A NOVEL VSR ALGORITHM FOR NETWORK SECURITY OPTIMIZATION

[1]Vani. N, [2]Sreelatha P.K, [3]Parvathy.S, [4]Sridevi Malipatil

Assistant professor, Dept of CSE, RYMEC, Assistant professor, , Dept of CSE, SVIT,
Assistant professor, Dept of ISE, AMC, Assistant professor, Dept of CSE, RYMEC
VTU, Bellary. VTU, Bangalore. VTU, Bangalore. VTU, Bellary.
Email : [1]vanimtech.z@gmail.com, [2]sreelatha.sajeev2@gmail.com, [3]s.parvathy.s@gmail.com, [4]sridevi.siddu@gmail.com

Abstract— To make complexity in cryptanalysis for all the types of attacks such as Brute force, eavesdropping, man-in-middle attack and sniffer attack. VSR network security algorithm provides high security with key size greater than 1024 bits. It reduces time taken for encryption and less memory usage and very complex to decrypt original plaintext for all types of attackers. It provides confidentiality, authentication, data integrity and access control. The main objective of this VSR security algorithm is secret key cryptography where more number of keys is shared for each stream of data and it is used to enhance complexity of encryption of private key, increased key size and encryption of symmetric stream cipher. This algorithm provides greater efficiency in transforming plaintext to cipher text.

Index Terms— Authentication, confidentiality, data integrity, non- repudiation

I. INTRODUCTION

The present security crisis in internet or cloud computing require high security algorithm to all over the world and suitable for all types of applications and platform interoperability.

Earlier security algorithm has key size very small and large number of rounds and vulnerable to Brute-force attack, eavesdropping and man-in-middle attack. There are 5 categories to provide efficient cryptographic techniques such as Authentication provides assurance that communication is authentic. Access control is prevention of unauthorized use of resources. Data confidentiality is used to provide protection of transmitted data from passive attacks. Data Integrity provides assurance that data received are exactly are sent by an authorized entity. Non Repudiation provides protection against denial of service by one of the entity involved in a communication [2]. Many schemes used for encryption and decryptions of cipher text are known as Cryptography [3].

II. EXISTING SYSTEM

The first network security algorithm is Data Encryption Standard is recommended by NIST. It is based on IBM proposed algorithm called Lucifer. DES is a block cipher that uses symmetric key algorithm. DES is now considered to be insecure for many applications and it has 56 bit key size being too small. It does not produce efficient software code. As enhancement of DES, 3DES

(Triple DES) was proposed. It is similar to DES but increased key length of size 168 bits, but tripled number of rounds. This algorithm is very slow in software implementation.

AES is a new encryption algorithm recommended by NIST to replace DES. AES is symmetric cryptography algorithm, where encryption and decryption is done with single key. AES has key size of 192,256 bits and it is faster. A drawback of AES does need for more processing and it require more number of rounds of communication as compared to DES.

RSA is a public key cryptography algorithm. A drawback of public-key cryptography for encryption is speed. Secret-key cryptography is sufficiently faster than public key cryptography because it has a higher rate of data throughput.

Blowfish is a block cipher. It uses huge keys, which is of 64 bits. Blowfish is efficient in software, at least on some software platforms. It uses key –dependent lookup table, hence performance depends on how the platform handles memory and caches. Bluefish is bit slower.

III. PROPOSED SYSTEM

This invention relates design of secret-key cryptography using different keys on each stream cipher -referred to as **"VSR ALGORITHM"** – and evaluation of performance such an speed, memory usage particular reference to enhanced key size greater than 1024 bits, more complexity for attackers to decrypt cipher text.

VSR is a high security algorithm with key size greater than 1024 bits. it provides authentication, confidentiality, integrity and access control. The plain text is converted in to cipher text with help of private key and private key is encrypted. VSR is a symmetric stream cipher developed by vani. It has following characteristics: Fast, simple, compact, high security, suitable for hardware and software, low memory requirement and complexity.

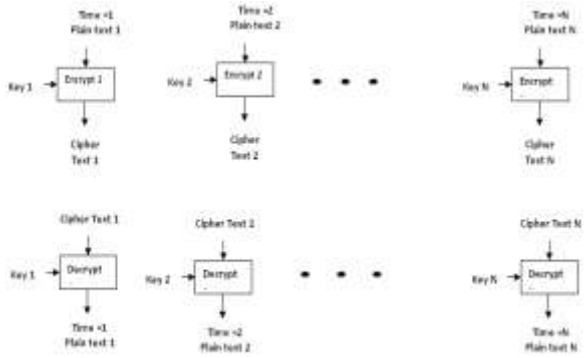

Fig 1: VSR Encryption decryption technique

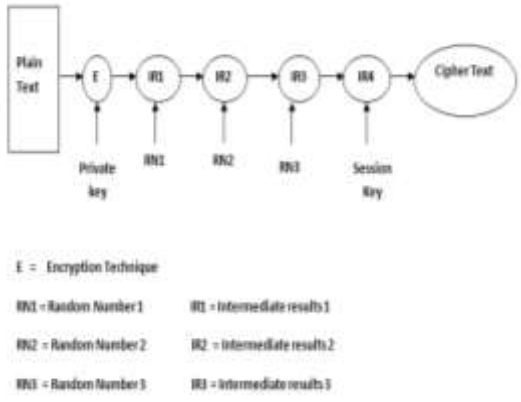

Fig 2: VSR Encryption Technique

IV. VSR ENCRYPTION ALGORITHM

Step 1: obtain ASCII value of a user input or plain text given by the user.

Step 2: Multiply encrypted private key with data and obtain IR1 (Intermediate result 1)

IR1 ← PK * Data 1

Step 3: Multiply RN1 (Random Number) with IR1 and obtain IR2 (Intermediate result2).

IR2 ← IR1 * RN1

Step 4: Multiply IR2 with RN2, obtain IR3.

IR3 ← IR2 * RN2

Step 5: obtain IR4 by multiplying IR3 with RN3.

IR4 ← IR3 * RN3

Step 6: identify position of key value inserted in cipher text. Calculate sum and average of plain text and compare number of elements in plain text with res1. A value returned from a function is a position of key inserted in cipher text.

```
if ( NE> =RES1 )
{
    Rem =res1%10
    Quiot= res1/10
    Value1=rem/quiot
}
Else
{
    Rem =res1%10
    Quiot= res1/10
    Value2=rem-quiot
}
```

Step 7: Append session key with IR4 which generates cipher text.

Cipher text ← IR4 append Session key

Example: Consider VSR algorithm to perform encryption for plain text A, B, C characters.

Step 1: plain text given by user is A, B, C, obtain ASCII value of each character.

A	**B**	**C**
↓	↓	↓
61	**62**	**63**
(Data1)	**(Data2)**	**(data3)**

Step 2: Random Number generator generates 3 numbers.

RN1 → 6
RN2 → 4
RN3 → 7

Step 3: Multiply encrypted private key with data and obtain IR1 (Intermediate result 1)

IR1 ← PK * Data 1

IR1 = 17.82 * 61

IR1 = 1087.02

Step 4: Multiply RN1 (Random Number) with IR1 and obtain IR2 (Intermediate result2).

IR2 ← IR1 * RN1

IR2 = 10087.02 * 6

IR2 = 6522.12

Step 5: Multiply IR2 with RN2, obtain IR3.

IR3 ← IR2 * RN2

IR3 = 6522.12 * 4

IR2 = 26088.48

Step 6: obtain IR4 by multiplying IR3 with RN3.

IR4 ← IR3 * RN3

IR4 = 26088.48 * 7

IR4 = 182619.36(CIPHER TEXT)

Random number	Encrypted values (Private Key)	Private key variables
RN1	17.82	PK1
RN2	59.59	PK2
RN3	83.6514	PK3

Table 1: Encrypted Private Key value Specifies

V. VSR PRIVATE KEY GENERATION

ALGORITHM FOR PRIVATE KEY GENERATION:

Step 1: use random number generator, it generates some number randomly.

Step 2: For random number 1 RN1, apply first encryption technique

```
Sum ← 0
For( i =1 ; i <=N; i ++)
{
    FET ← log10 ( i√RN1 )
    Sum ← Sum + FET
 }
IR1= Sum
```

Step 3: apply second encryption technique

```
Sum  =  0
For( i =1 ; i <=N; i ++)
{
      SET ← ∫0N IR1
    Sum ← Sum + SET
 }
IR2= Sum
```

Step 4: apply third encryption technique

```
Sum  =  0
For( i =1 ; i <=N; i ++)
{
      TET ← ∑x=0n IR2
    Sum ← Sum + TET
 }
IR3= sum
```

Step 5: the result of IR3 is called encrypted private key 1.

Pk1 ← IR3

182619.36	17.82
620689.44	59.59
885366.4176	83.6514
647168	

Table 2: Cipher text generated from encryption Technique

Example: To perform private key encryption technique

Step 1: Assume random number generator generates values are RN1= 6, RN2 = 4, RN3= 7.

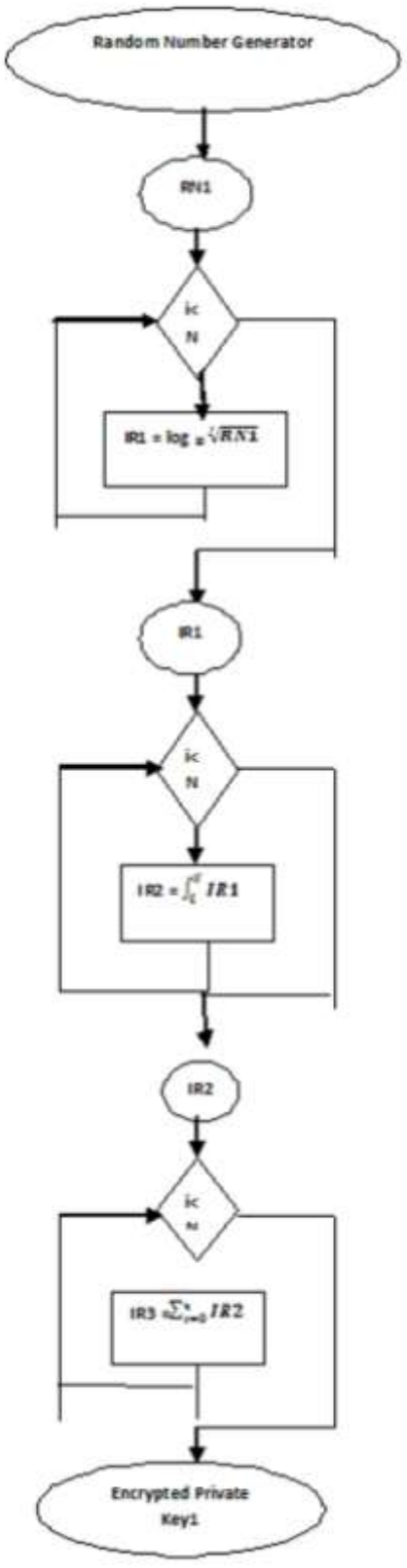

Fig 3: Flow chart Private Key generation

Step 2: use RN1 to perform first encryption technique
Assume N=3

Sum = 0
For (i =1 ; i <=3; i ++)
{
FET ← $\log_{10}(\sqrt[1]{6})$
Sum ← Sum + FET
}
IR1= sum
IR1 = 1.4183

Step 3: apply second encryption technique

Sum = 0
For(i =1 ; i <=N; i ++)
{
SET ← $\int_0^N 1.4183$
Sum ← Sum + SET
}
IR2= sum

Step 4: apply third encryption technique

Sum = 0
For(i =1 ; i <=N; i ++)
{
TET ← $\sum_{x=0}^{n} IR2$
Sum ← Sum + TET
}
IR3= sum

PLAIN TEXT	CIPHER TEXT	PRIVATE KEY
A	182619.36	17.82
B	620689.44	59.59
C	885366.4176	83.6514

Table 3: cipher text and private key value generation for 3 alphabets

VI. DECRYPTION ALGORITHM TECHNIQUE

Step 1: find largest double value is data values from cipher text and perform mapping technique.

Step 2: unmatched one is session key, recover session key from encrypted cipher text. find first digit number (FDN), second digit number(SDN) and third digit number(TDN).

Step 3: find IR1

$IR1 = I_{CT} \% FDN$

Step 4: find IR2

$IR2 = IR1 \% SDN$

Step 5: find IR3

$IR3 = IR2 \% TDN$

Step 6: find plain text

$IR4 = IR3 \% I_{PK}$

Step 7: obtain character from ASCII value.

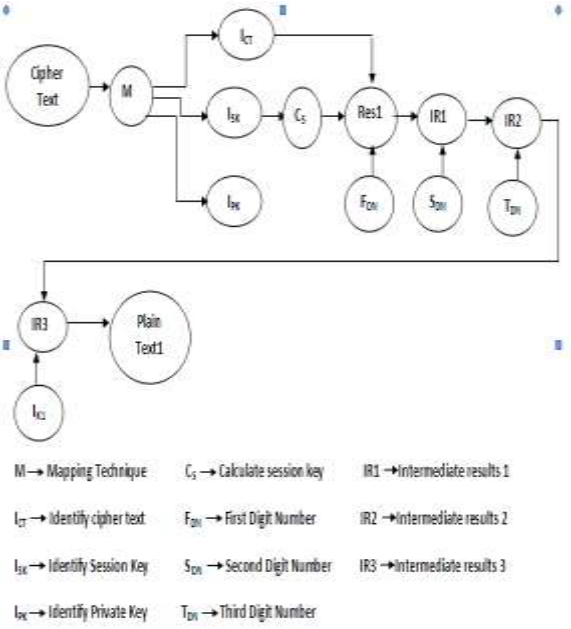

Fig 4:VSR Decryption Technique

EXAMPLE DECRYPTION ALGORITHM:

Step 1: find largest double value is data values from cipher text and perform mapping technique.

Step 2: unmatched one is session key, recover session key from encrypted cipher text. Find first digit number (FDN), second digit number (SDN) and third digit number (TDN).

Session key = 647168
Res1 =session key % 100
Res1 = 647
6 is first digit number (FDN)
4 is second digit number (SDN)
7 is third digit number (TDN)

Step 3: find IR1

$IR1 = I_{CT}$ % FDN
IR1 = **182619.36** % 6
IR1 = 30436.56

Step 4: find IR2

IR2 = IR1 % SDN
IR2 = 30436.56%4
IR2 = 7609.14

Step 5: find IR3

IR3 = IR2 % TDN
IR3 = 7609.14 % 7
IR3 = 1087.02

Step 6: find plain text

$IR4 = IR3 \% I_{PK}$
IR4 = 1087.02 % 17.82
IR4 = 61

Step 7: obtain character from ASCII value.

61 → A

VII. COMPARATIVE ANALYSIS

Algorithm	Clock cycles Per Round	Number of Rounds	No of Clock cycles per Bytes Encrypted
Bluefish	9	16	18
RC5	12	16	23
DES	18	16	45
Triple DES	18	48	108
RSA	15	10	18
VSR	30	40	50

Table 4: Comparative Analysis on clock cycles

Algorithm	Encryption /Decryption	Digital Signature	Key Exchange
RSA	YES	YES	YES
DES	YES	YES	YES
AES	YES	YES	YES
Triple DES	YES	YES	YES
Diffie-Hellman	NO	NO	YES
VSR	YES	YES	YES

Table 5: Comparative techniques for encryption and decryption

VIII. RESULTS AND DISCUSSION

VSR security algorithm performs efficient technique for encryption and decryption. It provides high security on cipher text. The opponent will be able to identify which is correct key and which is cipher text. A VSR result provides high performance and less delay and very complex technique to identify plain text by attacker.

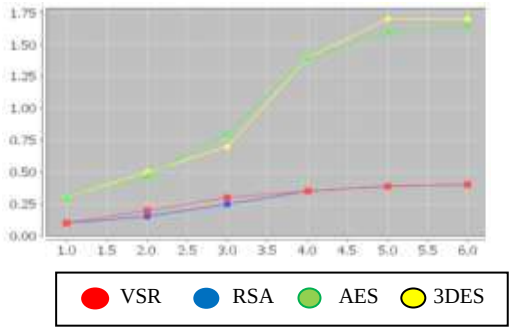

Fig 5: Processing Delay of Different security Algorithms

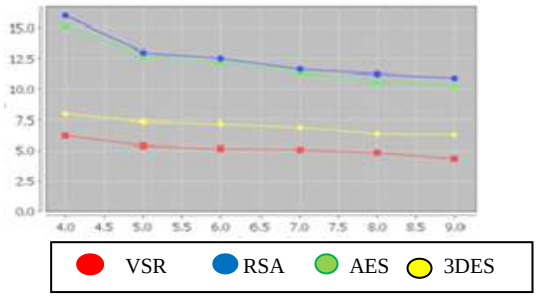

Fig 6: Processing Time of Different security Algorithms

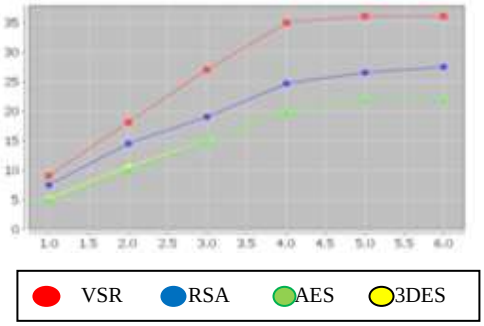

Fig 7: Comparison on Performance of different security Algorithms

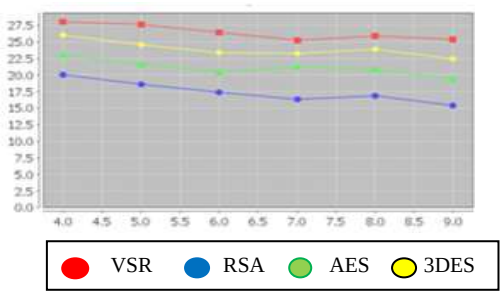

Fig 8: Complexity of Encryption and Decryption Techniques Of security Algorithms by attacker

REFERENCES

[1] D.Sharmila, Dr. R. Neelavani,"Performance Analysis of SAFER+ and Triple DES security algorithm for Blurtooth security system," IJCSNS, Sathyamangalam, Coimbatore, Tamil Nadu, Vol .9 No.2,Feb 2009.

[2] Neha Jain, Gurpret Kaur,"Implementing DES Algorithm in cloud for data security," VSRD-IJCSIT, vol.2 (4), pp316-321, Feb 2012.

[3] Nimmi Gupta,"Implementation of optimized DES Encryption Algorithm upto 4 Round on Sparatan3," IJCTEE, sehore, madhyapradesh Vol 2, Issue1, ISSN-2249-6343.

[4] Gohil Rikitaben Karasanbhai, Mary Grace Shajan,"AES Algorithm for Secured Wireless Communication," National conference on recent trends in engineering and technology, vadodara, India.

[5] Niels Ferguson," AES – CBC + Elephant diffuser a disk encryption algorithm for windows vista," Microsoft, Aug2006.

[6] Majithia schin, Dinesh Kumar,"Implementation and Analysis of AES, DES and Triple DES on GSM networks," IJCSNS, Vol 10 No.1,Jalandhar,India,Jan 2010.