Design and implementation of a secured SDN system based on hybrid encrypted algorithms

Samir Ghaly, Mahmood Zaki Abdullah
Computer Engineering Department, College of Engineering, Mustansiriyah University, Baghdad, Iraq

Article Info

Article history:

Received Nov 19, 2020
Revised Mar 1, 2021
Accepted Mar 10, 2021

Keywords:

Advanced encryption standard algorithm
Hybrid algorithm
Rivest–Shamir–Adleman algorithm
SDN

ABSTRACT

Software defined network suggests centralizing network knowledge in one network portion by separating the routing (control plane) mechanism from the transmission network packet operation (data plane). The control plane is composed of one, two or more controllers which are considered as software-defined networking (SDN) network brain where the real intelligence is incorporated. The process of separating the control unit from the data unit led to a problem related to poor security of data sent in the network, so solutions to these problems had to be found. In this paper, address this problem by implementing robust algorithms to encrypt information, based on advanced encryption standard (AES), Rivest–Shamir–Adleman (RSA), and hybrid encryption algorithms to guarantee data protection and authenticity. The results showed that the hybrid coding method is better in terms of security and improved time (faster than RSA alone) by applying several scenarios in the SDN network to a set of encrypted files.

Corresponding Author:

Samir Ghaly
Computer Engineering Department, College of Engineering
Mustansiriyah University
Al-Bab Al-Muadham Street, Baghdad, Iraq
Email: samir89ghaly@gmail.com, drmzaali@uomustansiriyah.edu.iq

1. INTRODUCTION

Currently, Internet systems such as cloud services and social networks adjust their network needs dynamically (e.g., topology, bandwidth requirements, and routing information). Software defined networks was developed as a new network architecture to solve the problem to make it more versatile in software-enabled network control. With software-defined networking (SDN), a centralized network with a controller based on software can maintain the network as a whole to simplify network architecture and operation since it is only logical [1].

SDN is a dynamic, cost-effective, manageable, and adaptable architecture that is suited for dynamic design of current technologies with high-bandwidth [2]. SDN works to strip the data plane from the control plane and programmatically it controls the flow entries using a high-level program. The SDN controller converts the applications layer specifications to the infrastructure layer instructions and configurations [3]. The operators in SDN can easily change the flow tables in switches, and the computing devices can operate as control systems to simplify the management and usage of SDNs [4]. Separation process leads to weakening the security ratio of the information sent in the network, so Protection of data is one of the important things that researchers care about, including the use of encryption methods. Protection is a primary concern for digital connections every day [5]. Encryption can protect data transformation and data authentication storage [6].

Irfan *et al.* [7] proposed developing a software specified network security architecture using a special controller type (flowvisor) with advanced encryption standard (AES) encryption algorithm and the measurement time of encryption and decryption files. Chao *et al.* [8] studied how can SDN help to identify and mitigate compromised switches under a practical model of threat. Three promising strategies introduced, compared and addressed the research problems. First is to detect errors, second is a way to detect malicious keys, and third is a method of minimizing malfunctions by encrypting the contents of the package. Tselios *et al.* [9] provide a summary of SDN protection in connection to internet of things (IoT) clouds, identify the Blockchain architecture leaders, and advocates the factors that make Blockchain an effective solution security element. This solution enables the encrypted transmission of data between interconnected nodes irrespective of network size or geographical distribution. Mahmud *et al.* [10] analyze the public and private key generation output of Rivest–Shamir–Adleman (RSA) and enterprise resource planning (ERP) central component (ECC) system to protect the patients' medical report based on a portable document format (PDF) file that comes from a database and the ECC method results, which gives the highest intensity per bit of any smaller key cryptosystem.

Sharma *et al.* [11] proposed a novel technique, i.e., the experimental results of the ILPS for safe sharing of confidential health information in big data by enabling fine-grained access using the RSA key mechanism. The results show that the proposed solution protects privacy with substantially reduced key management complexity. Sari *et al.* [12] study uses the RSA algorithm with the Genetic algorithm to generate a stronger and more quickly, and efficient presentation of the encryption to securely send an e-mail. The results show that the advantage of the avalanche effect has increased. Thus, key optimization affects the output of bit changes in the data encrypted. Furthermore, Rahmadani *et al.* [13] proposed rivest cipher 4 algorithm (RC4A)-RSA hybrid algorithm, which enhances RC4A keys security by encryption of keys before sending them to the recipient. RC4A encrypts the data, and RSA will encrypt the KSA RC4A key before sending it to recipients. The hybrid algorithm of encryption and decryption is 88.77% quicker than RSA. This paper assesses and contrasts the performance of certain encryption (AES+RSA) methods based on security and time.

2. RESEARCH METHOD

2.1. Rivest–Shamir–Adleman (RSA)

The RSA encryption method is one of the most common public-key encryption standard used to protect the transmission of data [14]. RSA is also referred to as public-key encryption where each user produces two keys [15]. The Overall process of the encryption and decryption algorithm shown in Figure 1. Maximum size of keys (4096 bits) is used in this article. To improve the robustness of the algorithm, padding bits will be used. OAEP is a common algorithm standardized in PKCS#1 used with RSA algorithm to generate pad bits randomly [16].

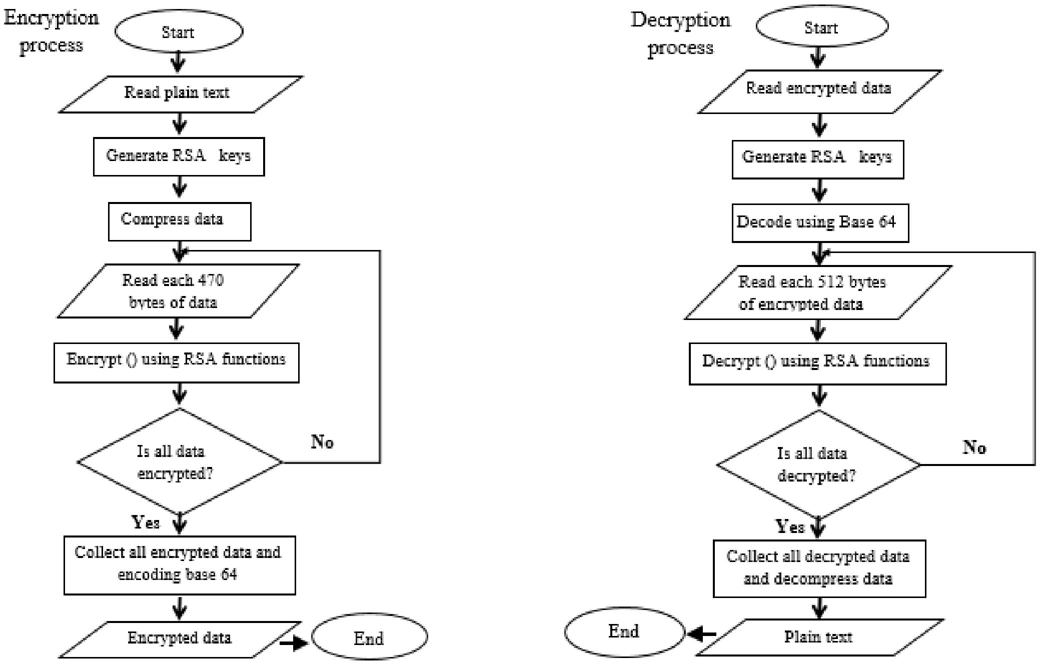


Figure 1. Flowchart of RSA encryption and decryption operations

2.2. Advanced encryption standard (AES)

NIST proposed the AES in 2001 [17]. It is a symmetric- key block cipher [18]. The key length of AES varying between 128, 192, and 256 bits [19]. AES handles 128-bit form plaintext blocks [20]. The 128-bit plaintext is 16 bytes, and the bytes are grouped in a 4*4 matrix that is, four rows and four columns, the key length decides the number of rounds to be performed, 10,12, and 14 rounds for 128, 192, and 256 bit key size, respectively [21]. It encrypts blocks of plaintext, each block contains 128 bits and using a different value of key 128 bit (16 bytes), 192 bit (24 bytes) or 256 bit (32 bytes) depending on the number of rounds 10, 12 or 14 [22]. The maximum size of key (256 bits) are used in this paper. The Overall flowchart of the encryption and decryption algorithm of the AES algorithm is shown in Figure 2.

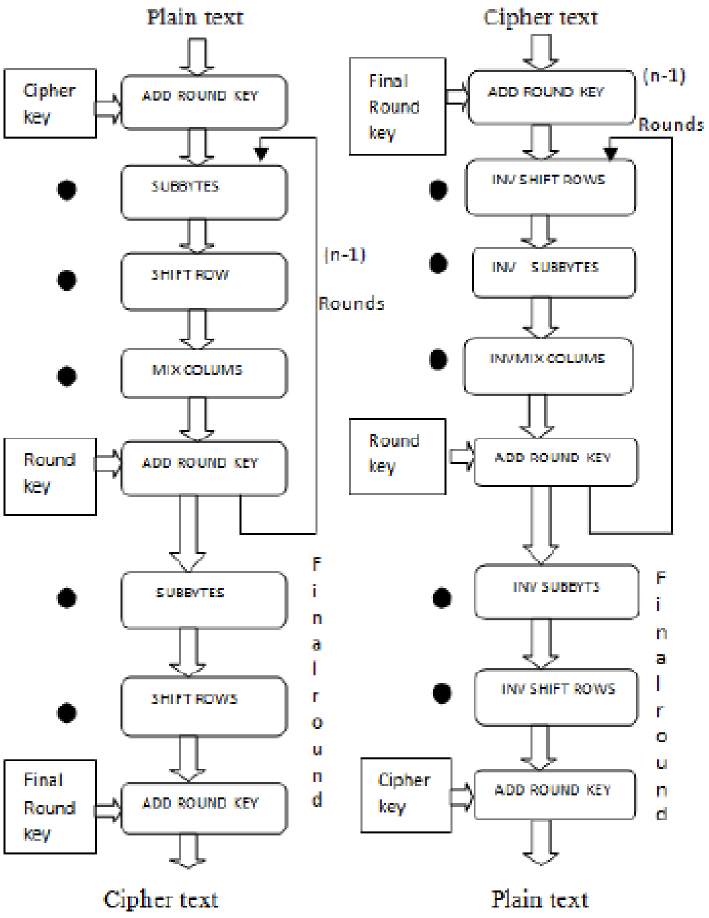


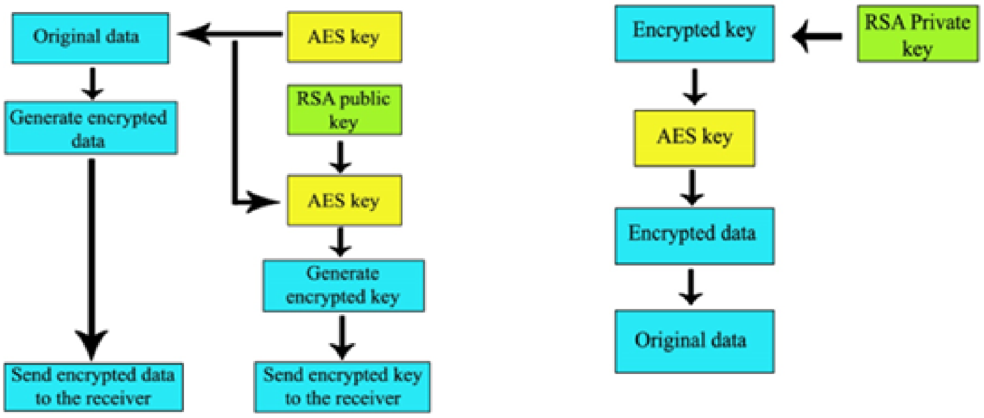
Figure 2. Design flow of AES algorithm [23]

2.3. Hybrid

The proposed cryptosystem presents a data protection solution; it combines two separate encryption algorithms. Both the symmetrical and asymmetrical algorithms (AES+RSA) are used and the strengths of the two algorithms are incorporated in the hybrid encryption system. In general, the public and private key remains more secure with hybrid encryption ciphers, which makes this hybrid algorithm less vulnerable to encryption [24]. It hybridizes the asymmetric key, key exchange and secret sharing [25].

2.3.1. Hybrid algorithm for encryption and decryption files

The original data will be encrypted by AES algorithm using 256 bits of key length to generate encrypted text. AES key is encrypted by using 4096-bit public key of the RSA algorithm to guarantee the protection of the AES algorithm, and an insecure third party cannot access the key. The decryption process is the opposite of encryption. The RSA private key is used to decode the new encrypted key to get the AES key. Finally, AES key decrypts the encrypted text to get the original data. The block diagram of the hybrid algorithm file encryption and decryption methods is shown in Figure 3.

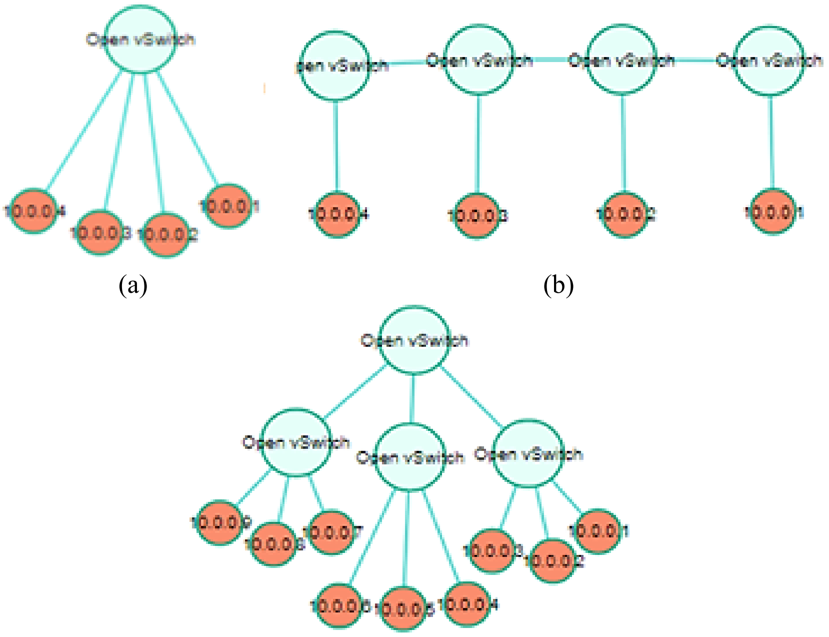


(a) (b)

Figure 3. Block diagram of the hybrid algorithm: (a) file encryption method, (b) file decryption method

2.4. Mininet

The most commonly used network simulator is Mininet. In a personal computer, create a network and develop the services can be done by the users [26]. It uses the virtualization of OS-levels to provide rapid simulation speeds and scalability strengths; the OpenFlow protocol is wholly supported and works with open-sourced SDN projects [27]. Mininet is simpler to use than any other simulation environment, and is also open source [28]. Three scenarios for SDN topologies (single, linear, and tree) as shown in Figures 4 (a), (b), and (c) respectively. Data sent during these scenarios is protected using the hybrid algorithm.



(a) (b)

(c)

Figure 4. SDN scenarios: (a) single SDN topology, (b) linear SDN topology, (c) tree SDN topology

3. EXPERIMENTS

Python 3.8 language to construct the algorithm, under Windows 10 64-bit, the Visual Studio Code Compilation Platform is used in this study. The CPU INTEL ® core(TM) i3-2310 M @2.1 GHz, RAM 4 GB DDR3 and HARD 320 GB are device specifications used. The experiment files type is ".txt". The results in this paper depend on three approaches as shown below.

3.1. Securing data

Securing data sent in SDN network by using reliable algorithms, which are AES and RSA algorithms, and building them in a way that reduces delay time, improved data security, and compares results with the published research Israa Hashim Latif [29]. Different sizes of text files were used. The results showed improvement in time (slightly higher than the AES algorithm and much less than the RSA algorithm), as shown in Table 1. The operations time is shown in Figure 5

Table 1. Total AES, RSA and hybrid algorithms encryption and decryption time

Text file size	AES Total Time (Sec.)	RSA Total Time (Sec.)	Hybrid Total Time (Sec.)
915 KB	0.05	0.57	0.54
5.384 MB	0.184	1.22	0.67
11.804 MB	0.41	2.17	0.90
35.350 MB	1.24	6.22	1.73
59.809 MB	2.1	10.3	2.59
106 MB	3.77	18.78	4.26

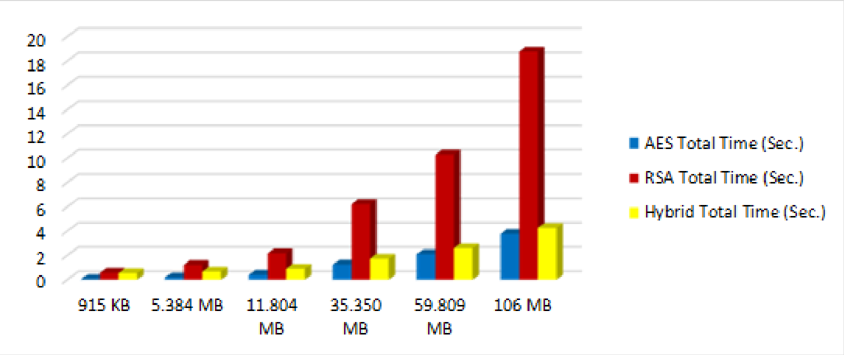


Figure 5. Operations time

3.2. Throughput

The production rate or the rate at which something is produced is the throughput. To calculate the throughput for each algorithm by dividing the sum of transmitted files size by algorithm total evaluation Time for coding and decoding operations [24]. Throughput of AES, RSA, and hybrid algorithms, as shown in Table 2. The throughput in (MB/Sec.) of AES, RSA, and hybrid algorithms is shown in Figure 6. The results showed increased throughput compared to the results of Israa Hashim Latif [29].

Table 2. Throughput values

Total Files Size	AES-Throughput	RSA-Throughput	Hybrid-Throughput
219.24 MB	169.95	33.52	123.16

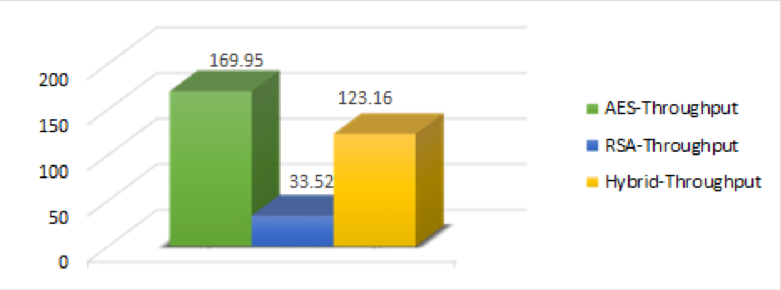


Figure 6. Throughput

3.3. SDN network

The files encrypted using the hybrid algorithm will be sent in the SDN network in three scenarios (single, linear, and tree). HPE VAN controller is used [30]. The time taken for transmission as shown in the Table 3. Total transmission time of files through SDN network as shown in Table 4. The Figure 7 shown the sending time of files. Figure 8 shows the overall time for sending files through SDN network.

Table 3. Files transmission time through SDN network

Encrypted text files	Single topology (Sec.)	Linear topology (Sec.)	Tree topology (Sec.)
Text1.encrypted	0.01	0.016	0.018
Text2.encrypted	0.03	0.04	0.07
Text3.encrypted	0.065	0.07	0.1
Text4.encrypted	0.2	0.25	0.3
Text5.encrypted	0.3	0.5	0.54
Text6.encrypted	0.7	1	1.2

Table 4. Total transmission time of files through SDN network

Topology	Single topology (Sec.)	Linear topology (Sec.)	Tree topology (Sec.)
Total time of all encrypted files	1.305	1.876	2.228

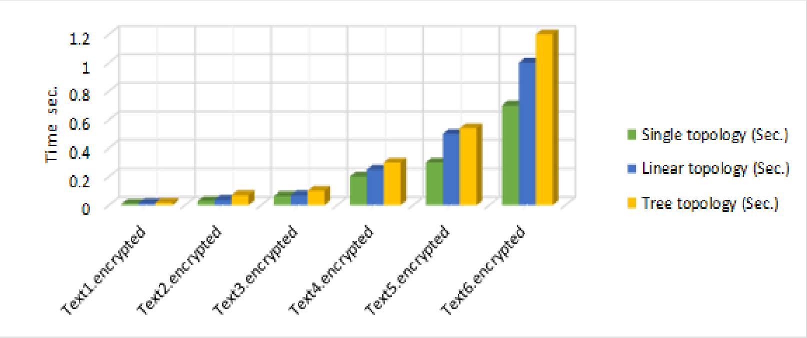


Figure 7. Sending time of files

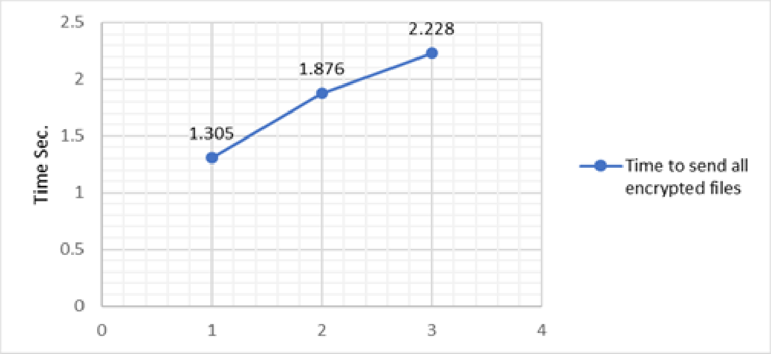


Figure 8. Overall time for sending files through SDN network

4. CONCLUSION

Based on the results mentioned above, it is possible to infer that the AES-RSA hybrid algorithm can boost security by encrypting keys in distributing AES keys before sending it to the recipient. According to encryption and decryption methods, the hybrid AES-RSA algorithm is 72.77% faster than RSA. The files encoded by the hybrid method were sent through the SDN network in three scenarios (single, linear, and tree), where the results showed that a single topology representation of the network gives less time while sending files.

ACKNOWLEDGEMENT

Many thanks for Mustansiriyah University (www. Uomustansiriyah.edu.iq) Baghdad, Iraq, and reviewers.

REFERENCES

[1] V. Monita, I. D. Irawati and R. Tulloh, "Comparison of routing protocol performance on multimedia services on software defined network," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 4, pp. 1612-1619, Aug. 2020, doi: 10.11591/eei.v9i4.2389.

[2] L. Ertaul, K. Venkatachalam and N. Star, "Security of software defined networks (SDN)," *ICWN'17-16th Int'l Conf Wirel. Networks*, vol. 17, no. 4, pp. 24-30, 2017.

[3] B. Mladenov and G. Iliev, "Optimal software-defined network topology for distributed denial of service attack mitigation," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 6, pp. 2588-2594, Dec. 2020, doi: 10.11591/eei.v9i6.2581.

[4] S. Yang, L. Cui, Z. Chen and W. Xiao, "An Efficient approach to robust SDN controller placement for security," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 3, pp. 1669-1682, Sept. 2020, doi: 10.1109/TNSM.2020.2994837.

[5] M. A. A. K. Al-Dabbas, A. Alabaichi and A. S. Abbas, "Dual method cryptography image by two force secure and steganography secret message in IoT," *TELKOMNIKA Telecommunication Computing Electronics and Control.*, vol. 18, no. 6, pp. 2928-2939, Dec. 2020, doi: 10.12928/TELKOMNIKA.v18i6.15847.

[6] A. W. A. Qader, I. E. Salem and H. R. Abdulshaheed, "A new algorithm for implementing message authentication and integrity in software implementations," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 18, no. 5, pp. 2543-2548, Oct. 2020, doi: 10.12928/TELKOMNIKA.V18I5.15276.

[7] A. Irfan, N. Taj and S. A. Mahmud, "A novel secure SDN/LTE based architecture for smart grid security," *Proc. 15th IEEE Int. Conf. Comput. Inf. Technol. CIT 2015, 14th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC 2015, 13th IEEE Int. Conf. Dependable, Auton. Se.*, 2015, doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.112.

[8] T. W. Chao, *et al.*, "Securing data planes in software-defined networks," *IEEE NETSOFT 2016 - 2016 IEEE NetSoft Conf. Work. Software-Defined Infrastruct. Networks, Clouds, IoT Serv.*, 2016, pp. 465-470, doi: 10.1109/NETSOFT.2016.7502486.

[9] C. Tselios, I. Politis and S. Kotsopoulos, "Enhancing SDN security for iot-related deployments through blockchain," *2017 IEEE Conf. Netw. Funct. Virtualization Softw. Defin. Networks, NFV-SDN 2017*, 2017, doi: 10.1109/NFV-SDN.2017.8169860.

[10] A. H. Mahmud, B. W. Angga, Tommy, A. E. Marwan and R. Siregar, "Performance analysis of AES-Blowfish hybrid algorithm for security of patient medical record data," *J. Phys. Conf. Ser.*, vol. 1007, no. 1, 2018, doi: 10.1088/1742-6596/1007/1/012018.

[11] K. Sharma, A. Agrawal, D. Pandey, R. A. Khan and S. K. Dinkar, "RSA based encryption approach for preserving confidentiality of big data," *J. King Saud Univ.-Comput. Inf. Sci.*, Oct. 2019, doi: 10.1016/j.jksuci.2019.10.006.

[12] I. C. Sari, M. Zarlis and T. Tulus, "Optimization of data encryption modeling using RSA cryptography algorithm as security e-mail data," *J. Phys. Conf. Ser.*, vol. 1471, no. 1, 2020, doi: 10.1088/1742-6596/1471/1/012068.

[13] R. Rahmadani, T. T. A. Putri, S. Sriadhi, R. D. Sari and H. D. Hutahaean, "Data security system using hybrid cryptosystem RC4A-RSA algorithm," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 830, no. 3, May 2020, doi: 10.1088/1757-899X/830/3/032008.

[14] W. Susilo, J. Tonien and G. Yang, "Divide and capture: An improved cryptanalysis of the encryption standard algorithm RSA," *Comput. Stand. Interfaces*, vol. 74, Feb. 2021, doi: 10.1016/j.csi.2020.103470.

[15] T. P. Imesi-ile and O. State, "Villanova journal of science, technology and management," *Villanova J. Sci. Technol. Manag.*, vol. 1, no. 1, pp. 42–51, 2019.

[16] S. Selvakumar, S. Baid and V. Shah, "Secure Sharing of Data in Private Cloud by RSA-OAEP Algorithm," vol. 115, no. 6, pp. 689-695, 2017.

[17] S. Khudhair Salah, W. Rasheed Humood, A. Othman Khalaf and Z. Khyioon Abdalrdha, "Subject Review: Comparison Between 3DES, AES and HiSea Algorithms," *Int. J. Sci. Res. Sci. Eng. Technol.*, Dec. 2019, doi: 10.32628/ijsrset196625.

[18] R. Nigoti, M. Jhuria and S. Singh, "A survey of cryptographic algorithms for cloud computing," *Cloud Computing*, May 2013.

[19] S. Zaineldeen and A. Ate, "Improved cloud data transfer security using hybrid encryption algorithm," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, pp. 521-527, 2020, doi: 10.11591/ijeecs.v20.i1.pp521-527.

[20] A. Y. Hindi, "A novel method for digital data encoding-decoding," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 18, no. 5, pp. 2772-2779, Oct. 2020, doi: 10.12928/TELKOMNIKA.v18i5.14279.

[21] V. S. Aparna, A. Rajan, I. Jairaj, and B. Nandita, P. Madhusoodanan and A. A. S. Remya, "Implementation of AES algorithm on text and image using MATLAB," *Proc. Int. Conf. Trends Electron. Informatics,* 2019, doi: 10.1109/ICOEI.2019.8862703.

[22] A. K. Bermani, M. E. Manaa and A. Al-Salih, "Efficient cryptography techniques for image encryption in cloud storage," *Period. Eng. Nat. Sci.*, vol. 8, no. 3, pp. 1359-1373, 2020, doi: 10.21533/pen.v8i3.1465.g619.

[23] Venkatesha G., Dinesh S., and Manjunath M., "AES based algorithm for image encryption and decryption," *Perspectives in communication, Embedded-Systems and Signal-Processing*, vol. 2, no. 11, pp. 342-345, Feb. 2019.

[24] E. Jintcharadze and M. Iavich, "Hybrid implementation of Twofish, AES, ElGamal and RSA cryptosystems," *2020 IEEE East-West Design & Test Symposium (EWDTS)*, Sept. 2020, doi: 10.1109/ewdts50664.2020.9224901.

[25] B. S. Al-Attab, “Hybrid data encryption technique for data security in cloud computing,” *Int. Conf. Innov. IT Manag.*, pp. 221-224, 2017.

[26] Y. Li, X. Guo, X. Pang, B. Peng, X. Li and P. Zhang, “Performance analysis of floodlight and ryu SDN controllers under mininet simulator,” *2020 IEEE/CIC Int. Conf. Commun. China, ICCC Work. 2020*, pp. 85-90, Aug. 2020, doi: 10.1109/ICCCWorkshops49972.2020.9209935.

[27] S. Lee, J. Ali and B. H. Roh, “Performance comparison of software defined networking simulators for tactical network: Mininet vs. OPNET,” *2019 Int. Conf. Comput. Netw. Commun. ICNC 2019*, Feb. 2019, doi: 10.1109/ICCNC.2019.8685572.

[28] H. M. Noman and M. N. Jasim, “POX controller and Open Flow performance evaluation in software defined networks (SDN) using Mininet emulator,” *IOP Conf. Ser.: Mater. Sci. Eng.* vol. 881 no. 1, 2020.

[29] I. H. Latif, “Time evaluation of different cryptography algorithms using labview,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 745, no. 1, 2020, doi: 10.1088/1757-899X/745/1/012039.

[30] A. Abdelaziz, *et al.*, “Distributed controller clustering in software defined networks,” *PLoS One*, vol. 12, no. 4, pp. 1-19, Apr. 2017, doi: 10.1371/journal.pone.0174715.

BIOGRAPHIES OF AUTHORS

Samir Ghaly received his Bachelor degree in Computer Engineering, from Al Mustansiriyah University, Iraq in 2012. His interests involve SDN and Virtualization Network Architecture

Mahmood Zaki Abdullah is one of an associate professor doctor at Mustansiriya University Baghdad - Iraq. He holds a PhD degree in computer engineering and has many books in computer engineering, networks, smart systems and information technology