Analysis of Security Threats on Data Centre in Internet of Things

Lee Loo Chuan[1], Mardeni Roslee[1](✉), Pang Wai Leong[1], and Indrarini Dyah Irawati[2]

[1] Faculty of Engineering, Multimedia University, 63100 Cyberjaya, Selangor, Malaysia
mardeni.roslee@mmu.edu.my
[2] Applied Science Faculty, Telkom University, Bandung 40257, Indonesia

Abstract. The recent surge in adoption of the Internet of Things (IoT) has accelerated integration and Internet access beyond smart devices, which in turn has made the Internet more and more pervasive in our daily lives and IoT devices open up endless new possibilities and simplify lives. Unfortunately, the current system able to spy on users of unprotected IoT systems. Thus, the predictive models taught by machine learning algorithms is demanded and have great potential to alleviate some of these problems as the looming crisis deepens. In this work, a lightweight encryption technique (SIT) to secure an IoT is proposed. It is a 64-bit block cypher that encrypts data with a 64-bit key. The proposed algorithm's architecture is a hybrid type and delivers significant security in just five encryption cycles in simulations. The technique is implemented in hardware on a low-cost 8-bit microcontroller. The impact of an intense attack and buffer size are discussed in this work to analyze the Distributed Denial-of-Service (DDoS) attacks on a server. Finally, the proposed mitigation approached shows a better performance according to the energy consumption level during the attacks and the mitigation applied. Thus, the DDoS attacks successfully being reduced.

Keywords: Wireless Networks · Internet of Things · 5G Communication

1 Introduction

The Internet of Things (IoT) refers to the countless of physical devices that are now connected to the internet to collect and exchange data all over the world. Connecting all of these diverse products and attaching sensors to them gives a level of digital intelligence to otherwise dumb devices, allowing them to relay real-time data without involving a human. With the increased participation of IoT devices and technology in daily lives, there will be seen a significant transition.

Regardless of the obvious benefits of IoT devices and services, it is vital to acknowledge that Internet connectivity continues to pose security problems. Connecting common household items to the Internet exacerbates the Internet's inherent risks. As a result of a single vulnerability, the number of attackers willing to launch other attacks may rapidly expand. Unprotected IoT devices allow hackers to gain access more easily than protected IoT devices.

M. Y. bin Alias (Ed.): MECON 2022, AER 214, pp. 377–389, 2023.
https://doi.org/10.2991/978-94-6463-082-4_33

DDoS attacks are now a regular occurrence in the lives of internet users. They happen all the time, and all Internet users, as a community, cause them, suffer from them, and even lose time and money to some degree. DDoS attacks have nothing to do with breaking into computers, gaining control of remote hosts on the Internet, or stealing sensitive data but, to overload the websites or online services with more traffic than the server or network can handle and becoming inoperable.

A simulation has been performed in this project to demonstrate on how to trace and mitigate the DDoS attacks. This work elaborates into the details of the systems.

2 Problem Statements

Privacy and security make up one of the most significant challenges faced by IoT systems and data centres. Continued advances in digitalization and computer technology have increased the popularity of IoT systems, with the effect of this being that these systems are now being applied in more fields than they had ever been used in the past, which include communication, education, transportation and logistics, as well as business in general. IoT is also the central part of the concept of hyper connectivity, which means that individuals and organizations can communicate with each other effortlessly from remote locations.

Those factors have made IoT an integral part of modern life and people's lifestyle has been massively improved by access to the Internet that it is inconceivable trying to figure out what life would be without it. However, the unchecked and uncontrolled expansion of IoT and its applications have come along with serious challenges regarding the security and privacy of the people using it as well as their information. For the IoT systems to function effectively, data centres need to be functioning just as effective.

When these centres are accessed by malicious applications, the sensitive data can be bleached and the consequence can be damning. Numerous researches have been conducted to this effect and many solutions continue to be developed. The essence of finding the most amicable solution is high, especially given the diverse nature of applications that target the IoT data centres and systems and also the increasing sensitivity of the data contained in IoT data centres, both physical and in the cloud. This study aims to develop an understanding of the security challenges that IoT face and simulate a suitable solution for the identified challenges.

3 Related Works

The continued expansion of IoT penetration and applications in the modern world has resulted in significant security challenges that evolve similar to the evolution of IoT in complexity and diversity. Data centres continue to evolve to provide infinite scalability and flexibility in order to support the changing strategic goals and the operating needs of diverse organizations. However, as it is the case with any progressive technology, IoT and data centres attract attacks from multiple sources and for several reasons. These attacks are the main reason for security concerns, given the extent of information entailed in IoT systems, its privacy, and the destructive nature of infiltration into such systems leading to information being in the hands of malicious people [1]. Security threats to

IoT systems can be physical in nature. These are the physical attacks or the terror attacks on IoT systems with the target of undermining the data centres and disabling their functioning. These attacks are more rampant in some geographic regions than in others, with the Middle East, Africa, and South Asia being among the places where these attacks are a significant security challenge [2]. The primary aim of DDoS attacks is to cause significant infrastructural damage on the data centres to the point where the business of the target organization is crippled or severely limited. While other attacks are after data breaches and stealing the information, DDoS attacks target the operability and time for an organization with a goal to have the organization out of business for a period. The attacks cause an outage to the organization's data, which is detrimental to most organization, which have an uptime guarantee of 99.99% [3].

Within the IoT ecosystem, these attacks and the presence of such tools elicits major concerns because while they appear similar to traditional cyber-attacks, these are especially harder to prevent, predict and control. Other security threats come from software intermediaries, such as application programming interfaces (APIs) whose task is to allow for communication between two applications. These interfaces can be a point through which attackers can access the IoT devices in an organization's network, and this includes the servers. Botnets, which are a series of devices that are connected to the internet, compromise networks, steal data, and send spam into the network [4].

Data centres are sensitive installations that can be targeted by people who want to physically access the building. This access can be through the use of brute force in the event of a robbery or burglary, or through softer access where the intruders bypass the security systems designed to keep unauthorized people out of the installation. Many organizations use a single-factor authentication system that is password-based. While it works for them, this security system puts them at a vulnerable position where they risk intrusion through simple password guessing, automated attacks, password cracking, and stolen credentials [5].

Data centres have to be secured both physically and digitally due to the sensitivity and importance of the information they hold, such as proprietary information like intellectual property and customer data. Physical security encompasses processes and strategies that protect the infrastructure from external attacks and interference. Paper [6] proposed a digital security encompasses software that prevents access into the system by cybercriminals through bypassing the firewall, cracked passwords, or other security loopholes in the system. Paper [7] proposed an authentication system which include scanning the visitors' personal identity verification (PIV) cards and then requiring them to enter personal passwords in a two-factor authentication process. Paper [8] introduced a tool which helps manage the security of a data centre by providing control and visibility of all components of the data centre from the access and alarm systems to all the security sensors installed out in the perimeter fence. At paper [9], the attacks were performed during the production line with the IoT components were fully operated, either from where the production line is located or from an external Internet network. Based on the both tables above, the SDFP and SDFB have a high correlation in the occurrence of DDoS attack which gives a lower result compared to the normal traffic. Paper [10] proposed the SFE for the attack traffic is much higher than in the normal traffic due to the high of flow entries.

Author at [11] proposed a process that occurs within the controller to operate the DDoS detection and mitigation. It will continuously measure the entropy for each time window. If it is below the threshold for three times in a row, it will be identified as a botnet host, and only then the mitigation approached will be implemented. Right after the mitigation has been executed, its IP addresses are going to be permanently blocked and they will no longer be able to send any more requests to the server. Author at [12] proposed an algorithm which has been divided into three phases; monitoring phase, bandwidth control phase, detection and mitigation phase.

4 System Model and Problem Formulation

In this paper, we consider a Support Vector Machine (SVM) including a proposed simulation of DDoS attacks which uses MATLAB simulation for the algorithms in detection and mitigation. SVM involve a python language whereas C or C++ language is implemented in MATLAB. It is involving a packets delay which will set a benchmark of DDoS attacks.

4.1 Secure of the Images on IoT

Data collection for images transmission and processing have extended across the digital age, and the issue of picture is becoming increasingly important, particularly in military and specific industries such as commerce and medical treatment. In this work, a Rivest-Shamir-Adleman (RSA) is used as a modern publicly of encryption algorithm which uses an asymmetric encryption method. In the following, the RSA is used as an example of an image encryption method that has been researched. The algorithm is used in picture encryption software.

The optimization of algorithm is the topic of this work in which the fake image is provided earlier on to act as a medium to be attacked. This is because, DDoS attacks can be prevented by using cryptographic techniques, which this technique has been applied on the fake image provided so it will be encrypted. In other words, the server encrypts the requested image before sending it. The file is then delivered to the client, who decrypts it and reads it. As a result, it is possible to conclude that more stable communication between server and clients is possible, and active communications remain unaffected even in the presence of DDoS attacks.

4.2 Algorithm Steps for Securing Network

In this work, the proposed algorithm uses an asymmetric cypher encryption system. The key and algorithm are separated over the whole encryption process.

Firstly, a variety of choices is implemented where a huge prime number a, b, followed by the 2 number products $m = ab$. Then, choose a large integer encryption key, d that meets the criteria d, as well as (a-1)(b-1) Coprime. $ed = 1\text{mod}(a\text{-}1)$ is the decryption key (b-1). Next, encrypt plain text P as cipher text $C(C = \text{Pdmod } m)$, then decrypt cipher text C to plain text.

4.3 Image Encryption

The algorithm requires a key. The key is multiplied exponentially and modulo computed. The key creation procedure comprises automatically creating and storing huge prime numbers.

4.4 Overall Steps for Creating Algorithm

In this work, the viewing of digital images is being encrypted and decrypted during the encryption and decryption process. A huge prime number, which is used to automate the development of large prime numbers and keys in order to reduce user actions. It also ensures that the prime number utilised by the key is large enough. The user can customize the length of the keys based on the situation, as well as the speed of encryption and decryption. Next, exporting a key file to ensure the security of the transfer or stored method by exporting the key file as a file.

4.5 Storage of Keys

The key two must be generated by the algorithm. 21024 is a big number which alternatively, bigger and safer. However, in computer languages, unsigned integers are used. This may store up to two bytes, which is significantly less than the length of an RSA security key. A unit of linear array is created to store huge prime numbers in programming which solve the storage problem of large prime numbers. So, it will be set to unsigned first before the large prime numbers are stored in a linear array of cells called a prime number table. If the length of a large prime exceeds unsigned, z as the number of units will assign space to manage the number of storage units and only then the array's length is predetermined.

4.6 Key's Operation

The original data operation method is no longer applicable because the resulting huge prime number exceeds 21024. Inter class derivation and association are used to realize a large number operation on the basis of large number storage. Flex unit is a term used to describe a flexible unit which take a long value as a starting point. The original long value class is associated with a new class long in, which implements operator overloading in the new long class. The calculation of numbers according to a specific number system is an example of this type of operation. The notion of vertical operation is also used to do multiplication and remainder.

4.7 The Proposed Scheme

Based on the steps above which explain in detail on how the fake image provided is used, the flowchart is designed to illustrate on how the detection of DDoS attacks will lead to the mitigation process. The fake image is used as a medium to be attacked (Fig. 1).

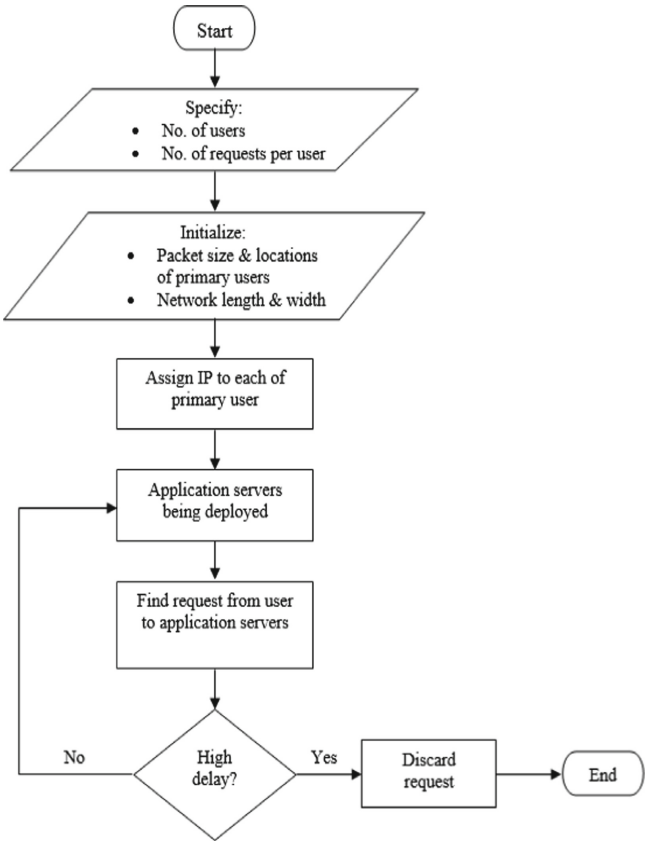

Fig. 1. Flowchart of the Proposed System

5 Performance Evaluation

5.1 The Impact of an Intense Attack

The simulation was carried out according to the parameters in Table 1 with varying intensities. In the table, there are four presence of attacks which are No, Low, Medium and High which provide different values of Probability-based Attack (%).

Figure 2 shows four types of throughput results varied with time. From the figure, it can be seen that when the presence of attack is small, the throughput gradually increases. However, the throughput instantly goes up when the presence of attack is medium and afterwards drops once it reaches the bandwidth of the link. The same goes to the high presence of attack where the throughput increases and decreases rapidly. This is due to the throughput is affected by the intensity attack in IoT system.

Figure 3 shows four types of link utilization results varied with time. From the figure, it can be seen that the link utilization is very low which is around 3% when there is no attack available. However, when the presence of attack is small where the attack begins at 2100th seconds, it will slowly rise up to 28% at 3600th seconds. As for the medium

Table 1. DDoS Attack with Varying Intense

Presence of Attack	Victim Nodes Count	Zombie Host (%)	Attack Starts (sec)	Period of Attack (sec)	Probability-based Attack (%)
No	1	0	0	0	0
Low	1	30	2100th	1500th	0.4
Medium	1	50	1200th	2400th	0.6
High	1	70	800th	2800th	0.8

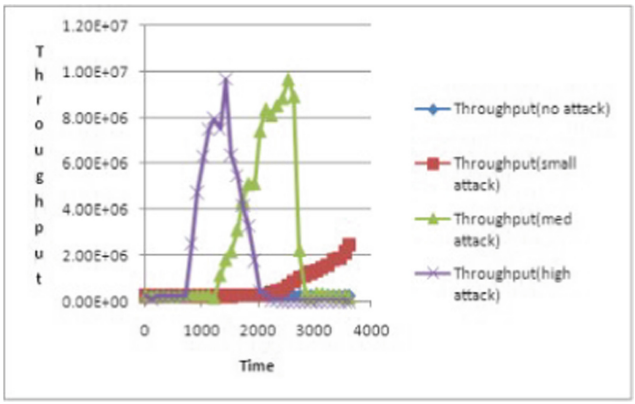

Fig. 2. Throughput against Time

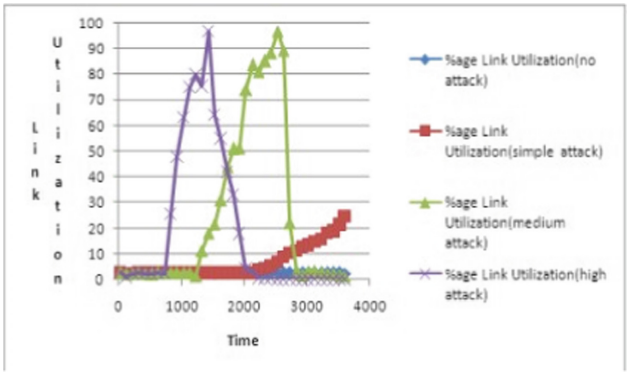

Fig. 3. Link Utilization against Time

presence of attack where it begins at 1200th seconds, it will rise up to 98% at 2500th seconds and afterwards drops while keeps constant around 3%. The same goes to the high presence of attack where it begins at 800th seconds then increases rapidly until 98%

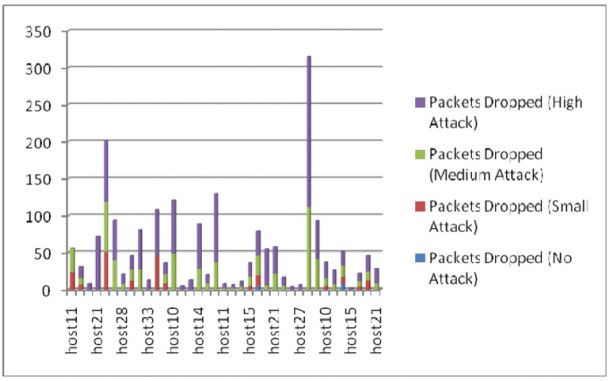

Fig. 4. Packets Dropped against host

Table 2. DDoS Attack with Varying Buffer Size

Buffer Size	Victim Nodes Count	Zombie Host (%)	Period of Attack (sec)	Probability-based Attack (%)
Normal	1	60	2500th	0.6
Low	1	60	2500th	0.6

at 1500th seconds and afterwards drops until it reaches zero. This is due to the intensity attack is affected by the link utilization in IoT system.

Figure 4 shows four types of packets dropped results varied with host. From the figure, it can be seen that the amount of packets being dropped goes up along with the intensity attacks. This is due to the packet dropped is affected by the intensity attack in IoT system.

5.2 The Impact of Buffer Size

The simulation was carried out according to the parameters in Table 2. From the table, it is shows the percentage of probability based attack is varied by the buffer size.

Figure 5 shows the throughput varied with time for two different throughputs which are normal (NRML) buffer and low buffer. From the figure, it can seen that the packet is rises with comparatively small buffer sizes which resulting the throughput to be dropped.

Figure 6 shows link utilization results varied with time for NRML and low buffer**.** It can be investigated that there are trade-off between Fig. 6 and Fig. 5. It is due to the percentage of bandwidth used for throughput. It can be seen that the throughput is directly proportional to the percentage of links that are utilized.

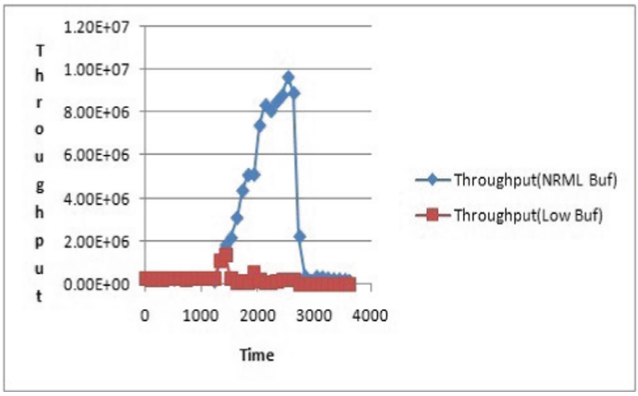

Fig. 5. Throughput against Time

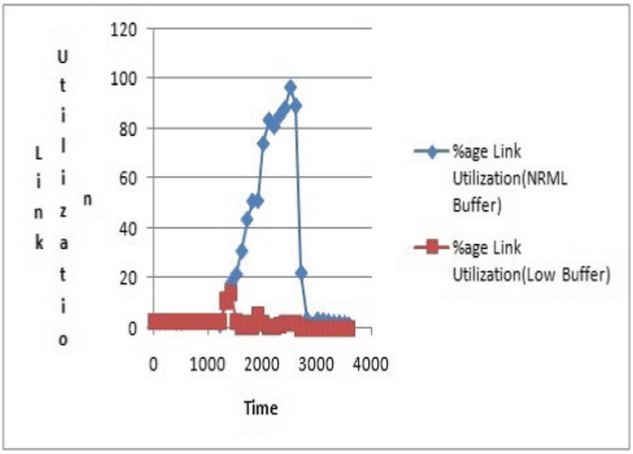

Fig. 6. Link Utilization against Time

Figure 7 shows two types of packets dropped results varied with host. From the figure, it can be seen that the packets dropped are lower in normal buffer size compare to the low buffer size. From this finding, it can be concludes that the packet dropped is affected by the buffer size in IoT system. Furthermore, a DDoS mitigation on fake image attacks is described.

Figure 8 shows the attacks on fake image as being explained before in accordance to the intensity attacks and buffer sizes. The graph illustrates on the status of the fake image either being encrypted or decrypted (original). The process of the image as a medium being used is explained before.

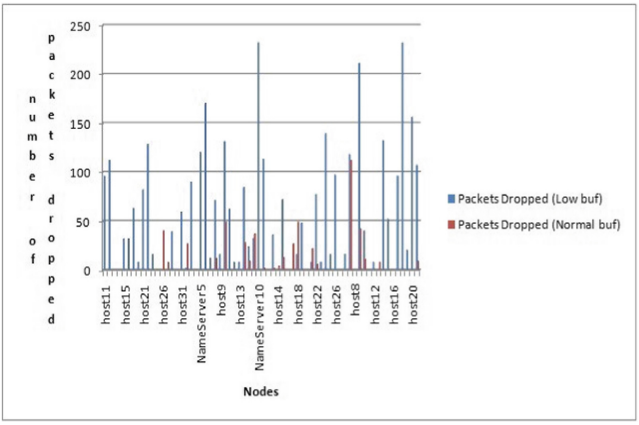

Fig. 7. Packets Dropped

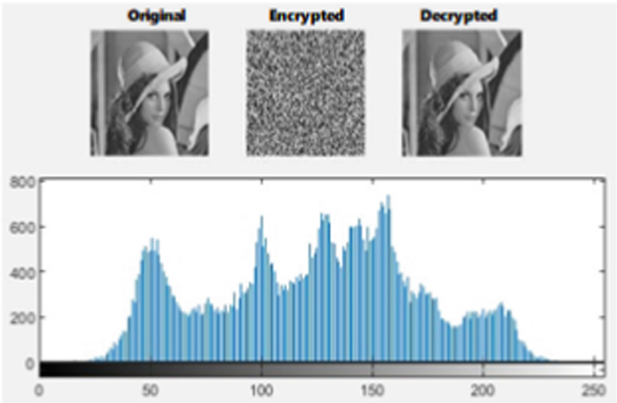

Fig. 8. Fake Image Attacks

In further analysis, Fig. 9 shows the packets delay fluctuation during the attack of simulation. It can be seen that the delay rate is high though the packets received is small. This has indirectly slowed the network execution and increased the network response time while degrading the network performance.

However, it appears in Fig. 10 that the packets delay rate is low due to the proposed mitigation being applied in this work and as a contribution in this field. It is due to that the proposed mitigation is successfully rejecting the pointless request with the low delay time. This indicates that the DDoS attack has less of an impact in the data center and IoT environment. Due to this, the approached mitigation able to reduce the effect of being attacked in this work.

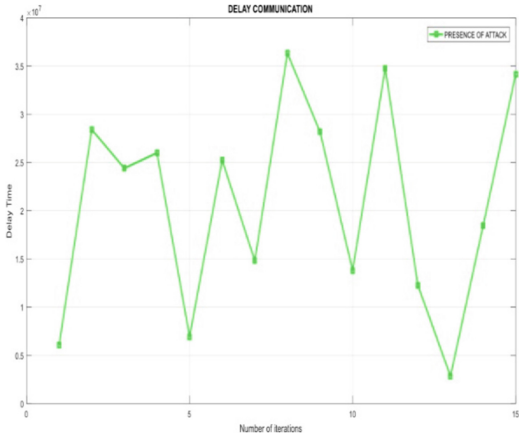

Fig. 9. Packets Delay during Attack

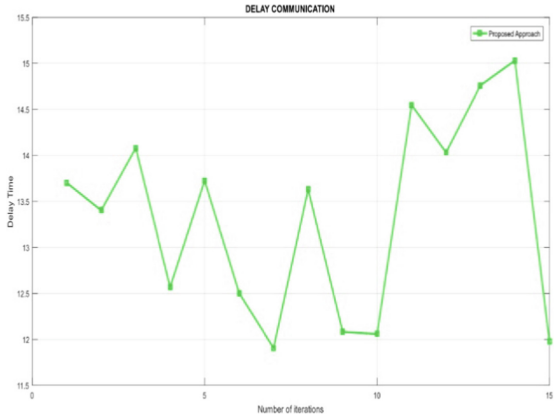

Fig. 10. Packets Delay after Mitigation

6 Conclusion

In this paper, the challenges in implementing the mitigation approached is that the security application takes a longer service time to get back to the normal traffic due to the attacks. More complex scheme need to be devised to inspect the incoming traffic packets in order to avoid this circumstance.

The attacks simulation need to be implemented so that the DDoS attacks can be analyzed and easily to understand in order to apply any preventative measures against the DDoS attacks. Based on the simulation network, the performance of a server has been deteriorated due to the increment of intensity attacks and buffer sizes.

Besides, the algorithm's biggest percentage computation able to control the generation of the final public and private keys, which directly impacts the algorithm's RSA performance. The realization of ideas is exponential constant bisection and the specific

procedure by converting a power module action into a multiplication module operation using the principles of multiplicative modules.

Finally, the proposed mitigation method is successfully implemented where there are reduction in the number of DDoS attacks in energy consumption in a server and it is able to reduce the effect of being attacked in IoT.

Acknowledgement. This work is supported and funded by the MMU-Tel U Join Research Grant, MMU/RMC-PL/TELKOM/AL/030, Telkom Universitas, Indonesia.

References

1. "The IOT attack surface: Threats and security solutions," *The IoT Attack Surface: Threats and Security Solutions - Notícias sobre segurança*. [Online]. Available: https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions. [Accessed: 22-Apr-2022].
2. Hassib, B. and Shires, J., 2022. Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy. *Middle East Policy*, 29(1), pp.90-103.
3. F. Fahim, "Top causes of website downtime," *ServerGuy.com*, 07-Aug-2021. [Online]. Available: https://serverguy.com/servers/cause-of-website-downtime/. [Accessed: 22-Apr-2022].
4. "Botnet attacks - everything you need to know," *CDNetworks*, 17-May-2021. [Online]. Available: https://www.cdnetworks.com/cloud-security-blog/botnet-attacks/. [Accessed: 22-Apr-2022].
5. Kaspersky, "Brute Force attack: Definition and examples," www.kaspersky.com, 05-Jul-2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/brute-force-attack. [Accessed: 22-Apr-2022].
6. "Security countermeasure," *Security Countermeasure - an overview | ScienceDirect Topics*. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/security-countermeasure. [Accessed: 22-Apr-2022].
7. W. Kenton, "Two-factor authentication (2FA)," *Investopedia*, 19-May-2021. [Online]. Available: https://www.investopedia.com/terms/t/twofactor-authentication-2fa.asp. [Accessed: 22-Apr-2022].
8. "What is Data Center Security?," *Forcepoint*, 06-May-2021. [Online]. Available: https://www.forcepoint.com/cyber-edu/data-center-security. [Accessed: 22-Apr-2022].
9. Huraj, L., Horak, T., Strelec, P., & Tanuska, P. (2021). Mitigation against DDoS Attacks on an IoT-Based Production Line Using Machine Learning. Applied Sciences, 11(4), 1847.
10. Iyer, S, & William Isaac, "SOFTWARE-DEFINED SECURITY," April 2018.
11. I. Sumantra and S. Indira Gandhi, "DDoS attack Detection and Mitigation in Software Defined Networks," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), 2020.
12. Alamri, H. A., & Thayananthan, V. (2020). Bandwidth Control Mechanism and Extreme Gradient Boosting Algorithm for Protecting Software-Defined Networks Against DDoS Attacks. IEEE Access, 8, 194269–194288.