seed values based on current time. CSPRNG SHA1 will generate random numbers in small and large periods without being able to be guessed before, the next step is to add the MWC mathematical algorithm challenge approach which is valid for generating final random numbers with the algorithm equation shown in (1) and (2) [12] [13].

$$x(n) = (ax_{n-r} + c_{n-r}) mod\ b \quad (1)$$

$$c(n) = \left[\frac{ax_{n-r}+c_{n-1}}{b}\right] \quad (2)$$

where a is as a multiplier, b is the base, c is the carrier, r is the initial value of the seed, x_0 is the system input c_0 is the a system input and $x_0, x_1, x_2, \ldots, x_n$, is a sequence of random numbers. The value of a is used as a multiplier of $x(n-r)$ the value of c as a carry has been raised in CSPRNG, and r is the initial number of seeds raised based on the current time. In addition, there are several looping functions and conditions intended to provide the generation of 6 digits random numbers that are positive. The random number generated will be used as the customer's OTP PIN for authentication to enter the ATM prototype. The PIN authentication step on the ATM prototype is a single authentication, meaning that the PIN for which the customer's PIN will be used 1 time in 1 transaction process. Customers can do the next transaction using a PIN that has been generated from the end of the previous transaction session, the PIN will change when it encounters the final stage of each transaction process on ATM prototype.

C. Backend System

Backend prototype system built using AWS cloud services. Web Server is made with the Ubuntu operating system 16.04 LTS which is in Amazon EC2. The web server runs using Hypertext Transfer Protocol (HTTP) with port number 80 on the TCP protocol. This web server will later become an end user so customers can get an OTP to login. The operating system specifications provided by Amazon EC2.

Database Server uses Amazon RDS which is one of the services at Amazon Web Services. The database server used is MySQL because it is a relational database on open source and most popular. On the database server using MySQL version 5.7.22. Amazon RDS will generate endpoints whose purpose is the connection between the application and the MySQL database. There is an Amazon VPC that functions as connectivity between Amazon EC2 and Amazon RDS. With the subnet group feature, one can assigns an IP address to the service to be used. The goal is to achieve one network so it is easy for connectivity. In addition to managing subnet groups, Amazon VPC needs to set up security groups that aim to filter protocols and access to the services that will be used. Then there an Amazon S3 service that functions as an intermediary to deploy data to the Amazon EC2 server.

IV. Result And Analysis

Tests in this study are based on testing parameters in order to improve security on the system created. Tests carried out are divided into three categories such as questionnaire, QoS System and performance of random number generator. The purpose of this test is to provide security to customers when transacting on ATMs, where skimming and PIN capturing techniques often occur by the attacker.

A. Questionnaire Analysis

This test is intended to test the validity and reliability of the respondents we surveyed. The range for filling the questionnaire is one week. From the results obtained by respondents will be known whether the prototype system that is made can be developed or not. In the average questionnaire are students with 79 respondents, 59 civil servants/private employees, 5 entrepreneurs and 22 others.

TABLE I. Questionnaire Assessment

Question	Score			
	1	*2*	*3*	*4*
1	0	0	24	137
2	3	3	76	80
3	5	24	73	60
4	2	9	73	78
5	2	9	6	84
6	3	14	63	82
7	7	23	72	60
8	2	17	71	72
9	3	12	75	72
10	5	16	71	70
1	0	0	24	137
Average	**3,2**	**12,7**	**66,5**	**79,5**

From Table I the results of a questionnaire recapitulation of 165 respondents have been given. The respondent is given 10 statements that have 4 answer options. The answers will be categorized based on the following values:

(i) Strongly disagree.
(ii) Disagree.
(iii) Agree.
(iv) Strongly Agree.

The following summary components of statements that have been presented previously to 165 respondents:

a) I agree that cybercrime is very dangerous and detrimental to many parties.
b) I agree that One-Time Passcode is an effort to prevent cybercrime, especially skimming.
c) The PIN changes periodically in every login, making me feel safe when making transactions at an ATM.
d) I agree that the One-Time Passcode (OTP) uses 6 (six) effective digits for security on the ATM / debit system?
e) I agree that the ATM/Debit system uses OTP verification to ensure the integrity of user data
f) Using One-Time Passcode avoids the tendency to forget your PIN when making transactions at an ATM
g) I agree that the use of OTP in transactions does not reduce convenience
h) The use of SMS, Smartphone Applications and Browsers as a medium for sending OTP is very effective for me
i) I agree if the One-Time Passcode concept is applied for ATM / debit card security
j) I agree that using the internet to access OTP is not that difficult.

From the data results in Table I then the validity and hypothesis testing are conducted by referring to the test PLS. The results of the test PLS using SmartPLS are as follows.

- Validity Test

Respondent data were tested for their validity using the outer model evaluation method. This test is done by looking at the outer loading assessment component of each component. Outer loading value is obtained with the help of SmartPLS software using the Partial least squares (PLS) algorithm. This outer loading value has a minimum limit of 0.5 which is called the convergent validity minimum limit.

Table II shows the outer loading results of the testing process for each question given to respondents. It can be seen from the table that the answers of the respondents almost all the answers to the questions of the respondents are worth more than the convergent validity limit. This means that the answer of the respondent is a valid answer. The question that has a value that is less than the convergent validity limit is question number 1 which asks whether cybercrime is a dangerous activity that can be ignored.

TABLE II. OUTER LOADINGS

Cyber Crime	0,427	**Q1**
	0,961	**Q2**
Security	0,774	**Q3**
	0,756	**Q4**
	0,836	**Q5**
Ease	0,639	**Q6**
	0,771	**Q7**
	0,818	**Q8**
	0,855	**Q9**
	0,750	**Q10**

- Hypothesis Test

Hypothesis testing is done to get conclusions from hypotheses from a number of data in the questionnaire. Hypothesis testing is done by doing a bootstrapping test of data that has been obtained in the questionnaire question. The statistical T value on the path coefficient assessment is used as a reference to draw conclusions from the hypothesis statement. The T-statistic value needs to be greater than 1.94 for the hypothesized results to be accepted.

In Table III lists the processing of the questionnaire against 165 questionnaires stating that all statistical T values exceed the standard value determined so that it can be concluded that any given hypothesis can be accepted. These hypotheses include "the implementation of OTP security as an effort to prevent cybercrime", "the implementation of OTP security system to improve security" and "the implementation of the OTP security system does not reduce the sense of comfort".

TABLE III. PATH COEFFICIENT

Desc.	***Original Sample*(O)**	***Sample Mean*(M)**	***Standar Deviation*(STDEV)**	***T Statistics* |O/STDEV|**
Cyber Crime	0,685	0,684	0,049	13,839
Security	0,885	0,886	0,021	42,356
Ease	0,945	0,945	0,012	78,322

B. QoS Analysis

The stage of testing and analysis includes the performance of the system that has been made. System testing and analysis is done from the beginning of the user login based on the smart card UID to the user logout and the system generates OTP. QoS measurements were performed on three random number generation, namely math-random, PRNG and CSPRNG SHA1 MWC.

TABLE IV. QOS FOR EACH RANDOM NUMBER GENERATOR

Description	**Math Random**	**PRNG**	**CSPRNG SHA1 MWC**
Transmission Delay	16,433 ms	16,386 ms	16,48 ms
Throughput	309,620 bit/s	309,525 bit/s	307,767 bit/s
Packet Loss	0%	0%	0%

Table IV shows the QoS result of the system. The analysis will be conducted based on TIPHON standard. First, the three algorithms did not experience packet loss at all with a value of 0%, meaning that the transmission of data packets did not fail at all. Throughput on the three algorithms varies, where the Math Random algorithm has a value of 309,620 bit/s, PRNG has a value of 309,525 bit/s, and CSPRNG SHA1 MWC has a value of 307,767 bit/s. The value of transmission delay in the three algorithms is worth 16,433ms in Math Random, 16,386ms in PRNG, and 16.48ms in CSPRNG SHA1 MWC.

When seen differences in measurements occur in the values of throughput and transmission delay of each random number generation process with different algorithms. For CSPRNG SHA1 MWC algorithm slightly increased in the value of transmission delay, this can indeed occur because in its use has experienced 2 random number generation. But if you look at the TIPHON standard, these three algorithms are still included in the "very good" category for the QoS parameters. With this the three algorithms can be used properly based on the QoS testing parameters.

C. Randomnes Test

At this stage, testing the probability of a number appearing Testing the randomness of a random number generator will show the frequency of occurrence of a number of 999,999 attempts. This test is done with the Java programming language by comparing 3 methods of generating random numbers. The three algorithms mentioned are Math Random, PRNG, and CSPRNG SHA1 MWC. The three algorithms will be assessed based on testing the randomness of a random number generator to determine the best use of the algorithm. A good random number generator will give a balanced test value for the appearance of numbers from 0 to 9. From the results of tests that have been carried out all four methods can generate random numbers up to 999,999 times the experiment, the value of the appearance of changes in numbers that occur also varies with each use of each algorithm. The appearance of one very large number will increase the likelihood that random numbers will be guessed after that number. This is done by testing the randomness of a random number generator made by Elliote Rusty Harold [14].

The results of the test can be seen in Table V. If we compare the value of occurrence of numbers between 0 to 9, the value of the CSPRNG SHA1 MWC algorithm is much better because it does not show a tendency to any random number. The fluctuation probability value in CSPRNG SHA1 MWC is close to 10% of each occurrence number. This is in accordance with the rule of Test the randomness of a random number generator that the better the generation algorithm is the one with the same value or a slight dispute between each number of its appearance. According to Elliote Rusty Harold, a good algorithm is one that has a narrow minimum and maximum range. Where the CSPRNG SHA1 MWC range is

narrower than other algorithms, the CSPRNG range is between 9.97% - 10.03% of the 10 raised numbers

TABLE V. RANDOMNESS OF RANDOM NUMBER GENERATOR

0-9	Math Random		PRNG		CSPRNG SHA1 MWC	
0	100135	10,01%	99793	9,98%	100309	10,03%
1	99989	10,00%	99660	9,97%	99795	9.98%
2	100041	10,00%	99828	9,98%	100347	10,03%
3	99872	9,99%	100975	10,10%	99800	9.98%
4	99071	9,91%	100165	10,02%	100314	10,03%
5	100492	10,05%	100037	10,00%	99882	9,99%
6	99615	9,96%	99722	9,97%	99964	10,00%
7	100246	10,02%	99902	9,99%	99992	10,00%
8	100313	10,03%	99507	9,95%	99850	9,99%
9	100225	10,02%	100410	10,04%	99746	9,97%
Desc	999999	**100%**	999999	**100%**	999999	**100%**

V. CONCLUSION AND FUTURE WORK

Based on the tests that have been done include testing the questionnaire to get the response to the use of otp on the ATM machine, testing the strength of CSPRNG SHA1 MWC in generating pin randomness and QoS testing of the system. As obtained from the results of the questionnaire that the use of OTP can increase security and not reduce the comfort of using an ATM machine. The random generator test shows that the value of appearance on CSPRNG SHA1 MWX has the most perfect number that is 9.97% - 10.03%. In QoS testing the CSPRNG SHA 1 MWC random generator has a good QoS value that has a transmission delay of 16.48ms, throughput of 307,767 bps and 0% packet loss which according to ITU is included in the "very good. Category

We are aware in making this prototype still has shortcomings both in terms of testing and in terms of equipment. In random randomness testing, we don't really talk about randomness statistics and only use 3 random generator algorithms. To develop this prototype an improved random number randomization algorithm will be sought using better statistical analysis

REFERENCES

[1] L. P. Simpanan, "Distribusi Simpanan Bank Umum Periode Juli 2018," Group Penanganan Premi Penjaminan, Juli 2018. [Online]. Available: http://lps.go.id/documents/604798/1348560/Distribusi+Simpanan+Bank+Umum+periode+Juli+2018.pdf/32b190e9-85ee-458b-8f79-4687962876cc. [Accessed 22 September 2018].

[2] A. Zaenudin, "Tirto.id," 19 Maret 2018. [Online]. Available: https://46879tirto.id/skimming-jurus-usang-yang-ampuh-bobol-uang-nasabah-bri- cGmb. [Accessed 22 September 2018]

[3] Y. M. Rihi, A. J. Santoso and I. Wisnubadhra, "Design of security system for ATM using fingerprint security verification," in National Seminar on Informatics, vol. E, pp. 31, 2013.

[4] I. G. Babatunde, A. O. Charles, M. J. Lange, and D. J. Olumuyiwa, "Experimental study of thumbprint-based authentication framewrok for ATM machines", in Proc. Int. Conf. Sci. Inf., pp 505-514, 2014.

[5] E. Derman, Y. K. Gecici, and A. A. Salah, "Short term face recognition for automatic teller machine (ATM) user", in Proc. Int. Conf. Electron. Comput. Comput. (ICECCO), pp. 111-114, 2013.

[6] F. Kouser, Nagaratna, V.R. Pavithra, B. Sree, and R. Kiran, "High secure multiple account bank affinity card a successor for ATM card," in Proc. Int. Conf. Des. Innov. Comput. Comun. Control (ICDI3C), pp 115-119, 2018.

[7] O.H. Embarak, "A two-steps prevention model of ATM frauds communication," in Proc. Inf. Technol. Trends Emerg. Technol. Artif. Intell., pp. 306-311, 2019

[8] A. Imran, "OTP based cardless transaction using ATM," in Proc. Int.Conf. Robot. Signal Process. Tech., pp 511-516, 2019.

[9] V. V. Jog, D. Jain, R. Arora, and B. Bhat, "Theft prevention ATM model using dormant monitoring for transactions," in Proc. IEEE Conf. Inf. Commun, Technol. (ICT), pp. 1156-1159, 2013.

[10] R. Laimek and N. Kaothantong, "ATM fraud detection using behavior model," in Proc. 5th Asian Conf. Defense Technol. (ACDT), pp. 21-25, 2018

[11] I H. S. Elganzoury, A. A. Abdelhafez and A. A. Hegazy, "A new secure one-time password algorithm for mobile applications," in Proc. 35th IEEE NRSC, vol. 18, pp. 250, 2018.

[12] M. Goresky and A. Klapper, "Efficient multiply-with-carry random number generators with maximal period," ACM Trans. Model. Comp. Sim., vol. 13, no. 4, pp. 1-12, 2003.

[13] B. Narasimhan, "JDiehard: An implementation of diehard in Java," in Proc. 2nd Int. Wksh. Dist. Stat. Comp., pp. 4, 2001.

[14] E. R. Harold, "Java I/O: Tips and Techniques for Putting I/O to Work," 2nd ed., O'Reilly Media Inc., 2006.