Implementation of Secure Work From Home System Based on Blockchain using NS3 Simulation

Mega Apriani
Departement of Electrical Engineering
University Indonesia
Depok, Indonesia
mega.apriani@ui.ac.id

Diwandaru Rousstia
Departement of Electrical Engineering
University Indonesia
Depok, Indonesia
diwandaru.rousstia@ui.ac.id

Fajar Achmad Rifai
Departement of Electrical Engineering
University Indonesia
Depok, Indonesia
fajar.achmad91@ui.ac.id

Ruki Harwahyu
Departement of Electrical Engineering
University Indonesia
Depok, Indonesia
ruki.hwyu @ui.ac.id

Riri Fitri Sari
Departement of Electrical Engineering
University Indonesia
Depok, Indonesia
riri@ui.ac.id

Abstract— **Work from Home (WFH) is an activity carrying out official duties, completing outputs, coordination, meetings, and other tasks from the residence of employees. Implement WFH many users use the zoom application has vulnerabilities. The network architecture used refers to the simple experiment network. In Secure WFH there are 3 offices connected through a router. Each client in each office is connected to the router via a Virtual Private Network (VPN) on a peer-to-peer (P2P). That architecture has 18 nodes that will be simulated. Secure WFH simulation with blockchain combines secure WFH with a bitcoin code simulator from Arthur Gervais's. Implementation of blockchain on secure WFH can increase security but the resulting speed decreases. The decrease in speed when implementing secure WFH is due to the generate block process and the verification process.**

Keywords— Secure Work From Home, Blockchain, NS3

I. INTRODUCTION

The Corona Virus Disease 2019 (COVID-19) pandemic has caused major problems in many countries, with many organizations implementing work-from-home (WFH). Some governments also close schools and implement schooling from home (SFH) to promote social distancing [1]. WFH is an activity carrying out official duties, completing outputs, coordination, meetings, and other tasks from the residence of employees [2]. By 17 June 2020, there have been 41.431 confirmed COVID-19 cases in Indonesia and 16.243 deaths related to the disease [3]. The existence of COVID-19 cases in Indonesia has an impact on organizations that implement WFH for their employees. Multiple online platforms are being utilized for learning / WFH, the main ones being Zoom, Microsoft Teams, Skype, Google Classroom, ClassDojo, WhatsApp and Other [4].

The extreme use of zoom application during pandemic COVID-19 and the establishment of the WFH, there some vulnerabilities. The zoombombing is a form of trolling where a random person shares disturbing content to shock participants during a Zoom call [4]. Security researchers have seen an increase in hackers attempting to exploit popular online communications platforms to compromise users' systems using malware. Although Zoom calls are secured with encryption, the encryption it uses is actually TLS or transport encryption, the same encryption technique used to secure connections to HTTPS websites. This is different from end-to-encryption because it means that Zoom has access to the video and audio content from meetings [5].

The increasing number of attacks on online communication platforms during the COVID-19 pandemic could compromise user privacy. There is an architecture for IoT device communication using a blockchain that provides a strong, secure, and scalable communication model between devices and provides flexibility for each device that wants to communicate with multiple devices [6].

Implementation of Blockchain used for certificate services or digital identity systems can provide several benefits. First, blockchain reduces the risk of downloading compromised certificates from key servers. Second, blockchain resolves the Man-in-the-Middle risk for the primary server. Third, blockchain speeds up synchronization between main servers to minutes from hours. Apart from that, blockchain provides a complete history of the main server status based on its default functionality [7].

The rest of this work is organized as follows. Section II defines IoT Simulator in NS3 and a Key-Based Authentication Architecture for IoT Devices using Blockchain, and we prefer the NS3 followed by literature studies. Section III presents a secure work from home system based blockchain and simulation. Section VI share the result and analysis of the expend. Finally, the conclusion is delivered in section V.

II. RELATED WORK

A. A Key-Based Authentication Architecture for IoT Devices using Blockchain

The increased development of IoT is offset by the increase in attacks on IoT devices. One of the attacks on IoT is DDOS attacks. One way to protect DDOS attacks is to use key-based authentication with block play for all IoT communications. There are 3 architectural models that are used to test attacks on this model. one of the architectural models used is Physical Unclonable Functions (PUF) based architecture [6]. The architecture based on PUF is a fully decentralized model for the communication of IoT devices using blockchain. This architecture removes all central authorities and is based on unique device identification via their ID. A PUF is required for the creation of these public key pairs whose private keys are not stored anywhere but are computed in the trusted zone when required. This requirement can be relaxed if the device has a trusted memory location to store the generated secret keys. PUF-based architecture is simulated by forming a simple network with 4 validators in the central network and 8 IoT nodes. This network topology is shown in Figure 1 [6].

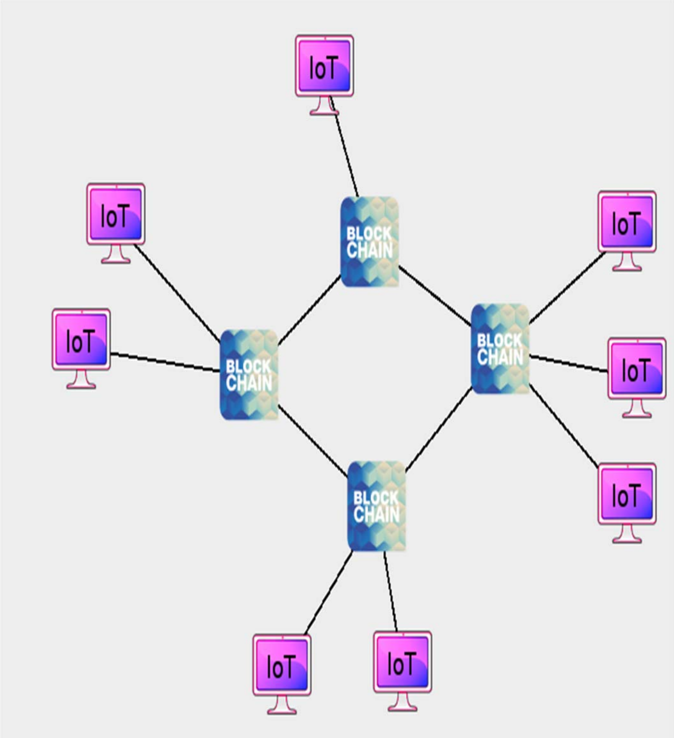

Fig. 1. Simple Experiment Network [6]

B. Blockchain

Blockchain was first put forward by Satoshi Nakamoto through the Bitcoin whitepaper: A Peer-to-Peer Electronic Cash System in 2008. In this paper the transaction is an electronic coin as a digital signature chain. Each owner transfers a coin to the next by digitally signing the hash of the previous transaction and the public key of the next owner and adding it to the end of the coin. The timestamp server works by taking the hash of a block of items to be timestamped and publishing that hash widely. The Proof-of-work involves scanning for values that when hashed, as with SHA-256, the hash starts with a number of zero bits. The required average job is exponential in the number of zero bits required and can be verified by executing one hash [14].

There are several applications of blockchain technologies: Bitcoin (digital currency), Ethereum (smart contract), Hyperledger, etc. Ethereum is an open source blockchain platform. Ethereum basically concepts are account, transaction, and client. accounts are required for everyone who wants to send any transaction to the blockchain. Every account is defined by a private key and public key. Ethereum includes two types of accounts, there are Externally Owned Accounts (EOA) and Contract Accounts. The transaction signs by EOA's private keys, after confirmation of a hash value returns which we can track all the blockchain transactions [15] Ethereum is configured to have a relatively short time interval between blocks: 13–15 s on average. Ethereum is an open source blockchain platform [16].

C. NS-3

Network Simulator 3 (NS-3) is a discrete event network simulator targeted primarily for research and open source educational use [7]. NS-3 supports almost all communication protocols as well as supports various modules that allow parallel simulation, distributed simulation, etc. Network simulators is important to obtain the detailed information of the results of the simulations. Simulation result is to generate output data for research purpose. This information can be obtained in different ways, for instance generating PCAP traces, printing files, graphics with gnuplot and flow monitor [8].

In the NS3 package, there is NetAnim which is an offline animator based on the Qt toolkit. NetAnim can animate the ns-3 network simulation using the resulting XML trace file as output during the simulation. So, the steps needed to create this XML trace file and set associated attributes must be done in the ns-3 simulation code itself.

III. Simulation

A. Secure WFH

WFH is an activity carrying out official duties, completing outputs, coordination, meetings, and other tasks from the residence of employees [2]. To support the implementation of WFH, a computer network architecture is required. The network architecture used refers to the simple experiment network in Figure 1 with minor modifications. In figure 2 there are 3 offices connected through a router (internet, etc.). Each client in each office is connected to the router via Virtual Private Network (VPN) on a peer-to-peer (P2P) basis. in the secure WFH scenario architecture it is assumed that there are 2 servers in each office. Then in this architecture there are 18 nodes that will be simulated. The following is an architectural image of a secure WFH scenario illustrated through GNS3. GNS3 offers an easy way to design and build networks with various sizes without requiring any hardware, so that this scenario represents a real basis.

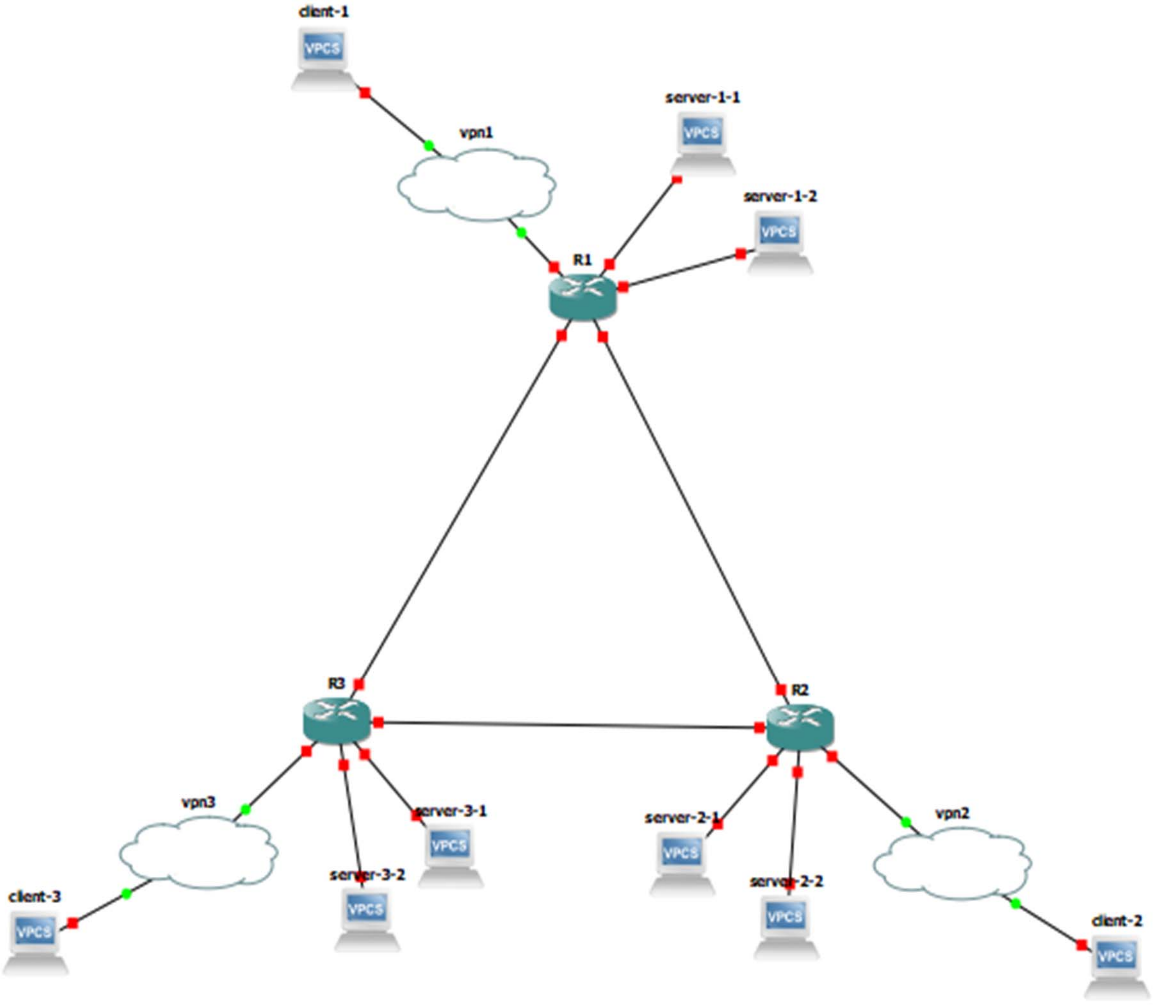

Fig. 2. Secure WFH Scenario

Secure WFH simulation with blockchain combines secure WFH with a bitcoin code simulator from Arthur Gervais's [9]. Bitcoin Simulator uses RapidJson to facilitate the communication process between nodes. This Bitcoin Simulator was built with NS3 making it suitable for simulating secure WFH architecture.

The change made is changing the cryptocurrency from Bitcoin [10] to Ethereum. This is based on the secure WFH blockchain simulation without using crypto currencies. Arthur Gervais' simulator only focuses on the effect of block propagation on the blockchain, so that transactions between modes cannot be known.

Ethereum itself provides two types of blockchain: public and private. Private blockchain from Ethereum can be used by network organizations belonging to those organizations that are not connected to public/central networks. By not connecting the blockchain node to the central network and the obligation to have permission to access the block network, Ethereum can be used for testing the blockchain [11].

The original Ethereum parameters will be used in the bitcoin simulator: block generation time interval, block size, and hash. Because the simulator does not simulate transactions between codes, to find the throughput of the blockchain we use an assumption of a transaction of 205 bytes.

With the latest data in the form of block size = 29,261 bytes, block average per hour = 265, and transaction average per hour = 37,840, a size of 205 bytes is obtained.

Blockchain as security aspect is implemented through the addition of miners in each office network. Every office has a miner who will validate every transaction between offices. Validation between miners is needed to validate that the office that will conduct the transaction is a reliable office that can be connected to a secure WFH architecture network. Blockchain is used before communicating in a network between nodes. In Figure 3 we can see the addition of miners to the secure WFH which is simulated using Netanim.

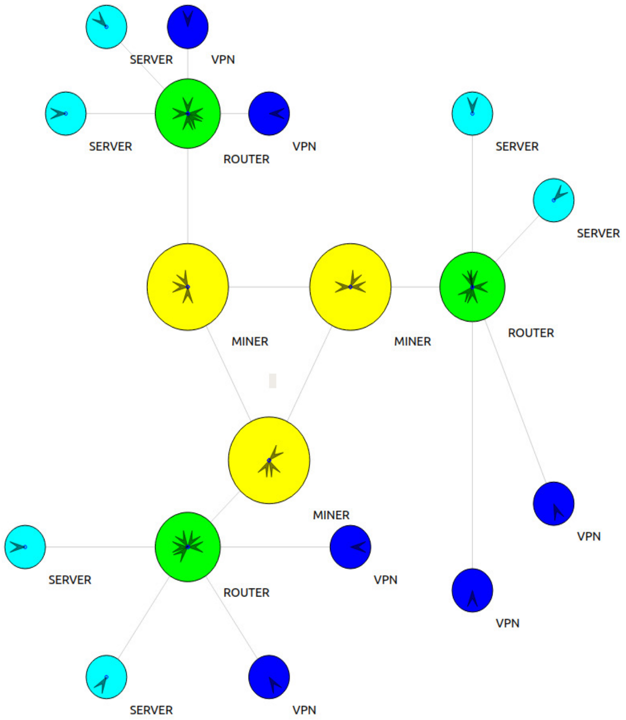

Fig. 3. Blockchain in Secure WFH Scenario

Secure WFH will be simulated using NS3 through 2 scenarios, namely scenario 1, secure WFH without blockchain and using blockchain and scenario 2 secure WFH using blockchain with the addition of DDoS (A Distributed Denial of Services) attack. Each scenario will be simulated in 5 trials. Based on the two scenarios, the velocity results will be measured and then the results will be compared.

B. Simulation Scenario

The parameters used are speed. Results of speed of two scenarios will be simulated to be compared, so as to be seen whether the implementation blockchain have a significant influence on the security of the WFH.

Scenario 1 is a comparison of secure WFH simulation using blockchain and secure WFH without using blockchain. To measure the speed of the results of simulation scenario 1 can be seen in the table below.

TABLE I.
SPEED RESULT A SECURE WFH SCENARIO 1 EXPERIMENT

FlowID	Speed Secure WFH before using blockchain	Speed Secure WFH after using blockchain
n	P1	P2

Notation:

P_1 = result in speed before using Blockchain
P_2 = result in speed after using blockchain

In second scenario using attack on secure WFH. The attacks used are attacks using DDoS attack. This attack is an attempt to make network resource unavailable to its intended users. The target of this attack is the server dan to compromise its availability.

In second scenario, the attacker will attack through router 1 (one) which is also used by user 1. The purpose of an attack on the secure WFH is to measure how effective the implementation of the blockchain is to secure the network.

IV. Result and Analysis

Based on the simulations that have been carried out with the research variables to be measured, the simulation results have been obtained on secure WFH.

A. Scenario 1 and Results

The secure WFH simulation without a blockchain from the client via VPN as a data sender (sender) to the server as a data receiver (receiver) using 18 nodes. The results obtained from the simulation are the speed of sending data packets per flow in units of Kbit / s and the travel time per flow in milliseconds. We take some of the flow associated with scenario 1, that is, the flow relating to the sender and receiver for scenario 2 so we get the following results.

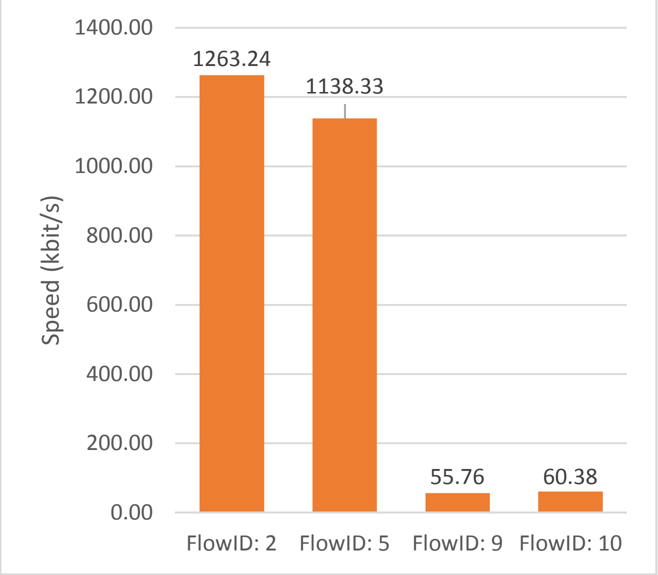

Fig. 4. Result in Speed Secure WFH without Blockchain

Scenario 1 experiment simulates a secure WFH network topology without a blockchain from the client via VPN as a data sender with the IP to the server as a data receiver with a total of 18 nodes used. The flow taken is flow with the goal through the same channel that is CSMA channel from router 3 namely flow id 2 and 10 and flow id 5 and 9. Sender flow id 2 is 172.16.12.1/49153 while receiver flow id 2 is 192.168.100.3/ 9000 then for data return using flow id 10 with sender that is 192.168.100.3/9000 while the receiver is 172.16.12.1/49153. For sender flow id 5 is 172.16.33.1/49153 while receiver flow id 5 is 192.168.100.2/9000 then for data return it uses flow id 9 with sender 192.168.100.2/9000 while receiver 172.16.33.1/49153.

The results obtained from the simulation are the speed of sending data packets per flow in units of Kbit / s and the travel time per flow in milliseconds. We take some of the flow associated with scenario 1, the flow associated with the sender and receiver for scenario 2, the data in flow 2, 5, 9 and 10 through CSMA channel from router 3. The diagram uses the sequence according to the id monitor flow so that the diagram appears figure 4. Simulation scenario 1 of secure WFH without using a blockchain, an average speed is 629.4275 Kbit/s.

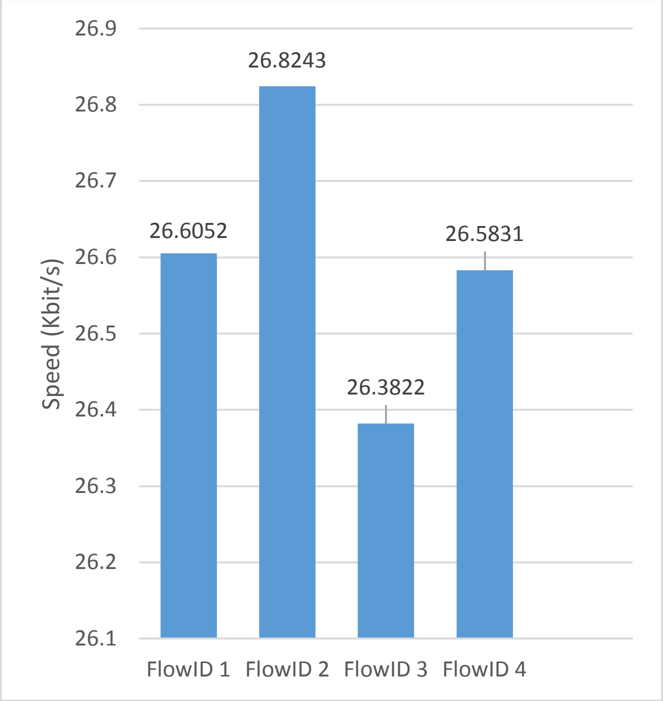

Fig. 5. Result in Speed Secure WFH using Blockchain

In Figure 5 visible results in the secure WFH speed with blockchain ranged between 26.3822 Kbit / s up to 26.8243 Kbit / s. blockchain implementation in secure WFH gives a relatively constant speed at 26 Kbit / s.

TABLE II.
AVERAGE RESULT IN SPEED A SECURE WFH SCENARIO 1 EXPERIMENT

n	WFH sample scenario	Speed (Y) before using blockchain	Speed (Y) after using blockchain
3	18 nodes	P1	P2
		629,4275 Kbit/s	26,46926 Kbit/s

In the first scenario, the effects of applying the blockchain will be measured. The average speed obtained in the simulation scenario 1 secure WFH without blockchain is 629,4275 Kbit/s while the average speed of simulation for scenario 1 secure WFH using blockchain is 26.46926 Kbit/s. There is a significant difference between the speed obtained after using the blockchain that is equal to 602,95824Kbit/s.

The difference between the speed results without blockchain secure and secure WFH with blockchain decreased significantly speeds. This is because there are additional processes on blockchain influencing that process generated block by block miner and verification processes. The number of the target block is 50 blocks. While the time required to perform of generating one block is 13.2 s.

B. *Scenario 2 and Results*

The second scenario is scenario using attack on secure WFH. scenario 2 is a secure WFH simulation that tries to be hacked using DDoS attack. DDoS attacks will be tested on a secure WFH without a blockchain and secure WFH uses a blockchain. attacker will try DDoS attack via router 1.

Experiments according to scenario 2 simulate a secure WFH network topology without a blockchain with attacks from clients via VPN as data senders to the server as data receivers with a total of 18 nodes used including 1 attack node. Flow taken is flow with the goal through the same channel, namely CSMA channel from router 3 namely flow id 2 and 9 and flow 6. Sender flow id 2 is 172.16.12.1/49153 while receiver flow id 2 is 192.168.100.3/9000 then for the data is reversed using a flow ID 9 with a sender that is 192.168.100.3/9000 while the receiver is 172.16.12.1/49153. For sender flow id 6 which is a flow attacker 172.16.13.1/49153 while receiver flow id 6 is 192.168.100.3/9000. For attacks using low TCP dos rates. The results obtained from the simulation are the speed of sending data packets per flow in units of Kbit / s and the travel time per flow in milliseconds. We take the flow related to the attacker, sender and receiver for the diagram that uses the sequence according to the id flow monitor so we get the following results.

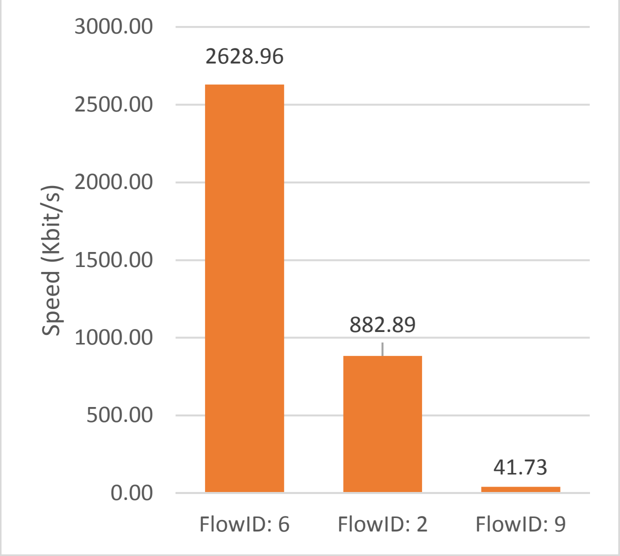

Fig. 6. Attack on Secure WFH without Blockchain

Attack in the secure WFH experiment using Blockchain used topology same as topology in scenario 2 with the attacker attacking through router 1. The number of blocks in scenario 2 is reduced to 10 blocks to facilitate observation when an attack is carried out. Speed on secure WFH using blockchain after attack also decreases speed as secure WFH speed without blockchain after attack. Node 17 (attacker) attacks node 5, to check the correctness of DDoS attack, node 16 sends packets to node 5. The flow of the attack is as follows:

- Flow ID 1: node 17 with UDP IP 1.0.17.2 attacks node 5 with IP 1.0.14.2
- Flow ID 2: node 16 with TCP IP 1.0.16.2 sending packets to node 5
- Flow ID 3: node 5 sends packets to node 16

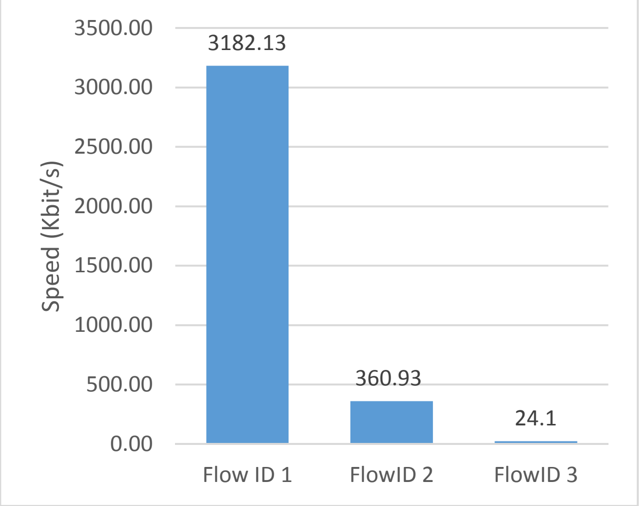

Fig. 7. Attack on Secure WFH using Blockchain

In Figure 7 it can be seen that the attack was carried out successfully so that the speed of 24.1 Kbit / s is obtained when the other node sends packets to the target node. The speed obtained after the attack with the speed before the attack has a difference that is not so far that is equal to 2, 822 Kbit / s.

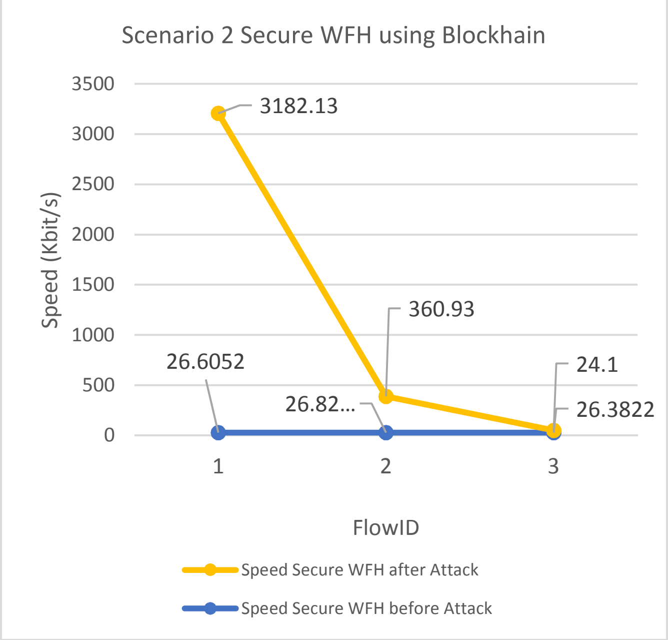

Fig. 8. Scenario 2 Attack on Secure WFH using Blockchain

In Figure 8 can be seen the effect of secure on the blockchain implementation on secure WFH. The speed of implementation of blockchain on secure WFH before attack gets constant results while the speed of implementation of blockchain on secure WFH after attack approaches the speed before attack. In other words, the application of blockchain to secure WFH can increase security on secure WFH with constant speed.

Blockchain implementation can prevent DDoS attacks due to the cryptographic aspects of the blockchain. Blockchain only allows authorized parties to make access.

V. Conclusion

The secure WFH system is modified from the simple experiment network model IoT with a default of 18 node. The simulation was carried out in NS3 by running 2 scenarios namely scenario 1 secure WFH without blockchain and by using Blockchain then scenario 2 using attack on secure WFH.

Implementation of blockchain on secure WFH can increase security but the resulting speed decreases. The decrease in speed when implementing secure WFH is due to the generate block process and the verification process. Secure WFH using Ethereum is the resulting in speed decreases. There are other blockchain platform such as Hyperledger Blockchain can be implemented to secure WFH for further research.

References

[1] Wyatt, Peter, *PDF in the Work-From-Home (WFH) World of COVID-19*, Assosiation for Digital Document Standards e.V, Germany: Deutsche Version verfügbar, 2020, https://www.pdfa.org/pdf-in-the-work-from-home-wfh-world-of-covid-19/
[2] Praptana, Agus Dwi et all, *Analysis of Effectiveness of the Implementation of Work From Home (WFH) for State Civil Apparatus*, Jakarta: Universitas Mercu Buana, 2020.
[3] https://covid19.go.id/
[4] *BruCERT Survey on Learning/Working From Home*, 2020, April 17-23.
[5] COVID-19 Response: Cyber Security, 2020, London: Global Guardian.
[6] Gan, Saptarshi, *An IoT Simulator in NS3 and a Key-Based Authetication Architecture for IoT Devices using Blockchain*, Departement of Computer Science and Engineering, Indian Institute of Technology Kanpur, 2017, Thesis.
[7] https://www.nsnam.org/docs/
[8] Lesly Maygua-Marcillo, *Statistical Framework in NS-3*, Preprints, 2018, doi:10.20944/preprints201808.0158.v1.
[9] Gervais, Artur, *Bitcoin Simulator*, Available from: https://arthurgervais.github.io/Bitcoin-Simulator/index.html.
[10] S. Nakamoto, *Bitcoin: a peer-to-peer electronic cash system*, 2008, online, http://bitcoin.org/bitcoin.
[11] Ethereum, Available from: https://github.com/ethereum/.
[12] Ethereum, Bitinfochart, Available from: https://bitinfocharts.com/ethereum/.
[13] Jogiyanto, *Metodologi Penelitian Sistem Informasi*, Andi Ofset: Yogyakarta, 2008.
[14] Lele, A, *Distruptive Technologies for the Militaries and Security, Smart Innovation Systems and Technologies 132*, Singapore: Springer, 2019, https://doi.org/10.1007/978-981-13-3384-2_12
[15] Rouhani, Sarah et all, *Performance Analysis of Ethereum Transaction in Private Blockchain*, IEEE, 2017, 978-1-5389-0497-7/17/
[16] Xu, Xiwei, et all, *Architecture for Blockchain Applications*, Switzerland: Springer, 2019.