COMPARATIVE ANALYSIS OF SYMMETRIC ENCRYPTION ALGORITHMS FOR DATA COMMUNICATION

M. Anand kumar[1], *S. Umadevi*[2]

ABSTRACT

The Internet today is being used by billions of users for a large variety of commercial and non commercial purposes. It was maintained by different administrative organizations. Internet is mainly used as an efficient means for communication, entertainment and education. There is a need for protecting confidential data because of the rapid growth of Internet. The Internet was however originally designed for research and educational purpose and not for commercial applications. Internet model was not designed with security in mind. Cryptography plays a vital role in the information and network security. This paper mainly focuses on three commonly used symmetric encryption algorithms such as Blowfish, Camellia and Rejindael. These algorithms are implemented and are compared to evaluate the performance of these algorithms.

Keywords—*Blowfish, Camellia, Cryptography, AES, Internet, Security, Symmetric algorithms*

I. INTRODUCTION

The usage of current version of Internet and TCP/IP Suite results in many flaws such as: Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. Repudiation is the ability of users to deny that they performed specific actions or transactions. Eavesdropping is process of capturing packets from the network transmitted by others computers and reading the data content in search of sensitive information like passwords, tokens, or any kind of secret information, Denial of service is the process of making a system or application unavailable [1].

Cryptography is the science that is widely used for the network security. Key aspects of cryptography are privacy, authentication, identification, trust and verification [2] [12]. 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, application and use The cryptographic algorithms can be broadly divided into three types namely Secret Key Cryptography (SKC), Public Key cryptography (PKC) and

[1] Lecturer, Department of Information Technology, Karpagam University, Coimbatore
E-mail : anand2kumar@gmail.com

[2] Lecturer, Department of Information Technology, Karpagam University,

Hash Functions Some of the secret key algorithms are Data encryption standard (DES), Advanced encryption standard (AES), CAST, Camellia, 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]. This work presents the performance evaluation of three most commonly used algorithms.

The rest of the paper is organized as follows. Blowfish, Camellia and AES algorithms are described in section II that is followed by related works in section III. In section IV Simulation and performance criteria of Blowfish Camellia and AES is presented. Results are given in section V and finally we conclude in section VI.

II Symmetric Cryptographic algorithms

Symmetric cryptographic algorithms [4] are also referred to as secret-key algorithms, single key algorithms, or one-key algorithms. In such algorithms, the encryption key can be calculated from the decryption key. In symmetric algorithms, the encryption key and the decryption key are trivially related, often identical. Encryption and decryption with a symmetric algorithm are denoted by

$$EK(M)=C \qquad (1)$$

$$DK(C)=M$$

These algorithms require that the sender and receiver agree on a key before they can communicate in a secured manner. Security of a symmetric algorithm is mainly based on keys; divulging the key means that anyone could encrypt and decrypt the information. As much as the communication needs to remain secret, the key must remain secret. Some examples of popular and well-respected symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, Camellia, 3DES, and IDEA. This work only focuses on Blowfish, Camellia and AES symmetric algorithms.

A. Blowfish: Blowfish: Blowfish [5] 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. Every round contains a key dependent permutation, a key and data-based substitution. Finally the operations are EX-ORs and additions on 32-bit words Blowfish is successor to Twofish

B. Camellia: Camellia [7] was jointly developed by Nippon Telegraph and Telephone Corporation and Mitsubishi Electric Corporation . This algorithm specifies the 128-bit block size and 128-, 192-, and 256-bit key sizes. It was based on feistel network cipher with 18 or 24 rounds.

- Main structure is similar to DES-like ciphers, not AES i.e. 18-round Feistel structure for 128-bit key and 24-round Feistel structure for 192- and 256-bit keys. The FL/FL-1 function layers are inserted every 6 rounds.

C. AES: AES [6] [13] is a block cipher .It has variable key length of 128, 192, or 256 bits; with the default 256.The algorithm encrypts data blocks of 128 bits in 10, 12 and 14 rounds mainly depends on the size of the key AES algorithm is fast and flexible when compared to other algorithms; it can be implemented on various platforms especially in small devices [6]. Also, AES has been carefully tested for many security applications [7] [14].

III. Related Works

The paper [8] introduced a new method to enhance the Bluefish Algorithm by building a new structure for the 16 rounds in the original algorithm and by replacing the OR operation with a introduced operation. The proposed structure makes use of multiple secrete keys. The principle of Cellular Automata (CA) is used to generate these multiple keys in a simple and effective way. It was concluded that proposed method provides high security and the system is very challenging to attempts of breaking the cryptography key. It is suitable and efficient for hardware implementation. Moreover the speed of encryption and decryption are also known to be faster than other popular existing algorithms

The paper [9] proposed an enhanced blowfish algorithm. The key size of the algorithm was increased to 448 bits. With the propose algorithm, 64 bit data can be encrypted into RGB values and plotted as a pixel in a bitmap image. It was concluded that the security of blowfish algorithm is enhanced by using water marking technology

The work [9] pointed out the strength and weakness of the AES algorithm. It was stated that the design's simplicity makes the algorithm easy to understand and implement efficiently. It also fa-cilitates understanding the mecha-nisms that give the algorithm its high resistance against differential cryptanalysis and linear cryptanal-ysis. The paper [15] pointed out that that AES-128 with the number of rounds reduced from 10 to 6, AES-192 with the rounds reduced from 12 to 7, and AES-256 with the rounds reduced from 14 to 7 had less than optimal security against chosen-plaintext attacks. The work also stated that the rebound attack illus-trated that hash function designs based on the AES design prin-ciples don't automatically inherit the security level. Indeed, AES's bounds rely on a secret key for their strength.

The paper [7] presented the cryptanalysis in the approach used to choose plaintexts or cipher texts in certain previously published square-like cryptanalytic results for Camellia and give two possible approaches to solve the problem. Finally by using the advantage of the previous abort technique and a few findings on the key schedule of the algorithm, the researcher presented impossible differential attacks on 10-round Camellia with the FL/FL-1functions under 128 key bits, 11-round Camellia with the FL/FL-1 functions under 192 key bits, 14-roundCamellia without the FL/FL-1 functions under 192 key bits and 16-round Camellia without the FL/FL-1functions under 256 key bits.

IV. Simulation

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.

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.

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 [3]. 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 which gives the rate of encryption. The throughput is calculated as the total encrypted plaintext in bytes divided by the encryption time. The time for decryption 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 which replicate the load of the CPU. The clock cycles of CPU are a metric, which reflects the energy use of the CPU while performing on encryption operations. Each cycle of CPU will consume a minute amount of energy [16].

V. 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 [10] 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. Table 1 show the time comparison of Base64 encoding and table 2 shows the details of hexadecimal encoding. 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 : I Time consumption (Base64 Encoding)

S.No	Packet Size (KB)	Time Consumption(Hexadecimal Encoding)		
		Blowfish	Camellia	AES
1	1024.00	510 ms	691 ms	507 ms
2	1498.00	614 ms	806 ms	629 ms
3	2103.02	706 ms	851 ms	682 ms
4	2514.12	757 ms	947 ms	749 ms
5	5103.08	1573 ms	1652 ms	1508 ms

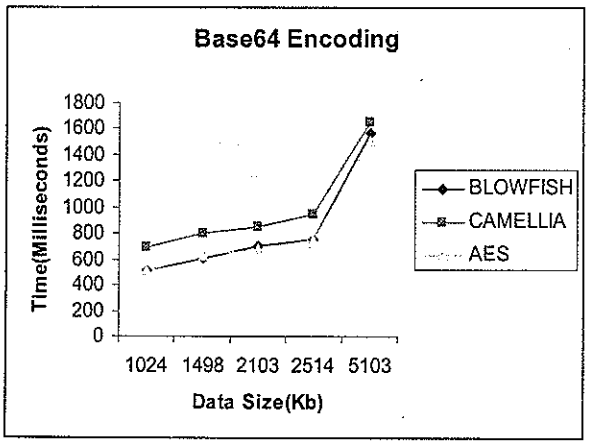

Figure 1: Time consumption (Base 64 Encoding)

TABLE II. Time consumption (Hexadecimal Encoding)

S.No	Packet Size (KB)	Time Consumption(Hexadecimal Encoding)		
		Blowfish	Camellia	AES
1	1024.00	515 ms	695 ms	507 ms
2	1498.00	614 ms	806 ms	629 ms
3	2103.02	706 ms	859 ms	679 ms
4	2514.12	749 ms	947 ms	749 ms
5	5103.08	1569 ms	1651 ms	1512 ms

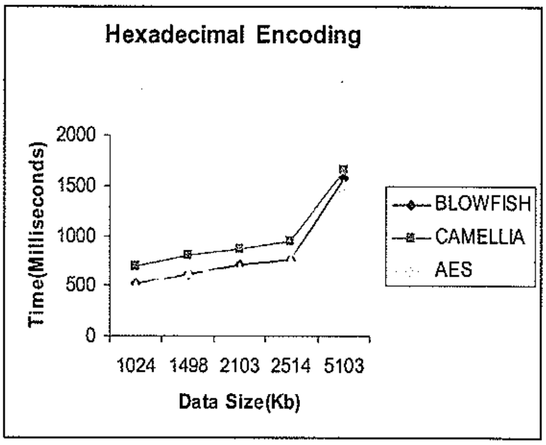

Figure 2: Time consumption (Hexa-Decimal Encoding)

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 Blowfish, Camellia and Rijindael algorithms. The encryption time is recorded for all the encryption algorithms. The average data rate is calculated for Blowfish, Camellia and Rijindael algorithms based on the recorded data. The formula used for calculating average data rate is

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

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 the encryption process. It specifies the speed of encryption. The throughput of the encryption process is calculated using the following formula

$$Throughput = \frac{Tp}{Et} \qquad (3)$$

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 3 shows the time consumption of algorithms for encryption where as Table 4 shows the time consumption for decryption.

TABLE III. TIME CONSUMPTION (ENCRYPTION)

S.No	Packet Size (KB)	Time Consumption(Encryption)		
		Blowfish	Camellia	AES
1	49	59	78	56
2	59	39	46	38
3	100	94	104	90
4	247	121	134	112
5	321	167	198	164
6.	694	234	267	210
7	899	254	342	258
8	963	213	456	208
9	5345	1324	1521	1237
10	7310	1432	1743	1366
Average		393	488.9	374
Throughput		4.06	3.26	4.27

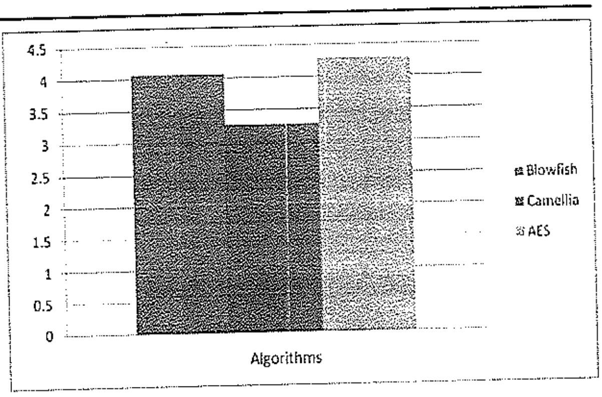

Figure 3: Time consumption (Encryption)

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 and Camellia. As the throughput value is increased, the power consumption of the encryption technique is decreased.

TABLE IV. TIME CONSUMPTION (DECRYPTION)

S.No	Packet Size (KB)	Time Consumption(Encryption)		
		Blowfish	Camellia	AES
1	49	65	78	61
2	59	45	56	43
3	100	89	97	79
4	247	120	131	112
5	321	167	198	168
6	694	243	301	212
7	899	223	378	259
8	963	334	423	309
9	5345	1224	1676	1216
10	7310	1435	1943	1363
Average		394	528	382
Throughput		4.05	3.02	4.18

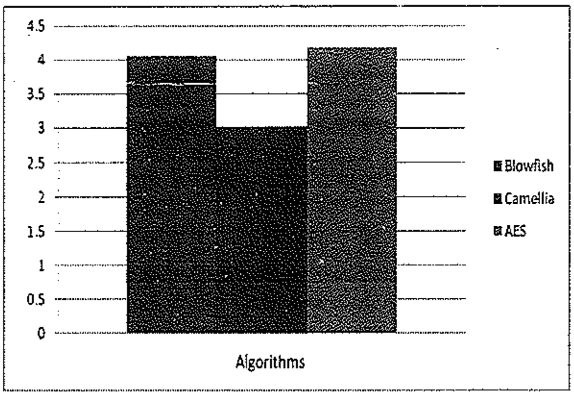

Figure 4: Time consumption (Decryption)

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, Camellia and Rijindael. Table 5 and 6 gives the time consumption for image encryption and decryption. 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 V. Time consumption (IMAGE ENCRYPTION)

S.No	Files	Packet Size (KB)	Time Consumption(Encryption)		
			Blowfish	Camellia	AES
1	Image1.jpg	27.81	69.98	72.61	63.72
2	Image2.jpg	59.07	75.87	89.81	45.28
3	Image3.jpg	92.21	94.51	112.23	81.16
4	Image4.jpg	143.25	124.83	187.39	114.21
5	Image5.jpg	187.04	171.92	251.61	170.11
6	Image6.jpg	241.50	247.87	292.08	214.07
7	Image7.jpg	301.02	227.84	321.23	261.24
8	Image8.jpg	375.04	248.54	389.78	208.07
9	Image9.jpg	763.17	1228.76	1391.07	1218.16
10	Samp1. jpg	943.23	1440.01	1678.12	1365.08

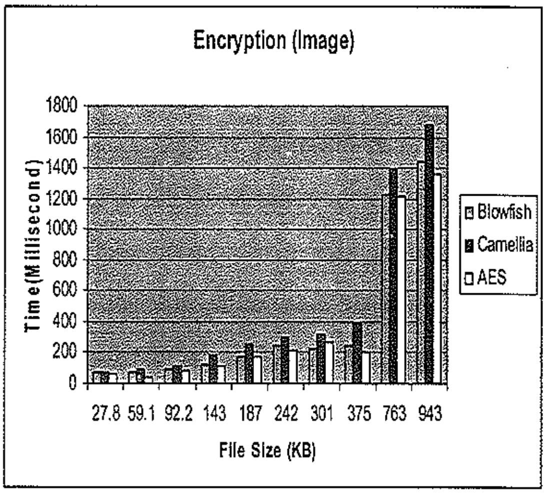

Figure 5: Time consumption (Image Encryption)

TABLE VI Time consumption (image Decryption)

S.No	Files	Packet Size (KB)	Time Consumption(Encryption)		
			Blowfish	Camellia	AES
1	Image1.jpg	27.81	69.99	74.12	63.73
2	Image2.jpg	59.07	75.88	86.54	45.29
3	Image3.jpg	92.21	94.52	107.09	81.17
4	Image4.jpg	143.25	124.84	185.12	114.22
5	Image5.jpg	187.04	171.93	247.05	170.12
6	Image6.jpg	241.50	247.88	292.72	214.08
7	Image7.jpg	301.02	227.84	334.14	261.24
8	Image8.jpg	375.04	248.54	376.12	208.07
9	Image9.jpg	763.17	1228.76	1323.02	1218.16
10	Samp1. jpg	943.23	1440.01	1612.08	1365.08

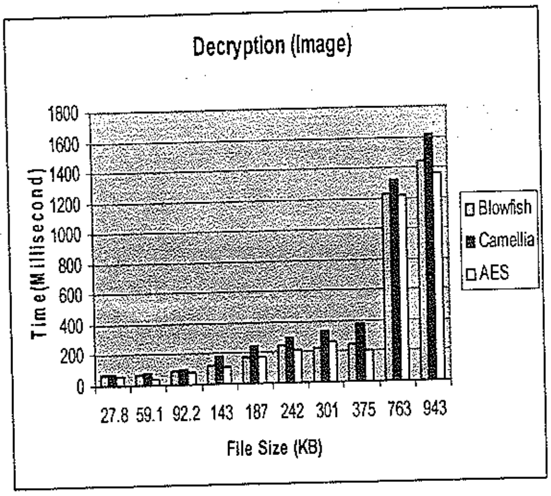

Figure 6: Time Consumption (Image Decryption)

VI .Conclusion

This paper presented the performance evaluation of three 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 AES is good for text based encryption as well as for image. 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] Caicedo, C. E., J. B. Joshi, and D. Tuladhar, 2009. IPv6 Security Challenges, IEEE Computer., 42(2): 36-42.

[2] Delgosha, F., and F. Fekri, 2006. Public-key cryptography using Para unitary matrices, IEEE Transactions on Signal Processing, 54(9): 3489-3504.

[3] Diaa Salama Abdul, Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, 2008. Performance Evaluation of Symmetric Encryption Algorithms, International Journal of Computer Science and Network Security, 8(12): 78-85.

[4] Elminaam, D. S. Abd., H. Kader, M. Abdual and Hadhoud., M. Mohamed, 2010. Evaluating the Performance of Symmetric Encryption Algorithms, International Journal of Network Security, 10(3): 216-222.

[5] Gurjeevan Singh, K. Ashwani Kumar, and S. Sandha , 2011. A Study of New Trends in Blowfish Algorithm, International Journal of Engineering Research and Applications, 1(2): 321-326.

[6] Hua li, and Jianzhou li, 2008. A new compact dual-core architecture for AES encryption and decryption, Canadian Journal of Electrical and Computer Engineering, 33(3): 209-213.

[7] Lu, J.; Wei, Y.; Fouque, P.A.; Kim, J., *"Cryptanalysis of reduced versions of the Camellia block cipher,"* Information Security, IET , vol.6, no.3, pp.228,238, Sept. 2012

[8] Afaf, M. Ali Al-Neaimi, and Rehab F. Hassan, 2011. New Approach for Modifying Blowfish Algorithm by Using Multiple Keys, International Journal of Computer Science and Network Security, 11(3): 21-26.

[9] Palaniswamy, N., M. Dipesh Dugar, N. Dinesh Kumar Jain, and G. Raaja Sarabhoje, 2010. Enhanced Blowfish algorithm using bitmap image pixel plotting for security improvisation, Education Technology and Computer, (1): 533-538.

[10] Daemen, J., and V. Rijmen, 2010. The First 10 Years of Advanced Encryption, IEEE Security and Privacy, 8(6): 72-74.

[11] Jingmei Liu., Baodian Wei, Xiangguo Cheng, and Xinmei Wang, 2005. An AES S-box to Increase Complexity and Cryptographic Analysis, Proceedings of IEEE International Conference on Advanced Information Networking and Applications, 1-5.

[12] Kartalopoulos, S.V. , 2006. A primer on cryptography in communications, IEEE Communications Magazine, 44(4): 146-151

[13] Li, Xiang., Chen, Junli, Liu, Weixiao, and Wan, Wanggen 2009. An improved AES encryption algorithm, Wireless Mobile and Computing 1(1): 694-698.

[14] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, 2007.A Modified AES Based Algorithm for Image Encryption, World Academy of Science, Engineering and Technology, 3(1): 526-531.

[15] Mohan H. S., and Raji Reddy, A. , 2011. Performance Analysis of AES and MARS Encryption Algorithms, International Journal of Computer Science Issues, 8(4): 363-368.

[16] Monika Agrawal, and Pradeep Mishra, 2012. A Comparative Survey on Symmetric Key Encryption Techniques, International Journal on Computer Science and Engineering, 4(5): 877-882.

Author's Biography

Dr. M. Anand Kumar has completed M.Sc in Bharathiar University and M.Phil computer science from Periyar University. He has Completed Ph.D in Karpagam University and currently working as a Lecturer in karpagam University having eight years experience in teaching.. His area of research includes network security and information security. He has presented twenty papers in national conferences and four papers in international conferences. He has published nine papers in international journals

S. Umadevi has completed MCA in Anna university and currently working as a Lecturer in karpagam University having two years experience in teaching.. Her area of research includes network security and information security. She has presented one paper in national conference.