ISSN: 2579-7298

THE IMPLEMENTATION ANALYSIS OF LAMPORT SCHEME WITH SHA-256 ON MOBILE E-OFFICE

Hendra Widodo[a,1], Mardiana[a,2], Melvi [a,3], Ardian Ulvan[a,4,*]

[a]*Department of Electrical Engineering, Universitas Lampung, Jl. S. Brodjonegoro No. 1, Bandar Lampung, Indonesia*
[1] *hendraawidodo@gmail.com*, [2]*mardiana@eng.unila.ac.id*, [3]*melvi@eng.unila.ac.id*, [4]*ardian.ulvan@eng.unila.ac.id*
**corresponding author*

ARTICLE INFO

Article history:

Received: 17 February 2021
Revised: 9 March 2021
Accepted: 15 March 2021

Keywords:
Mobile Electronic Office
Data Security
SHA-265
Lamport Scheme
Performance Analysis

ABSTRACT

Electronic administration system is one of the best solutions in the current digital era, electronic-based systems are considered to make it easier for an organization to process data and can reduce the possibility of data loss due to human error or natural disasters. The current administrative data management application is called the Electronic Office (E-Office). The E-Office handles data for incoming mail, outgoing mail and mail disposition. There are frequent delays in receiving information and validating letter files that are still carried out using physical files, so the mobile e-office is a solution that can be used by an agency to make it easier for workers to access information more quickly and can be done anywhere. Data security is an important thing that needs to be considered in an electronic transaction, so this research will add data security to the mobile e-office using sha-256 and lamport schemes. We present data on the results of this mobile e-office test on mobile devices and virtual private servers (vps), the data is in the form of functional application performance testing results and records of processing time performed by mobile and vps devices. From this data an analysis will be carried out to determine the appropriateness of the devices that can be used in running a mobile e-office.

I. Introduction

Electronic administration system has been considered as the effective and efficient solution for an organization to process the administration data and reduce the possibility of data loss due to human failure or natural misfortunes. One of the administrative data management systems in an organization is the Electronic Office (E-Office). E-Office is an administrative and centralized service used by organization, where data, information, and communication are stored and disseminated through several forms of telecommunications [1-2, in 3], including the most emerging platform that is mobile apps. Hereafter, the availability of mobile e-office system may intensify the efficiency of administration processes and cost, since all data are stored centrally, quick data access, accurate and real-time due to the use of internet network, and possibility to provide a prompt report based on the existing data. Mobile e-office also handles incoming and outgoing mail, instant messaging, including a fast letter disposition among staffs and managements.

In the process of signing the letter approval, the conventional and traditional way by giving the hand signature on the printed physical paper is still dominant. Apparently, the delay may occur when the authorized person is out the office or busy. In large scale, those delays may cause problems in the organization's business processes. Even though the electronic signature is officially valid under the law (Indonesian Government Regulation No.82/2012 concerning Implementation of Electronic System and Transaction). To cope with this issue, this study proposes a mobile e-Office system that can be used as a tool to validate the official letter and other administrative actions. The developed mobile e-Office utilizes the electronic signature as a media of approval in an electronic letter which is expected to reduce the risk of delay in the approval of an official letter.

DOI: 10.29099/ijair.v5i2.212

In an electronic system there is a part that must be considered, namely the data security of the system.

The developed mobile E-office proposes a data security system using Lamport's signature scheme with SHA-256 cryptographic hash algorithm. The scheme is used to verify the application users, where only authorized parties can receive and open data from the electronic mail. The focus of this study is to analyzes the performance of mobile devices and virtual servers in processing the SHA-256 and the Lamport scheme when deployed in the mobile e-Office system.

II. Research Methodology

A. Research and Development Method (R&D)

Research and Development (R&D) methods are one type of research method. This method can be interpreted as a scientific way to research, design, produce and test the validity of the products that have been produced. Accordingly, the activities can be shortened to 4P (Research, Design, Production and Testing) [4-7].

This research enters into level 4 i.e., making and testing the effectiveness of the product, namely the e-Office application based on mobile application. Developing a mobile e-Office application was completed by examining the potentials and problems, then conducting literature studies and gathering information, followed by designing products by making product designs which are then validated to see the deficiencies of the product designs being made. After the design is validated, then make the product as previously designed and will be tested into three tests, namely limited trials, main field trials and operational field trials. Each trial has a product revision stage to correct product deficiencies after being tested.

B. SHA-256

SHA-256 was designed by the National Institute of Standards and Technology (NIST) in 2002. SHA-256 produces a message digest with a length of 256 bits. SHA-256 is a one-way hash function, because it is not possible to find messages from the message digest generated [8-11]. Table 1 shows the comparison of hash functions.

Table 1. Comparison of hash functions

Algorithm and Variant	Output Size (bits)	Internal State Size (bits)	Block Size (bits)	Max Message Size (bits)	Word Size (bits)	Rounds	Operations	Collisions Found
SHA-0	160	160	512	2^{64} - 1	32	80	+,and,or,xor,rot	Yes
SHA-1	160	160	512	2^{64} - 1	32	80	+,and,or,xor,rot	None (2^{52} Attack)
SHA-256/224	256/224	256	512	2^{64} - 1	32	64	+,and,or,xor, shr,rot	None
SHA-512/384	512/384	512	1024	2^{128} - 1	64	80	+,and,or,xor, shr,rot	None

As can be seen from Table 1, SHA-0 and SHA-1 have bit length of 160 bits, this is weaker than SHA-256 which has bit length of 256 bits. Moreover, SHA-256 has smaller number of rounds compared to other hash functions which is as many as 64 rounds. This makes the SHA-256 hash more secure than the SHA-0 and SHA-1 hashes and faster in data processing than other hash functions above.

C. Lamport Schemes

Lamport scheme is a digital signature scheme that is used only once where the private keys are used as a tool to verify data [12-13]. By implementing Lamport scheme, each data transmission will be hashed, by which the results in a key that is divided into 2, namely the primary key and the public key. The primary key will be stored in the database and the public key is then distributed to the user as an authentication tool to access files. The two keys will produce two digital signatures, the first is the original digital signature consisting of the original private key and public key that has not been distributed to the user, and the second is the user's digital signature, which is a digital signature consisting of a public key that comes from a user requesting file access and a private key from the database. These two digital signatures will be validated and produce two conclusions, those are valid and invalid, if valid then the user can access the file and if it is not valid then the user cannot access the file.

III. Result and Discussion

A. Mobile E-Office Design

The mobile e-Office application was developed based on Android, with a minimum version of Android 7. The application was built using Android Studio 3.6.3, Apache Web Server 2.4.43, PHP 7.4 and MariaDB 10.4.11. Mobile e-Office is designed to be used by multiple users, which are grouped into user levels, namely level 1 to level n. Figure 1 describes the development flowchart of the proposed mobile e-Office.

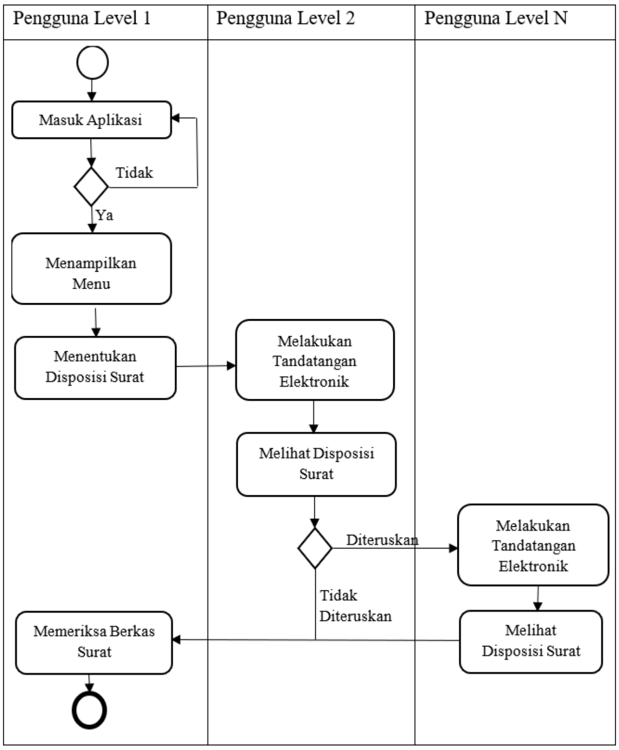
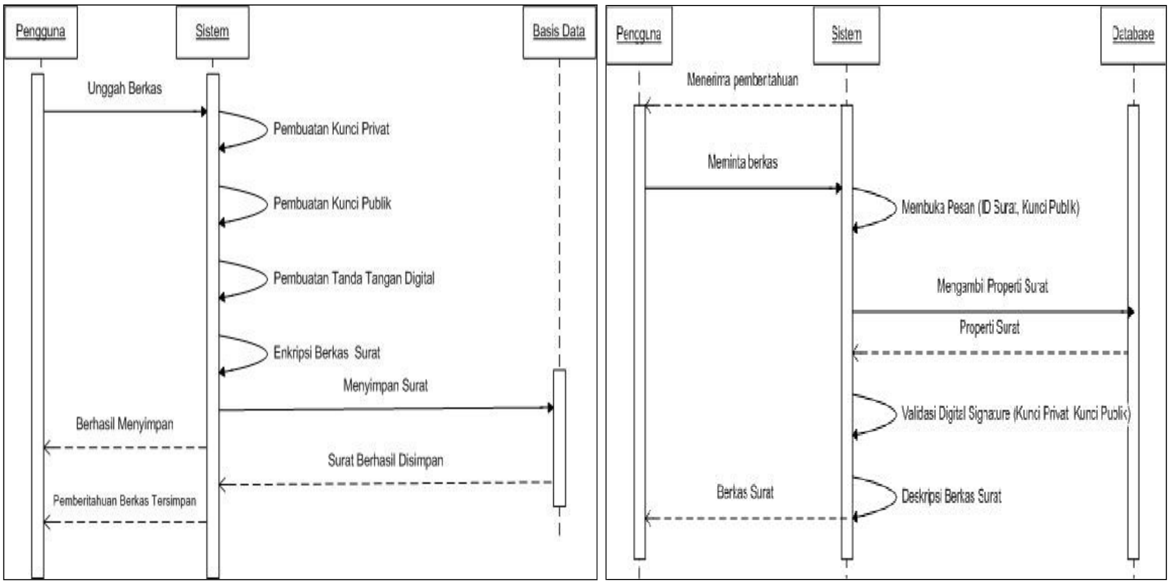


Fig. 1. Flowchart of Mobile e-Office

B. Implementation of SHA-256 and Lamport Scheme

The application of SHA-256 and the Lamport Scheme on the mobile e-Office is divided into two processes, namely the process of uploading files into the database and the process of retrieving files from the database [14]. The process of uploading files to the database included the creation of a private key, which is obtained by randomizing the number by the system, and then hashing it using SHA-256 to produce 256 pairs of bit numbers. After obtaining the private key, the next process is to create a public key that is obtained through the same hash process as in creating a private key by randomizing the number then hash the number using SHA-256. This public key will be published to each user as a key to verify data, the next step is to save the public key and private key that was previously created into the database for the data verification process. The next process is to combine the public key and private key that have been stored in a database called a digital signature [15]. The digital signature is not stored in the database since it is only used as a data verification tool. The next step is to encrypt the letter using SHA-256 and save it in the database. When the storage process is successful, the system will notify you that the file has been successfully saved into the database. Figure 2 shows the processes involved in mobile e-Office.



(a) (b)

Fig. 2. Process on Mobile E-Office, (a) Upload Files, (b) Retrieve Files

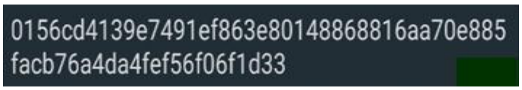
The process of retrieving files in the database will be displayed to the users who will validate them by means of an electronic signature on the electronic mail file. In the process, the user first gets a notification that there is a new letter that has not been read, then the user makes a request to open the file. After the request is received by the system, the system separates the message content in the form of a public key and a letter ID. The system will then retrieve the properties of the letter that have been stored in the database in the form of a private key, public key and letter file. Validation requires the original private key and public key that has been stored in the database before the public key is given to other users. The original private key and public key will be combined then hashed to produce a digital signature. The identical procedure is done with the public key obtained from a user request who is requesting access to a letter file. The user's public key will be combined with the private key that has been retrieved from the base. The data is hashed using SHA-256 which generates the digital signature of the user's request. After obtaining two digital signatures, the next process is to match the two digital signatures without saving them into the database, from this stage it will produce two conditions, i.e., valid and invalid, if the conditions are valid, the file will be decrypted by the system and then displayed to the user for validation. And the next thing is if the condition is not valid, then the file will not be decrypted by the system and a failure warning will appear on the system.

C. *Device Testing*

The testing of the device is divided into two groups, namely testing the functions in the application and testing the processing time in one work cycle [16]. Testing the application function is testing the functions of the e-office mobile application in implementing SHA-256 and Lamport scheme. Main functions of the tested Lamport scheme are private key generation, public key generation, file encryption, digital signature creation, digital signature validation and file decryption. Based on the functional testing of the developed mobile e-Office, the implementation of SHA-256 and the Lamport scheme was successfully carried out. The depicted picture can be seen at Figure 3 to Figure 8.

```
use Ramsey\Uuid\Uuid;
class Signature extends CI_Controller{
    public function private_key(){
        $privatekey = hash('sha256',Uuid::uuid4());
        echo $privatekey;
    }
```

(a)



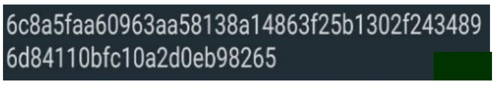
```
0156cd4139e7491ef863e80148868816aa70e885
facb76a4da4fef56f06f1d33
```

(b)

Fig. 3. Generate Private Key, (a) Modul Generate Private Key, (b) Result of Private Key

```
use Ramsey\Uuid\Uuid;
class Signature extends CI_Controller{
    public function public_key(){
        $publickey = hash('sha256',Uuid::uuid4());
        echo $publickey;
    }
```

(a)



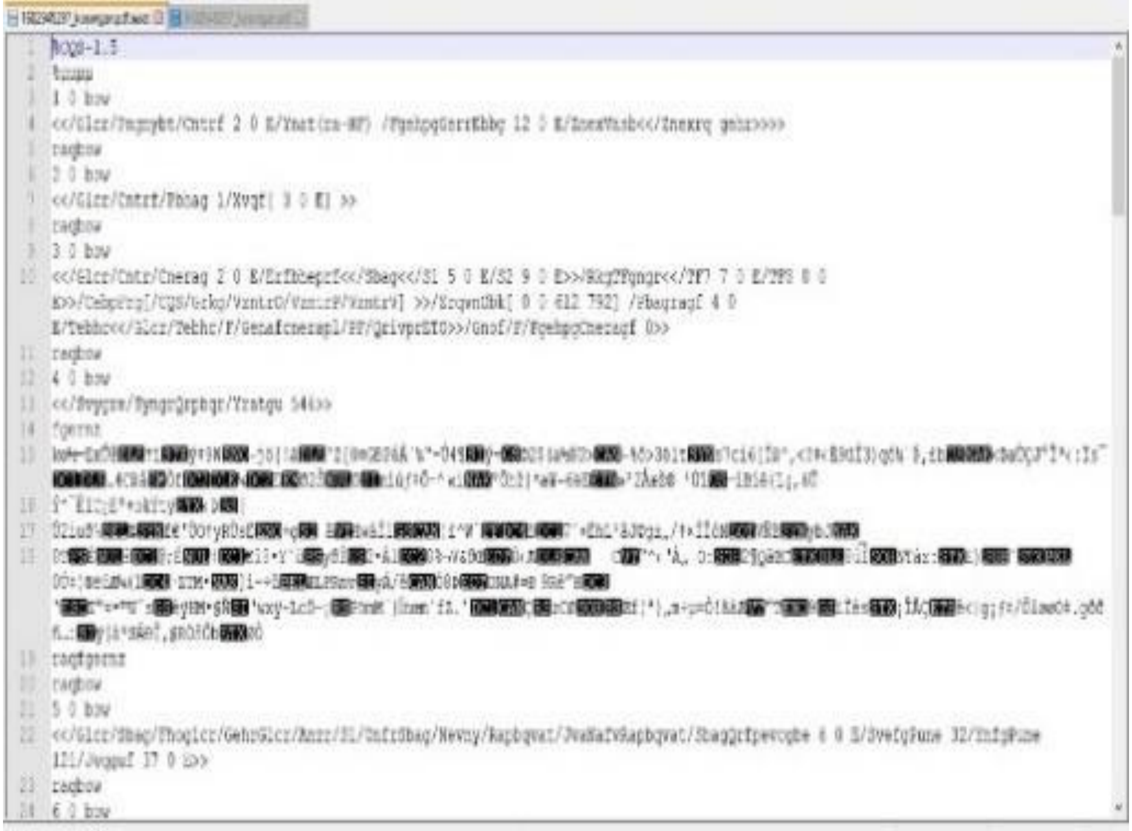
```
6c8a5faa60963aa58138a14863f25b1302f243489
6d84110bfc10a2d0eb98265
```

(b)

Fig. 4. Generate Public Key, (a) Modul Generate Public Key, (b) Result of Public Key

(a)

```
                                        function hw_encrypt_file($file, $destination, $passphrase){
                                         $handle = fopen($file, "rb") or die("Could not open a File.");
$contents = fread($handle, filesize($file));
                 fclose($handle);
                                                  $iv = substr(md5("\x1B\x3C\x58".$passphrase, true), 0, 8);
  $key = substr(md5("\x2D\xFC\xD8".$passphrase, true) . md5("\x2D\xFC\xD9".$passphrase, true), 0, 24);
                                                    $opts = array('iv'=>$iv, 'key'=>$key);
$fp = fopen($destination, 'wb');
               If(!$fp){
                                                                  return false;
                                                                     }
stream_filter_append($fp, 'string.rot13', STREAM_FILTER_WRITE, $opts);
                                        if(!fwrite($fp, $contents)){
                                                                  return false;
                                                                     }
fclose($fp);
return true;
                                                                   }
```



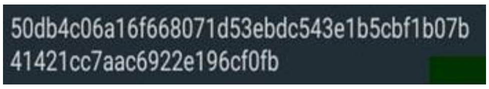
```
%CQS-1.5
%âãÏÓ
1 0 bow
<</Glcr/Pngnybt/Cntrf 2 0 E/Ynat(ra-HF) /FgehpgGerrEbbg 12 0 E/ZnexVasb<</Znexrq gehr>>>>
raqbow
2 0 bow
<</Glcr/Cntrf/Pbhag 1/Xvqf[ 3 0 E] >>
raqbow
3 0 bow
<</Glcr/Cntr/Cnerag 2 0 E/Erfbheprf<</Sbag<</S1 5 0 E/S2 9 0 E>>/RkgTFgngr<</TF7 7 0 E/TF8 8 0
E>>/CebpFrg[/CQS/Grkg/VzntrO/VzntrP/VzntrV] >>/ZrqvnObk[ 0 0 612 792] /Pbagragf 4 0
E/Tebhc<</Glcr/Tebhc/F/Genafcnerapl/PF/QrivprETO>>/Gnof/F/FgehpgCneragf 0>>
raqbow
4 0 bow
<</Svygre/SyngrQrpbqr/Yratgu 544>>
fgernz
[illegible]
[illegible]
[illegible]
[illegible]
raqfgernz
raqbow
5 0 bow
<</Glcr/Sbag/Fhoglcr/GehrGlcr/Anzr/S1/OnfrSbag/Nevny/Rapbqvat/JvaNafvRapbqvat/SbagQrfpevcgbe 6 0 E/SvefgPune 32/YnfgPune
121/Jvqguf 17 0 E>>
raqbow
6 0 bow
```

(b)

Fig. 5. File Encryption, (a) Modul File Encryption, (b) Result of File Encryption

```
$publicKey = hash('sha256',Uuid::uuid4());
$publicKey = hash('sha256',Uuid::uuid4());
$concat_key = $privateKey.$publicKey;
$signature = hash('sha256',$concat_key);
```

(a)



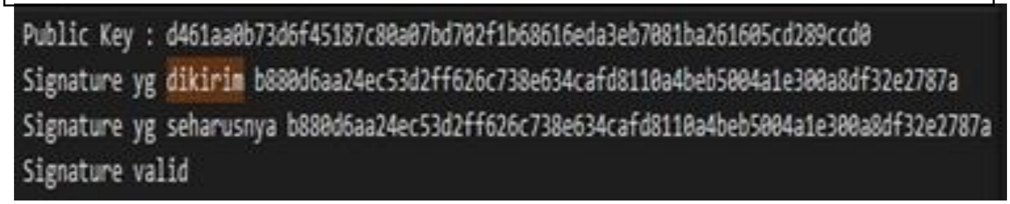
```
50db4c06a16f668071d53ebdc543e1b5cbf1b07b
41421cc7aac6922e196cf0fb
```

(b)

Fig. 6. Digital Signature Creation, (a) Modul Digital Signature Creation, (b) Result of Digital Signature Creation

(a)

```
$surat_ = $this->Surat_model->findFirst(['surat.surtId'=>$surat_Id]);
$public_key_db - $this->db->get_where('surat_public_key',['supkSurtId'->$surat_Id])->row();
$pub_key - $_POST['pubkey'];
$signature_db = hash('sha256',$surat_->surtPrivKey.$public_key_db->supkPubKey);
$signature_req – hash('sha256',$surat_->surtpPrivKey.$pub_key);
if($signature_db--$signature_req){
    @header('Content-Type:application/pdf');
    $decrypt_file = hw_decrypt_file(UPLOAD_ENC_FILE.$surat_->surtFile,$signature_db);
    fpassthru($decrypt_file);
    return;
}else{
    $status – 403;
    $message = ['message'=>'Signature tidak valid.'];
}
```



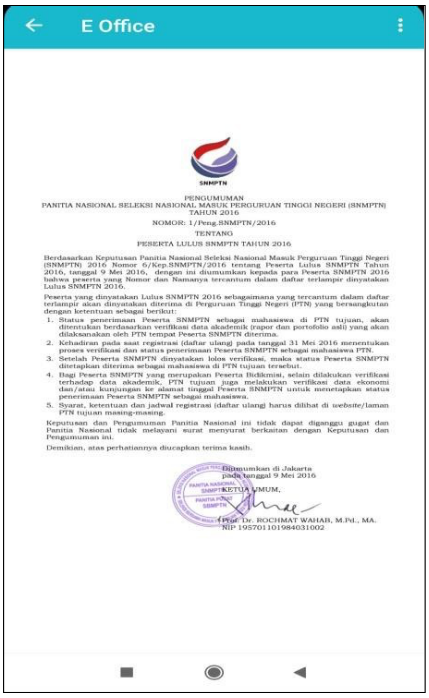
```
Public Key : d461aa0b73d6f45187c80a07bd702f1b68616eda3eb7081ba261605cd289ccd0
Signature yg dikirim b880d6aa24ec53d2ff626c738e634cafd8110a4beb5004a1e300a8df32e2787a
Signature yg seharusnya b880d6aa24ec53d2ff626c738e634cafd8110a4beb5004a1e300a8df32e2787a
Signature valid
```

(b)

Fig. 7. Digital Signature Validation, (a) Modul Digital Signature Validation, (b) Result of Digital Signature Validation

```
function hw_decrypt_file($file,$passphrase){
    $iv = substr(md5("\x1B\x3C\x58".$passphrase, true), 0, 8);
    $key = substr(md5("\x2D\xFC\xD8".$passphrase, true) . md5("\x2D\xFC\xD9".$passphrase, true), 0, 24);
    $opts = array('iv'=>$iv, 'key'=>$key);
    $fp = fopen($destination, 'rb');
    stream_filter_append($fp, 'string.rot13', STREAM_FILTER_READ, $opts);
    return $fp);
}
```

(a)



PENGUMUMAN
PANITIA NASIONAL SELEKSI NASIONAL MASUK PERGURUAN TINGGI NEGERI (SNMPTN)
TAHUN 2016
NOMOR: 1/Peng.SNMPTN/2016
TENTANG
PESERTA LULUS SNMPTN TAHUN 2016

Berdasarkan Keputusan Panitia Nasional Seleksi Nasional Masuk Perguruan Tinggi Negeri (SNMPTN) 2016 Nomor 6/Kep.SNMPTN/2016 tentang Peserta Lulus SNMPTN Tahun 2016, tanggal 9 Mei 2016, dengan ini diumumkan kepada para Peserta SNMPTN 2016 bahwa peserta yang Nomor dan Namanya tercantum dalam daftar terlampir dinyatakan Lulus SNMPTN 2016.

Peserta yang dinyatakan Lulus SNMPTN 2016 sebagaimana yang tercantum dalam daftar terlampir akan dinyatakan diterima di Perguruan Tinggi Negeri (PTN) yang bersangkutan dengan ketentuan sebagai berikut:

1. Status penerimaan Peserta SNMPTN sebagai mahasiswa di PTN tujuan, akan ditentukan berdasarkan verifikasi data akademik (rapor dan portofolio asli) yang akan dilaksanakan oleh PTN tempat Peserta SNMPTN diterima.
2. Kehadiran pada saat registrasi (daftar ulang) pada tanggal 31 Mei 2016 menentukan proses verifikasi dan status penerimaan Peserta SNMPTN sebagai mahasiswa PTN.
3. Setelah Peserta SNMPTN dinyatakan lolos verifikasi, maka status Peserta SNMPTN ditetapkan diterima sebagai mahasiswa di PTN tujuan tersebut.
4. Bagi Peserta SNMPTN yang merupakan Peserta Bidikmisi, selain dilakukan verifikasi terhadap data akademik, PTN tujuan juga melakukan verifikasi data ekonomi dan/atau kunjungan ke alamat tinggal Peserta SNMPTN untuk menetapkan status penerimaan Peserta SNMPTN sebagai mahasiswa.
5. Syarat, ketentuan dan jadwal registrasi (daftar ulang) harus dilihat di *website*/laman PTN tujuan masing-masing.

Keputusan dan Pengumuman Panitia Nasional ini tidak dapat diganggu gugat dan Panitia Nasional tidak melayani surat menyurat berkaitan dengan Keputusan dan Pengumuman ini.

Demikian, atas perhatiannya diucapkan terima kasih.

Diumumkan di Jakarta
pada tanggal 9 Mei 2016
KETUA UMUM,
PANITIA NASIONAL SNMPTN
PANITIA PUSAT SBMPTN
Prof. Dr. ROCHMAT WAHAB, M.Pd., MA.
NIP 195701101984031002

(b)

Fig. 8. File Decryption, (a) Modul File Decryption, (b) Result of File Decryption

.

The next test is testing the processing time. The test will be carried out using four units of mobile devices and two VPS with different specifications. The testing of processing time on the mobile e-Office has been carried out using five electronic mail files of different sizes. The specification of mobile devices and the VPS, and size of the files are shown respectively at Table 2, Table 3, and Table 4. Furthermore, the result of testing devices is shown in Table 5.

Table 2. Specifications of Mobile Device

Device Name	Operating System	Memory		CPU
		RAM	Internal Storage	
Mobile Device 1	Android 7	2 BB	16 GB	Octa Core 1.6 GHz
Mobile Device 2	Android 8	2 GB	16 GB	Octa Core 1.6 GHz
Mobile Device 3	Android 10	4 GB	64 GB	Octa Core 2.0 GHz
Mobile Device 4	Android 10	6 GB	128 GB	Octa Core 2.31 GHz

Table 3. Specifications of VPS

Device Name	Operating System	Memory		CPU	Data Transfer
		RAM	SSD		
VPS 1	CentOS 7	2 GB	50 GB	1 Core	2 TB
VPS 2	Linux Debian 10	4 GB	80 GB	2 Core	2 TB

Table 4. Size of Files Testing

Files Name	Size
File 1	177 KB
File 2	266 KB
File 3	1 MB
File 4	2 MB
File 5	3 MB

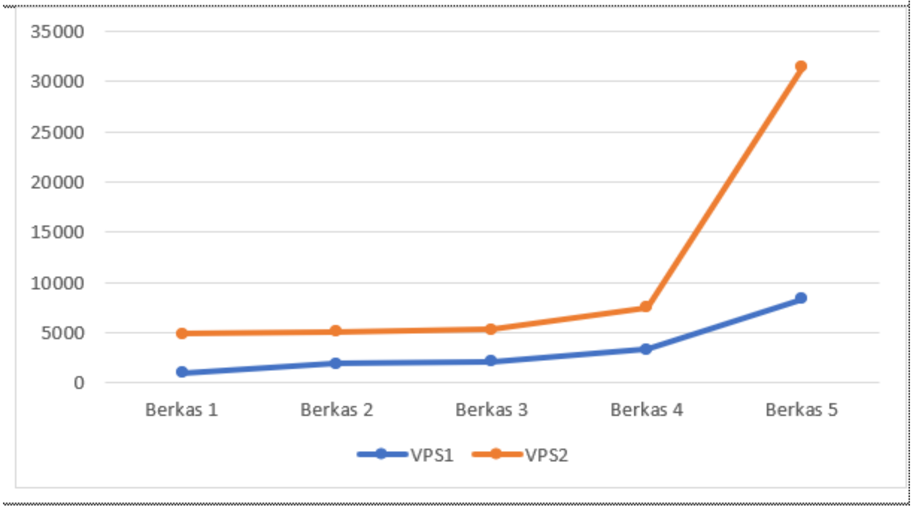
Based on the result, the larger size of the letter files processed by the mobile e-Office, the longer it will take for the system to process the electronic mail file data. Meanwhile, there is also an interesting result when the lower specification server (VPS1) outperformed the higher specification one (VPS2) when processing five electronic mail files using the same mobile device. The most basic difference between those two VPSs are in the embedded operating system, VPS 1 uses the CentOS 7 operating system and VPS 2 uses the Debian 10 Linux operating system. The embedded operating system of CentOS7 has significant impact in the processing time.

Table 5. Results of Testing Device

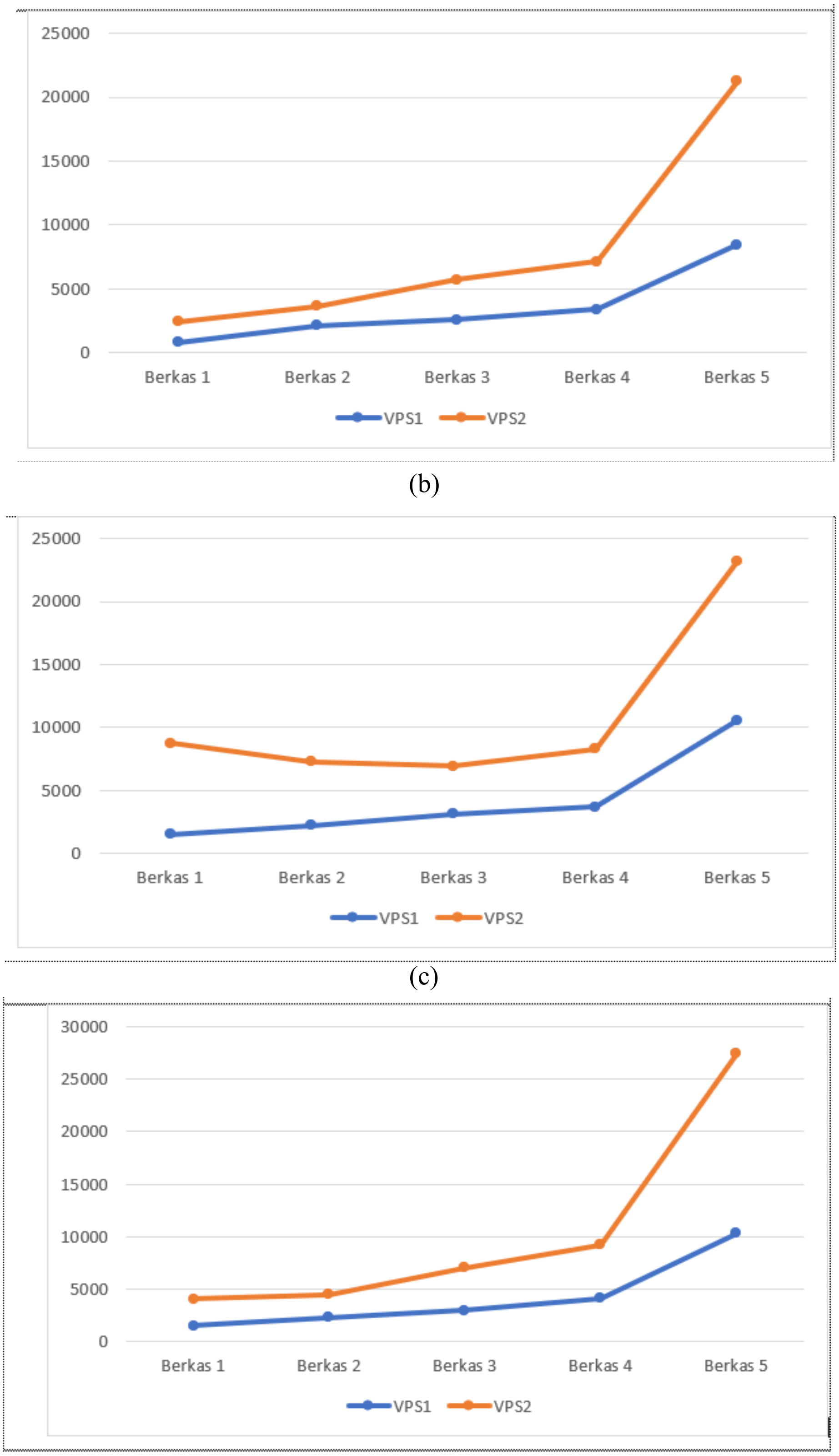
Type of Devices		**Total Completion Time of One Work Cycle**				
Mobile Devices	**VPS**	**File 1**	**File 2**	**File 3**	**File 4**	**File 5**
Mobile Device 1	VPS 1	1039,27	1903,49	2128,65	3318,45	8395,23
Mobile Device 1	VPS 2	3870,24	3210,92	3173,66	4195,07	23050,37
Mobile Device 2	VPS 1	842,66	2129,75	2602,23	3392,25	8440,96
Mobile Device 2	VPS 2	1570,98	1543,47	3118,55	3729,86	12778,28
Mobile Device 3	VPS 1	1541,76	2240,17	3131,77	3710,37	10597,67
Mobile Device 3	VPS 2	7227,07	5035,16	3803,25	4581,08	12590,74
Mobile Device 4	VPS 1	1531,93	2293,03	2983,25	4128,07	10287,83
Mobile Device 4	VPS 2	2538,72	2194,77	4035,97	5088,14	17164,96
	Average:	2520,33	2568,85	3122,17	4017,91	12913,26

D. *Analysis Performance*

As described previously, the proposed e-Office application has two level of security. The first level is the deployment of username and password when accessing the application. The second level is the deployment of SHA-256 and the Lamport scheme. Based on the test cases on these two security levels, the hardware and software used significantly affect the performance of the e-Office mobile application, as can be seen on Figure 9. Based on Figure 9, file 1 with a size of 117 kilobytes, the average total processing time is 2520.33 ms, making it the smallest average total processing time among the five files tested. Whereas file 5 which has the largest file size among the other files tested gets an average total processing time record of 12,913.26 ms with a file size of 3 megabytes, this makes file 5 has the longest average total processing record compared to other tested files. The test results show that the file size can also affect the performance of the device in processing letter files. The larger the file size being processed, the longer it will take to process electronic mail files.



(a)



(b)

(c)

(d)

Fig. 9. Result Mobile Device Testing, (a) Mobile Device 1, (b) Mobile Device 2, (c) Mobile Device 3, (d) Mobile Device 4

IV. Conclusion

Mobile e-office is a system that can be used to make it easier for workers in an agency to obtain information and take action on official letters anywhere. The results of the analysis show that the mobile device 1 with the lowest specifications of the device used for testing is by using the Android 7 operating system, 2 GB of RAM memory, 16 GB of internal storage memory and a Octa Core 1.6GHz CPU capable of running mobile application functions. E-Office which implements SHA-256 and the Lamport scheme as a method of data security for electronic mail files, thus enabling other devices that have specifications exceeding the specifications of to be able to run this mobile e- office. Based on the results of testing against time, data can be analyzed that the file size, the operating system used and the hardware of the mobile and VPS have an effect on the performance of mobile E-Office.

References

[1] Satish, C.G. (2004). Model View Controller (MVC) Architecture. Accessed on 16 January, 2021 from http://www.dotnetspider.com/resources/316-Model-View-Controller-MVC-architecture.aspx

[2] Leff, A. and Rayfield, J.T. (2001). Web-Application Development Using the Model/View/Controller Design Pattern. In Enterprise Distributed Object Computing Conference, 2001. EDOC'01. Proceedings Fifth IEEE International, IEEE, Seattle, WA, USA, 4-7 Sept. 2001, 118-127

[3] Subari, A. *et al* (2020). Design of E-office System in Vocational School Diponegoro University using Code Igniter Framework. *IOP Conf. Ser.: Mater. Sci. Eng.* **801** 012141.

[4] Grimpe, C. *er al* (2017). R&D, marketing innovation, and new product performance: A mixed methods study. Journal of Product Innovation Management, 34 (3), pp. 360-383

[5] Sugiyono. (2017). Metode Penelitian dan Pengembangan (Research and Development/R&D). Bandung:ALFABETA. ISBN: 978-602-289-158-1.

[6] Jogiyanto. (2005). Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktik Aplikasi Bisnis. Yogyakarta:ANDI. ISBN: 979-731-560-6.

[7] Pasolong, H. (2016). Metode Penelitian Administrasi Publik. Bandung:ALFABETA. ISBN: 978-602-9328-30-1.

[8] Federal Information Processing Standard (FIPS) 180-4 (2015). Secure Hash Standard (SHS). National Institute of Standards and Technology, US Department of Commerce.

[9] Fauziah, N.A. *et al* (2018). Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application. International Seminar on Research of Information Technology and Intellegent System (ISRTI). pp. 146- 151.

[10] Sembiring, H. *et al* (2019). Application of the Secure Hash Algorithm (SHA) Algorithm for Image Security. Media Informasi Analisa dan Sistem (MEANS). Vol. 4. No. 1. P-ISSN: 2548-6985. E-ISSN: 2599-3089.

[11] Sugiyatno, & Atika, P.D. (2018). Digital Signature with SHA-1 and RSA Algorithm as Authentication. Jurnal Cendekia. Vol. XVI. P-ISSN:0216-9436. E-ISSN:2622-6782.

[12] Zentai, D. (2020). On The Efficiency on The Lamport Signature Scheme. Land Forces Academy Review, Vol. XXV, No. 3 (99).

[13] Abdullah, G.M. *et al* (2018). Addoption of Lamport Signature Scheme to Implement Digital Signature in IoT. International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). pp. 1-4.

[14] Puspitasari, T.D., & Supriadi, Y. (2019). Implementation of Lamport Scheme on RFID Arduino Mega 2560 Based on Personel Access Control System (XYZ College Case Study). National Seminar on Innovation and Technology Application in Industry. pp. 91-98. ISSN 2085-4218.

[15] Lopes, H., & Chatterjee, M. (2014). Application H-Secure for Mobile Security. International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA). pp. 370-374.

[16] Nidhra, S., & Jagruthi, D. (2012). Black Box and White Box Testing Techniques – A Literature Review. International Journal of Embedded System and Application (IJESA). Vol. 2. No. 2. pp. 29-50.