(IJNCAA)

ISSN 2220-9085(ONLINE)
ISSN 2412-3587(PRINT)

INTERNATIONAL JOURNAL OF NEW COMPUTER ARCHITECTURES AND THEIR APPLICATIONS

Volume 5, Issue 1
2015

SDIWC

www.sdiwc.net

International Journal of
NEW COMPUTER ARCHITECTURES AND THEIR APPLICATIONS

Overview

The SDIWC International Journal of New Computer Architectures and Their Applications (IJNCAA) is a refereed online journal designed to address the following topics: new computer architectures, digital resources, and mobile devices, including cell phones. In our opinion, cell phones in their current state are really computers, and the gap between these devices and the capabilities of the computers will soon disappear. Original unpublished manuscripts are solicited in the areas such as computer architectures, parallel and distributed systems, microprocessors and microsystems, storage management, communications management, reliability, and VLSI.

One of the most important aims of this journal is to increase the usage and impact of knowledge as well as increasing the visibility and ease of use of scientific materials, IJNCAA does NOT CHARGE authors for any publication fee for online publishing of their materials in the journal and does NOT CHARGE readers or their institutions for accessing the published materials.

Publisher

The Society of Digital Information and Wireless Communications
Miramar Tower, 132 Nathan Road, Tsim Sha Tsui, Kowloon, Hong Kong

Further Information

Website: http://sdiwc.net/ijncaa, Email: ijncaa@sdiwc.net,
Tel.: (202)-657-4603 - Inside USA; 001(202)-657-4603 - Outside USA.

The issue date is January 2015.

IJNCAA

ISSN 2220-9085 (Online)
ISSN 2412-3587 (Print)

Volume 5, Issue No. 1 *2015*

CONTENTS

ORIGINAL ARTICLES

International Journal of New Computer Architectures and their Applications (IJNCAA) 5(1): 1-9
The Society of Digital Information and Wireless Communications, 2015 ISSN 2220-9085 (Online); ISSN 2412-3587 (Print)

Performance Efficiency of Modified AES Algorithm Using Multiple S-Boxes

Felicisimo V. Wenceslao, Jr.
Institute of Information and Computer Studies,
Northern Iloilo Polytechnic State College, Estancia, Iloilo, Philippines
fvwenceslao@yahoo.com

ABSTRACT

In our previous paper, we modified the Advance Encryption System (AES) algorithm by proposing to use multiple substitution boxes (S-Boxes). While many studies have been conducted specifically on modifying the S-box, these studies were made to replace the Rijndael S-box in the AES cipher. Our version of the AES algorithm used two substitution boxes where the first S-box is the Rijndael S-box and was used as is. The second S-box was constructed by performing an XOR operation and affine transformation. Furthermore, the second S-Box replaced the MixColumns operation within the internal rounds in the cipher. This paper aims to determine the performance efficiency of the modified AES algorithm using multiple S-Boxes. Based on the result of the experiments, it was found out that the modified AES algorithm using multiple S-Boxes has an achieved execution time performance efficiency of 22.986% for encryption and 109.76% for decryption processes. However, when tested using the avalanche effect, the changes in the output bits were below the minimum expected rate at 24.219% and 19.531% respectively.

KEYWORDS

AES algorithm, S-Box**,** Cryptography, Affine Transformation, Execution Time Efficiency

1 INTRODUCTION

In 1997, the National Institute of Standards and Technology (NIST) started a process to identify a replacement for the Data Encryption Standard (DES) which was generally recognized to be not secured due to fast advances in computer processing power. The goal of NIST was to define a replacement for DES that could be used for non-military information security applications by US government agencies. Additionally, commercial and other non-government users could also benefit from the technology as it can also generally adopted for commercial use.

The NIST invited experts in the field of cryptography and data security from around the world to participate in the discussion and in the selection process. There were five encryption algorithms that made to the final round of the screening process. Ultimately, the encryption algorithm proposed by the Belgium cryptographers Joan Daeman and Vincent Rijmen was selected. Prior to selection, Daeman and Rijmen used the name Rijndael (derived from their names) for the algorithm. After adoption, the encryption algorithm was given the name Advanced Encryption Standard (AES) which is in common use today[1].

In 2000, the NIST formally adopted the AES encryption algorithm and published it as a federal standard under the designation FIPS-197. It was chosen because of its security, performance, efficiency, implementability, and low memory requirements.

The AES algorithm is primarily composed of four core functions that are repeatedly perform to the n^{th} times depending on the keylength. The MixColumn function is an important property of the cipher. Generally, it provides strength against differential and linear attacks due to the complexity of its mathematical operations. These complex mathematical operations may require computational resources in software implementation. We assume that by replacing the MixColumn function, the speed performance of the AES algorithm will be improved.

In light of this study, this paper aims to determine the execution time performance efficiency of the proposed modified AES algorithm using multiple

S-Boxes against the original AES algorithm. It will also attempt to evaluate security properties of both algorithm versions.

2 REVIEW OF RELATED STUDIES

Modifying the AES algorithm to improve its performance, either in speed or in security and both, has been the subject of numerous studies that were previously conducted. However, most of these studies were focused in changing the original substitution box as designed by Daeman and Rijmen unto different version of the S-Box. For instance, [2] proposed a substitution box that made use of the RC4 key schedule algorithm (KSA). The resulting matrix is a key-dependent S-Box that is dynamically generated based from some key. In their work, they constructed the Sbox-RC4 by:

- Running the RC4 KSA to construct 256! S-boxes depend on input key; and
- Perform an affine transformation to the RC4-KSA S-Box to produce the final S-Box.

After they created their new RC4-generated S-Box, they use it to replace the Rijndael S-Box during the encryption and decryption processes.

In [3] proposed for yet another key-dependent S-Box that they intend to substitute for the Rijndael S-Box. In their paper, they modified the AES algorithm by placing another phase in the beginning of every round. They call the extra phase as the S-Box Rotation. The purpose of which is to rearrange the original matrix by way of rotating the Rijndael Sbox according to some round key. The round key is derived from the cipher key using the key schedule algorithm. The rotation value is dependent on the entire round key.

The results of their study showed that the enhancement on the original AES does not violate the security of the cipher. The enhanced version introduces confusion without violating the diffusion property.

In [4], proposed an enhanced version of the AES-128 algorithm by reducing the number of rounds from 10 rounds to 8 rounds. Their assumption was that with the less number of rounds, it will result in less processing time of the AES algorithm, and therefore increase the speed performance of the cipher. However, they also acknowledge that the reduction in the number of rounds to 8 is risky in as far as security attacks are concerned as such as differential attack and distinguishing attack. To offset such risk, their proposed enhanced AES-128 algorithm used a hashing function to compensate the attacks being mentioned. Hence, their enhanced AES algorithm, while less in the number of rounds yet an extra phase for the hashing function using the SHA-256 in every round is included. The result of their experiment revealed that the hashing function improved the security aspects of the cipher but required more number of operations.

3 BASIC CONCEPT OF THE AES ALGORITHM

The AES algorithm is a block cipher with a block length of 128 bits. The key which is provided as the input is expanded into an array of key schedule words, with each word has a size of four bytes. The total key schedule for the 128-bit key is 44 words.

AES allows for three different key lengths: 128, 192, or 256 bits. The encryption and decryption is consists of 10 rounds of processing for a 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. During the encryption and decryption processes, the 16 bytes of data will form a changeable (4*4) array called the state array[5].

For the encryption, the state array consists initially of the input data. This array will keep changing until the final encrypted data is reach. In the decryption process, the state array start from the enciphered data and will keep changing until the original data is produced. The encryption of AES is carried out in blocks with a fixed block size of 128 bits each. The AES cipher calculation is

specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Figure 1 shows the AES cipher structure.

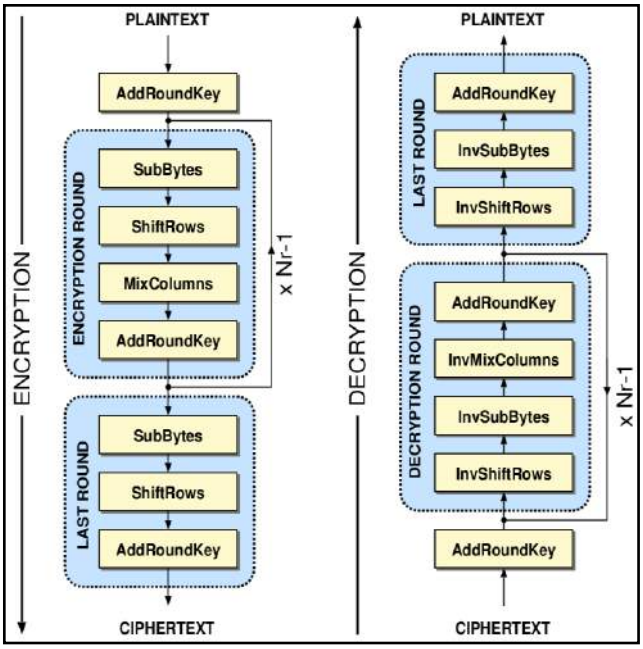

Figure 1. The AES Algorithm Structure.

Except for the last round in each case, all other rounds are identical. Inside each round are four different stages. These are:

3.1 Substitute Bytes (SubBytes Operation)

The SubBytes transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table (S-box)[6]. This is a major reason for the security of the AES. With the help of this lookup table, the 16 bytes of the state (the input data) are substituted by the corresponding values found in the table**.** Figure 2 shows the SubBytes operation.

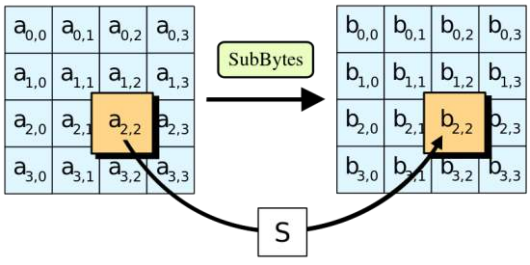

Figure 2. SubBytes Operation

3.2 Shift Rows (ShiftRows Operation)

The ShiftRows operation (figure 3) provides inter-column diffusion where the bytes in the last three rows of the states are shifted. Hence, the second row of the states is shifted by one byte position to the left of the matrix; the third row of the states is shifted by two bytes position to the left of the matrix; and the fourth row of the states is shifted by three bytes position to the left[6].

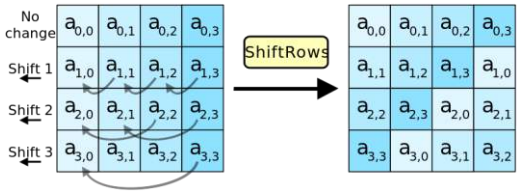

Figure 3. ShiftRows Operation

3.3 Mix Columns (MixColumns Operation)

Figure 4 shows the MixColumns operation that provides inter-byte diffusion where each column vector is multiplied by a fix matrix. The Galois Field is used in this operation. The bytes are treated as polynomials rather than numbers.

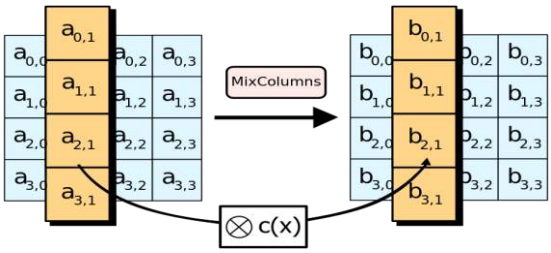

Figure 4. MixColumns Operation

3.4 Add Round Key (AddRoundKey Operation)

The AddRoundKey operation is simple. In this transformation, a round key is added to the state by a simple bitwise XOR operation. Each round key consists of *Nb* words from the key schedule[7]. It is performed by XOR-ing each byte of the state and the round key. Figure 5 shows the AddRoundKey operation.

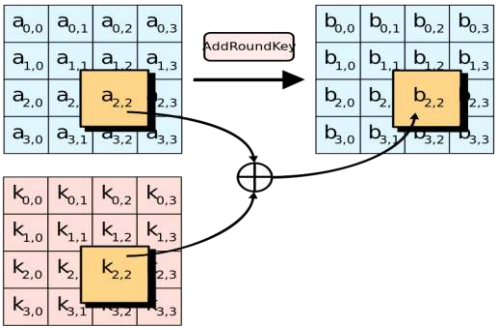

Figure 5. AddRoundKey Operation

For encryption, the individual transformations for the pseudocode computation consist of SubBytes(), ShiftRows(), MixColumns() and AddRoundKey(). These transformations play a role in processing the state[7]. The transformation (number of rounds) is performed depending on the key length. However, the final round is only consists of three stages: SubBytes, ShiftRows and AddRoundKey in producing the final encrypted data or ciphertext.

The decryption process is essentially the same structure as the encryption, following the nine rounds of Inverse ShiftRows, Inverse SubBytes, Inverse AddRoundKey and Inverse MixColumns transformation. In the final round, the Inverse MixColumns is no longer performed.

4 PROPOSED ENHANCED AES ALGORITHM USING MULTIPLE S-BOXES

In our previous paper[8], we proposed to modify the existing AES algorithm using two substitution boxes to enhance speed performance of the cipher. The SubBytes operation is less accessible from the standpoint of linear algebra because it is use to provide a non-linear step in the Rijndael cipher. A non-linear step in the cipher greatly increases its complexity and makes cryptanalysis more difficult[9].

On the other hand, among the four core functions of the AES algorithm, the MixColumns function is perceive to be requiring more computational resources in software implementation as compared to the other functions. This is due to the fact that the MixColumns function provides the critical security properties of the cipher to avoid from linear and/or differential attacks. It is through this assumption that replacing the MixColumns function by an alternative function, it may increase the speed performance of the AES algorithm.

The proposed enhanced version will become lightweight as it will employ two S-Boxes. The first S-Box is the Rijndael S-Box that is the default in the original structure of the cipher. It will be used as it is implemented in the original version. However, the second S-Box will be constructed and will replace the MixColumns function. It will be constructed using XOR operation and affine transformation.

In essence, the encryption process of the enhanced AES algorithm follows the sequence of SubBytes, ShiftRows, SubBytesXOR and AddRoundKey operations for nine rounds. In the final round, SubBytes, ShiftRows and the AddRoundKey operations will be performed to produce the ciphertext.

To decrypt, the enhanced AES algorithm is performed using the sequence of Inverse ShiftRows, Inverse SubBytes, Inverse AddRoundKey and Inverse SubBytesXOR operations for nine rounds. In the final round, the Inverse SubBytesXOR is drop to produce the plaintext. Figure 6 shows the proposed modified AES algorithm structure using multiple S-Boxes.

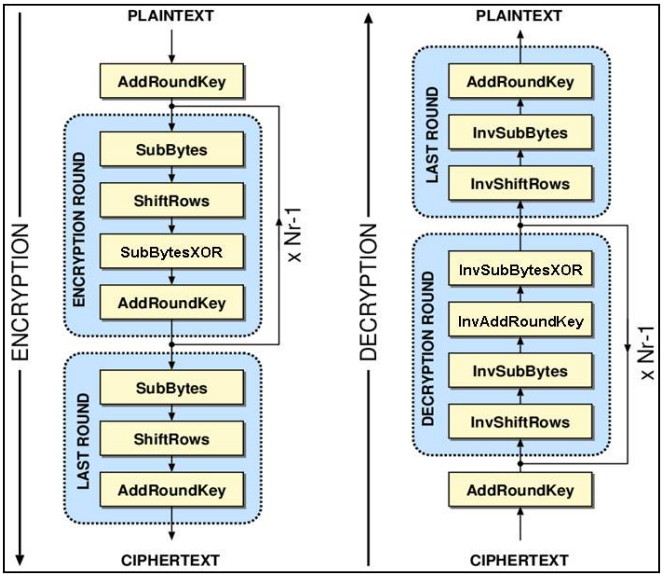

Figure 6. Modified AES Algorithm Using Multiple S-Boxes

5 CONSTRUCTION OF THE NEW S-BOX

The second S-Box is derived from the original S-Box as designed in the AES (hereafter referred as AES-Rijndael). It is constructed using the following process:

5.1 Exclusive OR Operation

The first step is to do an XOR operation to the AES-Rijndael using some Key[i]. The Key[i] shall be any hexadecimal value between 00 to FF. In this particular matrix, the key used was 7F. Hence, the new S-Box shall be referred to as AES-2SboxXOR$_{7F}$. For the initial values of the AES-SboxXOR$_{7F}$, each cell in the AES-Rijndael will be XORed with 7F (AES-Rijndael[x,y] $\otimes$ 7F).

5.2 Affine Transform Operation

After creating the initial values of AES-2SboxXOR, each cell will be subjected to affine transformation, as applied to the Sbox-Rijndael, to avoid any fix points and to make the new S-box invertible.

To scramble the bits in each byte value, we next apply the following transformation to each bit b_i as stored in the initial AES-2SboxXOR$_{7F}$:

$$b'_i = b_i \otimes b_{(i+4) \bmod 8} \otimes b_{(i+5) \bmod 8} \otimes b_{(i+6) \bmod 8} \otimes b_{(i+7) \bmod 8} \otimes c_i \quad (1)$$

where c_i is the i^{th} bit of a specially designated byte c whose hex value is 0x63 (c7c6c5c4c3c2c1c0 = 01100011).

For the inverse AES-2SboxXOR, the following transformation to each bit was used for bit scrambling:

$$b'_i = b_{(i+2) \bmod 8} \otimes b_{(i+5) \bmod 8} \otimes b_{(i+7) \bmod 8} \otimes d_i \quad (2)$$

where d_i is the i^{th} bit of a specially designated byte d whose hex value is 0x05 (d7d6d5d4d3d2d1ddc0 = 00000101).

5.3 Matrix Mapping Operation

At the end of the affine transformation, the final values are known. The next step is to map each value to the matrix as appropriate to create the final lookup tables. Table 1 shows the final AES-2SboxXOR$_{7F}$ while table 2 shows the final Inverse AES-2SboxXOR$_{7F}$.

Table 1. AES-2SboxXOR$_{7F}$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	13	0C	2D	32	6F	70	51	4E	EB	F4	D5	CA	97	88	A9	B6
1	E2	FD	DC	C3	9E	81	A0	BE	1A	05	24	3B	66	79	58	47
2	F0	EF	CE	D1	8C	93	B2	AD	08	17	36	29	74	6B	4A	55
3	01	1E	3F	20	7D	62	43	5C	F9	E6	C7	D8	85	9A	BB	A4
4	D4	CB	EA	F5	A8	B7	96	89	2C	33	12	0D	50	4F	6E	71
5	25	3A	1B	04	59	46	67	78	DD	C2	E3	FC	A1	BE	9F	80
6	37	28	09	16	4B	54	75	6A	CF	D0	F1	EE	B3	AC	8D	92
7	C6	D9	F8	E7	BA	A5	84	9B	3E	21	00	1F	42	5D	7C	63
8	9C	83	A2	BD	E0	FF	DE	C1	64	7B	5A	45	18	07	26	39
9	6D	72	53	4C	11	0E	2F	30	95	8A	AB	B4	E9	F6	D7	C8
A	7F	60	41	5E	03	1C	3D	22	87	98	B9	A6	FB	E4	C5	DA
B	8E	91	B0	AF	F2	ED	CC	D3	76	69	48	57	0A	15	34	2B
C	5B	44	65	7A	27	38	19	06	A3	BC	9D	82	DF	C0	E1	FE
D	AA	B5	94	8B	D6	C9	E8	F7	52	4D	6C	73	2E	31	10	0F
E	B8	A7	86	99	C4	DB	FA	E5	40	5F	7E	61	3C	23	02	1D
F	49	56	77	68	35	2A	0B	14	B1	AE	8F	90	CD	D2	F3	EC

Table 2. Inverse AES-2SboxXOR$_{7F}$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7A	30	EE	A4	53	19	C7	8D	28	62	BC	F6	01	4B	95	DF
1	DE	94	4A	00	F7	BD	63	29	8C	C6	18	52	A5	EF	31	7B
2	33	79	A7	ED	1A	50	8E	C4	61	2B	F5	BF	48	02	DC	96
3	97	DD	03	49	BE	F4	2A	60	C5	8F	51	1B	EC	A6	78	32
4	E8	A2	7C	36	C1	8B	55	1F	BA	F0	2E	64	93	D9	07	4D
5	4C	06	D8	92	65	2F	F1	BB	1E	54	8A	C0	37	7D	A3	E9
6	A1	EB	35	7F	88	C2	1C	56	F3	B9	67	2D	DA	90	4E	04
7	05	4F	91	DB	2C	66	B8	F2	57	1D	C3	89	7E	34	EA	A0
8	5F	15	CB	81	76	3C	E2	A8	0D	47	99	D3	24	6E	B0	FA
9	FB	B1	6F	25	D2	98	46	0C	A9	E3	3D	77	80	CA	14	5E
A	16	5C	82	C8	3F	75	AB	E1	44	0E	D0	9A	6D	27	F9	B3
B	B2	F8	26	6C	9B	D1	0F	45	E0	AA	74	3E	C9	83	5D	17
C	CD	87	59	13	E4	AE	70	3A	9F	D5	0B	41	B6	FC	22	68
D	69	23	FD	B7	40	0A	D4	9E	3B	71	AF	E5	12	58	86	CC
E	84	CE	10	5A	AD	E7	39	73	D6	9C	42	08	FF	B5	6B	21
F	20	6A	B4	FE	09	43	9D	D7	72	38	E6	AC	5B	11	CF	85

6 EXPERIMENTS METHODOLOGY

6.1 Test File

To test the speed performance of the proposed modified AES algorithm using multiple SBoxes, a text file with a size of 59 kilobytes was used in the experiment. The file was subjected to the encryption and decryption processes for 20 trials to encourage the reliability of the results.

The time trials were noted and subsequently subjected to statistical analysis to determine the performances of both versions.

6.2 Implementation Environment

In the conduct of experiments, the following implementation environment was used:

Processor:	Intel(R) Core(TM) i3-4010U CPU @ 1.70GHz
Main Memory:	4.00 Gb
Operating System:	64-bit
Runtime Environment:	JRE7
Development Platform:	Eclipse SDK 3.6.0

7 EVALUATION RESULTS

7.1 Speed Performance Difference

For the encryption, the AES-Rijndael version obtained a mean of 171.75ms while the proposed AES-2SBox obtained a mean of 139.65ms. Using the Data Analysis Tool from the Microsoft Excel 2010™, the t-Test for independent samples was used to statistically compute the significant difference in the speed performance. Based from the result of the test, the obtained P-value was 5.33936E-07. This is lower than the 0.05 level of significance, hence there is indeed a significant difference in the speed performance. Table 3 shows the t-Test Statistics for Independent Samples of the encryption process.

Table 3. Speed Performance Between the AES-Rijndael and AES-2SBox During Encryption

t-Test: Two-Sample Assuming Unequal Variances

	AES-Rijndael	*AES-2SBox*
Mean	171.75	139.65
Variance	359.1447368	190.7657895
Observations	20	20
Hypothesized Mean Difference	0	
Df	35	
t Stat	6.121727783	
P(T<=t) one-tail	2.66968E-07	
t Critical one-tail	1.689572458	
P(T<=t) two-tail	5.33936E-07	
t Critical two-tail	2.030107928	

For the decryption process, the AES-Rijndael obtained a mean of 195.00ms while the AES-2SBox version obtained a mean of 92.95ms. Similarly, the t-Test for Independent samples was used for statistical computation. Based from the result of the test, the P value obtained was 3.9442E-25 which is lower than the 0.05 level of significance. Again, there is a significant difference in the speed performance. Table 4 shows the t-Test statistics for independent samples of the decryption process.

Table 4. Speed Performance Between the AES-Rijndael and AES-2SBox During Encryption

t-Test: Two-Sample Assuming Unequal Variances

	AES-Rijndael	*AES-2SBox*
Mean	195	92.95
Variance	168.6315789	167.5236842
Observations	20	20
Hypothesized Mean Difference	0	
Df	38	
t Stat	24.89190009	
P(T<=t) one-tail	1.97221E-25	
t Critical one-tail	1.68595446	
P(T<=t) two-tail	3.94442E-25	
t Critical two-tail	2.024394164	

7.2 Time Execution Performance Efficiency

To compare the execution time performance efficiency (TEPE) of the two versions, the means were subjected to speedup comparison. Speedup is a metric for relative performance improvement when executing a task. The execution time of a program can be seen as a latency quantity type of the speedup comparison because it is in seconds per program [10].

For latency values, speedup is defined by the following formula:

$$ETPE(\%) = \left(\frac{Latency(T_{old})}{Latency(T_{new})} - 1 \right) * 100 \quad (3)$$

where ETPE(%) is the resultant execution time performance efficiency in percent; Latency(T_{old}) is the old mean execution time (i.e., without the improvement) and Latency(T_{new}) is the new mean execution time (i.e., with the improvement)[10][11].

Based from the obtained mean values of the AES-Rijndael and the AES-2SBox during encryption with 171.75ms and 139.65ms respectively, the execution time performance efficiency showed that the AES-2SBox is 22.986% more efficient than the AES-Rijndael version. Similarly, the obtained mean values of the AES-Rijndael and the AES-2SBox during decryption with 195.00ms and 92.95ms respectively, the execution time performance efficiency also revealed that the AES-2SBox is 109.79% more efficient that the AES-Rijndael version.

Table 5. Execution Time Performance Efficiency

Algorithm	Mean		ETPE%
	Latency(T_{old}) (AES-Rijndael)	Latency(T_{new}) (AES-2SBox)	
Encryption	171.75	139.65	22.986%
Decryption	195.00	92.95	109.79%

7.3 Test for Avalanche Effect

The avalanche effect refers to a desirable property of cryptographic algorithms. The avalanche effect is evident if, when an input is changed slightly (for example, flipping a single bit) the output changes significantly with at least half the output bits will be flip[12].

In[13], the calculation of avalanche effect can be derived by using equation:

$$\text{Avalanche Effect (\%)} = (NC/TN) * 100 \quad (4)$$

where NC is the number of changed bits in ciphertext and TN is the total number of bits in the ciphertext.

Here, we start to calculate the avalanche effect of the AES-2Sbox. The tests were performed by changing the plaintext bit from "11" to "10" and from "FF" to "F0". The results obtained were 24.219% with 31 bits that were changed and 19.531% with a flip of 25 bits respectively. The following table shows the result of the test for avalanche effect for AES-2Sbox.

Table 6. Avalanche Effect of the AES-2SBox

Plaintext	Ciphertext	Avalanche Effect
11111111111111111111111111111111	FE88B9C6D624C203A4345796445320E4	24.219% (31)
11111111111111111111111111111110	40A3CFC6D624C2D972345796B15320A4	
00112233445566778899AABBCCDDEEFF	9E53C352DBDF8A4F1034CABEAC05B1FB	19.531% (25)
00112233445566778899AABBCCDDEEF0	37F1B112DBDF8A221034848DAC05B1FB	

8 CONCLUSION

This paper presents a proposed modified AES algorithm using multiple Sboxes. The first Sbox (AES-Rijndael) stand as is in the cipher structure. Meanwhile, a new Sbox was constructed using XOR operation and affine transformation. This Sbox, which we call AES-2SBoxXOR, replaced the MixColumns step in the AES cipher rounds.

Two set of tests were conducted to the original version and the modified version of the AES algorithm. In the speed performance test, where the two versions, through an implementation model, encrypted and decrypted a file with a size of 59Kb for 20 trials. The t-Test statistics set at 0.05 level of significance revealed that in both encryption and decryption, there were significant differences in the speed performance between the two versions with the obtained P-values 5.33936E-07 and 3.94442E-25 respectively. For the execution time performance efficiency, it was found out that both in the encryption and decryption processes, the AES-2SBox was more efficient by 22.986% and 109.79% respectively that the original AES algorithm.

We also performed the test using avalanche effect on the proposed AES-2SBox algorithm. The results of the simulation revealed that the avalanche effect is slightly lower than the minimum expected output of at least 50% bit flip when 1 bit input is altered. The obtained changes in the bit sequence were computed at 24.219% and 19.531% for two set of plaintext.

From these results, we observed that the speed performance significantly increased in the modified AES algorithm using multiple S-Boxes, while the security side has slightly weakened.

REFERENCES

[1] Townsend Security: Introduction to AES Encryption: White Paper, TownSendSecurity.com, https://townsendsecurity.com/sites/default/files/AES_Introduction.pdf (2010).

[2] Abd-ElGhafar, I., Rohiem, A., Diaa, A. and Mohammed, F.: Generation of AES Key Dependent S-Boxes using RC4 Algorithm. In: 13 International Conference on Aerospace Sciences & Aviation Technology (ASAT- 13). May 26 – 28, 2009, Military Technical College, Kobry Elkobbah, Cairo, Egypt, (2009).

[3] Juremi, J., Mahmod, R., Sulaiman, S. and Ramli, J.: Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key, In: International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): The Society of Digital Information and Wireless Communications (SDIWC) 2012 (ISSN: 2305-0012), pp. 183-189 (2012).

[4] Manasa, S., Mullaimalar, P., Gnanaprakash Singh, G. B. and Manivannan, S. S.: Reducing the Key Generation Time Using Enhanced AES-128 Algorithm to Secure the Data over Wireless Networks. In: International Journal of Applied Engineering Research, ISSN 0973-4562, Vol. 8, No. 19, pp. 2453-2456 (2013).

[5] Pachori, V., Ansari, G., and Chaudhary, N.: Improved Performance of Advance Encryption Standard using Parallel Computing. In: International Journal of Engineering Research and Applications. Vol. 2, Issue 1, Jan-Feb 2012, pp. 967-971 (2012).

[6] Federal Information Processing Standards Publication 197, Announcing the Advanced Encryption Standard, http://csrc.nist.gov/publications/fips/fips197/ fips-197.pdf

[7] Man Young Rhee, Internet Security: Cryptographic Principles, Algorithms and Protocols. John Wiley & Sons Ltd: England, p.114 (2003).

[8] Wenceslao, F., Gerardo, B., and Tanguilig, B.: Modified AES Algorithm Using Multiple S-Boxes. In: Proceedings of the Second International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA2015), Manila, Philippines, pp. 71-78 (2015).

[9] Sears, I.: Rijndael AES. http://www.unc.edu/~marzuola/Math547_S13/Math547_S13_Projects/I_Sears_Section003_AdvancedEncryptionStandard.pdf

[10] WikiPedia.Com: SpeedUp. http://en.wikipedia.org/w/index.php?title=Speedup&oldid=648990695

[11] Martin, M.: Performance and Benchmarking. Retrieved on February 21, 2015, Retrieved from: http://www.cis.upenn.edu/~milom/cis501-Fall12/lectures/04_performance.pdf

[12] WikiPedia.Com: Avalanche Effect. http://en.wikipedia.org/wiki/Avalanche _effect, 2014.

[13] Patidar, G., Agrawal, N. and Tarmakar, S.: A block based Encryption Model to improve Avalanche Effect for Data Security. In: International Journal of Scientific and Research Publications, Volume 3, Issue 1, January (2013).

ABOUT THE AUTHOR

Felicisimo V. Wenceslao, Jr. finished his Bachelor of Science in Computer Science at the Computer College of the Visayas, Iloilo City, Philippines (1993) and his Master of Science in Information Technology at Hannam University, Republic of Korea (2005). He is currently pursuing his Doctor in Information Technology at the Technological Institute of the Philippines, Quezon City, Philippines. He is currently the Director of the Institute of Information and Computer Studies at Northern Iloilo Polytechnic State College, Estancia, Iloilo, Philippines. His research interests are in network security, mobile development, data mining and e-learning.

International Journal of New Computer Architectures and their Applications (IJNCAA) 5(1): 10-18
The Society of Digital Information and Wireless Communications, 2015 ISSN 2220-9085 (Online); ISSN 2412-3587 (Print)

A New Approach for Solving Equations Systems Inspired from Brainstorming

Liviu Octavian Mafteiu-Scai
West University of Timisoara, Romania
lscai@info.uvt.ro

ABSTRACT

This paper proposes a metaheuristic inspired from human brainstorming combined with concepts from graph theory for solving system of equations. The proposed method is able to find solutions of a given system of equations, even in cases where traditional methods fail. In the cases where no exact solution exists, an approximate solution is good and it can be obtained by the proposed method. Directions for future research are also provided.

KEYWORDS

metaheuristics, brainstorming, k-partite graphs, cliques, quasi-cliques, system of equations

1. INTRODUCTION

1.1 Creativity and Brainstorming

Creativity is probably one of the most remarkable attributes of the human being, which essentially distinguishes it from other creatures on our planet. A definition of the concept can be found in the paper [1]. There are many works that describe and analyze human creativity in terms of psychology, such as for example [2, 3] and as a consequence we will not insist here on the subject. In the computer era it was a natural occurrence of a study domain aiming imitating human creativity called *computational creativity* [4, 5]. Computational creativity is a subfield of artificial intelligence who study how to build computational models of creative thought in science and arts. Computational creativity has been applied in many directions as well: design [6], games [7], culinary recipes [8], music [9] etc.

At the same time, human creativity has always played an essential role in solving new problems or in finding new and more effective solutions to solve old ones. For this, there are two forms of creativity in terms of the number of persons involved: singular and collective creativity [4]. One collective creativity technique is the *brainstorming* [10], which mainly aims to the generation of a large number of creative ideas through intensive and freewheeling group discussion aiming to solve a problem.

The term *brainstorming* was introduced in 1963 by Alex Faickney Osborn [11]. There are four basic rules of brainstorming method:
- *focus on quantity;*
-*without criticism;*
-*welcome unusual ideas;*
-*combining and improving the ideas.*

The technique has generated much controversy in time, being many researchers who criticize it [12] and even some who entirely reject it. We will not do in this paper a complete description of brainstorming method and the problem generated by this because literature is very rich in this respect, a good survey being the work [13]. Anyway, over time, the technique proposed by Osborn has undergone improvements [14, 15]. One of the greatest innovations of the verbal brainstorming proposed by Osborne was the *electronic brainstorming* (EBS) [16].

In the second section of this paper we will review some psychological aspects of brainstorming that directly show interest in terms of the present work.

1.2 Optimization Problems Solved by Artificial Intelligenge Techniques

Optimization is one of the most important real problems. Over time there have been developed many mathematical methods, mainly heuristic techniques. In recent years, techniques inspired by artificial intelligence have made beneficial contributions to solving optimization problems. Some of them, known as *evolutionary algorithms* were inspired by biological evolution: *genetic algorithms* [17], *genetic programming* [18] etc. Algorithms inspired from nature, particularly from collectivities animal life –known as swarm intelligence- have been proposed during the past time: *ant colony optimization* algorithm (ACO)

[19], *bee colony optimization* algorithm (BCO) [20], *particle swarm optimization* (PSO) [21] etc. A hybridization of evolutionary algorithms, known as *memetic algorithms*, inspired by cultural evolution was first proposed in [22].

Shi proposes in paper [23] an optimization method inspired from human brainstorming process (BSO) as a reply to swarm intelligence. In the proposed algorithm by Shi, the population is composed of individuals represented by the proposed potential solutions for the problem to be solved, randomly generated values. In the next phase, individuals are evaluated and grouped into clusters. After that, each cluster in part is evaluated and modified by positioning the best individual in the center. Using probabilistic methods, new individuals are generated according to the cluster centers, using a selection similar with genetic elitism. The process ends after generating a predetermined number of individuals or a predetermined number of iterations is reached. In this algorithm, the size of population represents the number of ideas generated and an iteration represents a round of idea generation in the brainstorming process. The tests and results on the two benchmark functions presented in paper [23] by author validate the effectiveness and usefulness of the proposed brainstorming optimization algorithm.

A similar approach for multiple optimization problems is proposed in paper [24]. A technical application of BSO was proposed in paper [25]. A working parameters investigation of BSO process is presented in paper [26]. Also, an improved variant of BSO algorithm is proposed in [26]. In [27] the authors propose a brainstorming process modeling using a genetic algorithm like a search technique. In [28] a hybridization between BSO and Teaching-Learning-Based Optimization algorithm (TLBO) with applying in optimal power flow problems is proposed.

1.3 Some Used Concepts from Graph Theory

The next section proposes a modeling of creativity like a search space using graph theory, namely the concept of *k-partite* graph. It is known that a *k-partite* graph is a graph whose vertices can be partitioned into *k* disjoint sets so that no two vertices within the same set are adjacent. If *k=2* we have a *bi-partite* graph and so on. First we describe the modeling proposed for k=2 followed by an extension to the general case.

The following definitions are known in graph theory and used in our approach. So, in the case of a graph *G(S, A)*, where *S* is the vertices set and *A* is the edges set we have:

Def.1: A *biclique* $C=(S', A')$ is a subgraph of *G* induced by a pair of two disjoint subsets $S' \subseteq S$, $A' \subseteq A$, *such that* $\forall s \in S'$, a $\in A'$, *(s,a)* $\in$ E, meaning that a biclique in a bipartite graph is a complete bipartite subgraph that contains all permissible edges.

Def.2: A *maximum biclique* is a largest biclique in a bipartite graph. From this point of view there are two distinct variants of this problem: the *vertex maximum biclique* problem and the *edge maximum biclique* problem.

Def.3: A biclique within another bipartite graph is called a *maximal biclique* if it is not contained in a larger biclique.

The problem can be regarded distinctly in terms of the vertices respectively edges of graphs. The *edge maximum biclique* is often used in biological applications, web community discovery, and text mining because it models more balanced connectivity between the two vertex classes [29] and therefore over time many algorithms have been developed in this respect [30].

Def.4: A *quasi-biclique* is similar to biclique but contains almost of its edges. *Maximal quasi-bicliques* are proposed in [31] and are motivated by real-world applications where errors and missing data/information (edges in graph) are present. Also it was shown in paper [31] the versatility and effectiveness of maximal quasi-bicliques to discover correlated data sets.

Figure 1 illustrates the previous concepts as follows:

- graph:

$$\boldsymbol{G} = \langle \boldsymbol{V}, \boldsymbol{E} \rangle = \\ = \langle \{\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{e}\}, \{(\boldsymbol{x}, \boldsymbol{b}), (\boldsymbol{x}, \boldsymbol{c}), (\boldsymbol{x}, \boldsymbol{d}), (\boldsymbol{y}, \boldsymbol{a}), (\boldsymbol{y}, \boldsymbol{b}), (\boldsymbol{y}, \boldsymbol{c})\} \rangle$$

which have a

- bi-partite subgraph:

$$\boldsymbol{G_B} = \langle \boldsymbol{V_1} \cup \boldsymbol{V_2}, \boldsymbol{E} \rangle = \\ = \langle \{\boldsymbol{x}, \boldsymbol{y}\} \cup \{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}\}, \{(\boldsymbol{x}, \boldsymbol{b}), (\boldsymbol{x}, \boldsymbol{c}), (\boldsymbol{x}, \boldsymbol{d}), (\boldsymbol{y}, \boldsymbol{a}), (\boldsymbol{y}, \boldsymbol{b}), (\boldsymbol{y}, \boldsymbol{c})\} \rangle$$

with

- bi-cliques:

$$\boldsymbol{G_{BC1}} = \langle \{\boldsymbol{x}\} \cup \{\boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}\}, \{(\boldsymbol{x}, \boldsymbol{b}), (\boldsymbol{x}, \boldsymbol{c}), (\boldsymbol{x}, \boldsymbol{d})\} \rangle$$
$$\boldsymbol{G_{BC2}} = \langle \{\boldsymbol{x}\} \cup \{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}\}, \{, (\boldsymbol{y}, \boldsymbol{a}), (\boldsymbol{y}, \boldsymbol{b}), (\boldsymbol{y}, \boldsymbol{c})\} \rangle$$

$G_B = \langle \{x, y\} \cup \{b, c\}, \{(x, b), (x, c), (y, b), (y, c)\} \rangle$

the last being a maximum biclique from the *edge maximum biclique* problem point of view.

At the same time G_{BC1} and G_{BC2} are *vertex maximum bicliques*.

A quasi-biclique example is:

$$G_{BQ} = \langle \{x\} \cup \{a, b, c, d\}, \{(x, b), (x, c), (x, d)\} \rangle$$

where the edges *(x,a)* and *(y,d)* are missing.

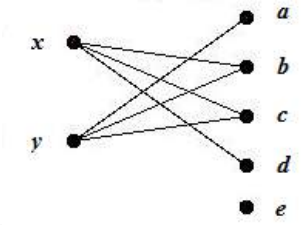

Figure 1 A bi-partite graph example

The previous concepts can be easily extended to the case of *k-partite* graphs, as can be seen in Figure 2. As previously mentioned, a *k-partite* graph is a graph whose vertices can be partitioned into *k* disjoint sets so that no two vertices within the same set are adjacent. We mention that for us it is sufficient to consider a particular case that the bicliques relate to a particular partition, hereinafter called the *main partition*, while the rest are called *secondary partitions*. The red edges from Figure 2 belong to a 4-clique graph. It is known the definition according to which a *n-clique* of an undirected graph is a maximal subgraph in which every pair of vertices is connected by a path of length *n* or less.

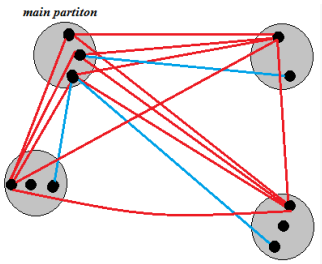

Figure 2 A 4-partite graph example

1.4 Solving the Systems of Equations

A frequent problem in numerical analysis is solving the systems of equations. That problem has generated in time a great interest among mathematicians and computer scientists, as evidenced by the large number of numerical methods developed. Besides the classical numerical methods, in the last years were proposed methods inspired by techniques from artificial intelligence. Hybrid methods have been also proposed along the time [32].

The classical methods are usually divided into exact/direct methods and iterative/indirect methods. In exact methods, the solution is obtained after a fixed number of operations, a number that is directly proportional to system size. In these cases the solutions are affected by rounding errors and are used only when the size of the system is small. The most known direct methods are: Cramer, Gaussian elimination, Gauss-Jordan elimination, LU factorization, QR decomposition etc. In iterative methods the iterative process will be stopped after a preset number of steps or after fulfilling certain conditions. The process involves truncation errors, that is the main disadvantage of these methods. However, because the rounding errors are not cumulated and because requiring a smaller number of operations, iterative methods are preferred especially for large systems of equations. A disadvantage of iterative methods occurs when the system size is smaller than the number of unknowns (under-determined system) when the classical iterative algorithms are not applicable in general. The most popular iterative methods are Gauss-Seidel, Jacobi, Newton, Conjugate Gradient and Broyden.

In the last years, techniques and methods from artificial intelligence have been used to solve systems of equations. In [33] is proposed an algorithm that uses a genetic approach to solve linear systems of equations. This problem is viewed in terms of an optimization task. In [34] the authors investigate the applicability and effectiveness of genetic algorithms in finding the solutions of systems of linear equations. Solving a system of equations is regarded again as an optimization problem. In the case of an infinite number of solutions the proposed algorithm is able to produce more than one set of solutions for a system of equations. In terms of the objective function, the approach is similar to that in [33] but the problem is interpreted as a multiobjective optimization task. Such a multiobjective optimization approach is not new, since similar approaches were proposed also in [35, 36, 37 and 38]. In [39] the proposed method for solving a linear system of equations is based on using a

particle swarm optimization algorithm and an artificial fish swarm algorithm, especially designed for ill conditioned linear systems equations. In paper [40] is proposed a memetic algorithm (MA) to solve linear systems of equations, by transforming the linear system of equations into an optimization problem. Such exploitation of knowledge obtained in a local search/optimization allows the evolutionary programming implementation to produce very good results at a relatively low computational cost.

2. THE BRAINSTORMING IN THE PROPOSED METHOD

At the base of the proposed algorithm in this paper are a few elements from modern process of human brainstorming. These will be described briefly below.

a) the need for experts

After a brainstorming process it is expected to result a better idea/solution than ideas/solutions proposed by each participant in part. In our opinion if all participants are unskilled in the working domain, it is unlikely to reach a good result. At the same time, the presence of experts would allow to remove those ideas that are not suitable from a technical point of view.

In our proposed method the main *expert* role is done by the fitness function of the evolutionary process. The chosen fitness function tells the algorithm how good a particular solution is. That is in fact the difference between left and right side of each equation in part after replacing the possible solution vector (an individual in population) in all the equations. If this difference is equal to zero we have an exact solution. If this difference is smaller than a preset value we say that we have an approximate solution

b) the diversity of participants

It is necessary to have a great diversity of groups from which participants arise, because the same origin of organizational groups can lead to a premature convergence of the ideas issued. The brainstorming ideas in the proposed method are represented by individuals in the population, where each individual represents a possible solution to an equation. The diversity is ensured by a controlled random number generator and by evolutionary processes (crossover and mutation).

c) starting point

The use in the early stages of brainstorming process the known solutions for similar problems can be beneficial in the sense that can position the starting point of new ideas in a favorable position. Obviously there is a risk of obtaining a contrary effect.

The *starting point* in our proposed algorithm is represented by an initial search space that is an arithmetic interval. This initial search space is used in first stage of the process and is determined by computing the degree of dissimilarity [41] of the current system of equations and other similar systems of equations solved, systems that are stored in a database. If the degree of dissimilarity isn't favorable, random real numbers are generated and assigned to individuals. So, in our algorithm, this means clustering and storage of the basic characteristics and solution for each equations system solved in a database.

In the proposed algorithm the individuals are represented by vectors of real numbers with dimension equal to the number of unknowns of the equations system to be solved.

In the next stages the search space is expanded, the expanding having two purposes: to avoid the process of population degeneration and to try to find new solutions in a larger search space. In reality the search space is infinite ($-\infty$, $+\infty$), but this approach has proven to lead to a very poor convergence of the algorithm, so that was chosen a method of successive expansion of initial arithmetic interval to the right and to the left with a preset value r. The r value is set by user at the beginning of the process.

d) ideas combination

Combining similar or redundant ideas can lead to improved brainstorming process.

In proposed algorithm, an iteration represents a phase in the brainstorming process. Except for the first iteration, in the rest of iterations only a part of the population will be generated randomly, the other part being obtained by genetic crossover and mutation of the best individuals of the previous

population, respecting the principle of genetic elitism.

e) ideas classification

The classification/clustering of ideas is necessary to determine which should take priority in next brainstorming ie next iteration in algorithm.

f) validation of ideas

Brainstorming can be viewed as a method for generating ideas without worrying about solving or not solving the problem. After ideas generation, can begin implementing and validating them as solutions for problem to be solved. So, at the beginning, ideas have to be generated and after that they must be validated to see if these can solve the problem. As mentioned in [42], generating new ideas in a software program is not difficult with artificial intelligence techniques, but the hard problem is their automating validation.

In the proposed algorithm, after replacing the values from possible solution vector in all the equations, the difference between left and right side of each equation in part shows how good a solution is and it is also an expertise in terms of a brainstorming process.

g) creativity like a search space

In work [42] the creative process is seen as a search process in a given space, space which can then be extended. May be, the term "explore" is more adequate than the classical "search", but we prefer the last in the approach of searching new ideas for a given problem. So, we have in a given space a set of objects, and between these, relationships can be established. Linking a group of objects through relationships will be a new idea. Validation of these new ideas/paths represents new solutions for a given problem. But -through an initial expertise- it's known that there are objects which cannot be linked by relationships or objects that only by some relationships can or cannot be linked. In this context it is necessary a first expertise to remove those pathways that contain impossible/forbidden links between objects in search space. This first expertise process will eliminate the bad ideas and no longer necessary their validation. The modeling of creativity like a search space in proposed method is made by using the *k-partite* graph concept .

h) termination of the process

A brainstorming process can be closed when it was found a solution for the problem or a preset number of stages was reached.

In the proposed algorithm the termination criteria are: finding an exact solution (fitness function satisfying), finding an approximate solution or reaching a preset number of iterations.

From solution finding point of view the differences mentioned at point g) represents one of the stopping criteria of the algorithm. The ideal case is when all the differences are zero, but in some cases a small enough value (preset by user) can be satisfactory.

3. ALGORITHM AND EXPERIMENTS

In accordance with the basic rules of brainstorming and considerations presented in the previous section, a metaheuristic algorithm designed to solve systems of equations (linear and nonlinear), inspired from human brainstorming process is proposed and described below.

In first variant of proposed algorithm, the problem is viewed as an optimization problem. In this case, finding a solution for the system of equation $f(X)$ -where $X=\{x_1, x_2, \ldots, x_n\}$ vector represents the unknowns- involves finding a solution so that every equation in the system is zero i.e.:

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) = 0 \\ f_2(x_1, x_2, \ldots, x_n) = 0 \\ \quad\quad . \\ \quad\quad . \\ \quad\quad . \\ f_n(x_1, x_2, \ldots, x_n) = 0 \end{cases} \quad (1)$$

A solution is an assignment of values to the variables $x_1, x_2, \ldots, x_n$ such that each of the equation is satisfied. The solution set is the set of all possible solution for equations system and there are three possible situations: unique, infinitely or no solution for system. In our approach the method is viewed as an optimization problem (finding a solution by minimized a given objective function). This function in our method is $abs(f_i(X))$ that in term of evolutionary process is named *fitness* function. This fitness function tells the algorithm how good a particular solution is.

The size of population ie the X vectors, represents the number of ideas generated from

brainstorming point of view. An iteration in proposed algorithm represents a round of idea generation in the brainstorming process.

These considerations are the base of the first method proposed for solving systems of equations inspired by human brainstorming process. The general structure of this algorithm is presented below:

```
Begin
  Read system and other working parameters
  Search Space Initialization
  Generating Random and Guided Initial Population
  Repeat
    Evaluate individuals by their fitness
    Put and Sort individuals in clusters
    Select for each cluster in part the elite group
    Crossover and Mutation for each elite group
    Add new individuals to population
    Repeat
      Random generating new individuals
      If Degenerate
        Expand Search Space
      Else
        Complete Population with new individuals
    Until Not Degenerated
    Compute Average deviation of solutions for each
    -equation in part and for entire system
  Until Termination Conditions
End
```

From an evolutionary process point of view, the crossover process explores the search space around the already found good or approximate solutions and the mutation process explores the search space for new solutions. In the crossover process it is used a middle point crossover. Two types of mutation were used in the proposed algorithm: first a *pure-random* mutation type to ensure a high diversity of the population in the search space and second, a *non-random* mutation with small random variations of promising chromosomes to increase the likelihood of promising chromosomes. In initial population generation stage, when there isn't a similar system in database, it is used a *selective initialization* that means: a large number of random solutions are randomly generated and then the initial population is selected from these, according to genetic elitism.

The termination conditions used in proposed algorithm were: finding an exact solution (fitness function satisfying), finding an approximate solution or reaching a preset number of iterations.

After experiments it was observed that the proposed method always finds a solution to a given system of equations (linear and nonlinear), an exact solution or an approximate solution, even in situations when conventional methods fail (determinant null, system is dependent, system doesn't satisfy the convergence conditions, convergence condition satisfied but an infinite number of solutions found/not found, etc.).

In the second approach the elements from graph theory presented in the first section were used to improve the first proposed method.

So, for a *n* dimensional system of equations a *(n+1)-partite graph* is generated.

The first partition, hereinafter called *main partition* is fixed from number of vertices point of view, the dimension being equal to *n*. In this partition the vertices are represented by equations.

The rest of partitions (*n* partitions), hereinafter called *secondary partitions*, the vertices are represented by numerical values of possible solution vectors, which are obtained by the evolutionary process described before. These partitions are variable from the number of vertices point of view, due to values coincidence of possible solutions. Each partition corresponds in fact to all possible solutions for each unknown of system in part.

The edges of the graph are determined by the fitness function and suggest that a numerical value from a particular secondary partition is a possible solution to some unknown and some equation of the system.

A solution vector for equations system from this graph representation of the problem is in fact a *(n+1)-clique*. Multiple solution are represented by multiple and distinct *(n+1)-cliques*.

The *quasi-cliques* represent a starting point for a new crossover process which aims to achieve more quickly the system solution. These quasi-cliques are sorting descending by number of edges and a first part of them are subject to a new evolutionary process, ie crossover and mutation.

In fact, this approach, based on evolutionary process overlapped by a heuristic based on graph theory, is a complex metaheuristic.

A sample example of this new approach can be seen in Figure 3. The graph representation is the final form of the associated graph, after the evolutionary process for a 3-dim system of linear equations:

$$\begin{cases} x + 2y + 3z = 14 \\ x + y + z = 6 \\ 3x + 2y + z = 10 \end{cases} \quad (2)$$

The system equation composed of by *e1*, *e2* and *e3* equations has multiple solutions, two of them were represented like cliques in Figure 3 (edges in red and blue) and quasi-cliques (one of them colored in yellow).

The main task consists of determining the cliques and if they don't exist, the task continues to determining the quasi-cliques and select the best of these after a greedy selection. In our approach the selected quasi-cliques will be subjects of a new evolutionary process.

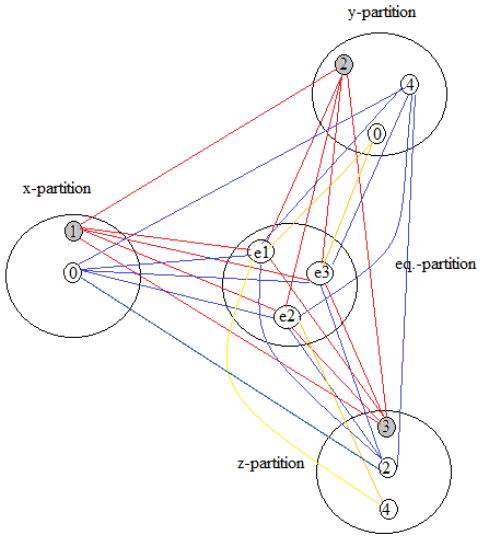

Figure 3: k-partite graph of equations system (1)

So, the first algorithm will be completed with the sequence:

```
…
If cliques found then
   print solution
else
   search for quasi-cliques
   sort quasi-cliques
   Apply crossover to elite of quasi-cliques
…
```

The values of the parameters used in the experiments were:

- r =10;
- population size of each generation =200
- maximum number of iteration = 1000
- value for maximum acceptable deviations $=10^1$

A comparison of system (1) solutions obtained with other methods is given in Table 1. Note that system (1) has an infinite number of solutions and Wolfram Mathematica software can produce a set of linearly independent vectors from which system solutions can be constructed. This test confirms the validity of the solutions provided by our algorithm.

It has been observed that using the *mass-mutations*, in which is kept a part of the initial configuration of elites, are the most productive evolutionary process in case of our method.

Also, we observed that using a more random population, increases the solution quality but also increases the execution time.

Table 1. Comparative solutions for system (1)

Gauss-elimination	**Gauss-Jordan**	**LU Factoriz.ation**	**Genetic Algorithm**	**Conjugate gradient**	**Wolfram Mathematica 10**	**Proposed Algorithm Inspired from human brainstorming**
fail	{4,-4, 6}	fail	{1, 2, 3} {0, 4, 2} {2, 0, 4}	{4,-16,14} fail	x=-2+z y=8-2z	**{1, 2, 3}**, **{0, 4, 2}**, {2, 0, 4}, {-2,8, 0}, {4, -4, 6}, {1.45, 1.08, 3.45}, {-4.13, 12.26, -2.13}, {75.2, -146.3, 77.2}

Another running example of the proposed method is given further. We consider three nonlinear equations:

$$(3x-2)^{1/4} + (15x+1)^{1/4} - 3 = 0 \quad \text{(a)}$$
$$2^x + 3^x + 6^x - 3x^2 - 5x - 3 = 0 \quad \text{(b)} \qquad (2)$$
$$2^{3x+1} - 13 \cdot 2^{2x} + 11 \cdot 2^{x+1} - 8 = 0 \quad \text{(c)}$$

In Table 2, for all possible systems of equations formed by these equations are given the exact and the approximate solutions obtained with the improved proposed method. Through "deviation" we mean the difference between left and right side of each equation in part after the approximate solution replaces the unknowns and show how good the solution is. To note that only integer solutions were searched.

Table 2. Solutions of non-linear system (2)

	The equations of the system	Exact solution	Approximate solution (deviation ≤5)	
			solution	deviation
1	(a)	1	2	0.77
			5	1.85
2	(b)	1	-2	4.61
		0		
		-1		
3	(c)	2	0	3
		1	-2	3.28
		-1		
4	(a)+(b)	1	2	-
5	(a)+(c)	1	2	-
6	(b)+(c)	1	-2	-
		-1		
7	(a)+(b)+(c)	1	2	-

4. CONCLUSION AND FUTURE WORK

The main conclusion is that the proposed method inspired from brainstorming process combined with concepts from graph theory can be very helpful in finding solution for equation and system of equations, linear and nonlinear. The proposed method can find solutions of a given system of equations, even in cases where traditional methods fail (Gauss-elim., Gauss-Jordan, Conjugate gradient etc). In the cases where no exact solution exists, an approximate solution is good and it can be obtained by the proposed method, solutions whose fitness is very close to 0. This approximate solution is good/acceptable in many real life application. Also, systems with multiple solutions can be solved, the proposed method has been able to find all the solutions inside of a given interval preset by user.

The major disadvantage of the proposed algorithm is the running time that is prohibitive in many cases for systems with dimension greater than 50. Even for smaller systems the execution time is greater if the values of the solution vector are distributed in a large interval. So, the proposed method should be refined, and especially made more effective through parallelization and these will be our future concerns.

REFERENCES

[1] Runco M.A., Jaeger G.J.: The Standard Definition of Creativity. Creativity Research Journal, 24(1), 92–96, ISSN: 1040-0419 (2012)

[2] Lytton H.: Creativity and Education. Ed. Routlegge, 2012 edition, ISBN:978-0-415-67549-9 (2012)

[3] Sawyer R.K.: Explaining Creativity. The Science of Human Innovation, second edition, ISBN-10: 0199737576 (2012)

[4] Maher M.L.: Computational and Collective Creativity: Who's Being Creative?. International Conference on Computational Creativity (2012)

[5] Colton S., Wiggins G.A.: Computational Creativity: the Final Frontieer?. ECAI 2012: 20th European Conference on Artificial Intelligence, eds. L. De Raedt, C. Bessiere,D. Dubois (2012)

[6] Gero J.S., Maher M.L.: Modeling Creativity and Knowledge-Based Creative Design. Lawrence Publ. ISBN:0-8058-1153-2 (1993)

[7] Merrick K.E., Isaacs A., Barlow M., Gu N.: A shape grammar approach to computational creativity and procedural content generation in massively multiplayer online role playing games. Elsevier - Entertainment Computing, Vol. 4, Issue 2, pp. 115–130, (2013)

[8] Pinel F., Varshney L.R.: Computational creativity for culinary recipes. ACM- Proceeding CHI EA '14, pp. 439-442, ISBN: 978-1-4503-2474-8 (2014)

[9] McDermott J.: Functional Representations of Music. Proceedings of the Third International Conference on Computational Creativity, ISBN: 978-1-905254668 (2012)

[10] Fen L.H.: A review on the pragmatic approaches in educating and learning creativity. International Journal of Research Studies in Educational Technology, ISSN: 2243-7738, Volume 1 Number 1, pp. 13-24, (2012)

[11] Osborn A.F.: Applied imagination. Principles and procedures of creative problem solving New York, NY: Charles Scribner's Sons (1963)

[12] Furnham A.: The Brainstorming Myth. Wiley Online Library, online: 6.01.2003, DOI: 10.1111/1467-8616.00154 (2003)

[13] Isaksen S.G.: A Review of Brainstorming Research. Creativity Research Unit, Creative Problem Solving Group, Buffalo, New-York, Monograph #302 (1998)

[14] Litchfield R.C.: Brainstorming Reconsidered: A Goal-Based View. Academy of Managent, July 1, 2008 vol. 33 no. 3 pp.649-668 (2008)

[15] Mongeau P.A., Morr M.C.:Reconsidering brainstorming , ABI/INFORM Global, pg. 14 (1999)

[16] Dennis A.R., Williams M.L.: Electronic Brainstorming: theory, research and future directions. Group Creativity : Innovation through Collaboration, eds. B. Arlington, Oxford University Press (2003)

[17] Holland J.H.: Adaptation in natural and artificial systems. MIT Press Cambridge, MA, USA ©1992 ISBN:0-262-58111-6 (1992)

[18] Koza J.R.: Genetic programming as a means for programming computers by natural selection. Springer, Statistics and Computing, June 1994, vol. 4, issue 2, pp 87-112 (1994)

[19] Dorigo M., Maniezzo V., Colorni A.: Ant system: optimization by a colony of cooperating agents. IEEE Systems, Man, and Cybernetics , vol. 26 issue:1, pp. 29-41, ISSN: 1083-4419 (1996)

[20] Nakrani S., Tovey C.: On Honey Bees and Dynamic Allocation in an Internet Server Colony. Proceedings of 2nd International Workshop on the Mathematics and Algorithms of Social Insects, Atlanta, Georgia, USA (2004)

[21] Kennedy J., Eberhart R.C.: Particle Swarm Optimization. Proc. IEEE International Conference on Neural Networks, vol. IV, pp.1942 -1948 (1995)

[22] Moscato P., Cotta C., Mendes A.: Memetic Algorithms. Springer, New Optimization Techniques in Engineering Studies in Fuzziness and Soft Computing, vol. 141, pp 53-85 (2004)

[23] Shi Y.: Brain Storm Optimization Algorithm. Springer, Advances in Swarm Intelligence, LNCS vol. 6728, pp 303-309 (2011)

[24] Xue J., Wu Y., Shi Y, Cheng S.: Brain Storm Optimization Algorithm for Multi-objective Optimization Problems. Advances in Swarm Intelligence, Springer, LNCS vol. 7331, pp 513-519 (2012)

[25] Duan H., Li S., Shi Y.: Predator–Prey Brain Storm Optimization for DC Brushless Motor. Magnetics, IEEE

Transactions, vol. 49 issue:10, pp. 5336 – 5340, ISSN :0018-9464 (2013)
[26] Zhan Z., Chen W, Lin Y., Gong Y., Li Y., Zhang J.: Parameter investigation in brain storm optimization. IEEE, Swarm Intelligence (SIS), 2013 IEEE Symposium, 16-19 April 2013 Singapore, pp.103 – 110 (2013)
[27] Rees J., Koehler G.: Brainstorming, negotiating and learning in group decision support systems: an evolutionary approach. IEEE Proc. of. HICSS-32, ISBN:0-7695-0001-3 (1999)
[28] Krishnanand K.R., Hasani S.M.F., Panigrahi B.K., Panda S.K.: Optimal Power Flow Solution Using Self–Evolving Brain–Storming Inclusive Teaching–Learning–Based Algorithm. Springer, Advances in Swarm Intelligence, LNCS vol. 7928, 2013, pp 338-345 (2013)
[29] Gilliss N., Glineur F.: A continuous characterization of the maximum-edge biclique problem, ACM DL, Journal of Global Optimization archive, vol. 58 issue 3, March 2014, pp. 439-464 (2014)
[30] Alexe G., Alexe S., Crama Y., Foldes S., Hammer P., Simeone B.: Consensus algorithms for the generation of all maximal bicliques. Elsevier, Discrete Applied Mathematics 145 , pp. 11 – 21, (2004)
[31] Sim K., Li J., Gopalkrishnan, V., Liu G.: Mining maximal quasi-bicliques: Novel algorithm and applications in the stock market and protein networks. Statistical Analysis and Data Mining**, v**ol. 2, issue 4, pp. 255–273 (2009)
[32] Mafteiu-Scai L.O.: Improved the Convergence of Iterative Methods for Solving Systems of Equations by Memetics Techniques. International Journal of Computer Applications (0975 – 8887) vol. 64, no.17 (2013)
[33] Al-Dahoud A., El-Emary I.M.M., El-Kareem M. A.: Application of Genetic Algorithm in Solving Linear Equation System. MASAUM Journal of Basic and Applied Science, vol.1, no.2 (2009)
[34] Ikotun Abiodun M., Lawal Olawale N., Adelokun Adebowale P.: The Effectiveness of Genetic Algorithm in Solving Simultaneous Equations. International Journal of Computer Applications (0975 – 8887) vol. 14 no. 8 (2011)
[35] Grosan C., Abraham A: Multiple Solutions for a System of Nonlinear Equations. International Journal of Innovative Computing, Information and Control ICIC International , ISSN 1349-4198, (2008)
[36] El-Emary I.M.M., Abd El-Kareem M.M.: Towards Using Genetic Algorithm for Solving Nonlinear Equation Systems. World Applied Sciences Journal 5(3): pp. 282-289, ISSN 1818-4952, (2008)
[37] Grosan C., Abraham A: A New Approach for Solving Nonlinear Equations Systems. IEEE Transaction on Systems, Man and Cybernetics-part A: Systems and Humans, vol. 38, no. 3 (2008)
[38] Mastorakis N.E.: Solving Non-linear Equations via Genetic Algorithms. Proceedings of the 6th WSEAS Int. Conf. on Evolutionary Computing, Lisbon, Portugal, June 16-18, pp. 24-28 (2005)
[39] Zhou Y., Huang H., Zhang J.: Hybrid Artificial Fish Swarm algorithm for Solving Ill-Conditioned Linear Systems of Equations. ICICIS 2011 Proceedings, Part 1, Springer, pp. 656-662 (2011)
[40] Mafteiu-Scai L.O., Mafteiu-Scai E.J.: Solving Linear Systems of Equations using a Memetic Algorithm. International Journal of Computer Applications (0975 – 8887) vol. 58, no.13 (2012)
[41] Mafteiu-Scai L.O.: A New Dissimilarity Measure between Feature-Vectors. International Journal of Computer Applications (0975 – 8887) vol. 64, no.17 (2013)
[42] Boden M.A.: Creativity and artificial intelligence. Elsevier, Artificial Intelligence 103 pp. 347-356, (1998)

International Journal of New Computer Architectures and their Applications (IJNCAA) 5(1): 19-28
The Society of Digital Information and Wireless Communications, 2015 ISSN 2220-9085 (Online); ISSN 2412-3587 (Print)

Sensors-enabled Smart Attendance Systems Using NFC and RFID Technologies

Cheah Boon Chew,Manmeet Mahinderjit-Singh, Kam Chiang Wei, Tan Wei Sheng, Mohd Heikal Husin, Nurul Hashimah Ahamed Hassain Malim

School of Computer Sciences, University Sains Malaysia,11800 Penang Malaysia
cbchew.ucom12@student.usm.my; manmeet@usm.my; [kcwei; twsheng].ucom12@ student.usm.my; [heikal; nurulhashimah]@usm.my

ABSTRACT

Attendance system is a system that is used to track the attendance of a particular person and is applied in the industries, schools, universities or working places. The traditional way for taking attendance has drawback, which is the data of the attendance list cannot be reuse and tracking and tracing student's attendance is harder. The technology-based attendance system such as sensors and biometrics based attendance system reduced human involvement and errors. Thus in this paper, a NFC-based attendance system is presented. A comparative study between this both NFC and RFID is also discussed thoroughly, especially in terms of their architectures, functionality features, benefits and weakness. Overall, even both NFC and RFID attendance system increases the efficiency in recording attendance, NFC system is providing more conveniences and cheaper infrastructure in both operational and setup cost.

KEYWORDS

Attendance system, Sensors, Near field communication (NFC), Radio frequency IDentification (RFID), Tags.

1 INTRODUCTION

Successful schools begin by engaging students and making sure that they will come to school regularly, so the attendance rate become very important. Attendance system is a system that is used to track the attendance of a particular person and is applied in the industries, schools, universities or working places. The attendance rate will be calculated based to the average percentage of students attending school in every class of the course. The attendance rate is important because students are more likely to succeed in academics when they attend class consistently. It's difficult for the lecturer and the class to build their skills and progress if a large number of students are frequently absent. Moreover, the students have given the right to have their own time management in university. This will cause the attendance rate of the class become a major problem because some student may choose to absent from the class. Therefore, students from university in Malaysia are required to attend the class not less than 80% per semester otherwise student will be barred from taking any examinations.

The traditional way for taking attendance has drawback, which is the data of the attendance list hard to reuse. If the lecturer wants to calculate the percentage of the students that attend to the class, he/she has to calculate manually or input by typing. This also easy lead to human error such as the lecturer may wrongly. The technology-based attendance system will reduce the human involvement and decrease the human error. There are various types of attendance systems that are applied in different fields. Mostly, the working places are still using the punch card system. But some of them had integrated their system into biometric attendance system. The biometric attendance system is based on fingerprint identification using extraction of minutiae techniques and it is very reliable and convenient to verify the identity of people. Human fingerprint is read by the reader to take the attendance as the uniqueness of human's fingerprints [1]. Another technology is Radio Frequency Identification (RFID) based attendance system that consists of RFID Reader, RFID Tag, LCD displays and

microcontroller unit [2]. RFID can be interfaced to microcontroller through Universal Synchronous, Asynchronous Receiver Transmitter (USART) [2]. Data is transferred from RFID cards to reader and from there to the microcontroller. These attendance systems are important for large scale organizations in order for them to process a large number of workers' attendances rapidly. It makes the work more efficient and produces accurate results.

The NFC based attendance system is another means to tackle conventional attendance system problems.above. Because the installation cost of NFC based attendance system is lower than the other advance attendance system likes the fingerprint attendance system. The main advantages of the NFC are the simple and quick way of using it and the speed of connection establishment is fast [4]. Besides that, other important advantages of NFC technology have also included the transmission range of NFC devices. The transmission range is so short, when the user separates the two devices more than the limited range, then communication is broken [5]. The NFC based attendance system can process the data collected in a quicker way compared to manual system which need to enter the data one by one. Besides, all the data will be saved on the server and this can avoid of losing any students' attendance. Students can also check their attendance rate using their smartphones through the login system from time to time to avoid any miss entering of attendance. Thus the main objective of this paper has present a new NFC based attendance system capable of recording and tracking students' attendance in the classroom. Second objective will look into two-different sensor based attendance system which is RFID and NFC-enabled.

The remainder of the paper is organized as follows, in section 2, it introduces about background and related work on the existing attendance system. Section 3 look into the Near Field Communication based attendance, the way the near field communication works and the units used to develop the (NFC) Attendance Based system project. Section 4 and 5 discussed NFC-enabled Attendance System and RFID –enabled Attendance System. Section 6 present discussion followed by a conclusion.

2 BACKGROUND & RELATED WORK ON TECHNOLOGY BASED ATTENDANCE SYSTEM

There have some researches that develop technology-based attendance system. Basically technology-based attendance system can divided into two groups; i) Biometric-based Attendance System and ii) Sensor-based Attendance System. Next we will discuss some of related systems within this two group.

2.1 Biometric-Based Attendance System

Biometric-based attendance system recognize a person identity based on the biological characteristic such as fingerprint, hand geometry, voice, retina, iris and face recognition which reliably distinguishes one person from another or used to recognized the identity. They have five subsystems: data collection, signal process, matcher, storage and transmission. However, the biometric system is suitable for highly secured system and mostly the biometric system is expensive [9]. Kadry and Smaili [10], implement an attendance system based on iris recognition. The system takes attendance as follows ;a) a digital image of one person's eyes to be verified is captured ;b) feature extracting algorithm is carried out;c) minutiae are extracted and stored as a template for verifying later; d) eople to be verified place his eye on the iris recognition sensor and e) matching algorithm is applied to match minutiae. Talaviya et.al [11], implement a system that takes attendance of student by using fingerprint sensor module. When the student enrolls his/her finger on the finger print sensor module, his/her fingerprint will matched with database to mark the attendance. Chintalapti and Raghunadh [12], implement an automated attendance management system based on face detection and recognition algorithm. Every time the student enter the class, his / her images will be capture by the camera placed in the entrance. The images will retrieve the identity of the student and take attendance for that student. They use Viola-Jones algorithm for

the face detection part. There are five performance evaluation conditions used by them for the face recognition part, which are PCA + Distance Classifier, LDA + Distance Classifier, PCA + SVM, PCA + Bayes, LBPH + Distance Classifier. As a whole biometrics systems are known for its more expensive means of setup and operational costs. In term of its accuracy, biometrics attendance system prevents cheating and has lesser false alarm rate.

2.2 Sensor-Based Attendance System

Barcode technology is a method of identification, which is used to retrieve in a shape of symbol generally in bar, vertical, space, square and dots which have different width with each one A reader of scanners are required to identify the data that represent by each barcode by using light beam and scan directly to barcode. During scanning process, a scanner measured intensity of reflected light at black and white region. A black region will absorb the light, meanwhile white region will reflect it [9]. Smart card is built with variety of chip with a simple memory consisting of byte of information may have range from 1K up to 64K of microcontroller or multi-application memory. Smart card can use as individual identification, building access and network access are part of a multi-tiered program that is in the final stages of rolling out. The data in smart card can be read when a physical contact has a reader [9]. Meng and Mahinderjit [9], implement an attendance, which take attendance by using RFID. Figure 1 shows the system architecture of the RFID attendance system[9].

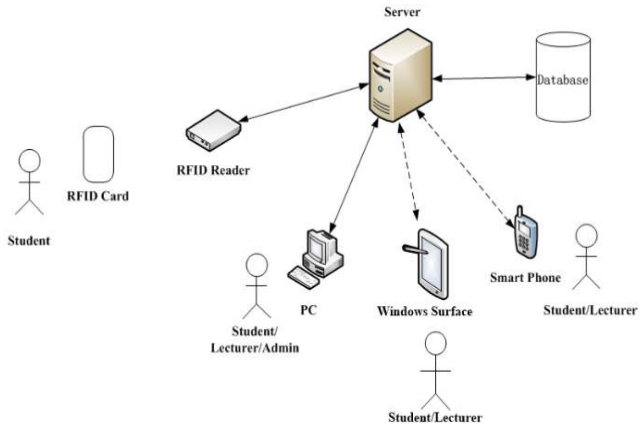

Figure 1. System Architecture for RFID attendance system[9].

RFID is an automatic identification method, whereby identification data are stored in electronic devices, called RFID tags (Transponders), and RFID readers (interrogators) retrieve these data. Based on the figure, students only needs to place their RFID tags which contain a unique id number on the reader and their attendance will be taken immediately. Every time the student enters / leaves the class, they need to scan their RFID tags with RFID reader. The RFID reader will read the identification code in the RFID tags and transfer the code to the PC, which connected with USB. A program in PC will retrieve the student's identity from the database using the identification code that received and take attendance for that student. RFID based attendance systems are costly and requires extra infrastructure for its operational. Ayu and Ahmad [13], implement NFC supported attendance system in a University Environment named as TouchIn. Before the class start, the lecturer will run a mobile application on his/her own NFC-enabled smartphone, students that want to take the attendance will run another mobile application which will fetch the student ID from file, read the device ID and beam (send) it to the lecturer's device by simply touching the device. The attendance of the student will be taken. This system has disadvantages if compared to this project such as the accuracy is low on the identification part. The student can help his/her friend taking attendance, although his/her friend is absent. They just need to borrow their smartphone to his/her friend and his/her friend can scan the

lecture's device with the smartphone and attendance will be taken.

3 NEAR FIELD COMMUNICATION ATTENDANCE SYSTEM OVERVIEW

A smartphone is a mobile phone with an operating system. Smartphones typically include the features of a phone with those other popular mobile devices, such as personal digital assistants, media player and GPS navigation unit. Most have a touchscreen interface and can run 3rd-party apps, and are camera phones. Later smartphones add broadband internet web browsing, WI-FI motion sensor and mobile payment mechanisms. Soomro, 2013[5], shows that almost 2 billion people all around the world will be using Smartphones, Laptop, Tablets and Desktops by 2014. This rapid growth for smartphones over the years shows the amount of users of smartphones are increasing and this means it will be easier to just put in an NFC tag on each of the smartphones for people to use it and it'll be more convenient. Besides that, most of the Android smartphones has the NFC tag.

NFC stands for Near Field Communication which is a wireless communication interface for the devices that equipped with NFC [3]. The working distance for NFC is just up to 10cm only, but the set up time is just less than 0.1s [3]. There are 2 kinds of modes which is active mode and passive mode for the NFC devices [3] (as shown in Table 1). The device which generates its own RF field is called an active device, while the device which retrieves the power from another device is called a passive device. Besides that, the device which starts the communication is called an initiator. The initiator is only in active mode and could have many targets which either active mode or passive mode. One initiator can only communicate with one target at one of time while other relevant targets will be ignored at first [3]. Hence, the broadcasting message is impossible in the NFC.

Table 1. Possible Combination Active/Passive with Initiator/Target [3]

Mode	**Initiator**	**Target**
Active	Possible	Possible
Passive	Impossible	Possible

NFC works on the principles of sending information over radio waves [3]. The technology used in NFC is based on Radio Frequency Identification (RFID) idea which uses the electromagnetic induction to transfer information. The transmission frequency of NFC is 13.56 MHz with the transfer speed of 424 Kbps, which is fast enough for data transfers [3]. NFC is currently supported for peer-to-peer mode, which means 2 devices with NFC-enabled are able to exchange information between each other.NFC has also supported read/write mode. An active device is able to read the information from another device. For example, a smartphone is reading the information from an NFC advert tag. Lastly, NFC device is able to act as a credit card or a contactless card in order to make payments in card emulation mode.

4 SYSTEM ARCHITECTURE NFC-ENABLED STUDENT ATTENDANCE SYSTEM

The proposed system in this project is a web based attendance system using NFC technology in Android smartphones. The system has two main components which are reader unit and server unit which is hardware and software components respectively. The hardware component of reader unit are NFC enabled Android smartphone and student materials card with NFC tag while the server unit is the computer that host web services and databases. This part of the paper consists of, how two sections that are User Interface which explains about the user interface of the project and the System interface which also explains about the System interface about how it works and how is it done. The figures 2 show the examples of the interfaces.

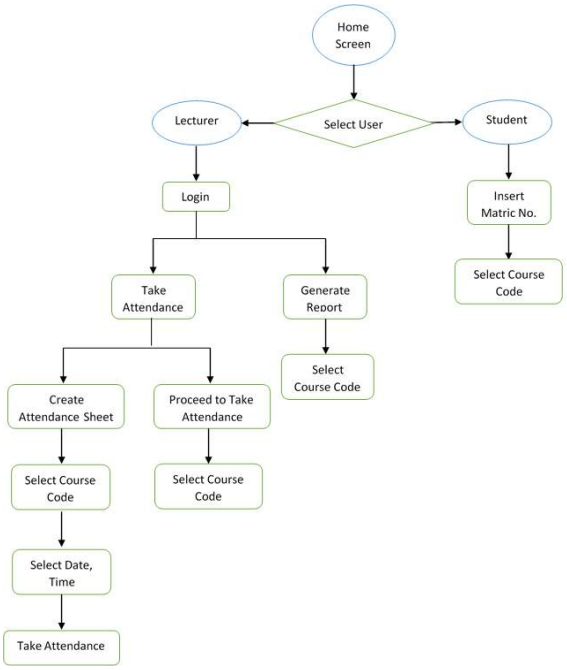

Figure 2. NFC-enabled Attendance System Interface

According to above figure, there are two classes of user which is the students and the lecturers.

Next we will discuss on the NFC based attendance and this is shown in Figure 3. Firstly, the administrator of the school needs to create an account for the students and lecturers in order for them to login to the system. The admins are able to update the account and delete the account in case of wrong data is entered. Besides that, admin should generate a list of the students that enrolled in the particular subject for lecturers' reference. On the mobile app, students need to login to their account in order to register for the attendance for each class that they attend. They also can view the amount of attendance for respective subjects on their phones. For the lecturers, they need to login to the system first and select the subject every time they want to record the attendance. The lecturers will be able to calculate the total attendance of the class and generate a report about the attendance rate at the end of the semester.

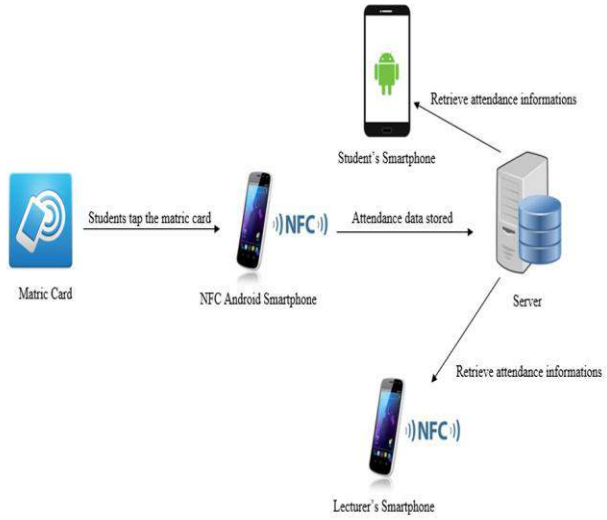

Figure 3. NFC-enabled System Architecture

The student has to tap the matric card towards the NFC android Smartphone and automatically the attendance will stored in the server. For the lecturers to check the attendance of the student, the system will retrieve the attendance information from the server to the Lecturer's smartphones. The system also does give the information to student's as well to check for them whether the days they have attended and did not attend for their own record. In this project, the implementation strategy used is bottom-up strategy. The implementation start from the lowest level of software unit such as view report, take attendance, generate reports and etc., which are the function within the student module and lecturer module. Then, all the lower units are linked together to form higher level units such as NFC module, student module and lecturer module. Next, the modules were designed and implemented, followed by the subsystems and finally the complete system.

In order to do the testing, users log in as the administrator, lecturer and students. RFID system, web page system, smartphone application and tablet application were fully tested. Below are the results of the functional testing shown in Table 2. Testing is the process of examining a component, subsystem, or system to determine its operational characteristic and whether it contains any defects. The lecturer will be assigned an account with ID

and password. They need to login to the system with their corresponding authentication to create an attendance sheet of the conducted classes and view the report of the attendance of the student. They only can create the course they have enrolled. The student needs to approach their NFC tag (Matric card) to login, system to view their attendance report. The student can only take 1 time attendance in each attendance sheet of class conducted. Students who enroll for the course only can take the attendance.

Table 2. NFC-based Attendance System Functional Testing

User	Function	Description	Working
	Select User Type	Select the user type based on their type	YES
Lecturer	Login	Login with ID and password	YES
	Home page	Display option for lecturer	YES
	Create attendance sheet	Select course, time and date to create a new attendance sheet	YES
	Take attendance	Able to manually take attendance or read student's NFC tag	YES
	Proceed to take attendance on the current sheet	Continue with take attendance activity without create a new sheet	YES
	Generate report	Display a list of attendance of the student by selecting the course	YES
	View particular student attendance report	click on the student in the report to view the detail report	YES
	Filter attendance by date	Display a list of student attended the class on the selected the date	NO
Student	Login with NFC tag	Scan NFC tag to view report	YES
	View personal attendance	Display attendance of the student	YES
	View date and time of Class, attendance and absence	Click on the attribute to view the date and time	YES

The lecturer will be assigned an account with ID and password. They need to login to the system with their corresponding authentication to create an attendance sheet of the conducted classes and view the report of the attendance of the student. They only can create the course they have enrolled. The student needs to approach their NFC tag (Matric card) to login, system to view their attendance report. The student can only take 1 time attendance in each attendance sheet of class conducted. Students who enroll for the course only can take the attendance.

5 RFID-ENABLED ATTENDANCE SYSTEM MANAGEMENT

In this section, RFID-enabled Attendance System Management presented by Meng and Mahinderjit-Singh[9] will be discussed. This project has two parts one is web page system and the others are smartphone and tablet application.After student enters or leaves the classroom by scanning RFID card lecturer could view the attendance situation of the class and the movement of different student through web page system, smartphone system and tablet system. Student could view his attendance only and movement only through web page system, smartphone system and tablet system. Besides that, lecturer or student could track the attendance history by both systems. This project is expected to provide a smart attendance system for different users to sign attendance and view situation of attendance. When the users enter the classroom or lecture hall, they have the option either to swipe their card on the reader or simply let the card detected by the reader. The card attached with RFID tag, which can be detected by the reader as long as certain range of distance between the tag and the reader is complying. Once the reader detect and obtain the information, it will be then saved to its own database automatically. In addition the lack of automated attendance system in the School of Computer Sciences especially in our lecture halls is our main motivation undesigning this prototype. Figure 3 shows the data flow of the whole system.

For web page system, Meng and Mahinderjit Singh [9] have used ASP.Net, CSS, and JavaScript through Microsoft Visual Studio 2013 to implement. The other two are Windows Phone application and Windows Surface application, in this application, we will adopt Windows Phone 8 platform to implement. The simulation algorithm, which is Monte Carlo, will be integrated as well. Monte Carlo simulation is a method for exploring the sensitivity of a complex system by varying parameters within statistical constraints.The system includes two different parts. The first part is the web page platform. The second is the ubiquitous platform. All this parts are integrated to function together. The system is able to function according to three different user roles. This roles and privileges follow the access control and authorization principles. We are following the Discretionary Access Control (DAC) model [12]. Among the three users listed below are:

a) Administrator- an user with the highest privileges and authorization. Typically, an

administrator can enroll students and lecturer, register course for students and lecturers, using Monte Carlo simulation.

b) Lecturer- an user who has enrolled by administrator. Typically, a lecturer can check and track the students' attendance and class movement.

c) Student- an user who has lowest privileges and authorization. Typically, a student can only check his attendance and class movement.

Next, the hardware used in the attendance system is presented next.

5.1 RFID Hardware

In RFID platform, MIFARE522_MODULE has been utilized as hardware reader. The tag used here is from the class of passive tag. RFID attendance platform has three main functions; which are attendance recording, duplication reading& miss reading, and monitoring of attendance record by lecturer, Figure 4 shows the RFID model and tags.

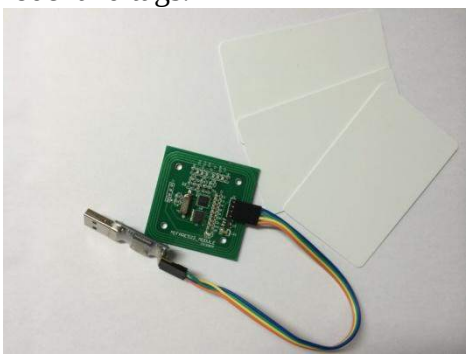

Figure 4. RFID Reader and Tags

Next is the detail of each function.

5.2 Smartphone and Tablet Platform (Windows Phone & Windows Surface)

For Windows Phone and Windows Surface platform, each of one has three main functions; which is the user login and monitoring of attendance records done by student and lecturer. All the capabilities of the system are listed below.

a) Login/Logoff Function

When user login the system (Windows Phone & Windows Surface part), user has to enter their correct username, password and choose correct use type. Username is the users email address, and initial password is user matric number or staff number. If one of the information does not correct user cannot login and system will show an error message to user.

b) Lecturer Checking Student Attendance & Movement

After lecturer login the Windows Phone & Windows Surface system, he/she could press View Attendance button to check student attendance for each class, which he taught. Next the system will show the course list base on teaching year, after the lecturer press one of the courses, system will list all the classes, which are set by admin. Next lecturer could press one of the classes and system will jump to Student Attendance interface. System will show the situation of attendance and if lecturer presses the Statistic button, system will jump to next interface and show the attendance statistic of this class. Next, lecturer could press any of the students to check his/her movement of this class. After lecturer press one of the students, system will jump to Student Movement interface and it will show the movement record of this student. At the bottom of this interface, system shows the time of this student staying in classroom. At last but not least, lecturer could press back button to check movement of another student. Figure 5 and Figure 6 show the interface of lecturers check student attendance.

Figure 5. Lecturers Check Students Attendance (Windows Phone)

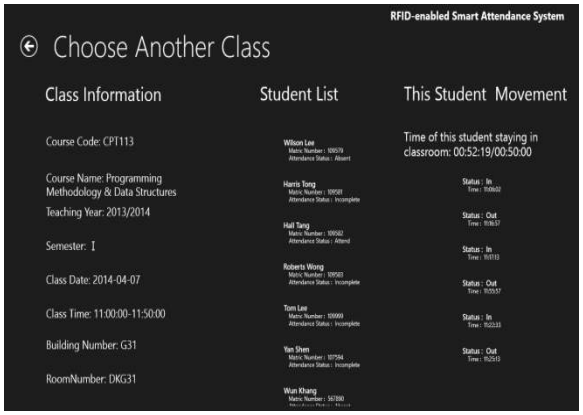

Figure 6. Lecturers Check Students Attendance (Windows Surface)

c) Student Checking Attendance & Movement

After student login the smartphone system or tablet system, he could press View Attendance button to check his attendance for each class. Next the system will show the course list base on teaching year, after the student press one of the courses, system will list all the classes, and his attendance status. And then, student could press one of the classes and system will jump to Student Movement interface and it will show his movement record. At the bottom of this interface, system shows the time of this student staying in classroom. At last but not least, student could press back button to check his movement of another class. Figure 11 and Figure 12 show the interface of students check student attendance.

d) RFID-Attendance event Duplication Reading

The aim of doing a duplication reading is in case of someone duplicate the card and sign attendance for students. After the students scan the card, system will check the validity of the card. If the card is a fake one, system will beep three times and it will not be record in the system. If the card is a real one, system will record the data in the system.

e) RFID-Attendance event Miss Reading

The aim of miss reading is to inform the user of event in which the automated system fails to record an attendance record. One way of tackling this is right after a student scans his card, the system will give a feedback by beep sound and send an email to student. If the student do not hear the beep sound and do not receive the email, it means system did not detect the card and the student will have to scan his/her card again.

f) Email Generation

In this function, system will send an email to user in two situations. One is when students scan the card, the system will send an email to students and inform them their current status. Second, if a person uses a fake card to sign attendance for a student, system will find it out and send an email to the real user to inform him that someone has duplicated their card.There are two scenarios in which an attendance system can be attack in term of its security. First scenario is when a student is absence from a class but would trick the system in showing he has attended all are 80% of the course class. The second scenario is when a student that has not enroll for the course but would like to join it without paying the fees for it.

6 DISCUSSION

In this section, benchmarking between various methods of attendance systems, comparison between RFID and NFC and security challenges within the attendance systems.

6.1 Comparisons Between Different Attendance Systems

No system is perfect. Every system will have their own advantages and disadvantages. Table 3 shows the comparison of several types of attendance system that mentioned earlier with the proposed solution. Table 4 shows the comparison between NFC and RFID. The proposed solution is a multifactor identification system, which integrate face detection and recognition function into sensor technology, NFC. Different aspect has been analysis through the comparison such as:

- Take student Attendance – The system can take the student's attendance successfully and provide information about student attendance status (Absent / Attend).
- Reuse Student Attendance Information – The student attendance information can be reuse for other system. The system can provide the statistic about class attendance and lecturers no need calculate on their own. The data about attendance information of each class will store in the database automatically.
- Prevent Cheating Issue – The system has higher accuracy on the identification part and eliminates the cheating issue. The student cannot take attendance on behalf of another student such as the student may help his / her friend for taking attendance but his / her friend is absent.
- Fault Tolerance – The taking student's attendance process still on-going if the system encountered any error. The system will become flexible and fault tolerance if the user can choose another method for taking student's attendance without any human involvement.
- Price – The implementation and employment cost of the system.

Table 3. Comparison of Several Types of Attendance system

Attendance System	Take student Attendance	Reuse Student Attendance Information	Prevent Cheating Issue	Fault Tolerance	Price
Traditional	√				Cheap
Biometric	√	√	√		Expensive
Barcode	√	√			Cheap
Smart Cards	√	√			Cheap
RFID	√	√			Medium
NFC	√	√			Medium

Overall, both RFID and NFC provide an efficient method of tracking and monitoring of students and the price of functional and operational are both medium.

Table 4. Comparison between RFID and NFC-based attendance system

Properties	RFID	NFC
Infrastructure	Additional readers and tags needed	Only Smartphone with in-built NFC (or else additional NFC tag)
Conveniences for setting up	Hard to setup	Medium
Conveniences for usage	Good	Excellence
Cost	High	Low
Efficiency in tracking & monitoring	Excellence	Excellence
Security/Functionality Features	Added functionality such as miss reading, duplication, basic security features	Minimal security features

Overall performance based on the comparison between RFID and NFC shows that both technologies have their weakness and benefits. However, in terms of conveniences, NFC-based attendance provide better performance. However, the current NFC attendance system only has minimal security features and can be improvised further in the future.

6.2 NFC/RFID Security Attacks in Attendance System & Mitigation

The first scenario in which an absent student could trick the system by the following technique such as; i) DOS attack – to compromised the server availability by performing jamming of server by multiple packet requests; ii) manipulation of data by either deleting and inserting additional data. This act can be done on the server by either an insider or an outsider (with the help of man in the middle attack) and finally iii) tag swapping in which genuine's tag data is replaced without the knowledge of its user. The second scenario on the other hand is an act of masquerading in which a genuine users information is manipulated by act such as eavesdropping and man-in-the middle.

This valid information is then changed and added on blank NFC tag. The system will be unable to detect this kind of behavior unless detection and constant monitoring mechanism is planted in hand. Overall, the effect of the attacks taking place compromises the availability, confidentiality and integrity of the user, devices and servers. The mitigation for data manipulation on server and tag would be to ensure data is trusted to be alive by usage of random numbers mechanism. Attack such as man in the middle and eavesdropping could be mitigated as well with the use of either nonces or high level random number generators. In addition, key encryption between the server and NFC tag by using either symmetric or asymmetric encryption key will also solve the issue of data manipulation and insertion, tag swapping and tag cloning since the integrity of user digital identity can be maintained.

7 Conclusion

In this paper, sensors based attendance system is presented. Two technologies, mainly the NFC and RFID are used. Architectures and functionality of both technologies are discussed in depth. Benchmarking between these two technologies with other types of attendance systems are also given. Overall, a brief discussion on the security related to both NFC and RFID is demonstrated. In the future, further work in adding functionality in term of security on the NFC-based attendance system will be done. In addition, the merges between biometrics identifiers such as facial features and sensors features such as NFC and RFID will also be implemented. As a whole, this new technology, NFC based attendance system is projected to provide some beneficial to the current generation Y students in universities. The main contribution with such move is to completely utilized the smartphone capabilities to maximum and to take advantage with the current smartphone phenomena among young users.

REFERENCES

1. C.Saraswat, A.Kumar, " An Efficient Automatic Attendance System using Fingerprint Verification Technique ", ChitreshSaraswat et al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 264-269
2. T.S.Lim, S.C. Sim,M.M. Mansor, "RFID Based Attendance System", 2009 IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009), October 4-6, 2009, Kuala Lumpur, Malaysia.
3. E.Haselsteiner, K. Breitfuß, "Security in Near Field Communication (NFC)", Philips Semiconductors Mikronweg 1, 8101 Gratkorn, Austria.
4. M.Ervasti, M.Isomursu, M.Kinnula, "Experiences from NFC Supported School Attendance Supervision for Children", 2009 Third International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies
5. T.R Soomro," Impact of Smartphones's on Society"College of Engineering & Information Technology Al Ain University of Science & Technology, Al Ain, United Arab. European Journal of Scientific Research 2013
6. O.K Kerem, V.COSKUN, N.Mehmet, B. OZDENIZCI, "Current Benefits and Future Directions of NFC Services", 2010 International Conference on Education and Management Technology（ICEMT 2010
7. S. K. Jain, U. Joshi, B. K. Sharma, "Attendance Management System," Masters Project Report, Rajasthan Technical University,Kota.
8. M. K. P. Basheer, C. V. Raghu, "Fingerprint attendance system for classroom needs," in Proc. India Conference (INDICON), 2012 AnnualIEEE, pp. 433-438, 7-9 Dec. 2012.
9. Z.Meng, M.Mahinderjit-Singh, "RFID-enabled Smart Attendance Management System" 2014, Lect. Notes Electrical Eng., Vol. 329, James J. (Jong Hyuk) Park et al. (Eds): Future Information Technology - II, 978-94-017-9557-9, 328439_1_En.
10. S,Kadry; K.Smaili , "A Design and Implementation of A Wireless Iris Recognition Attendance Management System", ISSN 1392 – 124X Information Technology and Control, 2007, Vol.36, No.3.
11. G.Talaviya; R.Ramteke; A.K.Shete, "Wireless Fingerprint Based College Attendance System Using Zigbee Technology", International Journal of Engineering and Advance Technology (IJEAT), ISSBN: 2249-8958, Volume-2, Issue-3, February 2013.
12. S.Chintalapati; M.V. Raghunadh, "Automated attendance management system based on face recognition algorithms," Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on , vol., no., pp.1,5, 26-28 Dec. 2013, doi: 10.1109/ICCIC.2013.6724266
13. M. Ayu, B. Ahmad, 'TouchIn: An NFC Supported Attendance System in a University Environment', International Journal of Information and Education Technology, vol. 4, no. 5, pp. 448-453, 2014.

International Journal of New Computer Architectures and their Applications (IJNCAA) 5(1): 29-38
The Society of Digital Information and Wireless Communications, 2015 ISSN 2220-9085 (Online); ISSN 2412-3587 (Print)

Testing Resource Allocation for Modular Software using Genetic Algorithm

Md. Nasar and Prashant Johri
School of Computing Science and Engineering
Galgotias University, Gr. Noida, INDIA
nasar31786@gmail.com, johri.prashant@gmail.com

ABSTRACT

Software testing is one of the important steps of SDLC. In software testing one of the important issues is how to allocate the limited resources so that we finish our testing on time and will deliver quality software. Number of Software Reliability Growth Models (SRGM) has been developed for allocating the testing resource in the past three decades but majority of models are developed in static environment. In this paper we developed model in a dynamic environment and also the software is divided into different modules. We also used Pontryagin Maximum principle for solving the model. At last one numerical example is solved for allocating the resource for a given module. For allocating resource optimally we used Genetic Algorithm (GA). GA is used as a powerful tool for solving search & optimization kind of problems.

KEYWORDS

Software Reliability, Software Reliability Growth Model (SRGM), Testing Effort Allocation, Modular Software, Genetic Algorithm (GA)

1 INTRODUCTION:

Here, we have proposed an alternate rationale for optimally allocating the resources for software consisting of modular structure using Genetic Algorithm under dynamic environment. These days software development is going to be very complex, for software development it is not possible to develop software by a single developer. Big software systems are generally developed in a multi-language and distributed environment and are run simultaneously on a variety of platforms. Software development is a very multifaceted process involving different factors. Though high reliability will be assured for hardware components, but for the software the same might not be right, as it is completely developed by human being. A fault has been introduced when a mistake occurred in software development by human being. A failure occurs when code enclosing the fault is executed [1]. Software bugs can be introduced into the software during any phase of the development process. These bugs should be recognized and removed by the software developer. Software reliability engineering is focused on engineering techniques for developing the software and maintaining software whose reliability can be quantitatively calculated. This employs different kinds of tools and scientific techniques during testing of the software to remove as many latent faults in the software as possible. Software reliability growth models (SRGMs) are the tools of Software Reliability Engineering (SRE) used to predict and estimate the reliability of software during testing and operational phase. To guarantee the quality of software product, software testing plays vital role. To verify and validate software reliability, software systems must be tested thoroughly before their launch in to the market. Software testing is one of the major stages of software development life cycle (SDLC). In this stage software is tested to identify and correct the faults. The testing is divided in different stages: Unit/Module testing, Integration testing and system testing [2]. Each and every software unit is tested separately during the first stage and then we integrated different units, which are tested in the integration testing. At the end of testing phase, the software system into which different units are integrated is tested under the simulated user environment this testing is called system testing. It is a well known fact that the testing phase of a software development life cycle is time consuming and very costly process. During software testing phase huge resources are consumed, which ensure the high quality and desired level of reliability. It has been

observed that these testing activities consume approximately 40%-50% amount of resources available for the software development [3]. Typically, unit/module testing is the very time consuming part of testing to be performed. But, at the same time the testing resource available during the testing time is limited. These testing resources include resources like human power, CPU hours, and elapsed time, etc. Hence, to develop high reliable software, a project manager should determine in advance how to effectively allocate these resources among the various unit/modules. Such kind of optimization problems is called "Resource Allocation problems". Therefore it is a essential problem for project managers to distribute the limited testing-resource in an efficient manner.

The main aim of all these research discussed earlier was to allocate testing resources to each software module or allocating testing resource for whole software based on time statically, so that the outcome i.e. maximization of reliability or maximization of number of faults removed or the remaining number of faults can be minimized after the testing phase is over. For solving the testing and debugging effort allocation problem formulated in this research paper we use Genetic Algorithm (GA). GA is used as a powerful tool for solving search & optimization kind of problems. In a Genetic Algorithm (GA) the problem is encoded in a series of bit strings that are manipulated by the algorithm. Genetic Algorithm (GA) was introduced by John Holland for the formal investigation of the mechanisms of natural adaptation [4].

The paper is subdivided into the following sections. Section two describes the related work of this research, three describes basic assumptions, and four describes the model development. In section five we describe cost optimization modeling, we discuss the solution Procedure. Section six discusses solution procedure, section seven describes a software system with three modules, and section eight describes a numerical example for distributing testing efforts. Finally, in section nine, we conclude our paper with a discussion on results and findings.

2 RELATED WORKS:

With the rapid growth in Information Technology almost all kind of work is controlled by the software. So the size and complexity of the software is going very high, today majority of software systems are composed of different quantity of units/modules. During the module testing stage, entire testing activities of different units are competing for the limited available resource. Thus, a main difficulty is to distribute the maximum available testing-resource among available software units in an optimal way so that we can test our application and we can remove maximum error in available resources. [5] Have discussed a general idea of the methods that have been developed since 1977 for solving a variety of reliability optimization problems including testing-resource allocation problems. [3] Discussed and solved two resource allocation problems for software-unit testing, taking into consideration that the total number of remaining faults in the software units/modules. When unit testing is finished, the actual amount of residual faults may turn out to be much larger than the mean, and hence [6] investigate a dynamic resource allocation plan for software unit testing. This approach takes into account the variations of the total number of identified faults throughout testing, re-estimates the different model parameters using all the existing fault identification data and allocates the testing resources to the software units dynamically.

Many authors have addressed the optimal resource allocation, Later, [2] investigate the resource allocation problem to minimize the total number of residual faults in the software units/modules with budgetary and reliability constraint and showed that whenever software module testing is complete the actual number of remaining faults may turn out to be much larger than the mean. [7] in their pioneer work used dynamic programming approach to solve an optimization problem for distributing testing resources in software having modular structure .In this research they maximized the total number of faults removed subject to the budgetary constraint, management aspiration on reliability for exponential, s-shaped SRGM and proposed that allocation of efforts should depend

upon the size and severity of faults. [8] Formulated an optimization problem for allocating the available resource among the modules. Author assumed that change point is generated in every module due to change in testing environment, defect density, testing strategy and testing skill such as total fault removal is maximized and cost of development of software will minimize. Author incorporated concept of imperfect debugging. The weightage of every module is specified. Author has also fixed a desired proportion of faults which are removed from each module.

[9] In this paper author solved optimal testing resource allocation problem. Author considered the problem as multi objective problem and the problem is divided in two parts. First consider the testing cost and reliability of the system as an objective. Second, the entire testing resource consumed is also taken into account as the third objective. The advantage of Multi objective approach over single objective approaches is that Multi objective performs well in comparison to single objective.

[10] Formulated an optimization problem in which the total number of faults removed from modular software which includes different types of fault like simple, hard and complex faults. Author developed model for evaluating simple faults, hard fault and complex fault. Following author has maximized the problem subject to the reliability and budgetary constraints. Authors have used genetic algorithm for solving the optimization problem. A mathematical example has been solved to the explanation of formulated optimal effort allocation problem.

[11] Discussed optimal resource allocation for minimization of software cost during the testing phase and operational phase author used optimal control theory for solving the problem.

[12] During software testing resource allocation is one of the major problems. In this paper author discussed about allocation of testing resource in a constrained approach such that the effort can be optimally allocated and overall budget will be minimized. Author proposed an imperfect debugging Software Reliability Growth Model (SRGM) during testing and resource allocation, wherein testing and resource allocation is done based on optimizing the reliability and effort. Here the problem is divided in two parts first by minimizing the total number of remaining faults in the software and second to allocating the testing resources to achieve the maximum reliability. A mathematical example is also solved for allocating the resource and total number of fault removed in the software. [13] Planned a model to guide a trade-off between cost and the number of test cases required to test each module in unit testing phase. They formulated simple optimization problems, which software managers face and provide a systematic solution to handle them. [14] Developed a Genetic Algorithm based approach to search the optimal solution for parallel-series modular software with the objectives of maximizing the reliability and minimizing testing cost using Goel and Okumoto Model [15]. [24] Solved testing resource allocation problem maximized the total number of faults removed from every module under budgetary constraint. [25] Discussed optimal resource allocation plan to minimize the cost of software during the testing phase and operational phase under dynamic condition using Genetic Algorithm (GA) method. Author has developed mathematical model for allocating testing and debugging resource. [16] Developed a two-dimensional SRGM which takes into combined effect of resource limitations and schedule pressure. For developing mathematical model authors used Cobb Douglas production function. Further, the projected two dimensional modeling frameworks are useful for determining testing time and optimal allocation of resources simultaneously to the software system which is available in modular structure. Authors investigated two dimensional optimization problems which assign manpower resources and testing time among the modules so that the total development cost of the software is minimized under the pre-defined amount of faults removal from each modules. In order to solve the formulated resource allocation problem authors used genetic algorithm (GA) technique. In this paper authors assumed that the mathematical model is developed under the perfect debugging environment and also a mathematical example is solved to demonstrate the formulation and solution of the resource allocation problem.

Notations Used:

a_i : Total number of fault content in the i^{th} module.

b_i : Fault exposure rate for i^{th} module.

$w_{i1}(t)$: Proportion of allocated effort for the testing purpose of the i^{th} module at any point of time t'.

$w_{i2}(t)$: Proportion of allocated effort for the debugging purpose of the i^{th} module at any point of time t'.

w_i : Total resource available on hand for testing i^{th} module.

$r_i(t)$: Number of fault removed from the i^{th} module at any point of time't'.

$d_i(t)$: Cumulative number of fault detected till time't' due to the testing effort $w_{i1}(t)$ from the i^{th} module.

c_{i1} : Cost of testing per module testing efforts for i^{th} module.

$c_{i2}(t) = c_{i2}(m_i(t), w_{i2}(t))$ Represents the debugging cost per unit at time't', a function of $m_i(t)$ and $w_{i2}(t)$.

$i = 1, 2, 3, ...n$

3 BASIC ASSUMPTIONS:

The software testing and debugging resource allocation model developed in this article is based on the following assumptions and observations:

1. The software system consists of number of units/modules. The total number of faults residual in each units/module is given by the differential equation.
2. The testing and debugging run concurrently for each module at any point of time't' during the unit/module testing phase. In the unit/module testing phase, every module is subject to failures at random caused by the remaining faults in the module.
3. Whenever a fault is detected it is removed immediately. The number of faults present in each module is fixed and no new faults are introduced to the system.
4. The resource expenditure is fixed for every module/unit. The project manager has to allocate the fixed resources between testing and debugging.

4 MODEL DEVELOPMENT:

The basic structure of the proposed modular software system can be depicted in figure 1. To formulate the mathematics of the proposed model, we are consistent with the assumption that whenever a fault is detected, it is removed immediately and the remaining faults in the module gradually decrease as the testing process goes on. Therefore the following differential equation holds good for each module.

$$r_i(t) = \frac{d}{dt} d_i(t) = b_i w_{i1}(t)(a_i - d_i(t)) \quad i = 1,2,3,.....n \qquad (1)$$

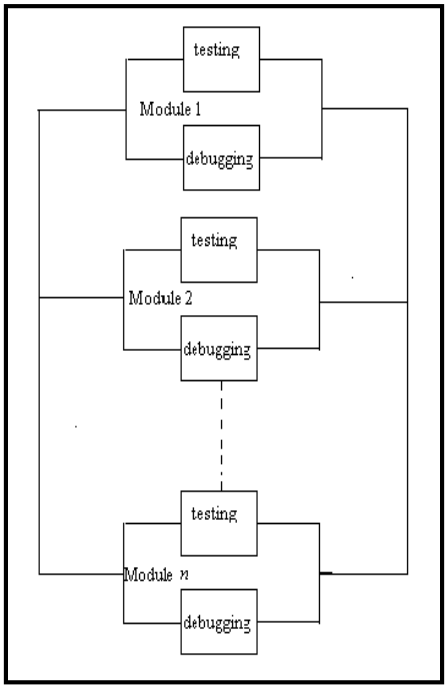

Figure 1: The Structure of Proposed Software System having Modular structure

5 COST OPTIMIZATION MODELLING:

The cost of software system having modular structure in figure 1 at any point of time *t'* will be

$$\sum_{i=1}^{n}\left[c_{i1}w_{i1}(t)+c_{i2}(t)r_i(t)\right] \qquad (2)$$

The cost $c_{i1}w_{i1}(t)$ represents the testing cost and $c_{i2}(t)x_i(t)$ is the debugging cost for i^{th} module. Adding these two costs and summing for the all modules we obtain the total cost at any point of time 't' ,which is given by (2).

Also the total resource for a module is fixed and can be written as

$$w_{i1}(t)+w_{i2}(t)=w_i \ \ for \qquad i=1,2,3,.....,n \quad (3)$$

Note that in the modeling, we have used modular reliability during the unit testing phase that each module achieves a minimum reliability level. For this purpose we have to define the measure of reliability as a ratio of cumulative number of detected faults to the number of initial faults which is equal or greater than a unique number.

$$\frac{d_i(T)}{a_i}\geq d_T\ ,0<d_T<1 \qquad (4)$$

Now suppose the software company wants to allocate the resources during the unit testing phase that minimizes the total expenditure over a given time horizon T. Then the objective function for the software can be given by:

$$J=\min\int_0^T\sum_{i=1}^{n}\left[c_{i1}w_{i1}(t)+c_{i2}(t)r_i(t)\right]dt$$

subject to

$$r_i(t)=\frac{d}{dt}d_i(t)=b_iw_{i1}(t)(a_i-d_i(t))$$

$$\frac{d_i(T)}{a_i}\geq d_T\Rightarrow d_i(T)\geq d_{d_i}(=a_id_T) \qquad (5)$$

where

$$w_{i1}(t)+w_{i2}(t)=w_i \ \ and \ \ d_i(0)=0$$

$$c_{i2}(d_i(t),w_{i2}(t))=c_0(w_{i2}(t))^{d_i(t)},$$

$$(w_{i1}(t),w_{i2}(t))\geq 0 \qquad i=1,2,3,.....n$$

6 SOLUTION PROCEDURE:

To solve the above optimization problem stated in equation (5), let T be an admissible control vector which transfers (d_{i0},t_0) to a target $(d_i(T),T)$, where final state $d_i(T)$ is specified but the final time T is not specified (t_0 and d_{i0} are the initial time and state and both are fixed, i.e. $(t_0,d_i(0)=(0,d_{i0}))$). Assuming that $d_i^*(t)$ is corresponding to $w_1^*(t)$, then by Pontryagin Maximum principle, for $w_{i1}^*(t)$ to be optimal, it is necessary that there exists a non-zero, continuous vector function $\lambda_i(t)$ such that [17]:

The Hamiltonian given by,

$$H(d_i(t),w_{i1}(t),\lambda_i(t),t)=-\sum_{i=1}^{n}\left[c_{i1}w_{i1}(t)+c_{i2}(t)r_i(t)\right]+\sum_{i=1}^{n}\lambda_i(t)r_i(t) \qquad (6)$$

$$w_{i1}^*=\underset{w_{i1}\in T}{Max}\,H(m_i(t),w_{i1}(t),\lambda_i(t),t) \ \ for\,each\ \ i \quad (7)$$

Except at the point of discontinuities of $w_{i1}^*(t)$ and adjoint variables are given by

$$\dot{\lambda}_i=\frac{\partial\lambda_i(t)}{\partial t}=-\frac{\partial H}{\partial d_i} \qquad (8)$$

Finally the transversality or boundary conditions for the above optimization problem can be given as:

$$-\lambda_i(t)\delta d_i(t)\Big|_{t=0}^{t=T}+H(t)\delta t\Big|_{t=0}^{T}=0\Rightarrow$$
$$-\lambda_i(T)\delta d_i(T)+H(T)\delta T=0 \qquad (9)$$

Moreover $\lambda_i(T)\leq 0(=0\,if\ \ d_i^*(T^*)>d_{d_i})$

The Hamiltonian maximizing condition is given by

$$H\left(d_i^*, w_{i1}^*, \lambda_i, t\right) \geq H\left(d_i^*, w_{i1}, \lambda_i, t\right) \quad (10)$$

An optimal solution with $T^* > 0$ must satisfy condition given by equation (7). The adjoint variable $\lambda_i(t)$ is the marginal value of faults at any given time't', which supposed to be negative because increasing the number of faults will increase the cost of debugging. We will interpret *H* as follows: For every module the adjoint variable $\lambda_i(t)$ stands for the future cost incurred as one more fault removed from the i^{th} module at any given time't'. Therefore the Hamiltonian in equation the (6) is the sum of total current cost and the future cost. In brief, Hamiltonian represents the instantaneous total cost of the company at any given time't'. Based upon Pontryagin's maximum principle, that gives the necessary conditions for an optimal solution, below is the necessary condition.

$$\frac{\partial H}{\partial w_{i1}} = 0 \quad for \quad i = 1, 2, 3, ..., n \quad (11)$$

Also the second order Hamiltonian maximization conditions are

$$\frac{\partial^2 H}{\partial w_{i1}^2} \leq 0 \quad for \quad i = 1, 2, 3, ..., n \quad (12)$$

From equation (11), the optimal value of testing efforts and debugging efforts at any point of time *t'* is given by

$$w_{i1}^*(t) = \left(\frac{\lambda_i(t) - c_{i2}(t)}{\frac{\partial c_{i2}(t)}{\partial w_{i1}(t)}} \right) - \left\lfloor \frac{c_{i1}}{\frac{\partial c_{i2}(t)}{\partial w_{i1}(t)}\left(a_i - d_i(t)\right)} \right\rfloor$$
$$for \quad i = 1, 2, 3, ..., n \quad (13)$$

And

$$w_{i2}^*(t) = w_i - \left(\frac{\lambda_i(t) - c_{i2}(t)}{\frac{\partial c_{i2}(t)}{\partial w_{i1}(t)}} \right) + \left\lfloor \frac{c_{i1}}{\frac{\partial c_{i2}(t)}{\partial w_{i1}(t)}\left(a_i - d_i(t)\right)} \right\rfloor$$
$$for \quad i = 1, 2, 3, ..., n \quad (14)$$

Integrating equation (8) with terminal condition, the future cost of removing a fault from the i^{th} module is given by

$$\lambda_i(t) = \lambda_i(T) + \int_t^T \left\lfloor \begin{matrix} b_i w_{i1}(t)\left(c_{i2}(t) - \lambda_i(t)\right) - \\ r_i(t)\frac{\delta c_{i2}(t)}{\delta d_i(t)} \end{matrix} \right\rfloor dt \quad (15)$$

From the equation (15) the future cost of removing a fault from i^{th} module is the sum of terminal cost $\lambda_i(T)$ and the integral of marginal surrogate cost $\frac{\partial H}{\partial d_i}$, from *t* to *T*.

7 DESCRIBING A SOFTWARE SYSTEM WITH THREE MODULES:

During the testing phase of Software Development life cycle (SDLC), a huge amount of resources are consumed to identify and correct the errors existing in the developed software. But in the starting, chief portion of resources is consumed in debugging process. This is due to the uncertain nature of errors. Later on as the potential fault content reduces the cost of testing captures the majority of the expenditure. Therefore, it can be reasonable to assume that the debugging cost gradually decreases with time. In this section we consider a simple example of software system having two modules, described by the figure 2 to solve the resource allocation problem for software systems having three modules, we have considered two cases, firstly when the debugging cost for each module is constant and secondly when the debugging cost follows learning curve phenomenon.

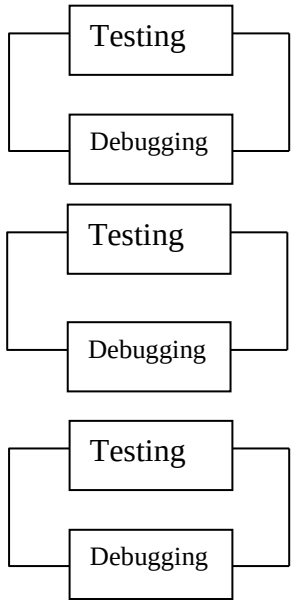

Figure 2: A Software System having three Modules

Here we are assuming that the cost per unit for cumulative fault removed for each module at time 't' is constant.

i.e. $c_{12}(t) = c_{12}$, $c_{22}(t) = c_{22}$ and $c_{32}(t) = c_{32}$ (16)

For the constant fault removal cost function, the objective/fitness function can be written as

$$J = \text{minimize} \int_0^T \left[\begin{matrix} c_{11}w_{11}(t) + c_{12}(t)r_1(t) + c_{21}w_{21}(t) + \\ c_{22}(t)r_2(t) + c_{31}w_{31}(t) + c_{33}(t)r_3(t) \end{matrix} \right] dt$$

subject to

$$r_1(t) = \frac{d}{dt} d_1(t) = b_1 w_{11}(t)(a_1 - m_1(t)) \ , m_1(0) = 0$$

$$r_2(t) = \frac{d}{dt} d_2(t) = b_2 w_{21}(t)(a_2 - m_2(t)), m_2(0) = 0$$

$$r_3(t) = \frac{d}{dt} d_3(t) = b_3 w_{31}(t)(a_3 - m_3(t)), m_3(0) = 0$$

$$m_1(T) \geq m_{d1}, m_2(T) \geq m_{d2}, m_3(T) \geq m_{d3}$$

where

$$w_{11}(t) + w_{12}(t) = w_1 \ , \ w_{21}(t) + w_{22}(t) = w_2,$$

$$w_{31}(t) + w_{32}(t) = w_3;$$

$$(w_{i1}(t), w_{i2}(t)) \geq 0 \quad for \ i = 1, 2. also$$

$$0 \leq w_{11}(t), w_{12}(t) \leq w_1, 0 \leq w_{21}(t), w_{22}(t) \leq w_2$$

(17)

Referring to equation (6), the Hamiltonian is given by

$$H = -\left\lfloor \begin{matrix} c_{11}w_{11}(t) + c_{12}r_1(t) + c_{21}w_{21}(t) + c_{22}r_2(t) + \\ c_{31}w_{31}(t) + c_{33}r_3(t) \end{matrix} \right\rfloor +$$
$$\lambda_1(t)r_1(t) + \lambda_2(t)r_2(t) + \lambda_3(t)r_3(t)$$

(18)

Referring to equation (15), the adjoint variables are given by the following differential equations:

$$\lambda_1(t) = \lambda_1(T) + \int_t^T b_1 w_{11}(t)(c_{12} - \lambda_1(t))dt \qquad (19)$$

Similarly

$$\lambda_2(t) = \lambda_2(T) + \int_t^T b_2 w_{21}(t)(c_{22} - \lambda_2(t))dt \quad (20)$$

And

$$\lambda_3(t) = \lambda_3(T) + \int_t^T b_3 w_{31}(t)(c_{32} - \lambda_3(t))dt \qquad (21)$$

In order to determine the optimal control that maximizes the Hamiltonian, rewriting the equation (18)

$$H = \Psi(d_1(t), \lambda_1(t), t)w_{11}(t) + \Phi(d_2(t), \lambda_2(t), t)w_{21}(t) +$$
$$\Gamma(d_3(t), \lambda_3(t), t)w_{31}(t)$$

(22)

where

$$\Psi(d_1(t), \lambda_1(t), t) = (\lambda_1(t) - c_{12})b_1(a_1 - d_1(t)) - c_{11},$$

$$\Phi(d_2(t), \lambda_2(t), t) = (\lambda_2(t) - c_{22})b_2(a_2 - d_2(t)) - c_{21}$$

and

$$\Gamma(d_3(t), \lambda_3(t), t) = (\lambda_3(t) - c_{32})b_3(a_3 - d_3(t)) - c_{31}$$

are the grouping of coefficients of $w_{11}(t)$ $w_{21}(t)$ and $w_{31}(t)$ called switching functions. while the control variables are bounded and also Hamiltonian in (18) is linear in control variables

$w_{11}(t)$, $w_{21}(t)$ and $w_{31}(t)$ therefore, equation (18) may attain either maximum or minimum value for each change in the sign of $\Psi(d_1(t),\lambda_1(t),t)$, $\Phi(d_2(t),\lambda_2(t),t)$ and $\Gamma(d_3(t),\lambda_3(t),t)$. We have the following bang-bang and singular solution for $w_{11}(t)$, $w_{21}(t)$ and $w_{31}(t)$ which maximizes the Hamiltonian in equation (18):

$$w_{11}^{*}(t)=\begin{cases} w_1 & if \quad \Psi(t)>0 \\ \text{undefined} & if \quad \Psi(t)=0 \\ 0 & if \quad \Psi(t)<0 \end{cases} \tag{23}$$

$$w_{21}^{*}(t)=\begin{cases} w_2 & if \quad \Phi(t)>0 \\ undefined & if \quad \Phi(t)=0 \\ 0 & if \quad \Phi(t)<0 \end{cases} \tag{24}$$

And

$$w_{31}^{*}(t)=\begin{cases} w_3 & if \quad \Gamma(t)>0 \\ undefined & if \quad \Gamma(t)=0 \\ 0 & if \quad \Gamma(t)<0 \end{cases} \tag{25}$$

From equation (23), (24) and (25), the control are readily found to be

$$w_{11}^{*}(t)=\begin{cases} w_1 & if \quad (\lambda_1(t)-c_{12})b_1(a_1-d_1(t)) \\ >c_{11} & \\ undefined & if \quad (\lambda_1(t)-c_{12})b_1(a_1-d_1(t)) \\ =c_{11} & \\ 0 & if \quad (\lambda_1(t)-c_{12})b_1(a_1-d_1(t)) \\ <c_{11} & \end{cases} \tag{26}$$

$$w_{21}^{*}(t)=\begin{cases} w_2 & if \quad (\lambda_2(t)-c_{22})b_2(a_2-d_2(t)) \\ >c_{21} & \\ undefined & if \quad (\lambda_2(t)-c_{22})b_2(a_2-d_2(t)) \\ =c_{21} & \\ 0 & if \quad (\lambda_2(t)-c_{22})b_2(a_2-d_2(t)) \\ <c_{21} & \end{cases} \tag{27}$$

And

$$w_{31}^{*}(t)=\begin{cases} w_3 & if \quad (\lambda_3(t)-c_{32})b_3(a_3-d_3(t)) \\ >c_{31} & \\ undefined & if \quad (\lambda_3(t)-c_{32})b_3(a_3-d_3(t)) \\ =c_{31} & \\ 0 & if \quad (\lambda_3(t)-c_{32})b_3(a_3-d_3(t)) \\ <c_{31} & \end{cases} \tag{28}$$

Once the numbers of faults detected increases the remaining faults in the module decrease and lesser information is required for fault removal process. The above problem will solve by Genetic Algorithm (GA). Genetic Algorithm (GA) is a powerful optimization algorithm for solving difficult kind of problem which is not possible to be solved by general methods [18-21]. In Genetic Algorithm (GA) first step is to initialize population within some limit here in this problem it will generate initial population for a given testing effort W, and then evaluate the solution based on objective or fitness function. If we get optimal solution then our algorithm will terminate or we have to do selection, crossover and mutation. These three are the basic operators of GA.

Selection: The process that evaluates which solutions are to be selected and permitted to reproduce and which ones deserve to eliminate. The main goal of the selection operator is to emphasize the best solutions and eliminate the worst solutions in a population while keeping the population size constant. We have different kinds

of selections like roulette wheel selection, rank selection, tournament selection etc.

"*Selects the best, discards the rest*"

Crossover: The crossover operator is basically used to generate new solutions from the existing solutions available in the mating pool after applying selection operator. This operator interchanges the gene sequence between the solutions in the mating pool. Generally we are using binary crossover.

Mutation: Mutation is the irregular introduction of new features in to the solution strings of the population pool to sustain variety in the population. In this we are flipping one bit at a time for better solution.

Below is the Genetic Algorithm procedure which includes GA operators [22].

```
function GA ()
{
Initialize population;
Calculate fitness function;
    While (fitness value != termination criteria)
    {
    Selection;
    Crossover;
    Mutation;
    Calculate fitness function;
    }
}
```

8 NUMERICAL SOLUTION:

In this section, we present a numerical example based on the genetic algorithm for allocating the resource for three modules. In this problem we assumed that software is consisting of three modules. We assumed that the parameters for allocating the resource has been already estimated using the failure data given in table 1. The total testing resource is assumed to be 20,000 and the total cost for removing the fault is 50,000.

Table 1: Displays data for solving the allocation problem.

Modules	a	B	r(0)	$\lambda_i(0)$
M1	100	0.06	2	50
M2	100	0.025	3	50
M3	100	0.08	3	50

Based on above value the resource allocation problem is solved using Genetic Algorithm. Below parameters have been used for GA [23]

Table 2: Parameters for GA

Parameter	**Value**
Population Size	105
Number of Generation	85
Selection Mode	Tournament
Crossover Probability	0.85
Mutation Probability	0.15

Below table display the optimal allocation of resource and cost using Genetic Algorithm

Table 3: Optimal allocation of effort and cost for three modules.

Modules	Effort (Wi)	Cost
M1	6611.42	14000.52
M2	7262.38	21587.52
M3	6125.36	14411.20
Total	19999.16	49999.24

9 CONCLUSION:

In this paper the main goal is to allocate the resource for different modules. For this we developed a mathematical model for testing effort

allocation we assumed that the software is divided in different modules. In this study we use Genetic Algorithm for dynamically allocation of testing resource and cost of testing for different modules. We used MATLAB for simulation; we found that the result is better than our static method. One numerical example is solved for dynamic allocation of effort for three modules. The result is described in tabular form for every module. This means the tester and developer can devote their resource to finish off their testing and debugging task for well controlled expenditure.

10 REFERENCES:

1. Kapur, P. K. et al. Contributions to hardware and software reliability. (1999).
2. Yamada, S. et al.'Optimal allocation policies for testing-resource based on a software reliability growth model', Mathematical and Computer Modelling, 22(10– 12), 295–301. (1995),
3. Ohetera, H., & Yamada, S. Optimal allocation and control problems for software testing resources. IEEE Transactions on Reliability, 39(2), 171–176. (1990).
4. Holland, J. H. Adaptation in Natural and Artificial Systems. University of Michigan Press. (1975)
5. Kuo, W., Prasad, V.R., An annotated overview of system reliability optimisation. IEEE Trans. Reliab. 49 (2), 176–187. (2000).
6. Leung, Y.W.,. Dynamic resource-allocation for software-module testing. J. Syst. Software 37 (2), 129–139. (1997)
7. Kapur, P. K., Bardhan, A. K. and Yadavalli, V.S.S. 'On allocation of resources during testing phase of a modular software', International Journal of Systems Science, 38(6): 493 - 499. (2007),
8. Kapur, P K, Anu G Aggarwal and GurjeetKaur Optimal Testing Resource Allocation for Modular Software Considering Cost, Testing Effort and Reliability using Genetic Algorithm. International Journal of Reliability, Quality and Safety Engineering. 16(6): 495-508. (2010).
9. Zai Wang,,KeTangandXin Yao, " Multi-Objective Approaches to Optimal Testing Resource Allocation in Modular Software Systems, " IEEE Transaction on Reliability, vol. 59, no. 3, SEPTEMBER (2010)
10. Anu G. Aggarwal, P. K. Kapur, GurjeetKaurand Ravi Kumar, " Genetic Algorithm Based Optimal Testing Effort Allocation Problem for Modular Software, " BVICAM's International Journal of Information Technology, Proceedings of the 4th National Conference; INDIACom-(2010)
11. P.K. Kapur, Hoang Pham, Udayan Chanda and Vijay Kumar: Optimal allocation of testing effort during testing and debugging phases: a control theoretic approach, International Journal of Systems Science, DOI:10.1080/00207721.2012.669861(2012)
12. SK. Md. Rafi, and Shaheda Akthar, " Resource Allocation to Software Modules in Software Testing with Imperfect-debugging SRGM, " International Journal of Computer Applications (0975 – 8887) Volume 18– No.2, March (2011)
13. Rani Rajan and Misra, K. B.,'Optimal testing resource allocation models for modular software', In Proceedings of annual reliability and maintainability symposium, RAMS'06 (pp. 104–109). (2006),
14. Dai, Y. S. et al.'Optimal testing-resource allocation with genetic algorithm for modular software systems', Journal of Systems and Software, 66(1), 47–55. (2003),
15. Goel , A. L. and Okumoto, K.,'Time dependent error detection rate model for software reliability and other performance measures', IEEE Trans. on Reliability, vol. R-28, no. 3, pp. 206–211. (1979)
16. P. K. Kapur, Anu G. Aggarwal, GurjeetKaur Simultaneous allocation of testing time and resources for a modular software International Journal of System Assurance Engineering and Management December 2010, Volume 1, Issue 4, pp 351-361, Springer Publication
17. Sethi, S. P. and G. Thompson 'Optimal Control Theory: Applications to Management Science and Economics', 2nd ed. Kluwer Academic Publishers, Boston, MA. (2000),
18. Goldberg, D. E., Genetic Algorithms: in Search Optimization and Machines Learning (New York: Addison-Wesley). 1989,
19. David, L. Handbook of Genetic Algorithms. New York : Van Nostrand Reinhold. 1991.
20. Deb K., Optimization for Engineering Design-Algorithms and Examples. Prentice Hall of India,New Delhi . 1995.
21. Holland, J. H. (1975) Adaptation in Natural and Artificial Systems. University of Michigan Press.
22. Dr. R.K Bhattacharjya, ―Introduction To Genetic Algorithms,‖ IIT Guwahati, pp.12, 2012.
23. Global Optimization Toolbox User's Guide R2012a The MathWorks, Inc.
24. Khan M, Ahmad N, and Rafi L. "Optimal Testing Resource Allocation for Modular Software Based on a Software Reliability Growth Model: A Dynamic Programming Approach, " Proceedings of the International Conference on Computer Science and Software Engineering (2008),
25. Nasar. Md., Johri Prashant, Udayan Chanda,"Dynamic Effort Allocation Problem Using Genetic Algorithm Approach", IJMECS, vol.6, no.6, pp.46-52, (2014) .DOI: 10.5815/ijmecs.2014.06.06

International Journal of New Computer Architectures and their Applications (IJNCAA) 5(1): 39-47
The Society of Digital Information and Wireless Communications, 2015 ISSN 2220-9085 (Online); ISSN 2412-3587 (Print)

Development of an Integrated Information Server System for IT Education through Server Virtualization Technology

Yoshio Moritoh[1], Yoshiro Imai [2]
[1] Kagawa Junior College
1-10 Utazu-cho, Ayautagun 769-0201,Japan
[2] Graduate School of Engineering, Kagawa University,
2217-20 Hayashi-cho, Takamatsu 761-0396 Japan
[1] moritoh@kjc.ac.jp [2] imai@eng.kagawa-u.ac.jp

ABSTRACT

Recent decade years, our educational environments have been already including several kinds of computing infrastructures according to user's requests. But we are sometimes suffering from lack of suitable methodology to accomplish effective improvement and efficient maintenance. Server virtualization technology is one of the most powerful and ecological solutions to realize information server system for so-called cloud computing.
System of our educational information server has been configured with such a virtualization technology and demonstrated in detail for the sake of robust and disturbance-avoiding education environment. Our case of utilization of server virtualization technology has been based on CITRIX Xen open-source virtualization technology because of its flexibility and expandability.
This paper describes how to construct educational computing environment with server virtualization and demonstrate some applications of information server into IT-based higher education through practical classroom lecture. And moreover it reports quantitative and qualitative evaluation of such an environment by means of questionnaire from learners, too.

KEYWORDS

Server virtualization, Improvement of educational system, Questionnaire-based analysis, Quantitative evaluation.

1 INTRODUCTION

An IT environment for education, in particular Computer Education, must provide educational tools effectively, flexible equipment efficiently, and applicable scheme fruitfully for several kinds of learners. Not only engineering education but also IT-based one have to employ several kinds of e-learning system in their institutions. Nowadays, almost all higher education of the world cannot avoid constructing their educational environments without IT facilities.
It is probably very difficult to maintain IT-based educational environment, however. Because there are some reasons, ones of which are according to so-called situational changes. For example, we are sometimes suffering from the lack of professional knowledge for keeping 'know-how' during utilization period. Additionally, several domains in education used to enjoy the benefit of IT and depend on IT products themselves very much deeply.
As you know, IT-based environment changes frequently and alters often drastically. IT revolution is perhaps named after not evolution of information technology but breaking away from the past. In such a case, we cannot keep our previous value of the past environment, and we must catch up new-coming concept/idea/strategy for next-stage information infrastructure in order to obtain the benefit from IT(-based) environment consequently. People may say little ironically, that must be 'IT revolution' exactly. Anyway, we have to prepare such an IT revolution and consider robust/ flexible procedure to override the relevant changes.
A lot of users do not really want to know detail of infrastructure based on IT environment and do definitely want to concentrate their working/ studying without disturbance from environmental changes. So managers of IT based education must construct suitable and robust IT environment for learners to enjoy working and studying their subjects independently from external disturbances.

Server Virtualization technology and Could Computing mechanism are very ones of powerful solutions for decreasing effects from such an unwanted IT revolution and expanding life time of the previous IT environment possibly.

This paper retrieves some useful related works about server virtualization technology and explains our approach for educational information server based on such technology. Although server virtualization and cloud computing are available for large-scaled IT application, we have already applied similar scheme and strategy into relatively small-sized educational environment. And we are managing such an environment for some classroom lectures and exercises. We will show some results from quantitative and qualitative evaluations through real education.

This paper describes related works in the next section and illustrates system configuration of our integrated information server with virtualization technology in the third section. It demonstrates some fruitful results of users' satisfaction about our system through quantitative and qualitative evaluation by means of questionnaire in the fourth section. And it summarizes our conclusions about this research and shows future plan of our study in the last section.

2 RELATED WORKS

This section introduces some of related researches about Server Virtualization for the sake of improvement of systems performance and maintenance.

First of all, Steinder and his team describe in [1], "Server virtualization opens up a range of new possibilities for autonomic data center management, through the availability of new automation mechanisms that can be exploited to control and monitor tasks running within virtual machines. It offers not only new and more flexible control to the operator using a capitals, use a management console, but also more powerful and flexible autonomic control, through management software that maintains the system in a desired state in the face of changing workload and demand." Their paper[1] explores the use of server virtualization technology in the autonomic management of data centers running a heterogeneous mix of workloads. And they present a system that manages heterogeneous workloads to their performance goals and demonstrate its effectiveness via real-system experiments and simulation. They also point out some of the significant challenges to wider usage of virtual servers in autonomic datacenter management.

Oguchi and Yamamoto of Fujitsu (Japan) explain in [2], "IT systems have become increasingly larger and more complex, thus making it more difficult to build an optimal IT infrastructure in today's rapidly changing business environment. Server virtualization represents a base technology for addressing this problem. It enables the flexible construction of virtual servers with almost no hardware limitations, and consequently reduces the total cost of ownership (TCO) and makes it easier to use virtual servers in the changing business environment.

Their Company, Fujitsu supplied server virtualization technology in the form of the Virtual Machine Function based on Xen open-source technology for the mission-critical IA server and PC server. Their paper[2] describes the background behind and latest trends in server virtualization, and outlines Fujitsu's Virtual Machine Function and the Xen architecture.

Jeff Daniels introduces in his paper[3] of ACM Magazine Crossroads, "Virtual machine technology, or virtualization, is gaining momentum in the information technology community. While virtual machines are not a new concept, recent advances in hardware and software technology have brought virtualization to the forefront of IT management. Stability, cost savings, and manageability are among the reasons for the recent rise of virtualization. Virtual machine solutions can be classified by hardware, software, and operating system/containers. From its inception on the mainframe to distributed servers on x86, the virtual machine has matured and will play an increasing role in systems management."

Ling Qian and his team of ChinaMobile in their paper[4] describe, " Internet service provider(IPS) invented the cloud computing in order to support the maximum number of user and elastic service with the minimum resource. Within a few years, emerging cloud computing has become the hottest technology. From the publication of core papers by

Google since 2003 to the commercialization of Amazon EC2 in 2006, and to the service offering of AT&T Synaptic Hosting, the cloud computing has been evolved from internal IT system to public service, from cost-saving tools to revenue generator, and from ISP to telecom." Their paper[4] introduces the concept, history, pros and cons of cloud computing as its overview.

Dale L. Lunsford of The University of Southern Mississippi in his paper[5] point out about information system as follows; "Information systems educators must balance the need to protect the stability, availability, and security of computer laboratories with the learning objectives of various courses. In advanced courses where students need to install, configure, and otherwise manipulate application and operating system settings, this is especially problematic as these activities threaten the stability of workstations and security of networks. Virtualization platforms offer the capability to integrate advanced topics into courses in a way that gives students control so that they can perform hands-on activities that would be infeasible on shared physical computers." And his paper provides an introduction to virtualization technologies, discussed the use of VMWare Workstation 6 in a classroom setting, outlined some challenges and limitations of virtualization, and presented some opportunities and benefits from using virtualization. Finally he concludes "Virtualization covers a wide range of techniques, from application virtualization to server virtualization. Desktop virtualization provides an opportunity for IS educators to introduce more advanced or risky topics in information systems courses, while safeguarding the computers in laboratories."

3 SYSTEM CONFIGURATION OF INTEGRATED INFORMATION SERVER

Our integrated information server for educational environment has been designed and developed based on server virtualization with reference to the previous suitable researches above described. This section illustrates system configuration of our information server.

A. Outline of Server Virtualization A. Outline of Server Virtualization

It is very efficient and comfortable for users of IT environment to realize parallel programs execution and receive smart services through parallel processing. If some applications need computing services with more powerful CPU performance, the relevant programs will be executed in parallel mode by means of virtualized CPUs by server virtualization technology. In such a case, some information servers are integrated as virtualized servers with their hypervisor. The later can adjust and assign application programs, Software as a Services, or Operating Systems (OSs) themselves onto its controlling virtualized servers. Figure 1 shows hypervisor window to control virtualized servers in our system. By means of operating hypervisor, some programs on the relevant OSs can be dispatched, transported and re-allocated from one virtualized server to another very much smoothly.

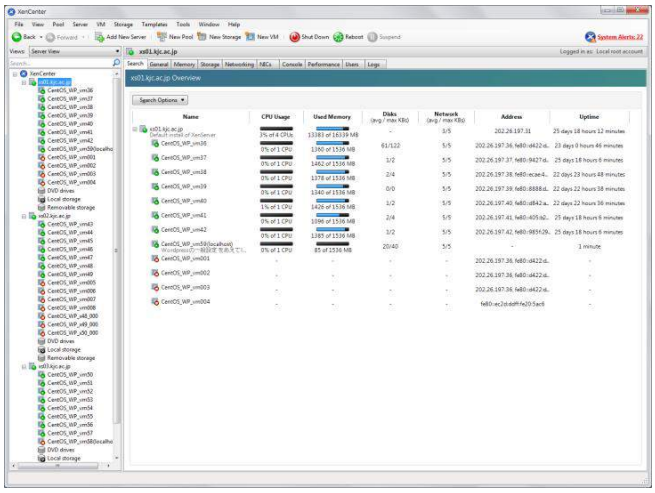

Figure 1. Hypervisor Window for Virtualized Servers

In server virtualization technology, we can choose almost three major candidates to realize server virtualization relatively in the easier ways. For example, there are major famous solutions such as VMware approach, CITRIX Xen server, and Microsoft Hypervisor. In our study, we had already chosen Xen server architecture because we are reliable on its open-source policy. So we have developed our integrated information server with Xen open-source virtualization technology.

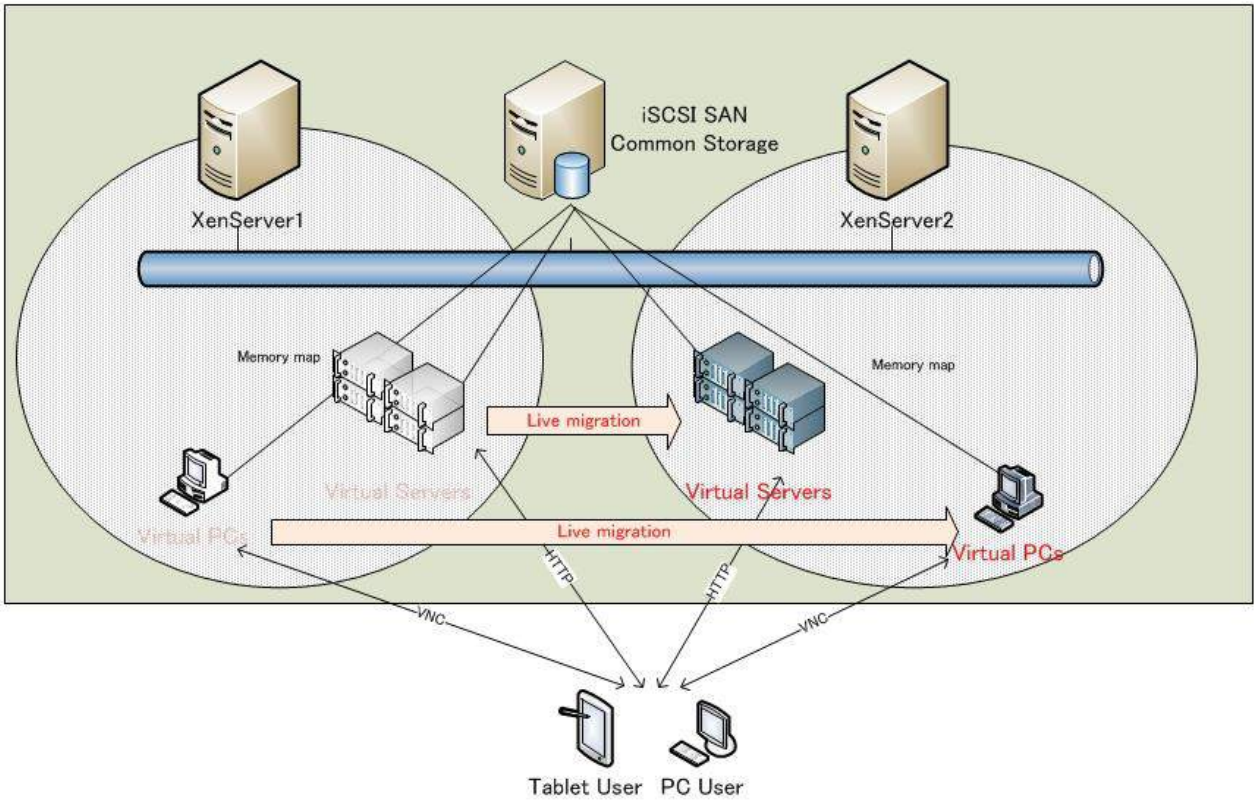

Figure 2. Outline of our Integrated Information Server and Live Migration as one of Characteristics of Server Virtualization

Figure 2 shows outline of our integrated information server which includes multiple computer clusters distributed on the high-speed communication channels. Each cluster has some virtualized servers powered "Xen Server" and storage server. Storage server can play a very important role to facilitate network storage services for each Xen Server independently. Its specification is shown in Table 1

Table 1. SPECIFICATION OF COMMON STORAGE SERVER

Machine Name	DELL PowerEdge R200
CPU	Intel Xeon 3065 2.3GHz 1P/4C
Main memory	4GBytes
Hard Disk#1	500GBytes(7.2Krpm SATA)
Hard Disk#2	2TBytes(7.2Krpm SATA)
NIC	1000 Base-TX 2
OS	NexentaStor 3.1
Transport Protocol	iSCSI
FileSystem	ZFS (Zettabyte File System)

NexentaStor is an OpenSolaris or recently Illumos distribution optimized for virtualization, storage area networks, network-attached storage, and iSCSI or Fiber Channel applications employing the ZFS file system. Like OpenSolaris, NexentaStor is a Unix-like operating system. Nexenta Systems started NexentaStor as a fork of another OpenSolaris distribution, Illumos (referred by Wikipedia). NexentaStor requests Storage Server to have two types of built-in Hard Disks for system itself (Hard Disk#1) and network storage (Hard Disk#2) for external servers.

We have employed one of the two different versions of NexentaStor, namely Community Edition because I have already studied the following experiences;

1) Server virtualization is suitable and very useful for application software to obtain more computing performance, however, it needs suitable storage facilities in deed.

2) Live migration describes above is one of the typical and powerful characteristics of server virtualization technology, in particular, Xen Server architecture. It is quite necessary for Xen to utilize suitable (in the other word, high-performance) network-attached storage.

Figure 3 shows a browsing view of current preference for our Common Storage Server based on NexentaStor (community version). Total performance of virtualized server may be regulated or dominated by capability of common storage. So it is very much important for system managers to tune up performance by means of adjusting machine specification and storage capability/setting. That must be deeply depended on "know-how" and several kinds of experience from system management.

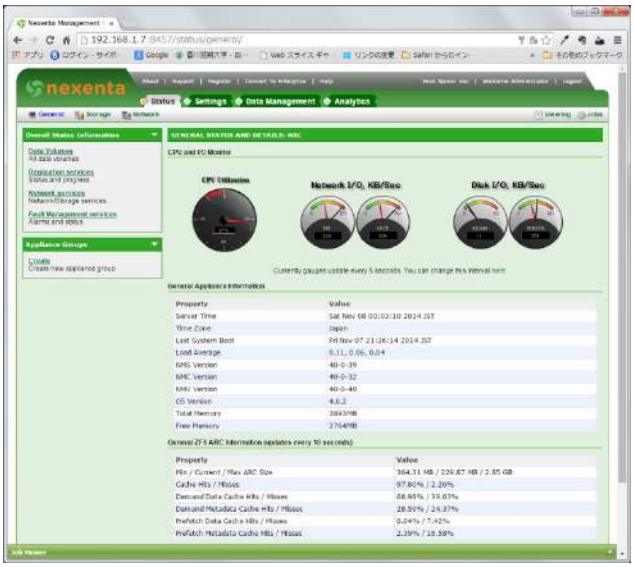

Figure 3. Preference for Common Storage Server based on NexentaStor

B. From Previous Standalone to Virtualized Server

We have newly developed our Integrated Information Server based on Xen open-source technology with high-performance network-attached storage, and then replaced the previous education environment with such Information Servers as shown in Figure 4. Of course, the previous environment is still now available for special users who are still not quite free of Legacy PCs and Legacy servers. So we can compare performance and interoperability between our Integrated Information Server and previous Legacy environment.

Web system and database were and still now are playing a very important role of educational tools and products at IT environment during about decade years from the end of 1990's. As you know, it is very popular for us, namely information systems educator as well as enterprise system administrators to set up information server together with Apache Web server and SQL one, such as very famous Web-DB model LAMP (Linux+Apache+ MySQL+PHP/Perl) or LAPP (Linux+Apache+ PostgreSQL+PHP/Perl). Such a Web-DB model has been useful and provided some foundation for educational environment to realize from e-Learning facilities to Q and A man-machine interfaces.

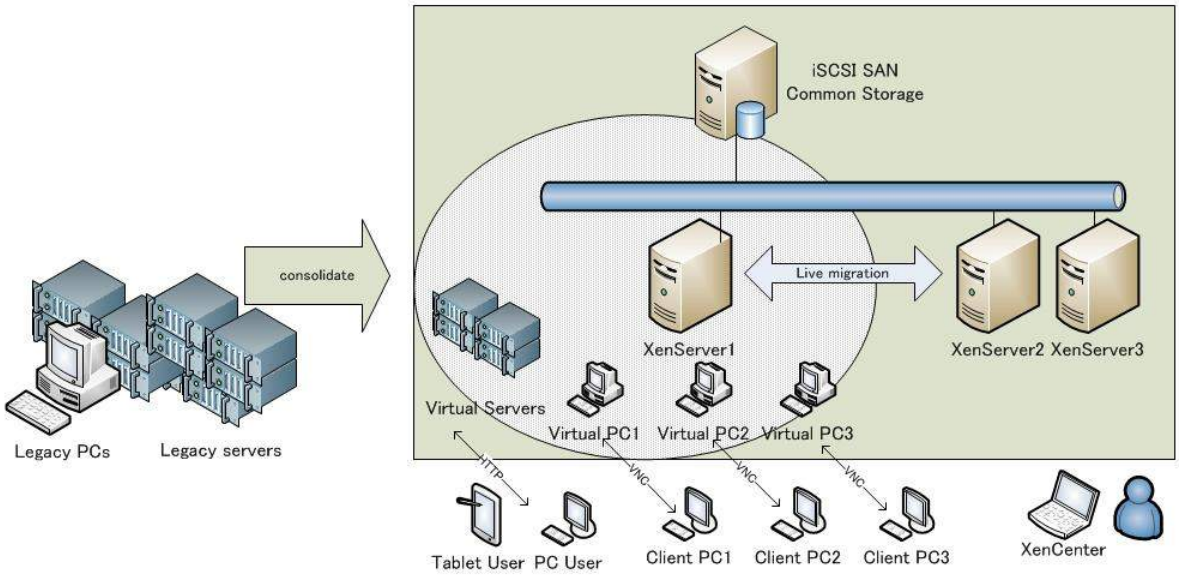

Figure4. Integrated Information Server Enhanced by Server Virtualization Technology and its Replaceability of Legacy Environment.

Many system designers had pointed out that XAMPP[6] might be the most popular PHP development environment. XAMPP was and still now is a completely free, easy to install Apache distribution containing MySQL, PHP, and Perl. The XAMPP open source package has been set up to be incredibly easy to install and to use. So we had developed the previous Legacy server with XAMPP open source package as our educational environment. Until last year, we had been providing an IT-based education environment for our learners to perform their studies, exercises and research at the classroom lectures.

WordPress[7] is a free and open-source blogging tool and a Content Management System(CMS) based on PHP and MySQL. Its features include a plugin architecture and a template system. WikiPedia explains "WordPress was used by more than 23.3% of the top 10 million websites as of January 2015. WordPress is the most popular blogging system in use on the Web, at more than 60 million websites."

A few years ago, we had decided to introduce more flexible and expandable environment for IT-based education by means of integrated information server based on server virtualization technology[8]. As one of typical applications executable on the above server, we have employed WordPress for educational tools used in Web Design Exercise. It is very useful for not only learners but also instructors/system managers to treat with WordPress in new developed environment provided by our integrated information server. So we select a case of Web Design Exercise using WordPress on our server as target to be evaluated in the real education environment. Detail of evaluation will be described in the following section.

4 EVALUATION OF OUR SYSTEM

This section demonstrates our trial evaluation of integrated information server based on server virtualization using Xen open-source virtualization technology. It describes the detail of our questionnaire at the first half of this section, and reports analyzed results of questionnaire as a quantitative evaluation for our system at the second one of this section.

A. Detail of Questionnaire

We had already reported different kinds of evaluation about Distributed Multiple Server System [9],[10]. This time, therefore, we wanted to investigate the user friendly level of our system, evocation of willingness to learn by our system and interoperability between related applications by means of carrying out questionnaire. So we have the following point of view to check whatever our system can provide user's advantages or not. The questionnaire includes following six questions [11];

Q#1 In the case that learners are requested to perform such operations as writing documents through VNC (as DaaS: Desktop as a Service). So we ask our learners which following level they think to perform operation through DaaS environment.

1) very slow – beyond bearing
2) poor
3) fair
4) good
5) very fast, comfortable – no stress to operate

Q#2 In the case that learners are requested to perform such operations as writing documents through major browser (as SaaS: Software as a Service). So we ask our learners which following level they think to perform operation through SaaS tool.

1) very slow – beyond bearing
2) poor
3) fair
4) good
5) very fast, comfortable – no stress to operate

Q#3 In the case that learners are requested to perform such operations as writing documents through VNC (as DaaS: Desktop as a Service). So we ask our learners which following level they are feeling to utilize DaaS environment.

1) never willing to utilize because of bad environment
2) poor
3) fair
4) good
5) clearly willing to utilize because of well environment

Q#4 In the case that learners are requested to perform such operations as writing documents through major browser (as SaaS: Software as a Service). So we ask our learners which following level they are feeling to utilize SaaS tool.

1) never willing to utilize because of bad environment
2) poor
3) fair
4) good
5) clearly willing to utilize because of well environment

Q#5 We had provided the previous environment which had employed XAMPP as main package to construct educational environment. Such an environment is a comparative one against our newly developed educational environment with virtualized server. So we ask our learners which following level they manipulate XAMPP.

1) very slow – beyond bearing
2) poor
3) fair
4) good
5) very fast, comfortable – no stress to operate

Q#6 Learners are requested to design Web contents on our educational environment with WordPress. So we ask our learners which following level they utilize WordPress.

1) very slow – beyond bearing
2) poor
3) fair
4) good
5) very fast, comfortable – no stress to operate

We have a class for students to utilize our integrated information server in order to perform WordPress during Web contents-making and creation exercise. Such a case is suitable for us to perform some evaluation for our system and to carry questionnaire investigation into execution. In 2014, the relevant learners of the above class have been asked to answer the above questionnaire and there are 14 numbers of students who kindly replied and answered their responses which are shown in Table 2 below.

Table 2. RESULT OF QUESTIONNAIRE ABOUT USER-FRIENDLY LEVEL OF OUR SYSTEM, EVOCATION OF WILLINGNESS TO LEARN BY OUR SYSTEM AND INTEROPERABILITY BETWEEN RELATED APPLICATIONS

Student	Q#1	Q#2	Q#3	Q#4	Q#5	Q#6
S01	3	3	3	3	3	3
S02	3	4	4	4	2	3
S03	3	3	5	5	3	3
S04	4	4	5	5	2	2
S05	4	4	5	5	5	5
S06	3	3	4	4	2	2
S07	3	3	4	3	5	4
S08	4	4	3	3	4	3
S09	4	4	5	5	2	5
S10	3	4	4	4	5	3
S11	4	3	4	5	4	5
S12	3	3	4	4	2	2
S13	5	5	5	5	3	3
S14	4	4	4	4	2	3
Avg	3.57	3.64	4.14	4.21	3.14	3.29

B. Quantitative Evaluation through Analysis of the Results of Questionnaire

While averaged score for question Q#5 is 3.14, averaged scores for questions Q#1 and Q#2 are 3.57 and 3.64 respectively. It means that our newly developed system clearly obtains higher scores from learners for the sake of easiness of utilization than the previous one does. Namely it is confirmed that learners can perform their manipulations and operations at the newly developed environment faster than (more comfortable than) at the previous one.

Categorized results of questionnaire are cumulated, averaged and visualized in the style of Radar Chart shown in Figure 5. This figure is suitable for glancing and checking balance of learners' responses for the whole questionnaire. Therefore, it can be considered that the averaged scores for questions Q#3 and Q#4 are especially good for learners through the above real experience based analysis by Quantitative approach with Criteria and Numbered Ranks.

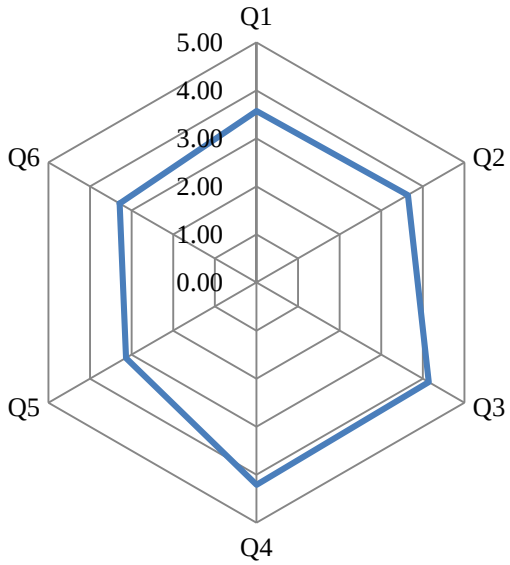

Figure 5. Radar Chart for the results of Questionnaire shown in Table 2

For example, it is a trial statistical analysis to calculate Student's *t-statistic (t)* expressed (1) for question Q#1, namely "to perform operation through DaaS environment".
At first, we assume that Null hypothesis H_0: "*To perform operation through DaaS environment* is no good in our newly developed system from learners".
Our statistical analysis is achieved in the following expression (1):

$$t = \frac{\overline{X} - \mu}{\sqrt{\sigma^2/\mathrm{n}}} \quad \text{-- (1)}$$

In the expression (1), $\overline{X}$ is average of samples, μ is target expectation (='3.00'), σ^2 is samples' variance and n is number of samples (= 14). From Table 2, $\overline{X}$ = 3.57, standard deviation: $\sigma = \sqrt{\sigma^2}$ = 0.646, and n = 14, $\sqrt{n}$ = 3.74. So we can calculate (1) into (2).

$$t = \frac{\overline{X} - \mu}{\sqrt{\sigma^2/\mathrm{n}}} = \frac{3.57 - \mu}{0.646/3.74} \quad \text{-- (2)}$$

In our case, target expectation: μ is assumed to be 3:00 according to the above discussion, value of Student's *t-statistic* can be calculated as t = 3.30868. .. = 3.308.
At the same time, number of samples is n, so degree of freedom is n - 1 (=13). So we can obtain the following values for two-sided 5% point (α=0.025) from Statistical Tables of Student's *t-statistic* distribution, namely, $t_{\alpha=0:025}$ (13) = 2.160, where α is significance level of probability. Two-sided *t-test* has been performed in the following expression (3):

$$t = 3.308 > t_{\alpha=0:025}(13) = 2.160 \text{ -- (3)}$$

And the result of such *t-test* can reject the previous Null hypothesis H_0: "*To perform operation through DaaS environment* is no good in our system from learners".
It is confirmed, therefore, that "*To perform operation through DaaS environment* is good in our system from learners" is significantly evaluated by the results of the relevant questionnaire. And then we believe that we can provide efficient and effective environment for IT-based education by means of our integrated information server with server virtualization technology.
In order to make assurance double sure, we have tied to apply the result of question Q#5 with calculation of Student's *t-statistic (t)* as follows;
In the case of Q#5, we can calculate such a value of *t-statistic (t)* with $\overline{X}$ = 3.14, its standard deviation: $\sigma = \sqrt{\sigma^2}$ = 1.231, and n = 14, $\sqrt{n}$ = 3.74.

$$t = \frac{\overline{X} - \mu}{\sqrt{\sigma^2/\mathrm{n}}} = \frac{3.14 - \mu}{1.231/3.74} = 0.434 \text{ -- (4)}$$

Just the same as above, target expectation: μ is assumed to be 3:00, the value of Student's *t-statistic* can be calculated as the above expression (4). Therefore, if we assumed that Null hypothesis H_0^*: "*To perform operation provided from the previous XAMPP* is no good in the previous environments from learners", with the following expression (5):

$$t = 0.434 < t_{\alpha=0:025}(13) = 2.160 \text{ -- (5)}$$

then we cannot definitely reject the above hypothesis. In other words, it may be probably confirmed or considered that learners have some uncomfortable feeling about the previous environment which had provided the previous educational tools and equipment before our newly developed "Integrated Information Server". And we have clearly recognized that the previous system can be replaced with our newly system.

5 CONCLUSION

This paper has reported our approach for development of Integrated Information Server for IT-based education with server virtualization technology, its detail of structure and behaviour in the real education environment and trial quantitative/qualitative evaluation through the questionnaire methodology for practical learners who are users of our system.

Our system usually equips efficient functionality for IT-based education environment because it employs server virtualization strategy through Xen open-source technology and prepare suitable computing power enough to realize parallel computation for multiple applications. Additionally, it can provide emergency recovering mechanism from some kinds of damages such as machine troubles, network ones, software ones and so on. Because of "Live Migration" supported by server virtualization, especially global context switching can be smoothly accomplished not only within multi-core systems' inside but also between virtualized servers working distantly by means of high-speed communication channels.

As a trial evaluation of our system, we had carried out questionnaire for our learners and analyzed the results of it. It is significantly evaluated that our learners may enjoy comfortable manipulations and/or operation through DaaS environment supported by our system from analyzed results of the relevant questionnaire. Additionally, it is considered that the previous system can be replaced with our newly developed Integrated Information Server according to the relevant questionnaire.

With our experience described above, it will be able to make the old-styled IT-based environment to be replaced more efficiently and effectively through server virtualization technology. In near future, we will apply our approach described above into other kinds of domains, for example, small scale of domestic companies for realization of robustly continuing business, local government for support of semi-non-stop e-Services to residents, and so on.

ACKNOWLEDGMENT

The authors would like to express many thanks to Professor Tetsuo Hattori, Professor Shigeaki Ogose and Professor Hitoshi Inomo of Kagawa University, Graduate School of Engineering for their kind supports toward one of the authors, Yoshio Moritoh, in order to obtain his PhD degree from Kagawa University very smoothly.

A part of this work includes such a fruitful resultants of his PhD dissertation. This research had been also partly supported by Research for Promoting Technological Seeds from Japan Science and Technology Agency (JST).

REFERENCES

1. M. Steinder, I. Whalley, D. Carrera, I. Gaweda, "Server virtualization in autonomic management of heterogeneous workloads," 10th IFIP/IEEE International Symposium on Integrated Network Management (INM2007), pp. 139–148, 2007.
2. Y. Oguchi, T. Yamamoto, "Server Virtualization Technology and Its Latest Trends," Fujitsu scientific and technical journal, Vol.44, No.1, pp. 46–52, 2008.
3. J. Daniels, "Server virtualization architecture and implementation," ACM Magazine "Crossroads", Vol.16, No.1, pp. 8–12, September 2009. Article #1, 29pages, 2003.
4. L. Qian, Z. Luo, Y. Du, L. Gun, "Cloud Computing: An Overview," Lecture Notes in Computer Science, Vol.5931, pp. 626–631, 2009.
5. D. L. Lunsford, "Virtualization Technologies in Information Systems Education," Journal of Information Systems Education, Vol.20, No.3 pp.339–348, 2009.
6. https://www.apachefriends.org/index.html
7. https://wordpress.org/showcase/
8. Y. Moritoh, Y. Imai, "A Cloud Approach on Distributed Multiple Servers for Distance Learning," IEEE International Conference on IT-based Higher Education and Training (ITHET2012), pp. 233–238, 2012.
9. Y. Moritoh, M. Imai, Y. Imai, "Trial Evaluation of Visual Educational Tool on Distributed Multiple Server System," IEEE International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE2013), pp. 439–445, 2013.
10. Y. Moritoh, Y. Imai, T. Hattori, "Evaluation for Distance Learning Scheme on Distributed Multiple Server System," International Journal of Artificial Life and Robotics (Springer) Volume 19, Issue 1, pp. 61–67 (February 2014).
11. Y. Moritoh, Y. Imai,"Trial Evaluation of Integrated Information Server for IT Education through Server Virtualization," IEEE International Conference on Education Technologies and Computers (ICETC2015) pp.82-87, 2015.

International Journal of
NEW COMPUTER ARCHITECTURES AND THEIR APPLICATIONS

The *International Journal of New Computer Architectures and Their Applications* aims to provide a forum for scientists, engineers, and practitioners to present their latest research results, ideas, developments and applications in the field of computer architectures, information technology, and mobile technologies. The IJNCAA is published four times a year and accepts three types of papers as follows:

1. **Research papers**: that are presenting and discussing the latest, and the most profound research results in the scope of IJNCAA. Papers should describe new contributions in the scope of IJNCAA and support claims of novelty with citations to the relevant literature.
2. **Technical papers**: that are establishing meaningful forum between practitioners and researchers with useful solutions in various fields of digital security and forensics. It includes all kinds of practical applications, which covers principles, projects, missions, techniques, tools, methods, processes etc.
3. **Review papers**: that are critically analyzing past and current research trends in the field.

Manuscripts submitted to IJNCAA **should not be previously published or be under review** by any other publication. Plagiarism is a serious academic offense and will not be tolerated in any sort! Any case of plagiarism would lead to life-time abundance of all authors for publishing in any of our journals or conferences.

Original unpublished manuscripts are solicited in the following areas including but not limited to:

- Computer Architectures
- Parallel and Distributed Systems
- Storage Management
- Microprocessors and Microsystems
- Communications Management
- Reliability
- VLSI