I. J. Computer Network and Information Security, 2012, 2, 22-28
Published Online March 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.02.04

Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms

[1]M. Anand Kumar and [2]Dr.S.Karthikeyan

[1]PhD Research Scholar, Karpagam University, India
[2]Asst. Professor, Department of Information Technology, College of Applied Sciences, Sultanate of Oman
anandm_ss@yahoo.co.in, skarthi@gmail.com

***Abstract*— The growth rate of the internet exceeds than any other technology which is measured by users and bandwidth. Internet has been growing at a rapid rate since its conception, on a curve geometric and sometimes exponential. Today, the Internet is moving exponentially in three different directions such as size, processing power, and software sophistication making it the fastest growing technology humankind has ever created. With the rapid growth of internet, there is need to protect the sensitive data from unauthorized access. Cryptography plays a vital role in the field of network security. Currently many encryption algorithms are available to secure the data but these algorithms consume lot of computing resources such as battery and CPU time. This paper mainly focuses on two commonly used symmetric encryption algorithms such as Blowfish and Rejindael. These algorithms are compared and performance is evaluated. Experimental results are given to demonstrate the performance of these algorithms.**

***Index Terms*— Blowfish, Cryptography, Encryption, Internet, Rejindael, Security, Symmetric algorithms**

I. Introduction

The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide [1]. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies With the rapid growth of internet, there is need to protect the sensitive data from unauthorized access. With the increasing use of Internet for business applications, there is a great demand for Quality of service. The application that is increasing day-by-day needs a consistent control protocols for providing quality of service (QOS). Because of these reasons the need for security in the Internet is stronger than ever.

Cryptography is the science that is widely used for the network security. Key aspects of cryptography are privacy, authentication, identification, trust and verification [2]. There are several ways of classifying cryptographic algorithms. They can be classified based on the number of keys that are employed for encryption and decryption, and further defined by their application and use The cryptographic algorithms can be broadly divided into three types namely Secret Key Cryptography (SKC), Public Key cryptography (PKC) and Hash Functions Some of the secret key algorithms are Data encryption standard (DES), Advanced encryption standard (AES), CAST, International data encryption algorithm(IDEA), Blowfish, Twofish, and Secure and fast encryption routine(SAFER). In these algorithms AES and Blowfish are the two algorithms proved to be strong in the modern world. RSA, Diffie-Hellman, Digital signature algorithm (DSA), Elgamal and Elliptic curve cryptography are some of the Public key cryptographic algorithms [3].

Blowfish: Blowfish [4] is a 64-bit symmetric block cipher with variable length key. The algorithm operates with two parts: a key expansion part and a data-encryption part. The role of key expansion part is to converts a key of at most 448 bits into several sub key arrays totaling 4168 bytes. The data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, a key and data-dependent substitution. All operations are EX-ORs and additions on 32-bit words Blowfish is successor to Twofish

AES: AES [5] is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256.It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices [6]. Also, AES has been carefully tested for many security applications [7].

This study evaluates two commonly used symmetric encryption algorithms such as Blowfish [4] and Rijindael [5] The performance measure of encryption schemes will be conducted using several performance metrics such as energy consumption, changing data types –such as text or document and images- power consumption, changing packet size and changing key size for the selected cryptographic algorithms. The rest of the paper is organized as follows. Blowfish and AES algorithms are described in section II that is followed by Performance metrics in section III. In section IV Performance evaluations of Blowfish and AES is

presented. Experimental results are given in section 5 and finally we conclude in section 6

II. Related Work

This section discusses some of the results obtained from other research papers to give more prospective about the performance of the compared algorithms such as Blowfish and AES algorithms..

It was identified from [6], [7] that AES operates faster and more efficient than other symmetric encryption algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation). Even under the scenario of data transfer it would be advisable to use AES scheme in case the encrypted data is stored at the other end and decrypted multiple times. Increasing the key size by 64 bits of AES leads to increase in energy consumption about 8% without any data transfer. The difference is not noticeable. Reducing the number of rounds leads to power savings but it makes the protocol insecure for AES and should be avoided. Seven or more rounds can be considered fairly secure and could be used to save energy in some cases.

A study in [8] is conducted for different popular secret key algorithms such as DES, DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms, to compare their performance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data.

In [9], [10] a study of security measure level has been proposed for a web programming language to analyze four Web browsers. This study consider of measuring the performances of encryption process at the programming language's script with the Web browsers. This is followed by conducting tests simulation in order to obtain the best encryption algorithm versus Web browser. It was concluded in [9] that Rijndael and Twofish achieved the highest performance on Ultras ARC, Pentium II and Itanium. It is recommended Rijndael and Twofish as AES algorithms in respect of their performance [11], [12].

III. Experimental Setup

This section gives detailed description about the simulation environment which is used to evaluate the performance of encryption algorithms. It also describes the system components that are used in the experiment. The experiments use the classes that are provided by .NET Environment for AES (Rijindael). Blowfish is implemented using BLOWFISH.NET. The implemented algorithm is optimized to give the maximum performance AES algorithm uses the managed wrappers that are available in the System.Security.Cryptography Name Space. The following Table shows the settings for the algorithms that are used in the experiment.

TABLE I Key and Block size

S.No	Algorithm	Key Size	Block Size
1	Blowfish	448	64
2	Rijindael	128	128
3	Rijindael	192	128
4	Rijindael	256 *	128

*Default length is 256.

A. Methodology

This section gives detailed descriptions about the methodology related parameter such as system parameters, experimental criteria(s) and simulation initial settings.

B. System parameters

The experiments are conducted using Pentium P4 2.4 GHz CPU with 2GB RAM. The experiments are performed several times to assure the results are constant and are valid to compare the different algorithms.

C. Experimental Criteria(s)

Several performance metrics are used to evaluate the performance of the encryption algorithms such as Encryption time, Decryption time, CPU process time, and CPU clock cycles and Battery[13],[14]. Encryption time is the total time taken to produce a cipher text from plain text. The calculated encryption time is then used to calculate the throughput of the encrypted algorithm. It gives the rate of encryption. The throughput of the encryption scheme is calculated as the total encrypted plaintext in bytes divided by the encryption time. Decryption time is the total time taken to produce the plain text from plain text. The calculated decryption time is then used to calculate the throughput of the decrypted algorithm. It gives the rate of decryption. The throughput of the decryption scheme is calculated as the total decrypted plaintext in bytes divided by the decryption time. The CPU process time is the time that is required to a CPU is dedicated only to the particular process of calculations. It reflects the load of the CPU. The CPU clock cycles are a metric,

reflecting the energy consumption of the CPU while performing on encryption operations. Each cycle of CPU will consume a minute amount of energy

D. Experimental Procedures

Several experimental procedures are used such as different encoding techniques for encryption, different packet sizes of data, different data types and different key sizes. In the case of encoding two types are used such as Base64 encoding and hexadecimal encoding. Packet size range from 0.5 MB to 20MB is used. Different data types such as text or document and images are used for each selected algorithms. Different key sizes are employed to trace the performance of the selected algorithms specifically power consumption.

IV. Results

This section describes the series of results based on the experimental procedures that are described in the previous sections such as encoding techniques, packet size, data types and keys. The experiments are performed several times to assure the results are constant and are valid to compare the different algorithms. Different system configurations are used o get better comparison results. Laptop , standalone PC and Networked PCs are also used to track the performance of the algorithms.

A. Results based on encoding techniques

Encoding techniques plays a vital role in cryptography. It is very necessary to use these techniques in evaluating the performance of cryptographic algorithms. In this work, two encoding methods are taken into consideration used such as Base64 encoding and hexadecimal encoding. Base64 is an encoding algorithm used to alter text and binary streams into printable and easy-to-process form to be consumed by various programs as well as transmitted over the network. The amount of information encoded by one hexadecimal digit is called nibble and is exactly a half of octet (8 bits). These techniques are employed for both the algorithm such as Blowfish and AES. The results are given in Fig 1 and Fig2 for the above mentioned algorithms with different encoding techniques. Fig 1 shows the result of base64 encoding and Fig 2 shows the result of hexadecimal encoding. From the result it is identified that there is no significant difference for both the encoding methods. It is identified that two methods almost gives the same result.

TABLE II Time consumption (Base64 Encoding)

Packet	Packet Size	Time (Millisecond)	
		Blowfish	Rijindael
P1	1024.00 Kb	508 Ms	647 Ms
P2	1500.02 Kb	621 Ms	712 Ms
P3	2100.50 Kb	854 Ms	902 Ms
P4	2512.67 Kb	978 Ms	1012 Ms
P5	3124.21 Kb	1021 Ms	1278 Ms
P6	5100.50 Kb	1520 Ms	1590 Ms

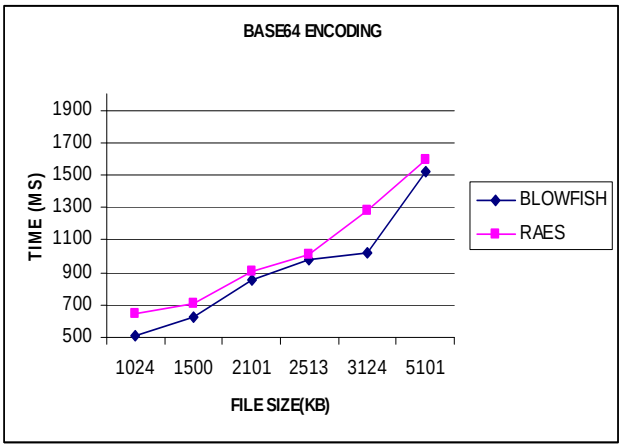

Figure 1: Time consumption (Base64 Encoding)

TABLE III Time Consumption Hexadecimal Encoding

Packet	Packet Size	Time (Millisecond)	
		Blowfish	Rijindael
P1	1024.00 Kb	508 Ms	647 Ms
P2	1500.02 Kb	621 Ms	712 Ms
P3	2100.50 Kb	854 Ms	902 Ms
P4	2512.67 Kb	978 Ms	1012 Ms
P5	3124.21 Kb	1021 Ms	1278 Ms
P6	5100.50 Kb	1520 Ms	1590 Ms

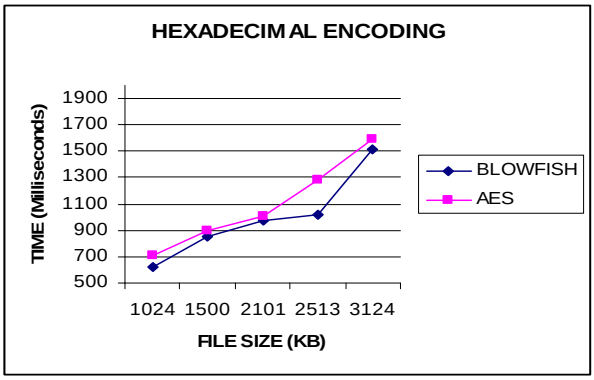

Figure 2: Time consumption (Hexadecimal Encoding)

B. Results based on different packet sizes

Encryption time is used to calculate the throughput ofan encryption scheme. It indicates the speed of encryption. Different packet sizes are used in this experiment for both Blowfish and Rijindael algorithms. The encryption time is recorded for both the encryption algorithms. The average data rate is calculated for Blowfish and Rijindael based on the recorded data. The formula used for calculating average data rate is

$$AvgTime = \frac{1}{Nb}\sum_{I=1}^{Nb}\frac{Mi}{ti}(Kb/s) \qquad (1)$$

Where

AvgTime = Average Data Rate (Kb/s)
Nb = Number of Messages
Mi=Message Size (Kb)
Ti=Time taken to Encrypt Message Mi

Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated using the following formula

$$Throughput = \frac{Tp}{Et} \qquad (2)$$

Tp= Total Plain text
Et= Encryption time

It is very important to calculate the throughput time for the encryption algorithm to known better performance of the algorithm.

TABLE IV TIME CONSUMPTION (ENCRYPTION)

Input Size(Kb)	Time (Millisecond)	
	Blowfish	Rijindael
45	40	58
76	72	87
102	90	102
500	121	134
900	220	234
1025	310	364
AvgTime	**143.8**	**175.5**
Throughput	**18.14**	**15.08**

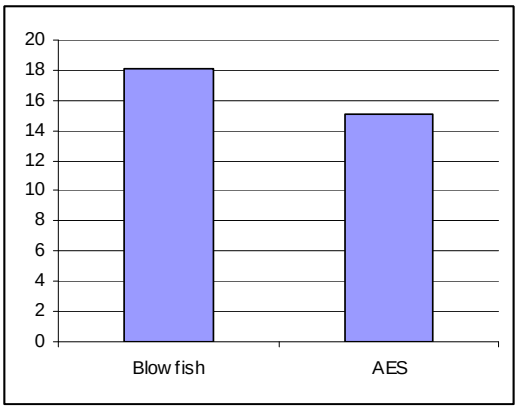

Figure 3: Time consumption (Encryption)

Figure 3 shows the result based on the throughput of the encryption with different packet size. It shows that the throughput is high for Blowfish when compared to that of AES. As the throughput value is increased, the power consumption of the encryption technique is decreased. So from the experiment it proves that blowfish encryption algorithm consumes less power for encrypting the text than that of AES.

TABLE V TIME CONSUMPTION (DECRYPTION)

Input Size(Kb)	Time (Millisecond)	
	Blowfish	Rijindael
45	38	56
76	86	94
102	93	105
500	130	167
900	206	267
1025	300	301
AvgTime	**142.1**	**165**
Throughput	**18.62**	**16.04**

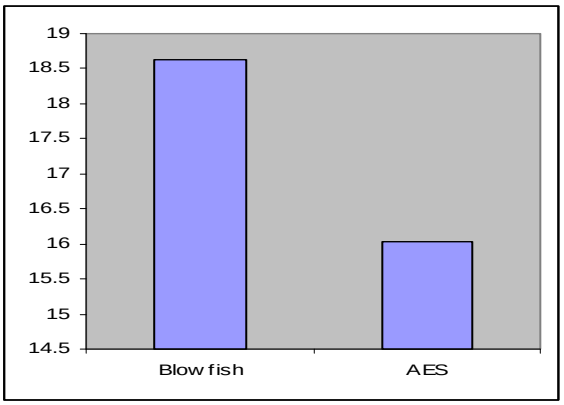

Figure 4: Time consumption (Decryption)

Figure 4 shows the result based on the throughput of the decryption with different packet size. It shows that the throughput is high for Blowfish when compared to that of AES. As the throughput value is increased, the power consumption of the decryption technique is decreased. So from the experiment it proves that blowfish decryption algorithm consumes less power for decrypting the text than that of AES.

C. Results based on different Data types

In the previous section, the comparison is conducted for the text and document data files. In this section it was identified that the Blowfish encryption has the good performance than AES for text and document data files. Now the comparison will be done for other data types such as images to identify the performance of Blowfish and Rijindael. Fig 5 shows the result for encryption and Fig 6 for decryption for images. Different formats of images are taken into consideration to track the performance of the algorithms.

TABLE VI TIME CONSUMPTION FOR IMAGE (ENCRYPTION)

Image(JPEG)	Time (Millisecond)	
	Blowfish	Rijindael
Img1	87	102
Img2	99	123
Img3	134	234
Img4	156	267
Img5	198	278
Img6	345	456
AvgTime	**169.8**	**243.3**
Throughput	**15.9**	**10.8**

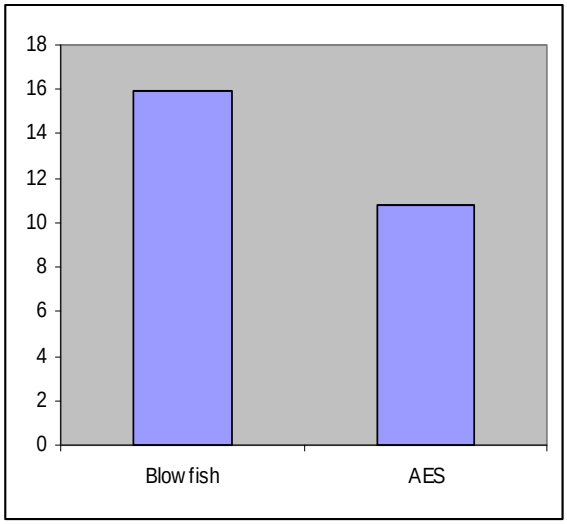

Figure 5: Time consumption (Encryption)

TABLE VII TIME CONSUMPTION FOR IMAGE (DECRYPTION)

Image(JPEG)	Time (Millisecond)	
	Blowfish	Rijindael
Img1	76	92
Img2	95	111
Img3	120	136
Img4	146	162
Img5	168	184
Img6	267	283
AvgTime	**145.3**	**161.3**
Throughput	**18.2**	**16.4**

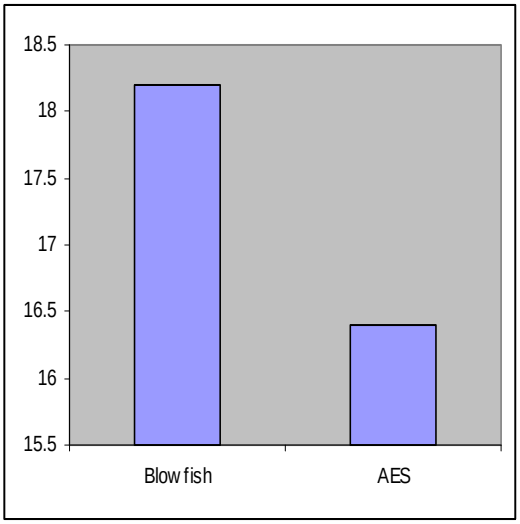

Figure 6: Time consumption (Decryption)

D. Results based on Different Key Size

The last performance comparison point is the changing different key sizes for AES and RC6 algorithm. In case of AES, We consider the three different key sizes possible i.e., 128 bit, 192 bits and 256 bit keys. In case of AES it can be seen that higher key size leads to clear change in the battery and time consumption. It can be seen that going from 128 bits key to 192 bits causes increase in power and time consumption about 8% and to 256 bit key causes an increase of 16%

TABLE VIII: TIME CONSUMPTION (DIFFERENT KEY SIZE)

Input Size(Kb)	Time (Millisecond)		
	AES 128	AES 192	AES 256
45	38	56	67
76	86	94	102
102	93	105	121
500	130	167	178
900	206	267	290
1025	300	301	320
AvgTime	**142.1**	**165**	**179.6**
Throughput	**18.62**	**16.04**	**14.73**

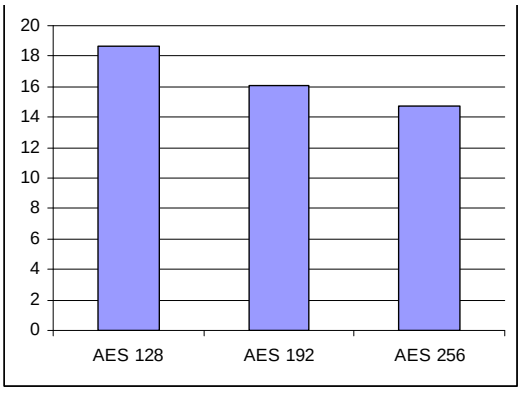

Figure 7: Analysis with different key size

V. CONCLUSION

This paper presented the performance evaluation of two commonly known symmetric cryptographic algorithms. These algorithms are tested with different performance metrics. The simulation results shows that Blowfish has better performance than AES in almost all the test cases. There is no significant difference in the result for base64 encoding and hexadecimal encoding techniques. It is found that blowfish is good for text based encryption where as AES has better performance for image encryption. It is also identified that there is change in performance when there is a change in key size of AES algorithm. Overall it is identified that AES can be used in circumstances where there is need for high security. In the case of performance aspects, Blowfish can be used. With this analysis future work is planned to introduce a new 512 bit block cipher.

REFERENCES

[1]. Choudhary, A.R. Sekelsky, A. “Securing IPv6 network infrastructure: A new security model”, IEEE International conference on Technologies for Homeland Security, 2010.

[2]. W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309 .

[3]. Marin, G.A.,” Network security basics”, IEEE Security and Privacy, 1[3], 68, 2005.

[4]. Tingyuan Nie Teng Zhang,” A study of DES and Blowfish encryption algorithm, Tencon IEEE Conference,, 2009

[5]. Xinmiao Zhang Parhi, K.K. “Implementation approaches for the Advanced Encryption Standard algorithm”, IEEE Circuits and Systems, 2[4], 2002.

[6]. R. Chandramouli, "Battery power-aware encryption - ACM Transactions on Information and System Security (TISSEC)," Volume 9 , Issue 2 ,May. 2006.

[7]. S.Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," university of Pittsburgh, April 9, 2003. Retrieved October 1, 2008,

[8]. Nadeem, A.; Javed, M.Y, "A Performance Comparison of Data Encryption Algorithms," IEEE Information and Communication Technologies, 2005. ICICT 2005. First International Conference, 2006-02-27, PP. 84- 89.

[9]. S.Z.S. Idrus,S.A.Aljunid,S.M.Asi, "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008 ,PP 20-25.

[10]. Krishnamurthy G.N, Dr. V. Ramaswamy, Leela G.H and Ashalatha M.E,” Performance enhancement of Blowfish and CAST-128 algorithms and Security analysis of improved Blowfish algorithm using Avalanche effect”, International Journal of Computer Science and Network Security, 8(3), 2008

[11]. Downnard.I,”Public-key cryptography extensions into Kerberos”,IEEE Potentials, 21(5), 30 – 34, 2003.

[12]. Dorothy E. R. Denning, Cryptography and Data Security. Massachusetts: Addison-Wesley, 1982.

[13]. Tingyuan Nie, Chuanwang Songa, Xulong Zhi (2010), “Performance Evaluation of DES and Blowfish Algorithms”, Proceedings of 2010 IEEE

International Conference on Biomedical Engineering and Computer Science (ICBECS 2010), 23-25 Apr 2010. pp 1-4

[14]. Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader Mohiy Mohamed Hadhoud (2010),"Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Diferent Data Types", International Journal of Network Security, Vol.11, No.2, Sept. 2010, pp 78–87.

M. Anand Kumar received the B.Sc. and M.Sc. degrees in Computer Science from Bharathiar University, Coimbatore, India, in 2001 and 2003 respectively. He is Lecturer at the Department of Information Technology, Karpagam University, India. He is pursuing his doctoral degree at Karpagam University. His area of research includes network security and information security. He has presented fifteen papers in national conferences and four papers in international conferences. He has published six papers in international journals

Dr.S.Karthikeyan presently working as Assistant Professor, College of Applied Sciences, Oman and previously he was a Senior Lecturer at Caledonian College of Engineering, Oman. He was a Professor & Director at Karpagam University, School of Computer Science and Applications, Coimbatore. He has total of 14 years of teaching and research experience. Dr.Karthikeyan completed his PhD at Alagappa University, Karaikudi, India in the area of Network Security, Computer Science and Engineering by Feb 2008. He has 32 research papers and guiding 11 PhD research scholars from various universities in India and he has also guided 19 M.Phil students. He is Chief and guest editor of various national and international journals. He has chaired many conference sessions and served as Technical Committee member of various boards at various colleges, universities and conferences.

