An Approach to Avoid Intruder Attack While Transmitting Large Message Over Insecure Channel

Khushbu D. Patel[1], Hitesh Chhinkaniwala[2]

[1] *Masters Engineering Student, Computer Science and Engineering, GTU PG School, Gujarat, India*

[2]*Associate Professor, Adani Institute of Infrastructure Engineering (AIIE), Ahmedabad, Gujarat, India*

Abstract

21st century is information century. Information technology is used in every area form earth to universe. Information security is important in today's world. Because in today's intruders are increasing to affect information security. Intruders are affect information security like to change, destroy, illegal access, selling information, etc. Especially when information is travelling in insecure network. In todays and past widely use cryptography to secure information from intruder in insecure channel. In cryptography has two methods to secure information. Both methods have own advantages and disadvantages. Symmetric key cryptography has use only one key for encryption and decryption. It is a secure when key is secure. To provide a security to key in transfer in insecure network use asymmetric key cryptography. In asymmetric key cryptography use two key one is public and another is private. Asymmetric key cryptography is providing more security compare to symmetric key cryptography. Symmetric key cryptography is fast and asymmetric key cryptography is slow compare to each other. Use hybrid cryptography for avoid intruder attack while transmitting large message over insecure channel.

Keyword: *symmetric key cryptography, asymmetric key cryptography, hybrid cryptography, intruder attack*

1. Introduction

Data security is in Demand in everyday life of digital world, since digital data can be reproduced much easily. An intruder is a person who attempts to gain unauthorized access of information or system, to damage that information or system. Intruders are attempt to violate security by interfering with information or system availability, confidentiality and integrity [1]. Cryptography is a science which uses mathematics concept to encrypt and decrypt information [2] [3] [4]. Cryptography is used to store sensitive information or transmit information securely in insecure channel so that it cannot be read by any person except intended receiver [5]. Cryptography has two basic techniques' encryption and decryption. Encryption is a process of translating original data into something that appear to be random and meaningless also it's called as cipher text or encrypted text. Decryption is a process of translating encrypted text to original data also it's called as plain text. To provide a security cryptography has two basic methods or types [5] [6]. That has categorize using its key and it is Symmetric key cryptography and Asymmetric key cryptography. In symmetric key cryptography has sender and receiver use only one key for encryption and decryption. In asymmetric key cryptography has sender and receiver use two different key but logically related key public key and private key for encryption and decryption. Principles of security are authentication, integrity, confidentiality, non-repudiation [13] [15]. These all principles are implement using either Symmetric Key Cryptography or Asymmetric Key Cryptography or using both cryptographic methods for more than one principles achieve.

1.1 Security Issues using symmetric and asymmetric key cryptography

Symmetric key cryptography and asymmetric key cryptography has security related issues. Issue using symmetric key cryptography is how to share secret key securely in network. In Symmetric key cryptography, has produce every user to different secrete key so, it is creating a problem to manage all these key and ensure to particular user has this particular key. Symmetric key cryptography has use sender and receiver both same key to encryption and decryption so it is not providing authenticity to data or information come from particular user [17]. It is a major issue because unauthorized person can send or receive data or information to authorize person. Big issue of asymmetric key cryptography is slower and need more processing power because of its complexity. It is a 1000 time slower than symmetric key cryptography [9].

2. Hybrid Cryptography

Achieve security requirement and solve issues related to symmetric and asymmetric key cryptography use hybrid cryptography. Hybrid cryptography mean using both cryptographic techniques symmetric and asymmetric key cryptography at same time to encrypt or decrypt data or information [8] [10]. Using hybrid cryptography, overcome disadvantage of symmetric and asymmetric key cryptography. To use of symmetric key cryptography to overcome disadvantage of more time consuming of asymmetric key cryptography [11] and asymmetric key cryptography to overcome disadvantage of key management and sharing a key of symmetric key cryptography [12]. Encrypt original large message using symmetric key cryptography so it is fast and encrypt symmetric key is not large compare to message and it is encrypted by asymmetric key cryptography. So, issue of asymmetric key cryptography is solving. Attack on hybrid model is too poor and gives strong strength to encryption approach.

3. Proposed Model

In hybrid cryptography process has taken a message (M). Calculate hash value of message (M). Using hashing it's provide data integrity that ensures data will not change or it is an original data. After that message (M) is encrypted using Session key (K). Here, for encryption use AES/Blowfish symmetric key algorithm. Use session key because of it is provided redundancy. here, symmetric key encryption is complete.

In second step provide a security to transfer symmetric key (k) using RSA/ECC asymmetric key algorithm. First encrypt session key (K) to sender's private key and get key (k1), it is decrypted by sender's public key so it is providing an authentication. But here problem is sender's public key is everyone knows so security is break. So, encrypt key(K1) again using Receiver's public key so it is decrypted by only receiver's private key so security is not broken and it's provide a confidentiality. Here asymmetric key encryption is complete.

Last step is transfer message digest, encrypted message and encrypted symmetric key over an insecure channel.

Receiver side decryption process is done accordingly encryptions and verify a message using hash value.

Encryption process and decryption process are shown in Fig.1 and Fig. 2 respectively.

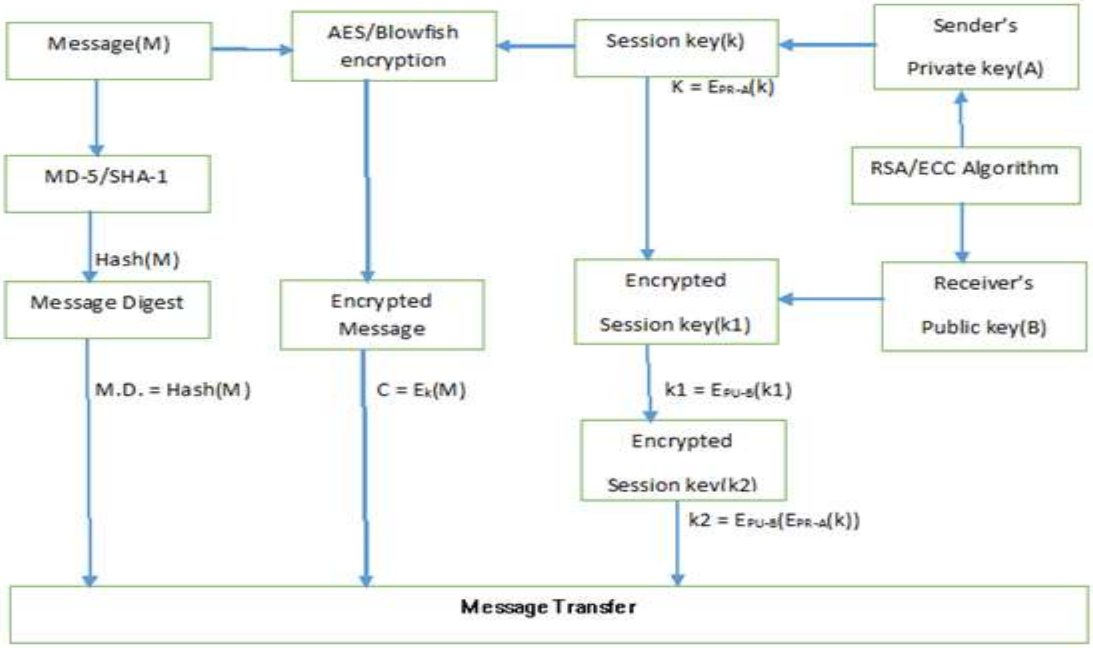

Fig-1 Sender Side Encryption

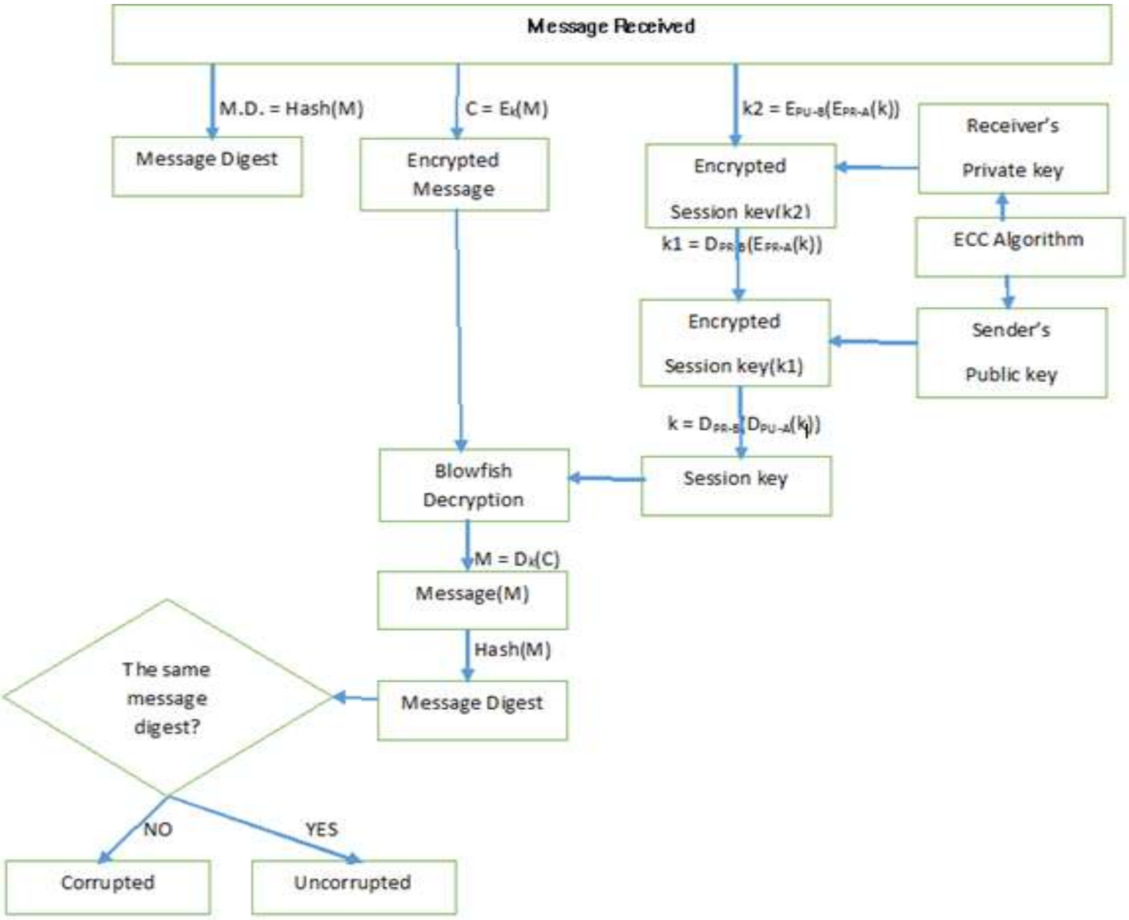

Fig-2 Receiver Side Decryption

4. IMPLEMENTATION

In this experiment use JAVA language for implementations, in JAVA use Java SE 8 Update 112 to implement a various algorithm in this experiment. Java has two elements that provide security: JCA (Java Cryptography Architecture) and JCE (Java Cryptography Extension). JCA provides digital signature and message digest, while JCE provides key agreements, encryptions, key generations and message authentication algorithms. To transfer a data between two parties socket programming is use. generatekey() is the method of KeyGenerator class which is used to generate secret key for symmetric key generation. generateKeyPair () is the method of KeyPairGenerator class which is used to generate public and private key for asymmetric key generation. Cipher is the class which is initialized either as encrypt mode or decrypt mode to perform relevant operation.

5. EXPERIMENTAL RESULTS AND ANALYSIS

This section contains the test results of our experiments for proposed approach. It shows an encryption and decryption total time taken by the various file size using different algorithms combinations. In experiment uses symmetric key algorithm AES and Blowfish, asymmetric key algorithms RSA and ECC and hashing algorithms MD-5 and SHA-1. Based on these algorithms find different combinations. This experiment is based on symmetric key size 128 bits and asymmetric key size are 1024 bits for RSA and 128 bits for ECC. Time is calculating in milliseconds. Table 1 shows results of 1MB, 3MB, 5MB and 10MB files. In results calculate individual algorithms time for encryption and decryption. After calculation of individual time sum a time value of different combinations to find total time of proposed system. Fig-3 shows graphical representation of encryption time for different combinations. Graph is generated for 1MB, 3MB, 5MB and 10MB file size. Graph shows comparison of different combinations based on encryption time. Graph shows BLOWFISH-MD5-ECC PRI-ECC PUB is a best combination for encryption. Fig-4 shows graphical representation of decryption time for different combinations. Graph shows comparison of different combinations based on decryption time. Graph shows BLOWFISH-MD5-ECC PRI-ECC PUB is a best combination for decryption.

Table-1: Total encryption and decryption time of different algorithm combinations

File Size	Different Algorithms combinations	Total Encryption Time (in ms)	Total Decryption Time (in ms)
1MB	AES - MD5 - RSA PRI - RSA PUB	266	173.69
	AES - SHA1 - RSA PRI - RSA PUB	281	189.69
	BLOWFISH - MD5 - RSA PRI - RSA PUB	234	155.66
	BLOWFISH - SHA1 - RSA PRI - RSA PUB	249	171.66
	AES - MD5 – ECC PRI - ECC PUB	156.51	64.12
	AES - SHA1 - ECC PRI - ECC PUB	171.51	80.12
	BLOWFISH - MD5 - ECC PRI - ECC PUB	125.58	47.12
	BLOWFISH - SHA1 - ECC PRI - ECC PUB	140.58	63.12
3MB	AES - MD5 - RSA PRI - RSA PUB	291	202.68
	AES - SHA1 - RSA PRI - RSA PUB	322	233.68
	BLOWFISH - MD5 - RSA PRI - RSA PUB	276	186.68
	BLOWFISH - SHA1 - RSA PRI - RSA PUB	307	217.68
	AES - MD5 - ECC PRI - ECC PUB	171.78	94.15
	AES - SHA1 - ECC PRI - ECC PUB	202.78	125.15
	BLOWFISH - MD5 - ECC PRI - ECC PUB	156.78	78.15
	BLOWFISH - SHA1 - ECC PRI -ECC PUB	187.78	109.15
5MB	AES - MD5 - RSA PRI - RSA PUB	315	205.74
	AES - SHA1 - RSA PRI - RSA PUB	345	236.74
	BLOWFISH - MD5 - RSA PRI - RSA PUB	312	203.74
	BLOWFISH - SHA1 - RSA PRI -RSA PUB	343	234.74
	AES - MD5 - ECC PRI - ECC PUB	189.59	112.27
	AES - SHA1 - ECC PRI - ECC PUB	220.59	143.27
	BLOWFISH - MD5 - ECC PRI - ECC PUB	187.56	110.15
	BLOWFISH - SHA1 - ECC PRI -ECC PUB	218.56	141.15
File	**Different Algorithms combinations**	**Total Encryption**	**Total Decryption**

Size		**Time (in ms)**	**Time (in ms)**
10MB	AES - MD5 - RSA PRI – RSA PUB	338	249.85
	AES - SHA1 - RSA PRI - RSA PUB	385	296.85
	BLOWFISH - MD5 - RSA PRI - RSA PUB	330	234.70
	BLOWFISH – SHA1 - RSA PRI -RSA PUB	377	281.70
	AES - MD5 - ECC PRI - ECC PUB	234.62	156.14
	AES-SHA1 - ECC PRI - ECC PUB	281.62	203.14
	BLOWFISH - MD5 - ECC PRI - ECC PUB	226.62	141.14
	BLOWFISH - SHA1 - ECC PRI -ECC PUB	273.62	188.14

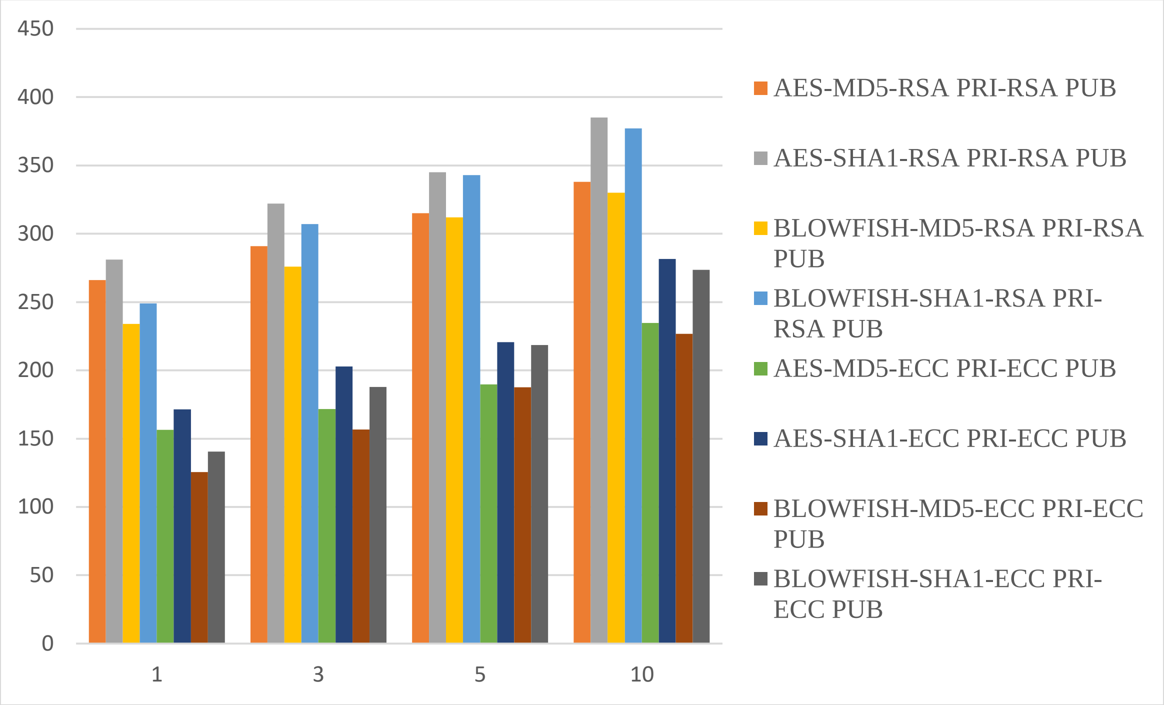

Fig-3 Comparisons of different combination based on encryption time

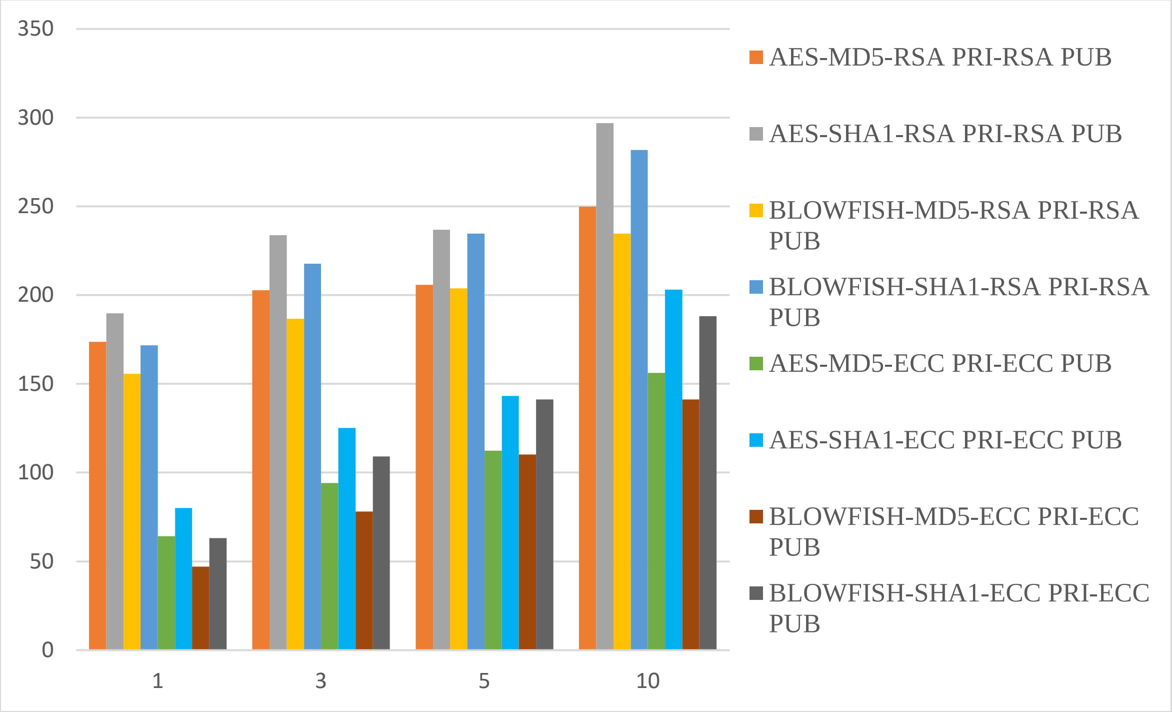

Fig-4 Comparisons of different combination based on decryption time

6. CONCLUSION

In this research work studied many papers related to hybrid cryptography according to study we found some problem related to security. Hybrid cryptography is provided a more efficiency and compensates each other’s weakness.

Proposed model is based on hybrid cryptography which might work to overcome the security problem. In our work hybrid cryptography, has use symmetric key algorithm, asymmetric key algorithm, and message digest/hash function in a proper way. Hybrid cryptography also provide the principle of security like authentication, confidentiality, integrity and non-repudiation.

Intruder attack has performed than it has easily identified using data integrity. Receiver known that in network some malicious activity performed so, it has asked a sender to resend data. This way we can avoid an intruder attack.

In result analysis shows total times of different combinations of algorithms. Based on results shows BLOWFISH - MD5 – ECC PRI – ECC PUB is best combination for encryptions and decryptions of data.

7. REFERENCES

[1] Jatoi, Piyar Ali, et al. "Exchanging information in wireless sensor networks at very low time consumption rate in an efficient hybrid cryptographic algorithm." Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronics Systems (VITAE), 2014 4th International Conference on. IEEE, 2014.

[2] Bhatele, Kirtiraj, Amit Sinhal, and Mayank Pathak. "A novel approach to the design of a new Hybrid security protocol Architecture." Advanced Communication Control and Computing Technologies (ICACCCT), 2012 IEEE International Conference on. IEEE, 2012.

[3] Chandra, Sourabh, et al. "A comparative survey of symmetric and asymmetric key cryptography." Electronics, Communication and Computational Engineering (ICECCE), 2014 International Conference on. IEEE, 2014.

[4] Blakley, G. R. "Twenty years of cryptography in the open literature." Security and Privacy, 1999. Proceedings of the 1999 IEEE Symposium on. IEEE, 1999.

[5] Kapur, Raj Kamal, and Sunil Kumar Khatri. "Secure data transfer in MANET using symmetric and asymmetric cryptography." Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2015 4th International Conference on. IEEE, 2015.

[6] Omura, Jim K. "Novel applications of cryptography in digital communications." IEEE Communications Magazine 28.5 (1990): 21-29.

[7] Guo, Wenping, Ying Chen, and Xiaoming Zhao. "A Study on High-Strength Communication Scheme Based on Signed Digital Envelope." Proceedings of the Second International Symposium on Networking and Network Security (ISNNS'10) Jinggangshan, PR China. 2010.

[8] Shen, Guicheng, and Xuefeng Zheng. "Java Cryptography Architecture and Security of Electronic Commerce." 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing. 2008.

[9] Jain, Amrita, and Vivek Kapoor. "Policy for Secure Communication using Hybrid Encryption Algorithm." *International Journal of Computer Applications*125.10 (2015).

[10] Alkady, Yasmin, Mohmed I. Habib, and Rawya Y. Rizk. "A new security protocol using hybrid cryptography algorithms." Computer Engineering Conference (ICENCO), 2013 9th International. IEEE, 2013.

[11] Karankar, Nilima, V. Kapoor, and C. P. Patidar. "An Innovative Digital Envelope Slant for an Unsecured Channel." (2014).

[12] Purevjav, Saranzaya, TaeYang Kim, and HoonJae Lee. "Email encryption using hybrid cryptosystem based on Android." 2016 18th International Conference on Advanced Communication Technology (ICACT). IEEE, 2016.

[13] Gobi, M., and K. Vivekanandan. "A new digital envelope approach for secure electronic medical records." IJCSNS 9.1 (2009): 1.

[14] Dubai, Manali J., T. R. Mahesh, and Pinaki A. Ghosh. "Design of new security algorithm: Using hybrid Cryptography architecture." Electronics Computer Technology (ICECT), 2011 3rd International Conference on. Vol. 5. IEEE, 2011.

[15] Ganesan, Ramachandran, and Kanniappan Vivekanandan. "A novel hybrid security model for e-commerce channel." Advances in Recent Technologies in Communication and Computing, 2009. ARTCom'09. International Conference on. IEEE, 2009.

[16] Mateescu, Georgiana, and Marius Vladescu. "A hybrid approach of system security for small and medium enterprises: Combining different cryptography techniques." Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on. IEEE, 2013.