Building Network Infrastructure and E-Hospital Using Cloud Computing

by Teguh Sutanto

Submission date: 19-Oct-2022 10:36AM (UTC+0700)
Submission ID: 1929327492
File name: 47-81-1-PB.pdf (592.11K)
Word count: 3913
Character count: 21183

Building Network Infrastructure and E-Hospital Using Cloud Computing

Norma Nihayah[1], Teguh Sutanto[2], Anjik Sukmaaji[3]
Information System Departement
Institut Bisnis dan Informatika Stikom Surabaya
Surabaya, Indonesia
norma@stikom.edu[1], anjik@stikom.edu[2], teguh@stikom.edu[3]

***Abstract* --The use of internet technology continues to increase, not least for the health world. Ease of access to information of a hospital is needed by people who want to do both emergency and periodic checks, one of which is the registration process and schedule information doctors at the hospital. In addition, easy access to information by doctors who do to know the history of patients who are treated is also very necessary. the existence of cloud computing technology, the problem can be solved by making network infrastructure by using one of cloud computing service that is Infrastructure as a Service (Iaas). With this infrastructure, one hospital with another hospital can connect to each other use cloud computing network, with the help of VMWare virtualization technology and Network Attached Storage (NAS) data storage. In addition, Mobile-based E-Hospital Applications are made. On the server made database that contains information about the patient registration data, life history, schedule doctors And the diagnosis of the patient. . In terms of data security application is applied encryption and data decryption using Blowfish algorithm so that data delivery process that happened can be more secure. In the encryption process E-Hospital so The length of the key used does not affect the timing of the encryption and decryption process.**

Keywords : Cloud Computing, Android, Blowfish

I. INTRODUCTION

The Internet is a computer network that can connect companies with the public domain, that is individuals, communities, institutions, and organizations as well as between companies[12][13][14]. This path is an effective path that a company can use. ranging from exchange of data and information to payment transactions can be done quickly and cheaply through the internet. Looking at technological developments that have progressed, it will be easier if the data transactions that occur in the hospital moved into a computation system. An e-hospital concept that is formed from an integrated system to be able to present data quickly, accurately and transparently. Patient data search process, patient medical history, doctor handling, diagnosis, and so forth can be done within minutes by using e-hospital service. In addition communication between hospitals can be easier starting from the patient's medical records and communication between doctors can be done using cloud computing[15][17][18][20].

The emergence of cloud computing is motivated by the needs of the industrial world and computerization will be the shared use of scattered computing resources, but can be used as needed [4]. Cloud computing refers to an on-demand, self-service Internet infrastructure that enables the user to access computing resources anytime from anywhere [1]. So cloud computing services can be available quickly and reduce interaction with cloud computing service providers. Appears several types of cloud computing based on network conditions, user scope and user needs specifications, resulting in private cloud, public cloud, community cloud and hybrid cloud computing [4][16][20].

There have been several studies that have been done previously related to the use of cloud computing in hospitals, including research on the implementation of mobile systems that enable data storage, update and data collection using cloud computing[16][19][20]. The Healthcare mobile app is developed using the google Android operating system that provides data and image management (supports DICOM format and JPEG 2000 coding) patient health. On the server side this research utilizes the Amazon's S3 Cloud Storage Service. [2]. In other studies utilizing sensor networks to monitor the health status of patients, in this case the sensor data collected and sent to the cloud. Different users like hospitals, clinics, patients or even researchers can access data from cloud networks. With the help of wireless Sensor Network (WSN) is expected to provide benefits such as saving the cost of hospital institutions with the creation of data management automation is done in real time from various sensors and disseminate information efficiently to the medical team [6] [8][9]

In terms of data security at the hospital there are some previous studies that have been done that is on research [5]

addressing security needs in online communication, especially in the E-Health domain focusing on providing different security for different types of communication in e-Health, where each communication transmits the type of information with different levels of sensitivity. This research uses Multi Agent System (MAS) to develop agent based system that can serve distributed process. This research integrates various types of encryption algorithms to provide different security needs for each type of information. MAgNet is a security model generated in this study consisting of eight agents, which are skilled to complete their goals as well as the overall system goals autonomously. In [3][10] Encryption and access control are required for ensuring proper authorization and confidentiality for patient records. Strong authentication and audit logs are required to ensure access only by those allowed. This research discuss differences in security technologies and details the ones used in system. A new encryption technology called policy-based encryption proves to be quite useful within a health care environment for both encryption and access control.

In this research is built cloud computing network infrastructure and e-Hospital applications that can access information that wanted to know by the public as quickly and as informative as possible. Especially in the world of health, where patients want that Hospital information in the form of doctor's schedule, inpatient information, patient history data, and others can be accessed easily[8]. By utilizing the progress of information technology, then the hospital data can be placed on the cloud computing network system to accelerate data access. So in this research will be applied Blowfish encryption algorithm on e-hospital system. Access information from the client used smartphone Android device. Data access consists of two types: public cloud e-hospital and private cloud e-hospital, it aims to distinguish data that can be seen by public or other hospitals with data that is private to the hospital itself

II. RESEARCH METHODS

Cloud Computing is a combination of the use of computer technology and Internet-based development. The latest developments in computer system technology that allows users to spend only in accordance with the usage so as to offer high-quality timely technology solutions.The access limititaion on the system right now, it can be handle with cloud computing, it is included by mobile user. the condition of internet connection available, health data in the cloud can be accessed anywhere and anytime. In this research is built Cloud Computing network infrastructure that can be a bridge to connect and integrate between hospital one with other hospital[19][20]. And followed by the creation of applications and data security to support this infrastructure.

A. Cloud Computing Network Infrastructure Design

Here is an overall system of integration of cloud computing networks:

Figure 1 is a cloud computing network infrastructure consisting of several network components such as on the server side there are 2 PCs used as simulation 2 hospital servers. On each PC server is installed VMWare ESX 4.1 as the virtualization host. Next to the external storage there is NAS (Network-Attached Storage) used for data storage on the server. NAS is integrated with 2 servers so NAS storage can be used to install 2 Vistual Machine in the form of Operating System which can be used as data center. Operating System used is Ubuntu Server and Windows 7. In each virtualization host there are 1 operating system Windows 7 to install e-hospital application, Application on every Operating System used in accessing 3 different user that is admin, doctor and patient. Inside the Cloud network there are 3 routes, namely mikrotik router. While on the Cloud network there is MPLS to connect a network.

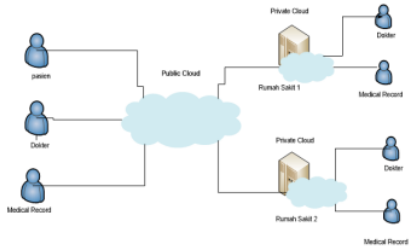


Fig 2. Public and Private Cloud Block Diagram On the Application Accessing side

Figure 2 describes the cloud work system in the hospital is divided into two categories: public cloud and private cloud. What distinguishes between public cloud and private cloud is the public cloud can be accessed by all users ie patients, doctors and medical records officer. While the private cloud can only be accessed by doctors and medical records, it aims to store the classified data in each hospital.

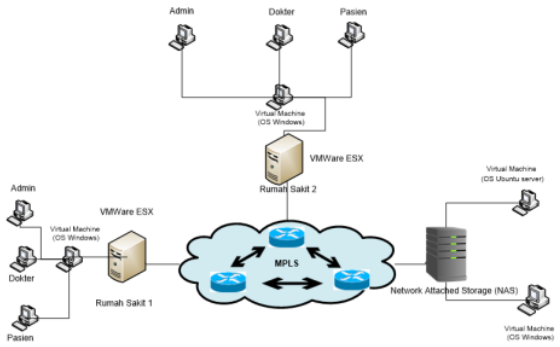


Fig 1. Illustration of Cloud Network Infrastructure

.

the data access from public cloud E-Hospital. It appears that the E-Hospital private cloud in each hospital is connected to the E-Hospital public cloud installed on the cloud service provider's premises. Doctors, medrec officers, and other systems in hospitals can access public cloud E-Hospital services through E-Hospital's private cloud. In addition, doctors and medrec officers can also directly access public E-Hospital services. Another thing that is different from public E-Hospital is public E-Hospital also provides services for patients to see the resume of his medical record. But here patients can not access in detail the medical record resume data on private E-hospital, because for the patient there is a separate limit for accessing data.

Here is the design stage to build cloud computing network infrastructure:

1. Cloud network infrastructure design
   The initial step of creating a cloud network infrastructure is to install Windows OS 7 64 bit on PC Server, then install and configure virtual host on PC Server that is with VMWare ESX 4.1. after the server is completed, the NAS is configured and connected with VMWare ESX 4.1 as its external storage server. The NAS application used is FreeNAS. After the external storage or data center server is connected, continued by connecting or searching the path using MPLS technology, once all is integrated then followed by testing system cloud.
2. Cloud Computing system design between server, client and NAS
   This cloud server system is done with NAS applications that are placed on the server side which will be connected on the client side that will access from the application to be created. Inside Freenas there is ISCSi setting which is a bridge connecting data center with server. On the client side used is VMWare ESX 4.1 as the host that will supervise some virtual machine operating system. The operating system used with virtual machines in is windows server 2003 Enterprise Edition SP 2. In the client side the access can be used via PC, laptop and Smartphone. And then all connected to the cloud network from the external side of storage, server and client with virtualization technology.
3. Designing server with virtual machine
   The step to build a cloud server using virtual machines ranging from VMWare Workstation 8 and VMWare ESX 4.1 configuration to virtual system integration. The initial process is done by configuring VMWare workstation 8 because it is software that can install and enable using more than one operating system. Next on VMWare Workstation install VMWare ESX 4.1 to get IP DHCP network. Still on VMWare workstation 8, install and configure again for windows server 2003 Enterprise Edition SP2 x64 until all installed, followed by configuring Vcenter Server 4.1 on windows server 2003 and static IP setting which IP is diguankan by Vcenter
4. Designing servers for public cloud and Private Cloud on the application
   Cloud working system in the hospital is divided into two categories: public cloud and private cloud. What distinguishes between public cloud and private cloud is the public can be accessed by all users ie patients, doctors, and medical record officer, while the private cloud can only be accessed by doctors and medical records because the data stored is classified confidential data for the hospital.
5. Designing Own cloud Data Application for E-Hospital Information System
   The design of own cloud data applications for E-Hospital information systems starting from accessing the database own cloud contained in the database server as the operating system. Furthermore, the user can login on the application created, either as admin or as a hospital doctor.

A. Design E-Hospital Application

In this research is made an e-hospital application that will integrate the information data from the hospital in the form of patient history, doctor schedule and diagnostic results that will be embedded in the cloud server where the data in inputkan will be in safe mengguanakan Blowfish method through encryption process and description. Applications that have been created will be accessed use Android platform. Here, data accessed by the user there are two kinds of data, namely private data and public data. Private data is data that can be accessed by certain parties only for example data that can only be seen by doctors, while public data is data that can be accessed publicly. Users who can access private data are doctors, while public data are patients and hospital medical personnel. To share data between hospitals can be accessed public data.

Figure 3 this below explains that the first step that occurs on the client side where the user is charging data accessed via smartphone (Android) and then done data encryption using blowfish method, before encryption process there is keyword. The keyword at the time of encryption is the same as the keyword in the decryption process (private key). After that the data that has been encrypted will be a chipertext (data that has undergone the encryption process). On the server side that is when the user wants to access the data that has been stored is done decryption process so that the ciphertext can be read by the user, enter the same keyword when doing the encryption. Then the server will look for it on the NAS (data center) and will be displayed.

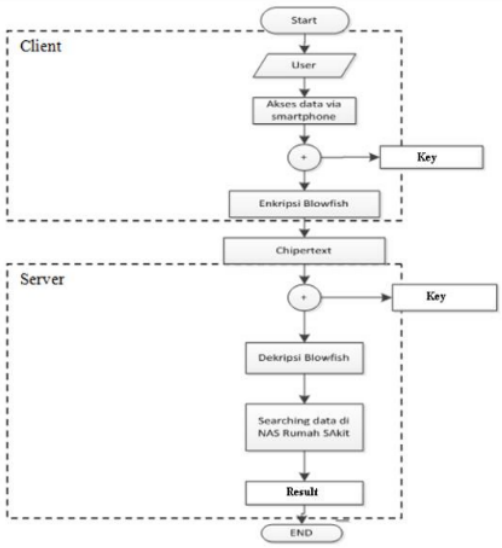


Fig 3. Flowchart System

B. Blowfish Algorithm [7][10][11]

Blowfish is included in 64-bit Cipher block encryption with key lengths ranging from 32-bit to 448-bit [7]. The Blowfish algorithm consists of two parts: Key-Expansion and Data Encryption. Data Encryption consists of a simple function iteration (Feistel Network) 16 times round. All operations are additions and XOR on 32-bit variables.

In the Blowfish algorithm[10], many subkeys are used. These keys must be calculated or generated first before encryption or decryption of data. In the feistel network, Blowfish has 25 iterations, the input is a 64-bit data element or call it "X". Blowfish is also a block cipher, which means during the encryption and decryption process, Blowfish will divide the message into blocks of the same length. The block length for the Blowfish algorithm is 64-bit. Messages that are not multiples of eight bytes will add additional bits (padding) so that the size for each block is the same.

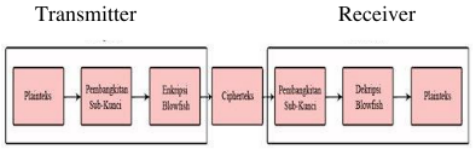


Figure 4 Block Diagram Modeling System on Blowfish

Blowfish includes encryption block Cipher 64-bit with key lengths that vary between 32-bit to 448-bit. Blowfish algorithm consists of two parts[10][11]:

1. Key-Expansion
   It functions to change the lock (Minimum 32-bit, Maximum 448-bit) into multiple subkey arrays with a total of 4168 bytes.
2. Data Encryption
   Consists of a simple function iteration (Feistel Network) 16 times round. Each round consists of key-dependent permutations and key- and data-dependent substitutions. All operations are additions and XOR on 32-bit variables. Other additional operations are just four table lookup of indexed arrays for each round.

Encryption use Blowfish Algorithm
Algorithm for encryption using Blowfish algorithm:

```
i= 1
loop from I to 16
Ri = Li-1 XOR Pi
Li = F(Ri) XOR Ri-1
        end loop
        L17 = R17 XOR P18
        R17 = L16 XOR P17
```

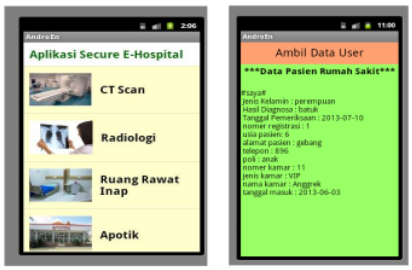
Descryption on Blowfish Algorithm
Algorithm for encryption using Blowfish algorithm:

```
i= 1
loop from I to 16
        Ri = Li-1 XOR P19-i
        Li = F(Ri) XOR Ri-1
end loop
L17 = R16 XOR P1
R17 = L16 XOR P2
```

The decryption process is almost identical to that of the encryption process. Sub-Keys P (1) to P (18) are used in reverse order P (1) to P (18), P (2) to P (17) and so on. In the decryption process the ciphertext is converted back into plaintext or its original state before it is encrypted.

B. RESULT AND ANALYSIS

Creation of E-Hospital mobile application user interface. Android based using eclipse software editor.



(a) (b)

Fig 5. E-Hospital Application Display

Figure 5 above if described then,. In the picture (b) is the view of the E-Hospital application After the user successfully perform authentication process on the client side So the user can see the required data in accordance with the level of the user. If the user is a patient then can see patient data in the form of self data, history of disease and result of doctor diagnose. When the user login as a doctor or medical record then the user can melihta patient data as well as physician data in the form of personal data and prescription drugs in accordance with patients handled.

Can be seen that the process of taking data from the client side successfully done. From the above view can dikethui Name, gender, doctor diagnosis, examination date and other patient data. The patient's user can display the history table of the disease where the table is related to the poly table, the chamber table and the diagnosis on the MySQL database. So it can be known poly examination of patients and information about the room for inpatients.

Fig 6 Results Of Encryption from Process Take Data

In Figure 6 is the data sent from the server to the client side. The data is encrypted data (chipertext) so that when an attack on the network, the data will not be read clearly because the data sent is random data.

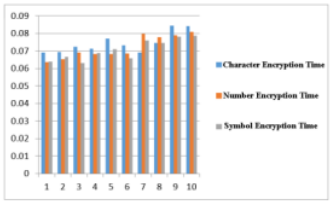


Figure 7 Graph of time comparison of encryption between characters, numbers and letters

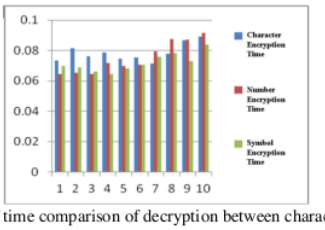


Fig 8 Graph of time comparison of decryption between characters, numbers and letters.

Average of time:

Enkripsi : $T_{rata2} = t_{total} / n$

$$= \frac{2.1721}{3} = 0.7 \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Dekripsi : $T_{rata2} = t_{total} / n$

$$= \frac{2.2562}{3} = 0.7520 \ldots\ldots\ldots\ldots\ldots (2)$$

From the above measurement results are tested on messages sent in the form of letters, numbers and symbols with the same number of inputs that the average time of encryption is faster than the decryption time. This is due to the addition of additional bits or padding at the time of encryption, thus causing the decryption process takes additional time as well.

A. Comparison of Encryption and Decryption with Key Length

Plaintext : surabaya

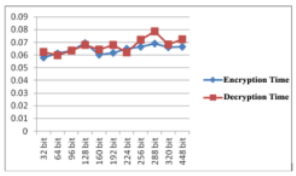


Fig 9 Comparison graph of Encryption and Decryption Time with different number of keys

From figure 9 above, visible by using different keyword sizes from 32 bits to 448 bits can't be done. The speed and process speed is the same as the blowfish processing algorithm the bits that exist in the data. The generation of subkeys done before the process of encryption or decryption do.

B. Testing of *Passive Network Attack*

At this stage tested attack on the system that has been made with the assumption that the client who is accessing e-hospital application with the attacker is on the same network. This passive attack using NetworkMiner software, so it will be seen starting the existence of important information contained in the data packet flow to suspicious images sent from the client to the server.

Testing is made with the concept of simulation, so the server is also in the same Wi-Fi network.

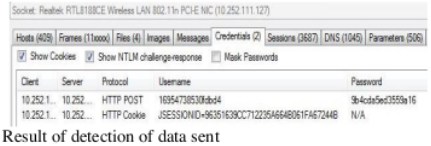


Fig 10 Result of detection of data sent

In Figure 10 is the result of a detection captured by the NetworkMinner software. But because the process of data transmission has been done first so that the encryption of data capture is a successful chipertext. This proves that the data on the client side successfully performed the encryption process.

CONCLUSIONS

1. The length of the key used does not affect the timing of the encryption and decryption process, because the blowfish algorithm processes the existing bits of the file and the generation of subkeys is performed before the encryption or decryption process is performed.
2. From the above test results show that the average time of encryption is faster than the decryption time. This is due to the addition of additional bits or padding at the time of encryption, thus causing the decryption process takes additional time as well.

REFERENCES

[1] Mell P, Grance T. "The NIST definition of cloud computing. Commun ACM". 2010;53(6):50.
[2] Doukas, C., Pliakas,T., & Maglogiannis,I. "Mobile Healthcare Information Management utilizing Cloud Computing and Android OS". Annual International Conference of the IEEE EMBS. 2010
[3] Garson,K., & Adams, C. "Security and Privacy System Architecture for an E-Hospital Environment". Proceedings of the 7th symposium on Identity and trust on the Internet, ACM. 2008
[4] Pratama, P.A. "Smart City beserta Cloud Computing dan Teknologi-teknologi pendukung lainnya". Informatika. Bandung. 2014
[5] Sulaiman, R., & Sharma, D. "Enhancing Security in E-Health Communications using Multi-Agent System". Journal of Computer Science 8 (5): 637-647, 2012
[6] Perumal.B, Pallikonda Rajasekaran.M and Ramalingam.H.M. "WSN Integrated Cloud for Automated Telemedicine (ATM) Based E-HealthCare Applications". *International Conference on Bioinformatics and Biomedical Technology. 2012*
[7] Pratiwi, A., Lhaksmana, K., & Rizal, S. "Implementasi Enkripsi Data Algoritma Blowfish Menggunakan Java Pada Aplikasi Email". Politeknik Telkom Bandung. 2011.
[8] Aminian, M., & Naji, H. R. (2013). A hospital healthcare monitoring system using wireless sensor networks. J. Health Med. Inform, 4(02), 121
[9] Chipara, O., Lu, C., Bailey, T. C., & Roman, G. C. (2010, November). Reliable clinical monitoring using wireless sensor networks: experiences in a step-down hospital unit. In Proceedings of the 8th ACM conference on embedded networked sensor systems (pp. 155-168). ACM.
[10] Singh, P., & Singh, K. (2013). Image encryption and decryption using blowfish algorithm in Matlab. International Journal of Scientific & Engineering Research, 4(7), 150-154.
[11] Bani Younes, M. A., & Jantan, A. (2008). Image encrytion using block based transformation algorithm.
[12] Diaz, J. A., Griffith, R. A., Ng, J. J., Reinert, S. E., Friedmann, P. D., & Moulton, A. W. (2002). Patients' use of the Internet for medical information. Journal of general internal medicine, 17(3), 180-185.
[13] Spencer, S. A., & Davies, M. P. (2012). Hospital episode statistics: improving the quality and value of hospital data: a national internet e-survey of hospital consultants. BMJ open, 2(6), e001651.
[14] Ajuwon, G. A. (2003). Computer and internet use by first year clinical and nursing students in a Nigerian teaching hospital. BMC medical informatics and decision making, 3(1), 10.
[15] Rolim, C. O., Koch, F. L., Westphall, C. B., Werner, J., Fracalossi, A., & Salvador, G. S. (2010, February). A cloud computing solution for patient's data collection in health care institutions. In eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED'10. Second International Conference on (pp. 95-99). IEEE.
[16] Doukas, C., Pliakas, T., & Maglogiannis, I. (2010, August). Mobile healthcare information management utilizing Cloud Computing and Android OS. In Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE (pp. 1037-1040). IEEE.
[17] Doukas, C., & Maglogiannis, I. (2012, July). Bringing IoT and cloud computing towards pervasive healthcare. In Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on (pp. 922-926). IEEE.
[18] Lupşe, O. S., Vida, M. M., & Tivadar, L. S. (2012). Cloud computing and interoperability in healthcare information systems. In The First International Conference on Intelligent Systems and Applications (pp. 81-85).
[19] Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems, 56, 684-700.
[20] Ermakova, T., Huenges, J., Erek, K., & Zarnekow, R. (2013). Cloud Computing in Healthcare–A literature review on current state of research.

Building Network Infrastructure and E-Hospital Using Cloud Computing

ORIGINALITY REPORT

16%	12%	12%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Yaya Sudarya Triana, Astari Retnowardhani. "Blowfish algorithm and Huffman compression for data security application", IOP Conference Series: Materials Science and Engineering, 2018 Publication	2%
2	citeseerx.ist.psu.edu Internet Source	2%
3	docshare.tips Internet Source	2%
4	ocs.dinamika.ac.id Internet Source	1%
5	researchsystem.canberra.edu.au Internet Source	1%
6	Tao Cai, Shiguang Ju, JunJie Zhao, Wei Zhong. "Performance Study of Cryptographic Storage Area Network", 2007 IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007), 2007 Publication	1%

7	zambrut.com Internet Source	1 %
8	Doukas, Charalampos, Thomas Pliakas, and Ilias Maglogiannis. "Mobile healthcare information management utilizing Cloud Computing and Android OS", 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology, 2010. Publication	1 %
9	Nattaruedee Vithanwattana, Glenford Mapp, Carlisle George. "mHealth - Investigating an Information Security Framework for mHealth Data: Challenges and Possible Solutions", 2016 12th International Conference on Intelligent Environments (IE), 2016 Publication	1 %
10	doaj.org Internet Source	<1 %
11	www.zettagrid.id Internet Source	<1 %
12	Anjik Sukmaaji, Eko Mulyanto Yuniarno, Mochamad Hariadi, I. Ketut E. Purnama. "New Approach to Flicker Removal in Underwater Images", International Review on Computers and Software (IRECOS), 2015 Publication	<1 %

13	pdfs.semanticscholar.org Internet Source	<1 %
14	repository.dinamika.ac.id Internet Source	<1 %
15	iaetsdjaras.org Internet Source	<1 %
16	repository.petra.ac.id Internet Source	<1 %
17	G Sujatha, Jeberson RetnaRaj. "Optimizing the performance of Image Deduplication system for effective storage in cloud using Enhanced Prefix Hash Tree", Research Square Platform LLC, 2021 Publication	<1 %
18	I-Ching Hsu. "Multilayer context cloud framework for mobile Web 2.0: a proposed infrastructure : Mobile Web 2.0 Context-aware Healthcare System", International Journal of Communication Systems, 10/2011 Publication	<1 %
19	www.intechopen.com Internet Source	<1 %
20	www.sciencepubco.com Internet Source	<1 %
21	"Computer Networks & Communications (NetCom)", Springer Science and Business	<1 %

Media LLC, 2013
Publication

22	E Aribowo, A Suryadi. "The insertion of confidential information into digital images using blowfish cryptography and end of file steganography", IOP Conference Series: Materials Science and Engineering, 2020 Publication	<1 %
23	ijircce.com Internet Source	<1 %
24	www.amrita.edu Internet Source	<1 %
25	J RITTINGHOUSE. "Securing Communications", Cybersecurity Operations Handbook, 2004 Publication	<1 %
26	aisel.aisnet.org Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		