IJCSMA

Reshmi. S *et al*, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 10, October- 2017, pg. 123-130 **ISSN: 2321-8363**
Impact Factor: 4.123

SHIELDING NETWORK VIRTUALIZATION USING CBC-MAC FOR IMMINENT INTERCONNECTED NETWORKS

Reshmi. S[1], Kirthika. B[2], Deepa. B[3]

[1,2,3]Assistant Professor, Department of Information Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India
reshmismca@gmail.com, kirthikab@skasc.ac.in, deepab@skasc.ac.in

Abstract

The aim of using CBC-MAC (Cipher Block Chaining (CBC) Message Authentication Code) for network virtualization is to protect from the interlopers, who is more capable of larceny data during transmission. This concept fully focusses on encrypting the chunk data for authentication purpose. Starting variable is used in the mode of data transmission. This is mainly used for transmitting the information randomly. Our approach is to introduce a virtual network in between the nodes to have more secured transmission and safer transmission. First the information is encrypted using cipher block chaining and authentication code is set with the help of another encryption done by virtual network using SSL3 Client Authorization Algorithm. SSL3 algorithm is used with MD5 (RSA data security) and SHA hash with RSA private key. Our approach is to make the information more secured while transmitting in these imminent interconnected networks.

***Keywords**:* Network Virtualization, Cipher Block Chaining-Message Authentication Code, SHA Hash, SSL3 Algorithm, RSA Private Key.

1. Introduction

To attain a secured data, mathematical functions (hashing algorithm) is used to a randomized data. SHA, MD5 are few algorithms in hashing which produces some value or a portion of information as a communication to transmit [1]. Hash objects and functions are used to set the constraints to set keys for security purpose. In cryptology or secret node, a message authenticated code is generated for each set of ciphered text using CBC-MAC procedure. Recent cryptology is relied on mathematical theory and manipulation expectations which is hard to break [2]. Likewise, here the two algorithms are used for the security purpose that is two times encrypted. Hardware and software resources are combined together to form a virtual network, the wrapped information's are send to this virtual network for further encryption.

A hash function is used to plot the data of random sized data to a static one [3] [2]. Hash values and codes are used to detect any replica records in larger files. Hashing is the renovation of a string of characters which represents original data. This data will be shorter and in fixed-length value with secret key representation. This method is used to repossess the items in a database as well as catalogue all the items in a database to find items easier and faster with the help of keys. The crux of hashing is to enable the next level incisive method as compared with binary search or linear search [4][1].

Data structures uses the hash function for hasty data lookup and the return value are its hash values. Hashing is also used in Java for its unique number that represents a value. Each value uses different algorithms to calculate codes in hash. Hash Smash bout is an effort to treasure two strings of hash function with immeasurable input length and pre-defined output length and with this hash result is produced. If there are two different inputs, same output hash is produced for those inputs. There are few different hash functions to encrypt the data for data transmission. Basically, in cryptography, Secure Hash Algorithm (SHA) is a cryptographic hash function designed to yield a hash value of 20 Byte used for message abridgment [5] [2].

Network Virtualization is the amalgamation of hardware and software resources with virtual network which provides network like functionality to software ampoules on a solo web server. There is no need to test the software physically as network virtualization empowers the inventers to rival the acquaintances between applications, services and end users [6]. The switching hub otherwise termed as MAC bridge is a network device that connects all devices together by using sachet transferring to accept, develop and headlong data to the terminus device. The network switches use hashing algorithm to choose links based on the input of its algorithm [7] [5].

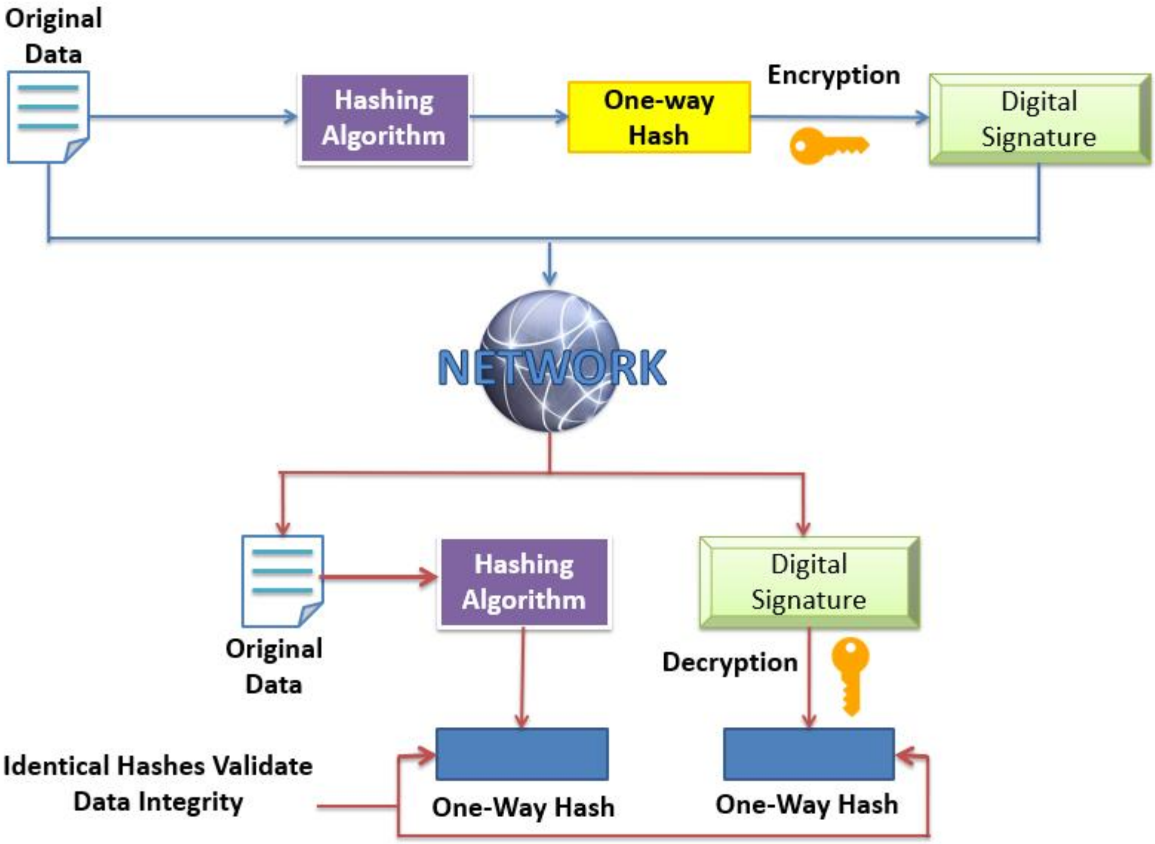


Figure 1: Overall Architecture of network architecture with hashing algorithm

In the above figure, the overall architecture of network architecture is illustrated. First the original data is wrapped using one-way hashing algorithm. This wrapped data is encrypted using a secret key and digital signature, it is further wrapped and send to the networks [8] [1]. In the destination end, Data integrity is validated using one-way hash and decrypted using the hashing algorithm and digital signature.

Using this concept, Data integrity is maintained. This is fully based on the data quality, maintenance, data accuracy and its consistency [9] [3]. The usage of the system used to store, process and retrieves data in a database, and data hayloft. Based on the utility of the data used, the consistency is judged. In all salvage situations the backup copies for the purpose of production are used instead of novel data.

2. SSL3 Algorithm

SSL3 algorithm is mainly used for the patron validation, which includes both MD5 hash and SHA hash with digital signature and RSA key to encrypt the data. Secure Socket Layer is truncated as SSL mainly to afford secure communication in API (Application Programming Interface) [10] [2]. The API is set of subroutines to physique an application software with certain protocols, tools. This is based on public key and private key cryptography to authenticate itself when client sends message and server responds to it. The secret keys with proper authentication is exchanged and secure communication between the server and the client is recognised. This algorithm layered in the socket layer and wires manifold applications layer etiquettes [11] [3].

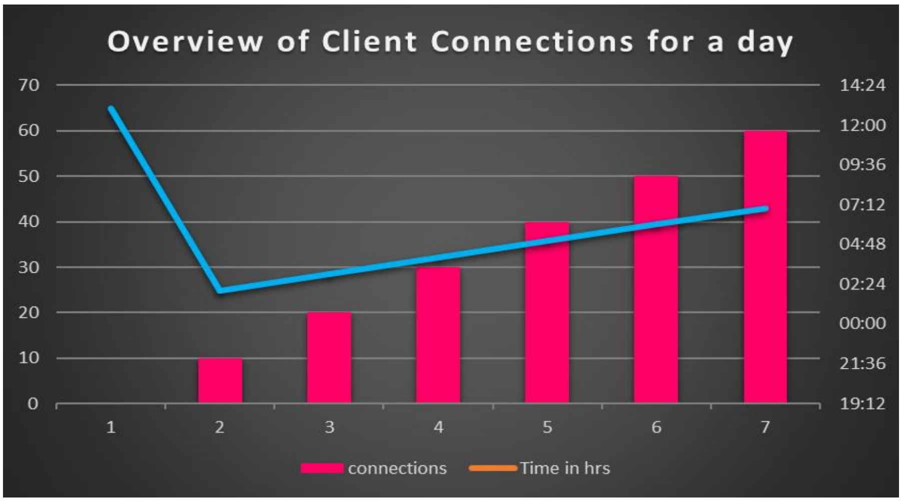


Figure 2: One-day overview of a client connection

With this algorithm the security risks like message seizure, message fiddling and message counterfeit. The message seizure is based on the quality control over various output produced with certain limits because it makes the content alters, damages in an order [12] [5]. Message fiddling is a sort of code or signal that breaks the proper communication otherwise called as intercepted. Message counterfeit is a sort of fake content that are sent to the destination as real sender sends.

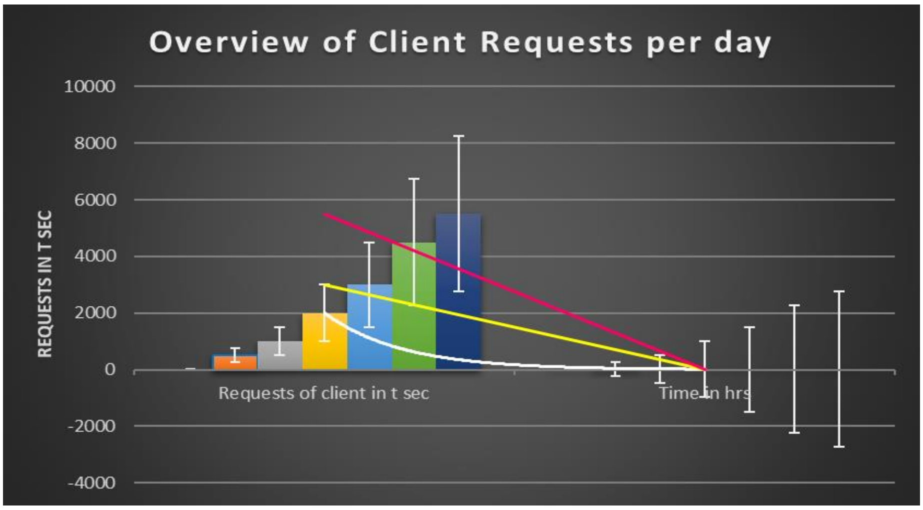


Figure 3: Client requests chart per day

3. CBC-MAC Technique

The block of information is ciphered with CBC algorithm and a hawser is created with these blocks. This hawser is based on the previous and the imminent content. Without encryption keys, messages are not revealed to the destination [13] [7]. The message is sent to the destination with a secret key, with this key and the XORed content is send to another wrapper message to wrap with the help of XOR and send it another. Likewise, it goes on until the whole message content is encrypted fully. Every message is wrapped with the help of secret key in this CBC-MAC algorithm [13].

MAC (Message Authentication Code) is mainly used for authentication purpose. For starting this process, a symmetric key has to be shared among the two ends, which is generated by MAC [14] [2] [4]. MAC encrypts the message along with a checksum. It is a portion of evidence used to indorse a message as a docket. This docket ensures that the message reached the destination.

CBC-MAC (Cipher Block Chaining Message Authentication Code) is a technique in cryptography which authenticates the block cipher. Block is a set of bits comprised in a solo component with a cipher key applied to entire block. This is processed based on the starting variable or initialization vector for each length of bits [15] [6]. If MAC is used alone for authentication is insecure so that CBC is used along with it for any fixed and randomized length of bits. Using this original data is authenticated and this data will not be modified in the mid of transmission. Using this authentication, the encryption will ensure secrecy, candour and genuineness oaths on the data. This CBC-MAC is to prove the distinctiveness of two end parties.

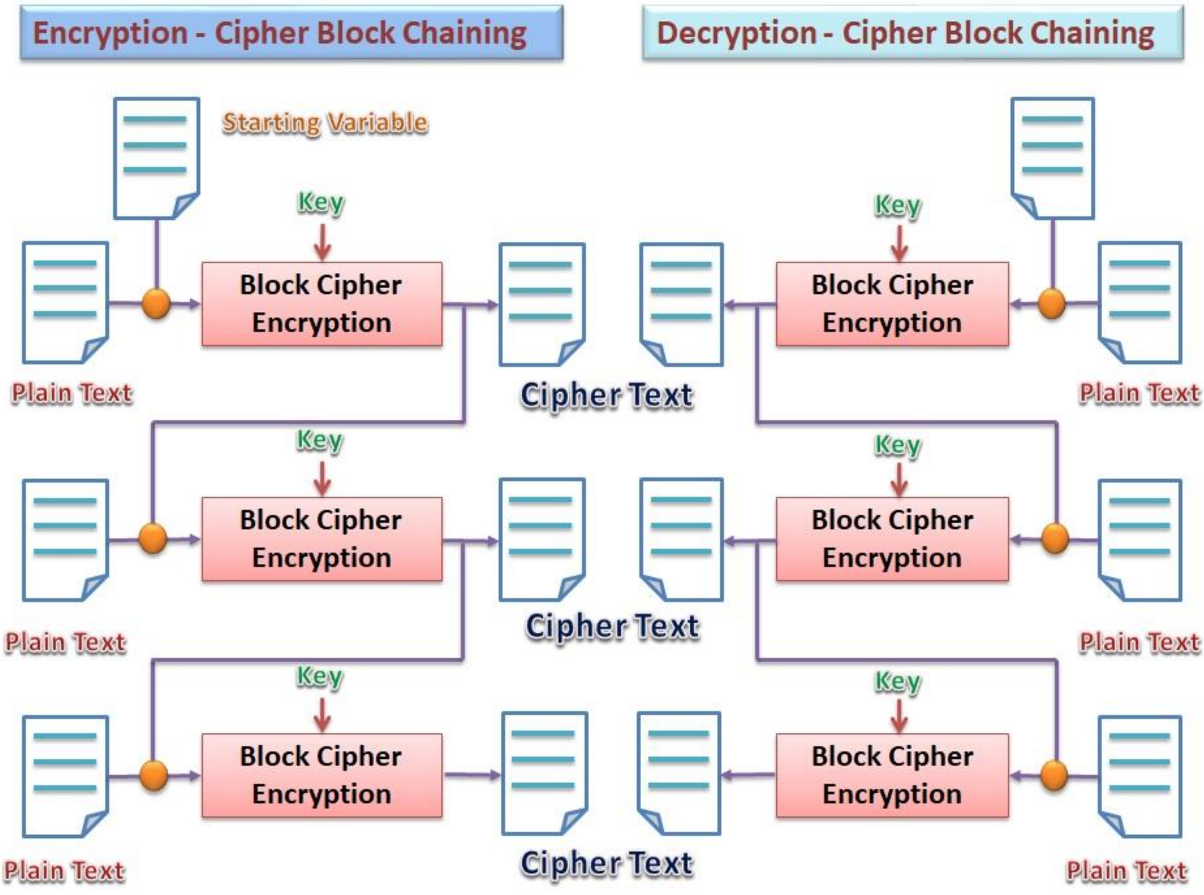


Figure 4 : Encryption and Decryption Process

Encrypting and decrypting cipher block chain is done while transmitting. Starting variable is used initially with the plain text to XOR the content fully and then it is send to a container where all the data are combined to form a block [16] [8]. This block cipher is then encrypted using a secret key to form cipher text. The ciphered text then transmitted with another set of plain text to XOR and then encrypted using the private key and ciphered. This process goes on until the full content is wrapped and sent to the destination end. In destination end, all the blocks are collected and then segregated according with the help of secret key. The cipher data is separated by XORing again to plain text. Finally, all the plain text is combined together and original data is fetched in the receiver side [16] [11].

In network security, there are different types of encryption and decryption based on the transmission of data. Encryption is a procedure of renovating plain text message into cryptogram text which can be cracked back into its original content. For which public key or private key is used based on the algorithm [17]. To use this, mathematical functions are included with a key, that can be a word or a number or a phrase etc., to encrypt. Mainly used for security purpose where the keys are distributed among the end users to either encrypt or decrypt. But to avoid intruders to hack such confidential information, algorithms are used. Here CBC-MAC algorithm is used along with SSL3, which in turn comprises of MD5 and SHA with RSA private key [17] [14].

4. MD5 Algorithm

MD5 algorithm or Message Digest 5 Algorithm is a one-way hash function produces 128-bit hash value. It was primarily premeditated as a cryptographic hash function invented by Ronald Rivest in 1991. This is based on transmitting randomized data (text or binary) as an input. A hash value is generated with a secured size as the output. It produces a message digest with a subjective length of 128-bit long. MD5 is fastest than any other hashing algorithm with "thumbprint" as the input. A MD5 checksum is used to compute on a file with 32-character hexadecimal number. If two files are to be same then similar MD5 checksum value is assigned.

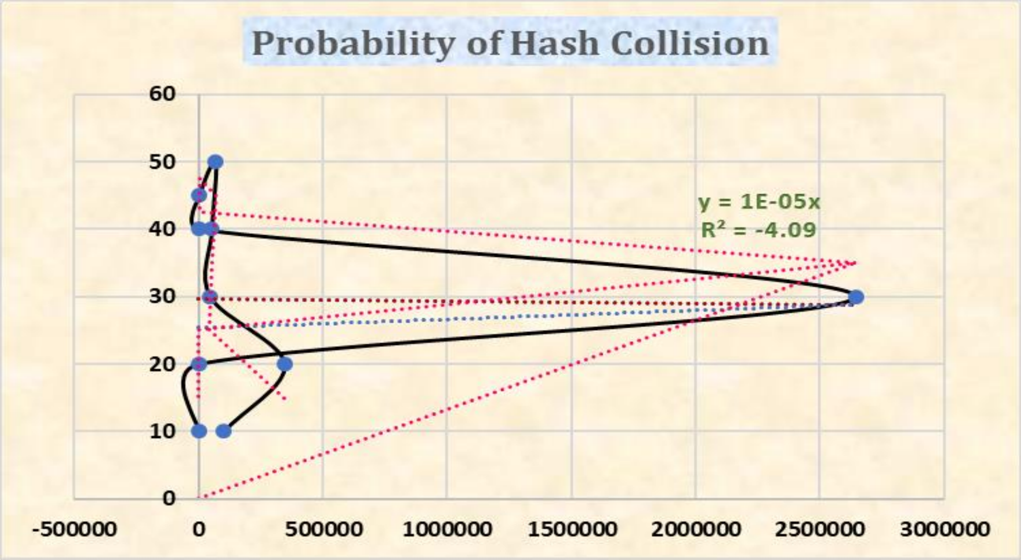


Figure 5: Hash Collision Detection with the help of MD5 algorithm

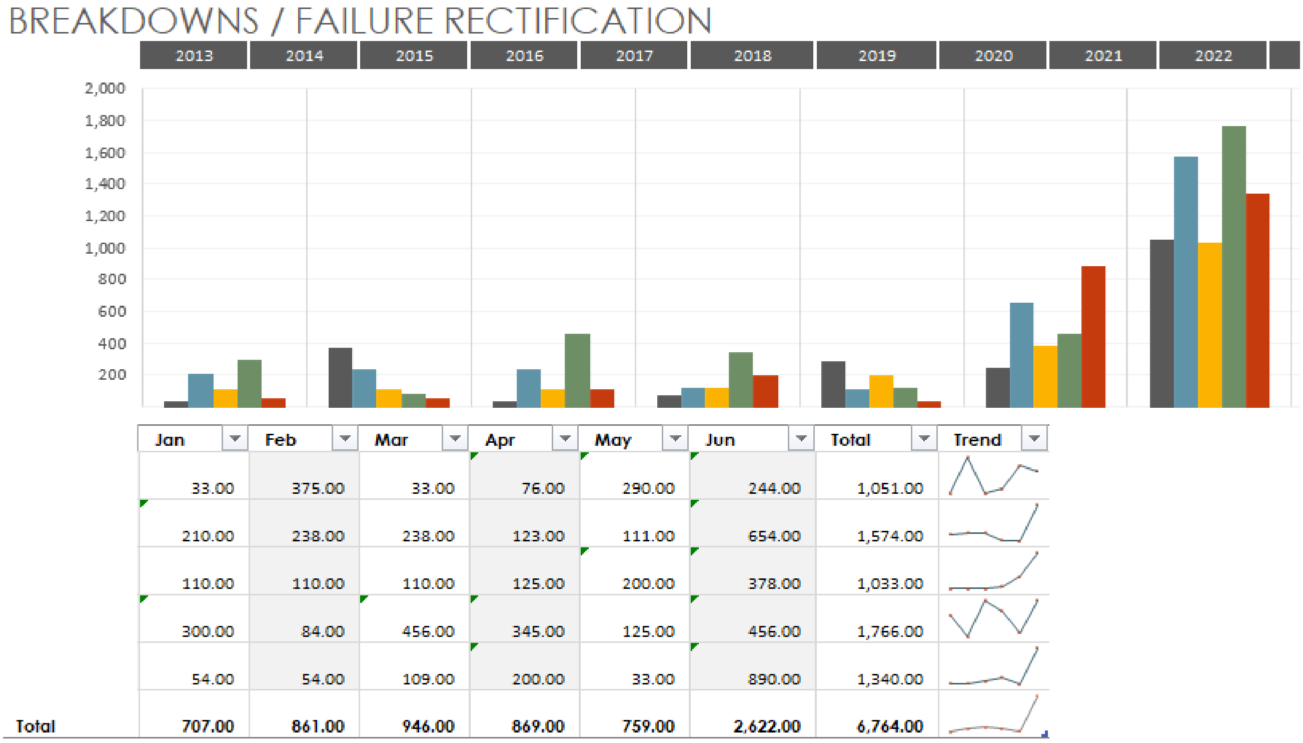
The algorithm Message Digest 5 or MD5 accomplishes many binary operations to calculate a 128-bit "hash". Most of the hashing functions' output are epitomised as hex digits, for example, MD5 vintages hexadecimal digits of 32 characters [18] [13]. Using this multiple contender keywords per second on a single network. MD5 is faster but has 128-bit output and there have been successful attacks against it.

MD5 is used for calculating checksums and authenticating data in faster manner to find and compute the collisions. If you scramble it as a hexadecimal string you can scramble 4 bits per character, giving 32 characters and not possible to decrypt the message to the original string. It is a computer sequencer that computes and authenticates 128-bit MD5 hashes.

The MD5 hash functions as a compressed ordinal thumbprint of a file. Unlimited number of files have MD5 hash as hashing algorithm. In these imminent interconnected networks, MD5 hashes and other hashes are pre-calculated for all sort of functions, strings and are stored in easy manner.

5. SHA hash with RSA private key

Secure Hash Algorithm abbreviated as SHA is also a hash algorithm. SHA is mainly used for certification to authorize the digital signatures. It generates a unique identification hash value for each file. SHA hash value has 160 bits long for randomized fixed length in strings. It uses 40 characters that is 4 bits per character [19] [9] [10]. This is also a computer program to compute and verify SHA hash values. It is installed in UNIX operating system to verify the veracity of files. This is also one sort of message digest to encrypt the hash value. SHA hash is used with RSA private key with values and functions for security purpose in the path of transmission.



	Jan	Feb	Mar	Apr	May	Jun	Total	Trend
	33.00	375.00	33.00	76.00	290.00	244.00	1,051.00	
	210.00	238.00	238.00	123.00	111.00	654.00	1,574.00	
	110.00	110.00	110.00	125.00	200.00	378.00	1,033.00	
	300.00	84.00	456.00	345.00	125.00	456.00	1,766.00	
	54.00	54.00	109.00	200.00	33.00	890.00	1,340.00	
Total	707.00	861.00	946.00	869.00	759.00	2,622.00	6,764.00	

Figure 6: Outages of RSA private key demonstration chart

Recent computers use RSA to encrypt and decrypt data or messages that are to be sent to the destination. It is a sort of an algorithm based on two different keys called as asymmetric cryptographic algorithm, mainly public key cryptography. RSA (cryptosystem), the Rivest-Shamir-Adleman cryptosystem, a cryptosystem for public-key encryption.

RSA is a computational amount scheme to factorize a set of prime numbers. Here our approach deals with private key to encrypt the data for security purpose. To factorize very larger number in more simpler way using RSA public key encryption algorithm [19] [12] [15]. This is another type of cryptosystem extensively used to secure data broadcast. There are two keys to encrypt and decrypt the message, one is public key and another one is private key. One key is used to encrypt the data and the other one is used to decrypt the data. This private key of RSA is used for data refuge, data substantiation, to establish Session layers, which will create SSL certificates for the entire transmission.

Based on the key length, both public and private keys are assigned a value. These values are bourgeoned with private and public key to find the link between them and key length is generated. Apart from this, RSA algorithm includes key cohort, key circulation, encryption and decryption. All users who use this knows public key, which is used for encrypting the messages [20] [11] [18]. This encrypted message can be decrypted with certain time period and retrieval mechanism using private key.

6. Conclusion

In this paper, we analyse the different hashing algorithms as the proposals of the Imminent Interconnected networks with more challenges. Here along with CBC-MAC, SSL3, SHA and MD5 are included to design more secured content transmission. Double secure layered is formed in this architectural process which fills the gaps and challenges in network virtualization. There are many drawbacks in the existing transmission to overcome those constraints the above mixture technique is implemented. The entire mountable and heterogeneity of the fundamental architecture provides the segregation of all sort of transmission techniques by its unique hash value. Therefore, in future we will examine the overall architecture of encryption and decryption ideologies and improve them for each set of blocks in a single node, then gauge the architype with widespread investigation.

References

[1] Ira Nath and Dr. Rituparna Chaki, “BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET”, International Journal of Advanced Research in Computer Science and Software Engineering, 2(8), August 2012, ISSN: 2277 128X, Pg: 113-121.

[2] Reshmi. S, and M. Anand Kumar, “Survey on Identifying Packet Misbehavior in Network Virtualization”, Indian Journal of Science and Technology, INDJST & ISSN (Online): 0974-5645, Vol 9; Issue 31, August 2016, Pg: 1-11.

[3] Reshmi. S, and M. Anand Kumar, “Secured Structural Design for Software Defined Data Center Networks”, International Journal of Computer Science and Mobile Computing, IJCSMC & ISSN 2320–088X, IMPACT FACTOR: 5.258, Vol.5 Issue.6, June- 2016, pg. 532-537

[4] M. Anand Kumar, Dr. S. Karthikeyan (2011), “Security Model for TCP/IP Protocol Suite”, Journal of Advances in Information Technology, 2[2], 87-91.

[5] M. Anand Kumar and Dr. S. Karthikeyan (2012),” Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms” International Journal of Computer Network and Information Security”, 4[2]: 22-28

[6] M. Anand Kumar and Dr. S. Karthikeyan 2012),” A New 512 Bit Cipher - SF Block Cipher” International. Journal of Computer Network and Information Security”, 4[11]:55-61.

[7] Dr. M. Anand Kumar.and Dr. S. Karthikeyan (2013),” An Enhanced Security for TCP/IP Protocol Suite” International Journal of Computer Science and Mobile Computing, 2[11]:331-338.

[8] Rajendra Aaseri, Pankaj Choudhary, and Nirmal Roberts, “Trust Value Algorithm: A Secure Approach Against Packet Drop Attack in Wireless Ad-Hoc Networks”, International Journal of Network Security & Its Applications (IJNSA), 5(3), May 2013.

[9] Nishu Kalia, Harpreet Sharma, and Nishu Kalia, “Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol”, International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397, 8(5) May 2016, pg 160 – 174.

[10] Manar Jammala, Taranpreet Singh, Abdallah Shami, RasoolAsal, Yiming Li, “Software-Defined Networking: State of the Art and Research Challenges”, Elsevier’s Journal of Computer Networks, October 2014, 72(1), Doi no: 10.1016/j.comnet.2014.07.004.

[11] Munoz-Arcentales Jose, Zambrano-Vite Sara, Marin-Garcia Ignacio, “Virtual Desktop Deployment in Middle Education and Community Centers Using Low-Cost Hardware”, International Journal of Information and Education Technology, 2013 December, 3(6), Doi no: 10.7763/IJIET.2013.V3.355.

[12] Mohamed Ali Kaafar, Laurent Mathy, Thierry Turletti, Walid Dabbous, "Real attacks on virtual networks: Vivaldi out of tune", In Proceedings of the SIGCOMM workshop on Large Scale Attack Defense LSAD, 2006 September, 1(1), Doi no: 10.1145/1162666.1162672.

[13] J. Younge, R. Henschel, J. T. Brown, G. von Laszewski, "Analysis of Virtualization Technologies for High Performance Computing Environments", Cloud Computing (CLOUD), 2011 IEEE International Conference, 2011 July, 1(1), Doi no: 10.1109/CLOUD.2011.29.

[14] Ali Dorri and Hamed Nikde, "A new approach for detecting and eliminating cooperative black hole nodes in MANET", Information and Knowledge Technology (IKT), 7th Conference on IEEE, 2015.

[15] Pooja and Chauhan. R. K, "An assessment based approach to detect black hole attack in MANET", Computing, Communication & Automation (ICCCA), 2015 International Conference on. IEEE, 2015.

[16] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, "Detecting Black Hole Attack on AODV based Mobile Ad hoc networks by Dynamic Learning Method", International Journal of Network Security, 2007 Nov,5(3), Doi no: 10.1.1.183.2047.

[17] Anand A.Aware and Kiran Bhandari, "Prevention of Black hole Attack on AODV in MANET using hash function", Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 3rd International Conference on IEEE, 2014.

[18] Kriti Patidar and Vandana Dubey, "Modification in routing mechanism of AODV for defending black hole and worm hole attacks", IT in Business, Industry and Government (CSIBIG), 2014 Conference on IEEE, 2014.

[19] Vishvas Kshirsagar, Ashok M. Kanthe, and Dina Simunic, "Analytical approach towards packet drop attacks in mobile ad-hoc networks", Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on IEEE, 2014.

[20] N. M. Mosharaf Kabir Chowdhury, Raouf Boutaba, "Network Virtualization: State of the Art and Research Challenges", Communications Magazine, IEEE, 2009 July, 47(7), Doi no: 10.1109/MCOM.2009.5183468.