ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Security Performance and Analysis of Rivest-Shamir-Adleman (RSA) Algorithm for ATM Transactions

Dr. Pradeep B Dahikar, *Minakshi S. Tumsare

Associate Professor, Dept. of Electronics, Kamla Nehru Mahavidyalaya, Nagpur, India

*Assistant Professor, Dept. of Electronics and Computer Science, RTM Nagpur University, Nagpur, India

ABSTRACT: In the current scenario, Data Security is required to transfer confidential information over the network. In inclusive range of applications, Security is also challenging. The cryptography is one of the useful techniques to transfer the unreadable data format by using public and private key. For data security Cryptographic algorithms play a vital role against spiteful attacks. In the popular performances of Public Key Infrastructures, RSA algorithm is extensively used. The Rivest-Shamir-Adleman (RSA) Asymmetric key algorithm is one of the most popular and secures public key encryption methods. The RSA cryptosystem is widely used in the world. It can be used in both public key encryption and digital signature. RSAuses two different but statistically linked keys, one public and one private. In this paper the most standard encryption algorithms (RSA) are used to study the implementation of online security and ATM transactions coming up with the best algorithm to be used for comparing the various parameters which will getthe results by using SPSS16 tool.

KEYWORDS: Cryptographic algorithms; Public Key; Private Key; digital signature.

I. INTRODUCTION

The Rivest-Shamir-Adleman (RSA) Asymmetric key algorithm is one of the most popular and secure public key encryption methods. RSA is the Thealgorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.RSA is an internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the web browsers from Microsoft and Netscape. The encryption system is owned by RSA security. The technologies are part of existing or proposed Web, Internet and computing standards.[1][2]

II. RELATED WORK

In [1] the author has presented data encryption and decryption in a network environment that was successfully implemented and data can be transferred from one computer terminal to another via an unsecured network environment. In [2]author proposed a method for implementing a public-key cryptosystem whose security rests in part on the difficulty of factoring large numbers. It permits secure communications to be established without the use of couriers to carry keys, and it also permits one to “sign" digitized documents. In [4] the total security system works with qualitative data and quantitative data of human and identifies human characteristics, which is highly beneficial for Bank, Military, Crime branch etc. In [6] author focused on the different security services that are necessitated for conveying information reliably -through the network. After unraveling the efficient algorithms in different services, improvements have been attempted on these areas resulting in proposing new algorithms. In [7]a comparative analysis of performance of this algorithm was carried out using cryptographic algorithm metrics in order to establish its stronger performance above the existing algorithms. The result shows that the improved algorithm (XOR-RSA) performed better than prominent data encryption algorithms in the likes of RSA, SKIPJACK, DES1 and 3DES. In [8] author present two challenge/response Internet banking authentication solutions, one based on short-time passwords and one certificate-based, and relate them to the taxonomy. The solutions can be easily extended for non-repudiation (i.e.,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

transaction signing), should more sophisticated content manipulation attacks become a real problem. In [9] author study Algorithm analysis of E-commerce describes some algorithm that can be used to implement the online payment transaction security services. In [10] Author contribution is to increase the security of ATM machine for the customer authentication for Securing Financial Transactions on ATM Terminal. The designing part hardware design and software design both were designed by the rules of embedded system. In[11] author focused on different data encryption methods which are used in Secure ATM Transactions. And study the comparisons between AES & triple DES encrypted algorithms. In [12] author introduces three factor authentication metrics in Biometric Strategy Measure for enhancing ATM Security. Author has proposed a combined technique i.e. ATM ID number, PIN number, and biometric fingerprint

III. RSA ALGORITHM

RSA RC4 is a Highly Secure, High Speed Algorithm The RC4 algorithm, developed by RSA Data Security Inc., has rapidly become the de-facto international standard for high -speed data encryption. Despite ongoing attempts by cryptographic researchers to "crack" the RC4 algorithm, the only feasible method of breaking its encryption known today remains brute-force, systematic guessing, which is generally infeasible. RC4 is a stream cipher that operates at several times the speed of DES, making it possible to encrypt even large bulk data transfers with minimal performance consequences. RC4_56 and RC4_128 RC4 is a variable key-length stream cipher. The Oracle Advanced Security option release 8.1.5 for domestic use offers an implementation of RC4 with 56 bit and 128 bit key lengths. This provides strong encryption with no sacrifice in performance when compared to other key lengths of the same algorithm. [3]

IV. SECURITY WITH QUANTITATIVE DATA

Quantitative data which is in numerical form is used for security and it is generated by mathematics. There are several types of Mathematical algorithms which convert plaintext(readable) messages into ciphertext(unreadable) messages known as encryption and its reverse process convert ciphertext into plaintext known as decryption. Process of encryption and decryption is known as cryptography. There are several algorithms used in cryptography. [4]

V. REVIEW OF THE RSA ALGORITHM

A) KEY GENERATION

For the RSA cryptosystem, we first start off by generating two large prime numbers, 'p' and 'q', of about the same size in bits. Next, compute 'n' where n = p q, and 'x' such that, x = (p-1) (q-1). We select a small odd integer less than x, which is relatively prime to it i.e. gcd (e, x) = 1. Finally, we find out the unique multiplicative inverse of e modulo x, and name it'd'. In other words, Ed = 1 (mod x), and of course, 1 < d < x. compute private exponent d= e-1 mod x Now, the public key is the pair (e, n) and the private key is d. [5]

B) RSA ENCRYPTION

Suppose Bob wishes to send a message (say 'm') to Alice. To encrypt the message using the RSA encryption scheme, Bob must obtain Alice's public key pair (e, n) at the time of key generation. The message to send must now be encrypted using this pair (e, n). However, the message 'm' must be represented as an integer in the interval [0, n-1]. To encrypt it, Bob simply computes the number 'c' where c = m ^ e mod n. Bob sends the cipher text c to Alice.

C) RSA DECRYPTION

To decrypt the cipher text c, Alice needs to practice her own private key d (the decryption exponent) and the modulus n. simply computing the value of c ^ d mod n yields back the decrypted message (m).

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

D) Algorithm 1.3.4: RSA
Step 1: Choose two large prime numbers P and Q.
Step 2: Calculate N = P*Q.
Step 3: Select the public key (encryption key) E such that it is not a factor of (P-l) and (Q-l).
Step 4: Select the private key (decryption key) D such that the following equation is true:(D*E) mod (P-I) * (Q-I) = 1
Step 5: Encrypt the plain text PT to form the cipher text CT as followsCT = PTEmod N
Step 6: Send CT as the cipher text to the receiver.
Step 7: Decrypt the cipher text CT to form the plain text PT as followsPT=CTDmodN
The crux of RSA is that factoring N to find P and Q is not at all easy but it is quite complex and time consuming. [6]

VI. MESSAGE TYPES AND OBSERVATIONS

The analysis done for following four message type based on defined eight parameters:

- **Pin Type Message**sends and receives PIN identification data of customer.
- **Transaction message** work for transaction pattern means cash transfer, cash debit or purchase etc. after satisfying above details.
- **Customer details** would be send by server to ATM machine.
- **Operational details** means transaction success or failure acknowledgement would be send and receive between server and machine.

The following 8 parameters have been observed for each of the message type:

1. **Time:** Time to Process the message type in millisecond.
2. **Energy Level:** It is measured in decibel for the octave message type of the wireless data or frame which is send to the server for processing.
3. **Send Bytes:** The number of data byte sends while processing each message type.
4. **RCV bytes:**The number of data byte received while processing each message type
5. **Hop Count:**It represents the count of repetitive data/ request send in case of failure of communication acknowledgement between sending and receiving.
6. **Attack generated:** The attack generated while processing each message type.
7. **Attack observed:** The numbers of attacks observed while applying attack on each message type
8. **Attack Defended:**The percentage of attack defend in system after applying the attack

VII. STATISTICAL DESCRIPTION AND GRAPHICAL RESULTS

The following parameter graphical results observed for each of the message type for RSA algorithm.
There are four message types:
1 Pin transaction Message
2 Transaction type Message
3 Customer data Message
4 Operational Message

1. PIN Transaction Type Message

The one-way analysis of variance using SPSS16 Statistics is used to determine whether there are any significant differences between the means of two or more independent (unrelated) groups. The PIN type message is processed and Descriptive table is generated based on the eight parameters against three messages which are shown in the below table. The mean, Std. Deviation and Std. Error other values of the descriptive table are derived for the eight parameters. It is observed that Standard Deviation and Standard Error are high for Energy and low for Attack Defended, and Average values for Send and Receive.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Statistical Descriptive Table

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
Time	MSG1	1	40.00	.	.	.	.	40	40
	MSG2	1	48.00	.	.	.	.	48	48
	MSG3	1	49.00	.	.	.	.	49	49
	Total	3	45.67	4.933	2.848	33.41	57.92	40	49
Energy	MSG1	1	82.00	.	.	.	.	82	82
	MSG2	1	64.00	.	.	.	.	64	64
	MSG3	1	63.00	.	.	.	.	63	63
	Total	3	69.67	10.693	6.173	43.10	96.23	63	82
Send	MSG1	1	53.00	.	.	.	.	53	53
	MSG2	1	64.00	.	.	.	.	64	64
	MSG3	1	65.00	.	.	.	.	65	65
	Total	3	60.67	6.658	3.844	44.13	77.21	53	65
Rec	MSG1	1	50.00	.	.	.	.	50	50
	MSG2	1	60.00	.	.	.	.	60	60
	MSG3	1	61.00	.	.	.	.	61	61
	Total	3	57.00	6.083	3.512	41.89	72.11	50	61
Hop_Count	MSG1	1	6.00	.	.	.	.	6	6
	MSG2	1	8.00	.	.	.	.	8	8
	MSG3	1	8.00	.	.	.	.	8	8
	Total	3	7.33	1.155	.667	4.46	10.20	6	8
Att_Gen	MSG1	1	22.00	.	.	.	.	22	22
	MSG2	1	25.00	.	.	.	.	25	25
	MSG3	1	25.00	.	.	.	.	25	25
	Total	3	24.00	1.732	1.000	19.70	28.30	22	25
Att_Ober	MSG1	1	3.00	.	.	.	.	3	3
	MSG2	1	6.00	.	.	.	.	6	6
	MSG3	1	6.00	.	.	.	.	6	6
	Total	3	5.00	1.732	1.000	.70	9.30	3	6
Att_Defe	MSG1	1	19.00	.	.	.	.	19	19
	MSG2	1	19.00	.	.	.	.	19	19
	MSG3	1	19.00	.	.	.	.	19	19
	Total	3	19.00	.000	.000	19.00	19.00	19	19

Figure 1.1 PIN Statistical Descriptive Table

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

According to above parameter graph has been plotted mean against Msg type which shows the statistical graphical result.

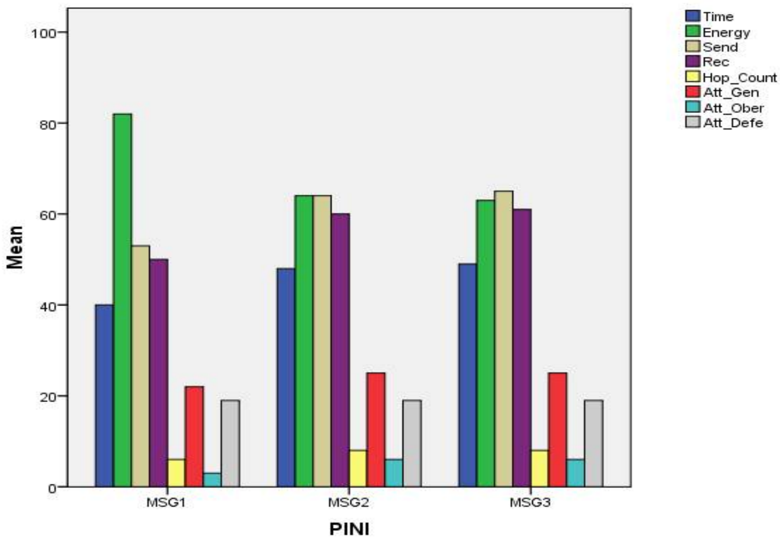

Figure 1.2PIN Statistical Graph

2. Transaction Type Message

The one-way analysis of variance using SPSS16 Statistics is used to determine whether there are any significant differences between the means of two or more independent (unrelated) groups. The Transaction type message is processed and Descriptive table is generated based on the eight parameters against three messages which are shown in the below table. The mean, Std. Deviation and Std. Error other values of the descriptive table are derived for the eight parameters. It is observed that Standard Deviation and Standard Error are high for Time,Send and Receive and low for Attack Defended, Hop Count and Average values for Attack Generated and Attack observed.

Statistical Descriptive

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
Time	**MSG1**	**1**	**65.00**	**.**	**.**	**.**	**.**	**65**	**65**
	MSG2	**1**	**79.00**	**.**	**.**	**.**	**.**	**79**	**79**
	MSG3	**1**	**81.00**	**.**	**.**	**.**	**.**	**81**	**81**
	Total	**3**	**75.00**	**8.718**	**5.033**	**53.34**	**96.66**	**65**	**81**
Energy	**MSG1**	**1**	**50.00**	**.**	**.**	**.**	**.**	**50**	**50**
	MSG2	**1**	**39.00**	**.**	**.**	**.**	**.**	**39**	**39**
	MSG3	**1**	**38.00**	**.**	**.**	**.**	**.**	**38**	**38**
	Total	**3**	**42.33**	**6.658**	**3.844**	**25.79**	**58.87**	**38**	**50**
Send	**MSG1**	**1**	**87.00**	**.**	**.**	**.**	**.**	**87**	**87**
	MSG2	**1**	**106.00**	**.**	**.**	**.**	**.**	**106**	**106**

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

	MSG3	1	108.00	.	.	.	.	108	108
	Total	3	100.33	11.590	6.692	71.54	129.13	87	108
Receive	MSG1	1	81.00	.	.	.	.	81	81
	MSG2	1	99.00	.	.	.	.	99	99
	MSG3	1	101.00	.	.	.	.	101	101
	Total	3	93.67	11.015	6.360	66.30	121.03	81	101
Hop_count	MSG1	1	10.00	.	.	.	.	10	10
	MSG2	1	13.00	.	.	.	.	13	13
	MSG3	1	13.00	.	.	.	.	13	13
	Total	3	12.00	1.732	1.000	7.70	16.30	10	13
Att_Gen	MSG1	1	35.00	.	.	.	.	35	35
	MSG2	1	40.00	.	.	.	.	40	40
	MSG3	1	40.00	.	.	.	.	40	40
	Total	3	38.33	2.887	1.667	31.16	45.50	35	40
Att_Obs	MSG1	1	8.00	.	.	.	.	8	8
	MSG2	1	13.00	.	.	.	.	13	13
	MSG3	1	13.00	.	.	.	.	13	13
	Total	3	11.33	2.887	1.667	4.16	18.50	8	13
Att_defe	MSG1	1	27.00	.	.	.	.	27	27
	MSG2	1	27.00	.	.	.	.	27	27
	MSG3	1	27.00	.	.	.	.	27	27
	Total	3	27.00	.000	.000	27.00	27.00	27	27

Figure 2.1 Transaction Type Statistical Descriptive Table

According to above parameter graph has been plotted mean against Msg type which shows the statistical graphical result.

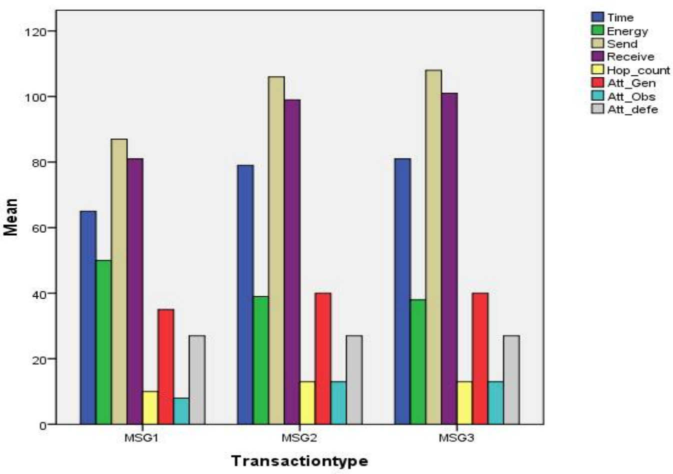

Figure 2.2 Transaction Type statistical Graph

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

3. Customer Type Message

The one-way analysis of variance using SPSS16 Statistics is used to determine whether there are any significant differences between the means of two or more independent (unrelated) groups. The Customer Type Message is processed and Descriptive table is generated based on the eight parameters against three messages which are shown in the below table. The mean, Std. Deviation and Std. Error other values of the descriptive table are derived for the eight parameters. It is observed that Standard Deviation and Standard Error are high for Time, Send and Receive and low for Attack Defended, Hop Count and Average values for Attack Generated and Attack observed. According to below parameter graph has been plotted which shows the statistical graphical result in figure 3.2

Statistical Descriptive

						95% Confidence Interval for Mean			
		N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
Time	MSG1	1	108.00	.	.	.	.	1-08	108
	MSG2	1	130.00	.	.	.	.	130	130
	MSG3	1	134.00	.	.	.	.	134	134
	Total	3	124.00	14.000	8.083	89.22	158.78	108	134
Energy	MSG1	1	30.00	.	.	.	.	30	30
	MSG2	1	23.00	.	.	.	.	23	23
	MSG3	1	23.00	.	.	.	.	23	23
	Total	3	25.33	4.041	2.333	15.29	35.37	23	30
Send	MSG1	1	145.00	.	.	.	.	145	145
	MSG2	1	174.00	.	.	.	.	174	174
	MSG3	1	180.00	.	.	.	.	180	180
	Total	3	166.33	18.717	10.806	119.84	212.83	145	180
Receive	MSG1	1	135.00	.	.	.	.	135	135
	MSG2	1	163.00	.	.	.	.	163	163
	MSG3	1	168.00	.	.	.	.	168	168
	Total	3	155.33	17.786	10.269	111.15	199.52	135	168
Hop_count	MSG1	1	18.00	.	.	.	.	18	18
	MSG2	1	21.00	.	.	.	.	21	21
	MSG3	1	22.00	.	.	.	.	22	22
	Total	3	20.33	2.082	1.202	15.16	25.50	18	22
Att_Gen	MSG1	1	57.00	.	.	.	.	57	57
	MSG2	1	64.00	.	.	.	.	64	64
	MSG3	1	66.00	.	.	.	.	66	66
	Total	3	62.33	4.726	2.728	50.59	74.07	57	66
Att_Obs	MSG1	1	25.00	.	.	.	.	25	25
	MSG2	1	22.00	.	.	.	.	22	22
	MSG3	1	24.00	.	.	.	.	24	24
	Total	3	23.67	1.528	.882	19.87	27.46	22	25

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Att_defe	MSG1	1	42.00	.	.	.	.	42	42
	MSG2	1	42.00	.	.	.	.	42	42
	MSG3	1	42.00	.	.	.	.	42	42
	Total	3	42.00	.000	.000	42.00	42.00	42	42

Figure 3.1 Customer Data statistical descriptive table

According to above parameter graph has been plotted mean against Msg type which shows the statistical graphical result.

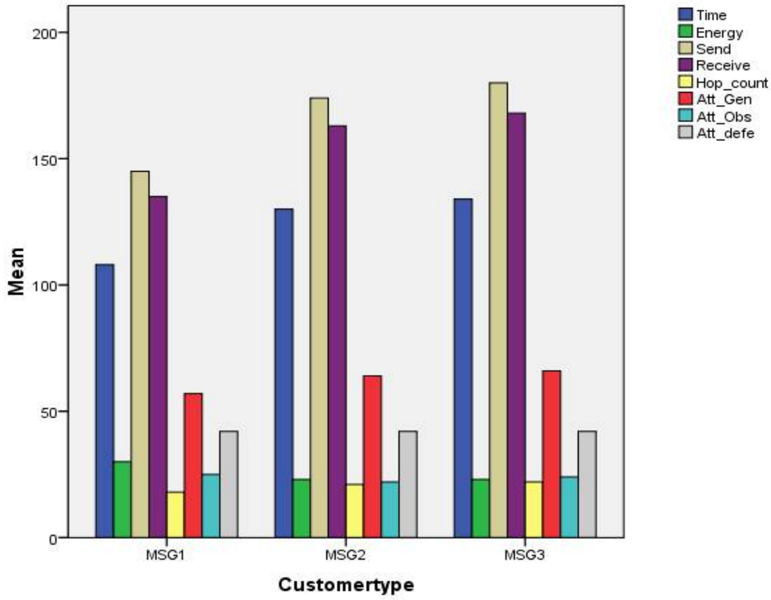

Figure 3.2 Customer Data Statistical Graph

4. Operational Type Message

The one-way analysis of variance using SPSS16 Statistics is used to determine whether there are any significant differences between the means of two or more independent (unrelated) groups. The Operational Type Message is processed and Descriptive table is generated based on the eight parameters against three messages which are shown in the below table. The mean, Std. Deviation and Std. Error other values of the descriptive table are derived for the eight parameters. It is observed that Standard Deviation and Standard Error are high for Time, Send and Receive and low for Attack Defended, Hop Count and Average values for Attack Generated and Attack observed.

Statistical Descriptive

						95% Confidence Interval for Mean			
		N	Mean	Std. Deviation	Std. Error	Lower Bound	Upper Bound	Minimum	Maximum
Time	MSG1	1	161.00	.	.	.	.	161	161
	MSG2	1	194.00	.	.	.	.	194	194
	MSG3	1	199.00	.	.	.	.	199	199
	Total	3	184.67	20.648	11.921	133.37	235.96	161	199

DOI: 10.15680/IJIRCCE.2016. 0407136

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Energy	MSG1	1	20.00	.	.	.	.	20	20
	MSG2	1	15.00	.	.	.	.	15	15
	MSG3	1	15.00	.	.	.	.	15	15
	Total	3	16.67	2.887	1.667	9.50	23.84	15	20
Send	MSG1	1	216.00	.	.	.	.	216	216
	MSG2	1	260.00	.	.	.	.	260	260
	MSG3	1	267.00	.	.	.	.	267	267
	Total	3	247.67	27.647	15.962	178.99	316.34	216	267
Receive	MSG1	1	202.00	.	.	.	.	202	202
	MSG2	1	243.00	.	.	.	.	243	243
	MSG3	1	249.00	.	.	.	.	249	249
	Total	3	231.33	25.580	14.769	167.79	294.88	202	249
Hop_count	MSG1	1	27.00	.	.	.	.	27	27
	MSG2	1	32.00	.	.	.	.	32	32
	MSG3	1	33.00	.	.	.	.	33	33
	Total	3	30.67	3.215	1.856	22.68	38.65	27	33
Att_Gen	MSG1	1	82.00	.	.	.	.	82	82
	MSG2	1	93.00	.	.	.	.	93	93
	MSG3	1	95.00	.	.	.	.	95	95
	Total	3	90.00	7.000	4.041	72.61	107.39	82	95
Att_Obs	MSG1	1	25.00	.	.	.	.	25	25
	MSG2	1	36.00	.	.	.	.	36	36
	MSG3	1	38.00	.	.	.	.	38	38
	Total	3	33.00	7.000	4.041	15.61	50.39	25	38
Att_defe	MSG1	1	57.00	.	.	.	.	57	57
	MSG2	1	57.00	.	.	.	.	57	57
	MSG3	1	57.00	.	.	.	.	57	57
	Total	3	57.00	.000	.000	57.00	57.00	57	57

Figure 4.1 Operational Type Statistical Descriptive Table

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

According to above parameter graph has been plotted mean against Msg type which shows the statistical graphical result.

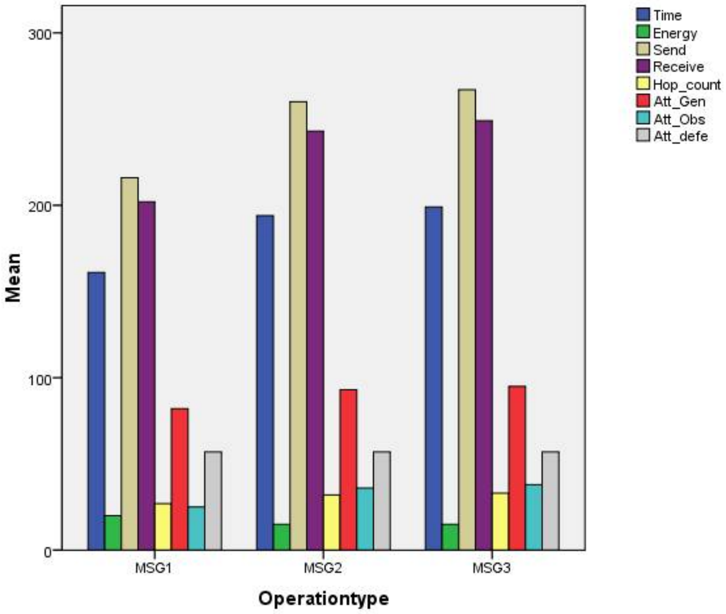

Figure 4.2Operational Types Statistical Graph

VIII. CONCLUSION AND FUTURE WORK

RSA algorithm is studied to understand how the message become secured by applying the key and how the encryption and decryption is done while sending and receiving the message. The RSA algorithm is studied for the four message typeof the ATM transaction processand analysis is done with different parameters.The analysis is done in SPSS and received the descriptive statistics for the parameter we analyzed and received the approximate significance level of the parameters.The descriptive statistics table of the messages shows the RSA is the significant algorithm for the ATM transaction process.The current analysis is done using eight parameters but this can be increased and can be used different statistical tool to get result.

REFERENCES

1. NentaweGoshwe, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment", IJCSNS, Vol.13 No.7,July 2013
2. Rivest, L. Shamir &Adleman L."A method for obtaining digital signatures and public key cryptosystems", communication of the ACM,vol.21,120-126.
3. RSA SecurID Authentication, a Better Value for a Better ROI.
4. Sneha Patel & Joshi "Mathematical Model Based Total Security System with Qualitative & quantitative Data of Human", IJMSA, Vol.3, No.1, Jan-June 2013, ISSN No:2230-9888, www.journalshub.com.
5. William Stalling, Cryptography and Network Security text book, principles and practices.
6. Sheena Mathew, "Studies, Design and Development of Network security Enhancement Services Using Novel Cryptographic Algorithm", Department of Computer Science, June-2008
7. Afolabi, A.O & E. R. Adagunodo 2012, "Implementation of an Improved data Encryption Algorithm in a Web Based Learning System", International Journal of Research and Reviews in Computer Science, Vol.3 No.1.
8. ALAIN HILTGEN, et al. "Secure Internet Banking Authentication",Published ByThe IEEE Computer Society IEEE Security& Privacy**24**.
9. Barskar, Deen, Ahemed and Bharti, "The Algorithm Analysis of E-commerce Security Issues for Online Payment Transaction System in Banking Technology" IJCSIS, Vol.8, no.1, April 2010
10. PremKishan, Vishwanath, Nandigama, Khamuruddeen, Kasibhatla, D.Pavani, G.Sweth "Real Time SMS-Based Hashing Scheme for Securing Financial Transactions on ATM Terminal" (IJRES) ISSN (Online): 2320-9364, www.ijres.org Volume 1 Issue 3 ǁ July. 2013 ǁ PP.27-33
11. CH. Krishna Prasad et al "Data Encryption Methods Used in Secure ATM Transactions" IJCSMC, Vol. 3, Issue. 6, June 2014, pg.230 – 233, Research Article, ISSN 2320–088X
12. Sri Shimal Das, Smt. JhunuDebbarma "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System" International Journal of Information and Communication Technology Research Volume 1 No. 5, September 2011 ISSN-2223-4985 http://www.esjournals.org