EMITTER International Journal of Engineering Technology
Vol. 7, No. 1, June 2019
ISSN: 2443-1168

Medical Health Record Protection Using Ciphertext-Policy Attribute-Based Encryption and Elliptic Curve Digital Signature Algorithm

Novi Aryani Fitri, M. Udin Harun Al Rasyid, Amang Sudarsono

Politeknik Elektronika Negeri Surabaya
Kampus PENS, Jl. Raya ITS, Sukolilo Surabaya
E-mail: naryanif@gmail.com, {udinharun, amang}@pens.ac.id

Abstract

Information on medical record is very sensitive data due to the number of confidential information about a patient's condition. Therefore, a secure and reliable storage mechanism is needed so that the data remains original without any changes during it was stored in the data center. The user must go through an authentication process to ensure that not an attacker and verify to ensure the authenticity and accuracy of the data received. In this research, we proposed a solution to secure medical data using the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Elliptic Curve Digital Signature Algorithm (ECDSA) methods. Our system can secure data centers from illegal access because the uploaded data has patient control over access rights based on attributes that have been embedded during the data encryption process. Encrypted data was added to the digital signature to pass the authentication process before being sent to the data center. The results of our experiments serve efficient system security and secure with with low computing time. We compare the proposed system performance with the same CP-ABE method but don't add user revocation to this system and for our computing times are shorter than the previous time for 0.06 seconds and 0.1 seconds to verify the signature. The total time in the system that we propose requires 0.6 seconds.

Keywords: Medical record data security; CP-ABE; Digital Signature; ECDSA; Access Policy

1. INTRODUCTION

Record patient health information allowing medical documents to be threatened if they are stored in hardcopy. The use of electronic media (digital) in the patient medical data archiving could be a solution with the development of a system of a secure web server. This can also provide convenience to health workers in taking care actions. A system must be built to ease in sharing information in a collaborative so as to achieve the purpose of the complex goals in today's fast-paced tech-dominant world [1]. Systems that are built must have a safety mechanism places to protect the data. The encryption

algorithm is used to secure communication by making changes to the plaintext message (the original message before encryption) and converting it into a ciphertext (random message after encryption) [2]. Then adding access control can also protect the privacy of patients where only transmits the documents authorized doctors to patients. In healthcare allow the owner's privacy health record to set the specific access policies [3]. Some security and privacy threats and attacks to the patient sensitive information sent over wireless channels and data stored on the datacenter. Examples of threats include eavesdropping, impersonation, data integrity, data breach, collusion, and so on. This type of attack is considered in the model attack PrivacyProtector [4], Patients data leakage and destruction, collusion attacks, insider attacks, handle a large amount of data and the amount of data storage.

The patient's medical database system administrator can also reveal sensitive physiological data which were attack people inside. To protect the privacy of patients, many approaches have been proposed to provide access control to the patient documents when giving health care services. However, the most current system does not support fine-grained access control or consider additional security such as encryption and digital signatures [5]. For the sake of guaranteeing confidential data integrity and system security as a requirement on medical records privacy conscious [1].

In the CP-ABE scheme [1-2] [6], the user's secret key was associated with a set of attributes and each ciphertext embedded with top access policy attributes. After registration and authentication, users can decrypt the ciphertext file when needed, and then consult safely. This system requires an encryption process to protect data in the data center before storing it in the data center [7]. With the integrity of attribute-based encryption, the recipient can only decrypt files if and only if the set of secret key attributes meets the access policy in ciphertext [8].

Previous research [9], references to the previous paper have carried out the design of medical data security systems using the CP-ABE algorithm. This study continues with the addition of digital signatures in uploaded medical documents to validate data from the data center to ensure there are no changes as long as the data is stored. In the literature analysis, there are various of the digital signature algorithm, but there are only three that have been standardized by the National in the Institute of Standards and Technology (NIST) such Rivest-Shamir-Adleman (RSA), Digital Standart Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA). DSA has been used for the transmission of electronic funds, interchange of data, distribution of software, storage of data Digital signature's security depends upon the private key of the signer [10]. ECDSA is the elliptic curve algorithm analog of DSA where its security was based on different log losses on a curve point group elliptic over a finite field [11].

The goal of this study is to protect all patient medical record privacy information from loss, theft, or disclosure of medical information that can be misused by Parties not authorized to action fraud. Medical data should be stored on a server that has a good level of security. Protect patient medical information from security threats using cryptographic algorithms. Therefore, before being sent to the data center, medical documents need to go through the encryption process using CP-ABE and add ECDSA signatures to prove the identity of the sender and the authenticity of the message sent without changing the content, and then prevent forgery.

2. RELATED WORKS

Some research has been done to give the patient medical data security as a reference to get the solution in this article. Yinghui Zhang, et al. [3] proposed research using the scheme CP-ABE in ensuring data security s-health records (SHRs), SHR on behalf of patients encrypted to cloud smart health (s-health). Hospital encrypts SHR using CP-ABE access policies under "(SSN: 123-260-6 AND Status: Normal) or (affiliation: City Hospital and Department: Cardiologist)", and then to outsource the ciphertext along with a policy of access to the cloud. These studies analyze the SHR encryption and decryption test time based on the complexity of the access policy and The Number of Attributes in the Universe.

Munsyi et al. [12] proposed the CP-ABE algorithm to build a web-based security system as a medium for retrieving sensor data in data centers for environmental monitoring systems. The researcher analyzes the processing time for the encryption, description and revocation process using different data sensor sizes. The time of the study was carried out differently such as one day, one week and one month. The results of this study indicate that computational time for describing data takes a long time with users who have entered the revocation list.

Ho Hui Chung et al. [6] proposed the method of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) as the authority of the owner of the private key. Then add the key revocation process as a feature on the system model. Dynamic Key Update and Delegation (DKUD) in CP-ABE as an update to the user attribute key of the Key Management Server (KMS). Users with private keys registered in the identity key (IDK) can use IDK identity keys to request the document Key Encryption Key (KEK) to the cloud.

B Eswara Reddy et al. [1] proposed secure storage of Electronic Health Records (EHR's) on the cloud platform that allows the public auditor to verify the patient's identity without revealing EHR. Use the CP-ABE method for Key Generation Authority (KGA) and cloud servers in a role to specify any part of the file to the auditor. The results obtained based on the increase in the number of attributes from 10 to 100, obtained encryption and decryption time which increased significantly.

Jie Zhang et al. [13] proposed a safe system for pervasive social network (PSN) -based healthcare services. Two protocols designed are IEEE 802.15.6

and blockchain techniques for sharing health data between PSN nodes. The protocol package was used HMAC that uses 512 Secure Hash Algorithm (SHA) to realize digital signatures using Elliptic Curve Digital Signature Algorithm (ECDSA). In looking for averages for different protocols or algorithms this study measures elliptic curves approved by Federal Information Processing Standards (FISP) Curves P-192, P-256, P-384, and P-521.

Wei Li et al. [14] proposed a new attribute-based encryption scheme for fine-grained access control and flexible to Personal Health Record (PHR) data in cloud computing. Patient medical data, consisting of some of the data, information, and data information on where these classes have different privilege level. The other attribute, among others, Dermatology, Neurology, Pneumologi, pharmacists, doctors, and nurses. PHR using CP-ABE for the encryption process. The results obtained from the third time decryption scheme all increased with increasing number of the attribute in the tree. Study on improving the efficiency of the process of encryption and decryption. Decryption time faster than any other scheme because the medical staff in different classes have different computational time.

Young Sil Lee et al. [15] proposed the security management scheme and key efficiency based on Elliptic curve cryptography (ECC) algorithms to protect patient medical information in the health care system. this system uses 4 phases such as setting, registration, verification, and key exchange. The identification code used relates to the SIM card number on the patient's smartphone to produce the user's private key. The measurement results obtained by comparing the signature ECDSA which indicates a very low energy consumption compared Rivest-Shamir-Adleman (RSA) signature and verification ECSDA be in a reasonable range of RSA verification. The key generation for ECC only involves random number generation, which was the key to user privacy. Al Imem Ali [16] compare performance evaluations of RSA and ECDSA digital signatures. The results shown for ECDSA key generation time was significantly faster than RSA because of differences in the key length. The execution time between RSA and ECDSA results was significant.

3. ORIGINALITY

In this section, we propose a security mechanism for medical records of patients treated with the concept carried out on previous studies [3][13]. Using the CP-ABE scheme where the attributes of each user are related to patients in the hospital. Users who have access rights can download data stored in the data center. Then, we added the ECDSA digital signature concept to a system that provides data security in authenticating the sender's identity then verifies data integrity by reducing the key size so that the authenticity of the document or message sent as suggested by [14-16]. As explained in the previous study [16] regarding the standard curve, in this study, we followed one of the approved Federal Information Process Standards (FIPS), namely P-384. This authentication scheme can provide trust to users because the authenticity and integrity of data are guaranteed when communication

between the user and the central server. Users must go through a registration process to access data stored on the server. The system we have developed will send a private key in a file to an email and registered active users during registration. Key files sent were CP-ABE private key that can be used for the decryption process and ECDSA public key for verification purposes. While previous research [6] [10], the user must enter the system to get the key attributes of the document to be downloaded. Our system can provide higher security mechanisms to protect the medical records and the ease in obtaining the key for the authentication process.

4. SYSTEM DESIGN

In this section, we described the overall construction of the proposed system to protect medical records using the ciphertext policy attribute-based encryption and elliptic curve digital signature algorithm. The results of computing would be analyzed transmission time during the encryption process, decryption, signing, and verification.

4.1 Ciphertext-Policy Attribute-Based Encryption

In the CP-ABE scheme [17], each user has a different attribute when the secret key is issued as policy determinant that made to describe the message. Messages (M) are encrypted using several public key parameters (PK) and access policies (τ) related to attributes then generate ciphertext (CT). When generating the secret key the algorithm uses the master key (MK) and a set of attributes (S) for each user. Decrypt CT based on matching access policy (τ) and the secret key (SK). Only data that have an attribute that matches the access policy can successfully decrypt and download M. In the CP-ABE scheme, there are four algorithms as follows:

Setup: This algorithm randomly generates the public key (PK) and the master key (MK). The master key (MK) is entered into the key generator stage (Keygen) to generate a secret key (SK). The PK is sent to all users for the encryption and decryption mechanism.

Keygen: This algorithm uses MK, PK, and S to produce SK. The user requests the SK to the trusted party and the key generate server (KGS) executes to produce the user's SK.

Encryption: The process of with a M with the access policy rules (τ) represents the attribute for the process of decryption. The encryption process message M is converted into ciphertext format (CT) that sent to the user. All participating users in the system will act as an encryptor.

Decryption: The process of running the decryption algorithm in CT messages by entering SK that has been tied to τ and S. The M message can only be decrypted while setting the S attribute in SK that fulfills the access policy used to generate CT from M.

4.2 Elliptic Curve Digital Signature Algorithm

Elliptic curve cryptographic (ECC) [18] operations are in general defined over an underlying finite field. ECC is tied to the scalar multiplication in elliptic

curve points. The Weierstrass equation for elliptic curves over prime fields can be represented as:

$$y^2 = x^3 + ax + b \quad (1)$$

Where a, b, x, y $\in$ GF (p), b $\neq$ 0

Variable x and y are the points on the elliptic curve calculated by the signer to make a digital signature and verification performed by the recipient or enemy, a and b are parameters of the elliptic curve where each change in values a and b in equation (1) will produce different elliptic curves. Finite Field (FF) or commonly called Galois Field (GF) is a field that has a finite number element. Finite fields used in cryptography are p = q, where p is an odd prime number that each calculated with modulo and q is the rank of prime then there is only one limited field of degree q which is symbolized by Fq field or GF (q). Characteristics of a finite field Fq that produces point G is q.

Elliptic Curve Digital Signature Algorithm (ECDSA) is elliptic curve DSA. ECDSA first proposed in 1992 by Scott Vanstone in response to a request for NIST's (The National Institute of Standards and Technology) for public comment upon their first proposal to DSS. It was accepted in the year 1998 as ISO (International Standards Organization) standard (ISO 14888-3), received in the year 1999 as the standard ANSI (American National Standards Institute) (ANSI X 9.62), and received in the year 2000 as IEEE (Institute of Electrical and Electronics Engineers) standard (IEEE 1363-2000) and standard FIPS (FIPS 186-3) [19-20]. The ECDSA Protocol in which will perform a digital signature, elliptic curve domain parameters have the form D = {q, FR, a, b, G, n, h}. Couples the secret key and public key dA QA. Thus, the parties will conduct a verification of a digital signature has a copy of the message is authentic and D public key QA. ECDSA has three phases such as Key generation, Signing Generation and signature verification [11][21-22].

1. *Key Generation*
   Parameter domain EC D = (q, FR, a, b, G, n, h). E is the elliptic curve which was defined as Fq, and P is prime point n in E (Fq), q is prime numbers. Each entity keyA do the following:
   a. Select a random integer in the interval [I, n- I].
   b. Calculate QA = dA x G = (x_1, y_1) ,where G is the prime generator op the field. The private key dA is the public key QA
2. *Signing Generation*
   Signatures operate on multiple parameters domains, the private key d, and message m. The result is a signature (r, s), where the signature component of r and s are integers, and the results are as follows.
   a. Select a random integer or pseudorandom k in the interval 0 < k < n -1.
   b. Calculate QA = k x G = (x_1, y_1) and r = X_1 mod n (where X_1 was considered as an integer between 0 and q-l). If r = 0 then return to step I.
   c. Calculate k-l mod n. Calculate e = SHA-1 (m), e = Hash value

d. s = k^{-1} {h (m) + d.r} mod n, k^{-1} is invers from k, h is a hash function. If s = 0, then go back to step l.
e. Signature for message m is S = r, s. Where r is component x and s is signature.

3. *Verification*

To verify that r dan s are integers in the interval1 ≤ r ≤ n-1] then compute hash value e = SHA-1 (m).

a. Calculate w = s-1 mod n, where w is inverse multiplication inverse of s^{-1}.
b. Calculate U_1= ew mod n dan U_2 = rw mod n. Calculate U_1 x G + U_2 x QA = (x_1, y_1) , if x = 0 then reject S , else compute v = x_1 mod n
c. Accept validation if and only if v = r .

Figure 1 below presents the step-by-step operation of the ECDSA cryptosystem in the mode of signing.

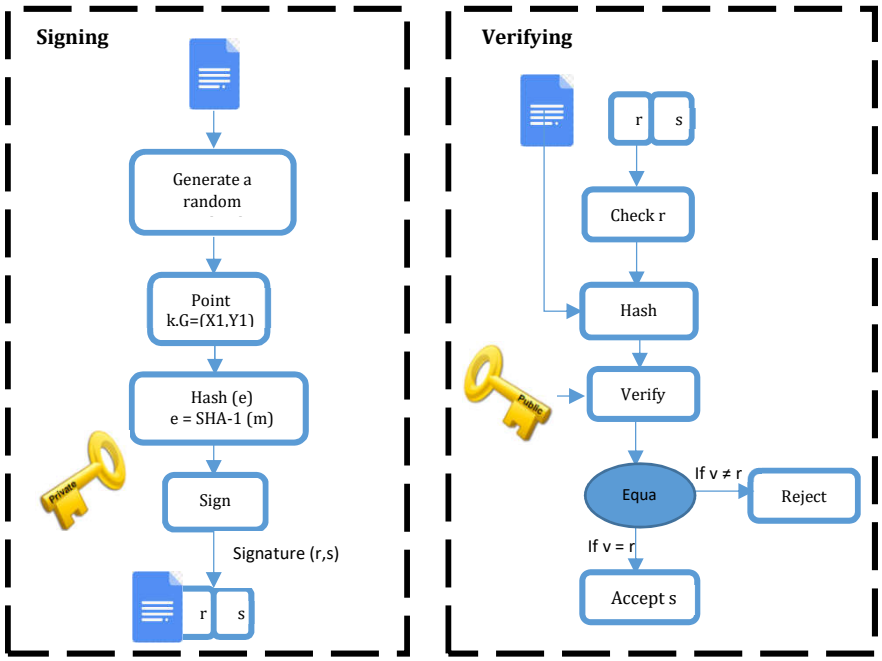


Figure 1. ECDSA cryptosystem in signing mode

4.3 Proposed Method

In this research, we implemented the CP-ABE method to protect and guarantee the rights of access system that is embedded in the data center. We integrate the system created using CP-ABE by protecting all data to be uploaded and must be encrypted and signed using the ECDSA. We've created a system that can secure data and ensure the authenticity and integrity of data in which all data sent through a verification process to validate originality in the data center. So that this mechanism can ensure the data does not change during storage.

Our system involves 5 users such as admin, user consisting of doctors, nurses, patients, and managers. In order to get the key, the user must be

registered first by the admin as a trust third party (TTP). Figure 2 illustrates the mechanism in our system where an admin has the responsibility to send medical record data to the data center so that it can be stored more safely. In our CP-ABE design, after the medical document encryption process is continued by signing using the ECDSA algorithm to prove the authenticity of the sender's identity and the authenticity of the message sent without changes to the contents, then prevent message forgery through sender authentication. Medical record data can be accessed by the treating physician, the nurse on duty and responsibility for his patients and the patients themselves via the wireless network. Patients have the right to see her medical data for its security system ensures that data can only be seen by patients themselves. If anyone wants to see the patient's medical record be it other than the doctor or nurse from the doctor in charge, then need to fill in the guest book in order to make known their necessity for what medical record documents because the very secret should not be accessed by users who are not authorized.

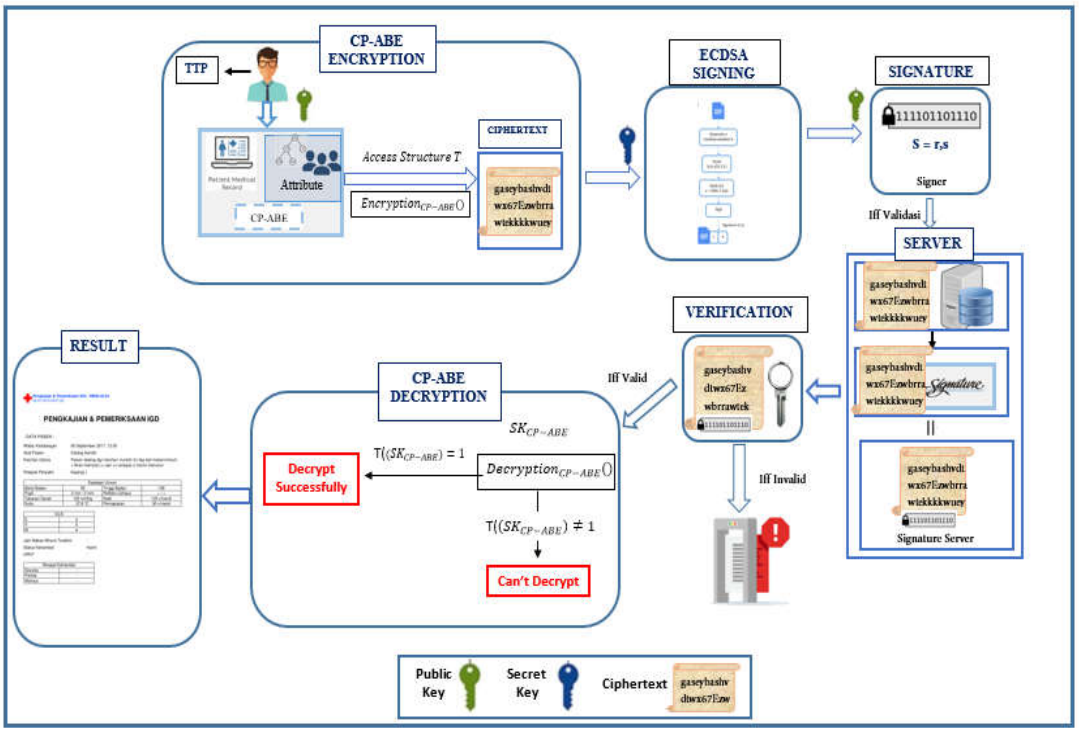


Figure 2. Our system model

The data used in this study is in the form of 9 main disease data in the hospital where the survey consists of Diarrhoea And Gastroenteritis of Presumed Infection Origin as P1, Mild Dehydration as P2, Dehydration as P3, Typhoid Fever as P4, Acute Pharyngitis Unspecified as P5, Leiomyoma of uterus as P6 , Acute Upper Respiratory Infection as P7, Impacted Teeth as P8, and Anemia as P9. Disease data are taken from the disease of patients treated by doctor specialist so that in this study only 10 patients are taken from each grouping based on the department at the hospital. Departments intended are

Gynecology, Internal Diseases, Child Health, and Dental and Oral. Some access permission policies on the system are based on the department in the hospital as shown in figure 3.

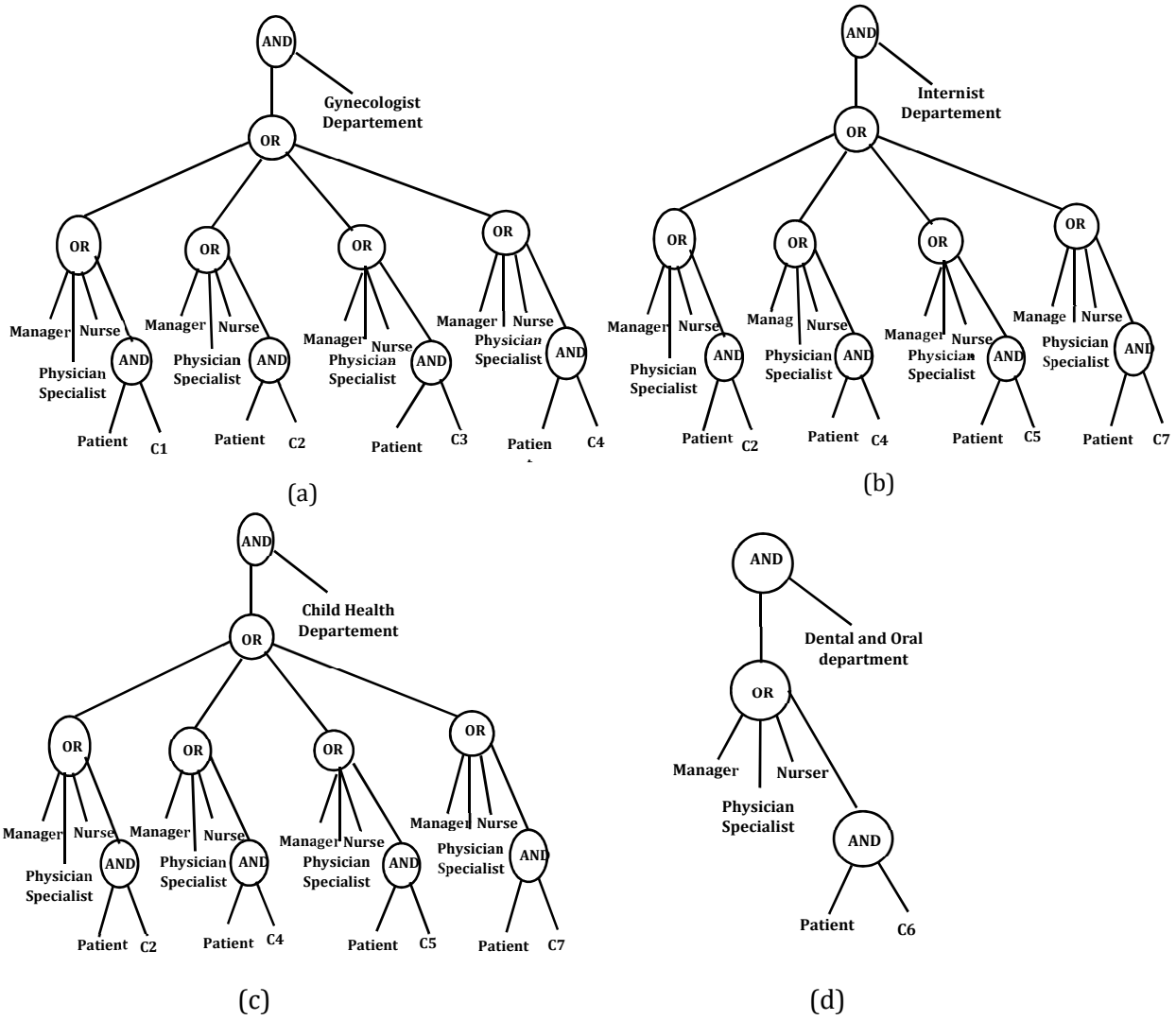


Figure 3. Groups 1 can be accessed by users from the Gynecology Department (a), Groups 2 can be accessed by users from the Internal Diseases Department (b), Groups 3 can be accessed by users from the Child Health Department (c), Groups 4 can be accessed by users from the Dental and Oral Department (d)

Figure 3 above divides the distribution of different access T policies for each group. In figure rule 3 (a) Groups 1 are included in the content department which consists of C1, C2 C3 and C4. Where describes the access attribute policy T_1 that is used to carry out the process of requesting medical record documents obtained from the search results of cluster diseases such as C1, C2, C3 and C4. This policy applies logic gates assuming that only manager OR specialist doctors OR nurses who work in gynecology department OR patients AND the main cluster diagnosis that can get information related to

their medical data. Rule 3(b) Groups 2 enter into the internal disease department which consists of C4, C2, C5, and C7, illustrating the T_2 access attribute policy to respond to requests for medical record documents relating to the condition of the main diagnosis in internal medicine such as C2, C4 , C5, and C7. Only managers OR specialist doctors OR nurses who work in the internal medicine department OR patient AND the main cluster diagnosis who can get information related to their medical data. Rule 3(c) Groups 3 enter into the child health department which such as C4, C2, C5, and C7, the access policy for T_3 has the same access structure as the department of internal medicine by requesting medical record documents obtained from the search for cluster results such as C2, C4, C5, and C7. Rule 3(d) Groups 4 enter into the internal dental and oral department which consists of C7, the T_4 access policy that was used to check the results of disease clusters such as C7.

5. IMPLEMENTATION

To protect confidentiality and data integrity, we proposed a security mechanism using CP-ABE by adding digital signatures ECDSA to provide data integrity checks. The ECDSA algorithm applied to our study is calculated on the P348 curve as standardized by NIST [13][23]. This system is built using specification as seen in the table 1 below.

Tabel 1. Specification of used in experiment

Actor	Data Center	User and Third Trust Party
Hardware	Processor Intel®Core ™ i5-7200U CPU @ 2.50GHz, RAM 12 GB.	Processor Intel®Core ™ i5-7200U CPU @ 2.50GHz, RAM 12 GB.
Software	OS Ubuntu 14.04 LTS 1.4 GiB memory, PHP 5.5.9-1ubuntu4, Server version Apache/2.4.7 (Ubuntu) , Framework CodeIgniter , Apache 2.4.7 (Ubuntu), databases MySQL, CP-ABE-0.11, gmp-6.1.2, pbc-0.5.14, libbswabe-0.9, PHP ECC library simplito/bn-php, Wireless Communication protocol 802.11n WPA2-Personal 2,4 GHz	VMware® Workstation 9.0.2 build-1031769, OS Ubuntu 14.04, Memory 2,6 GB, Processors 2, Hard Disk (SCSI) 40 GB, Mozilla Firefox for Ubuntu canonical-1.0, Wireless Communication protocol 802.11n

During the registration process, the user would be generated by including attributes for each patient. This attribute contains an access policy used during the decryption process. Attributes that are used consist of user name, date of birth, gender, role, and department. Figure 4 shows the implementation of the CP-ABE and ECDSA algorithms to the data center in securing medical data that to use by users.

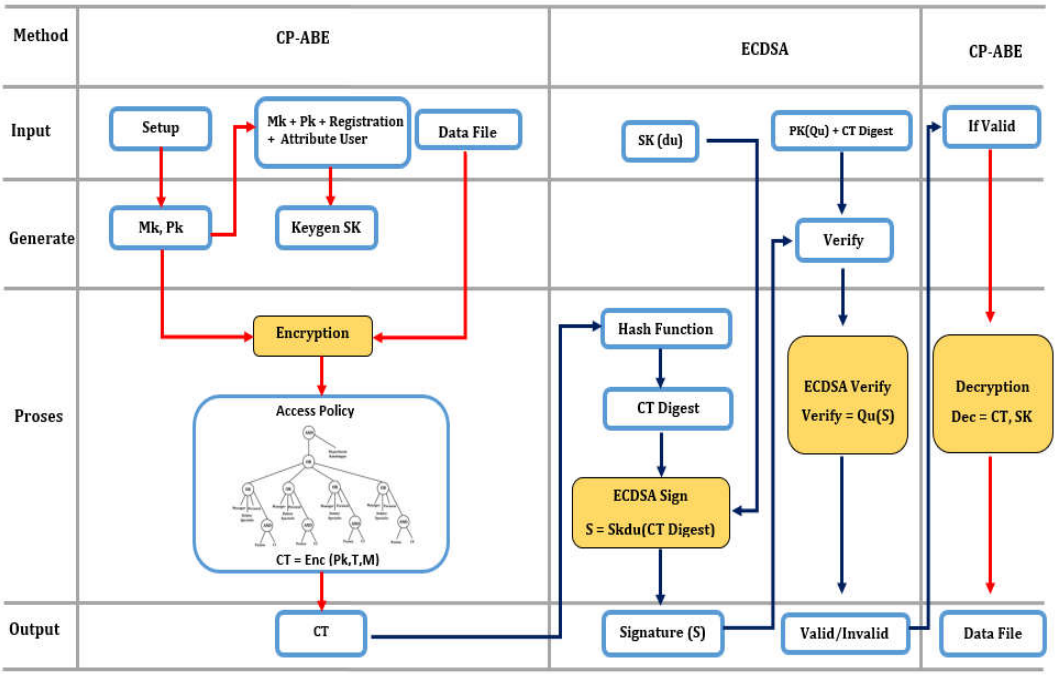


Figure 4. Implementation CP-ABE with ECDSA method of data center

Medical data that have been encrypted will go through the process of signing in using ECDSA 384 before store into the data center, by taking the ciphertext results for is converted into message digest (MD), MD = Hash (CT). The time when the delivery process takes place automatically the system sends the ECDSA public key and private key CP-ABE to email the user who has the correct access rights over the documents that have been sent to do the process of validation and decryption.

This algorithm [17] takes the parameters $\{\mathbb{G},g,\ \}$ to generate a public key (PK) for all users and the master key (MK) entered into the keygen stage. The public key (PK) sent to all users are used for the mechanism of the medical data encryption and decryption stage as shown in equation 2, while MK used to generate the secret key (SK) of each user during the Keygen process, calculate g^{α} and $e(g,g)^{\alpha}$ as a master secret parameter pair, which can be obtained by equation 3. Input parameters, the calculation begins with the stage of selecting bilinear group G0 from Prime order p, generator g so that it produces two random elements $\alpha \in \beta$ and Zp where $e\ (g,\ g)$ are bilinear pairs, e: $\mathbb{G}\ 0 \times \mathbb{G}\ 0 \rightarrow \mathbb{G}\ 1$.

$$PK=\mathbb{G}0,g,\ =g^{\beta},f=g^{1/\beta},e(g,g)^{\alpha} \quad (2)$$

$$MK=(\beta,g^{\alpha}) \quad (3)$$

When the registration process occurs, make the SK key using MK, PK input and a set of user S. The secret key is generated by chooses a random number $r \in Zp$ for each user attribute, then random $r_j \in Z_p$ for each attribute $j \in S$ as shown in equation 4. The user in the registration attribute has S specified according to the proposed.

$$SK=D= g^{(\alpha+r)/\beta},\forall j\in S: Dj= g^{r}.H(j)^{rj},D'j=g^{rj} \quad (4)$$

At this stage, the user registration process that carried out by a trusted admin to give the user access rights. Figure 5 shows the registration scheme, where the user who wants to participate including the manager asks for their secret key with the admin.

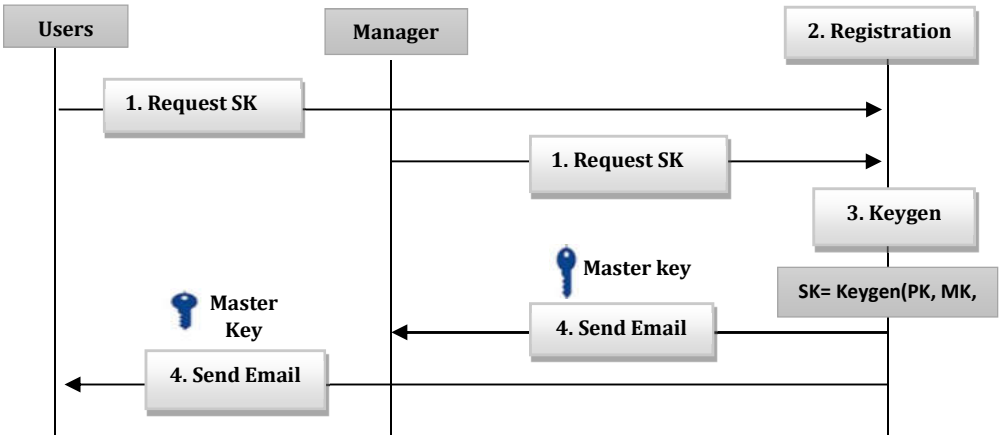
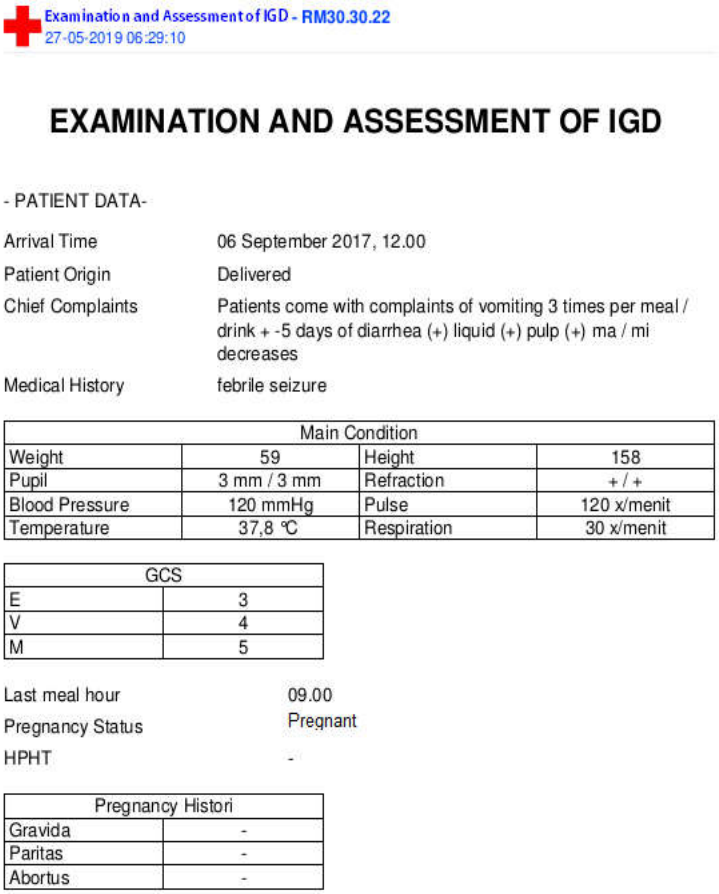


Figure 5. Scheme generated key

The encryption process of M messages that are converted to CT format under the τ tree access structure would the sent to the user. This algorithm selects the polynomial q_x for each node x in tree τ sets the degree of polynomial d_x = k_x -1 where k_x = 1 for OR gate and k_x = num_x for AND gate. choose random $s \in Z_p$ and set q_R (0) = s as in equation 5. We added the feature of a digital signature algorithm ECDSA to provide increased security in the data center storage of medical data. So the data confidentiality, authentication, and integrity of the can be met simultaneously. When the digital signature generation, compute the signature correlated to the message CT using a hash function and a randomly generated master key $x \in Z_p$, CT that generates when the encryption process is taken to change into MD = Hash (CT) used to create the signature. This signing operations also form a key pair (du,Qu). The key pair used together with the signature. The user must get the public signature (Qu) key made by the signer (admin).

Figure 6 shows the M message in the form of a patient assessment file that will be uploaded by the admin to the database. When the admin upload personal files using CP-ABE (encryption) to a database by entering attribute S user goals. The signing operation (signing operation) renders an input string M (CT) in which the message is signed. Medical data into the output of the S = (r, s) on M (CT) that consists of r and s in the form of an integer.

$$CT=(\tau,C=M.e(g,g)^{\alpha s},C= s,$$
$$\forall y\in Y: Cy=g^{qy(0)},C'y=H(attr(y))^{qy(0)}), \quad (5)$$
Sign = H (CT)



Examination and Assessment of IGD - RM30.30.22
27-05-2019 06:29:10

EXAMINATION AND ASSESSMENT OF IGD

- PATIENT DATA-

Arrival Time	06 September 2017, 12.00
Patient Origin	Delivered
Chief Complaints	Patients come with complaints of vomiting 3 times per meal / drink + -5 days of diarrhea (+) liquid (+) pulp (+) ma / mi decreases
Medical History	febrile seizure

Main Condition			
Weight	59	Height	158
Pupil	3 mm / 3 mm	Refraction	+ / +
Blood Pressure	120 mmHg	Pulse	120 x/menit
Temperature	37,8 ℃	Respiration	30 x/menit

GCS	
E	3
V	4
M	5

Last meal hour	09.00
Pregnancy Status	Pregnant
HPHT	-

Pregnancy Histori	
Gravida	-
Paritas	-
Abortus	-

Figure 6 Examination and assesment of IGD file that will be upload to the data center

Figure 7 shows the main process our schema where the documents are encrypted based on user attributes in accordance with the policy rules, further stored in the data center in the form of ciphertext. Medical data stored in the data center consists of a user registration form, examination of the patient's progress while being treated by a doctor and nurse then a patient's medical resume.

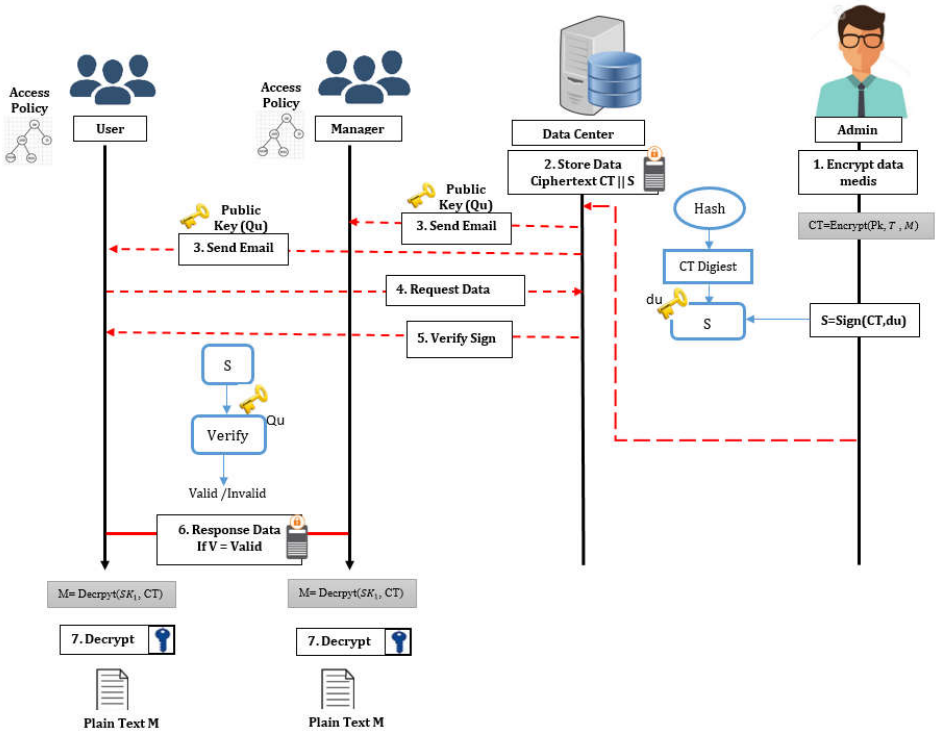


Figure 7. The main process of our scheme

When medical data is uploaded via wireless communication the encryption process occurs, then the ciphertext will form a digital signature which will then be sent to the server. The server center stores patients' medical record information that has been encrypted and has a digital signature CT || S, then when the user downloads the medical data, the user will go through the signature verification stage and ciphertext decryption. In this study there are two steps in the download process such as, the first one verifies the integrity of the digital signature sent valid or invalid and the second decrypts the message to determine whether τ was embedded in the ciphertext according to the user attribute in the SK. The CT message is verified first by entering the Qu, if verification is valid then proceed to the CT decryption stage by entering SK.

The CT decryption process to get M will succeed if S of the user meets the access policy rule of ciphertext then Decrypt (CT, SK) will calculate and return $e(g,g)^{rs}$. If access policy meets then the user will get his medical data (M). Calculation of the process of decryption and verification is shown in equation 6.

$$Decrypt(CT,SK) = \left[\begin{array}{c} Verify\ (CT,S,Qu) = \frac{Valid}{Invalid}, \\ \frac{Cx.A}{e(C2,D)} = \frac{C1.e(g.g)^{rs}}{e(h^{S},g^{\alpha+r/\beta})} = \frac{M.e(g,g)^{\alpha s}}{e(g,g)^{rs}} \end{array} \right] \quad (6)$$

In this scheme there are two stages of validation, the first stage is the process of running the ECDSA algorithm for document verification and the second stage decrypting CT messages using the CP-ABE algorithm. In this

study, we added a digital signature in the ciphertext to provide assurance and authentication of the data sent did not change during the storage process. The user must enter the SK to decrypt the message and Qu for the signature verification process. If the value in the verification algorithm is the same, then the data does not change during the storage and shipping process. Then when the signature is declared valid by the system, proceed with the CT decryption process by entering the SK. Messages can only be decrypted during the S settings in the SK that meets the access policy.

6. EXPERIMENT AND ANALYSIS

The authors have made experiments in the form of testing mechanisms to obtain computation time, key generation, encryption, decryption, transmission time, total time, signing, and verification of digital signatures based on the number of access policy trees. We compare the encryption-decryption processing time and sign and verify digital signatures with users in one department who have access rights to the policy rules in the ciphertext. The uploaded file contains a set of rules for access control in determining the authority of each user. Even though it is in one department, files on different clusters cannot be decrypted by doctors, patients, and nurses, but the user manager in one department can decrypt all cluster files that are in the rule data medical access policy

Figure 8 shows the results of increasing time in stages when the process generates the master key with an increasing number of users. The number of users consists of 25 people for each user consisting of managers, doctors, nurses, and patients. The increasing number of users will affect the length of time the key generation but the increase was not significant. When the process of generating a key, the role of patients require a longer time than other roles. This is because patients have attribute characteristics that are more compared to other users such as managers, doctors, and nurses during the registration form registration process.

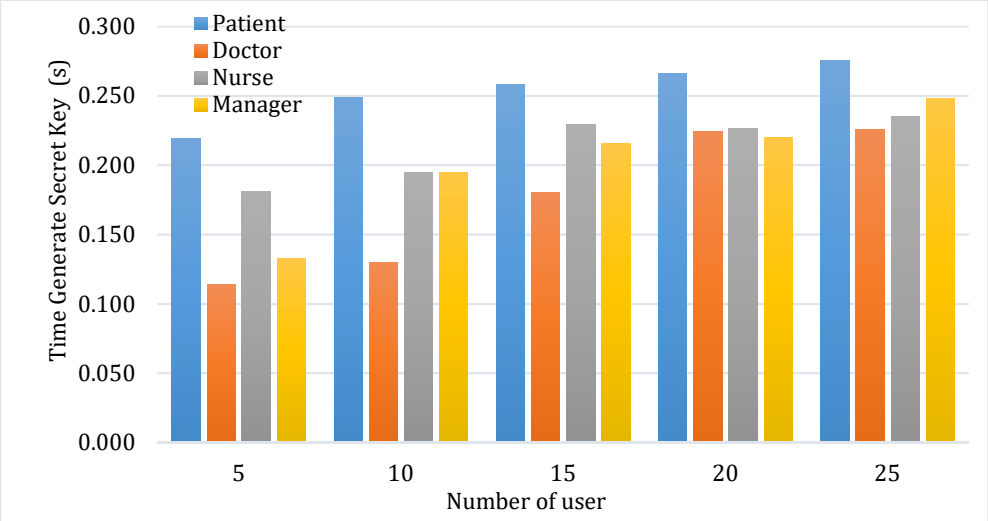


Figure 8. Key generation time

We measure the consumption of time during the encryption and decryption process without and with the signature. The size of the uploaded file the same for each user, document medical examination and assessment of IGD with the original file size 22.2 kB. The uploaded file is shown in Figure 6. Table 2 shows the results of the comparison execution encryption and decryption process when the system was only using CP-ABE algorithm without adding a signature ECDSA with added system ECDSA algorithm. From this result, we will get a comparison during the execution process.

Table 2. Comparison of processing time with and without the use of a digital signature algorithm ECDSA

Number of access policy	Processing time CPABE without ECDSA (s)		Total Time (s)	Processing Time CP-ABE with ECDSA (s)		Total Time (s)
	Encryption	Decryption		Encryption	Decryption	
1	0,045	0,036	0,081	0,376	0,0620	0,438
2	0,052	0,041	0,093	0,444	0,0654	0,509
3	0,066	0,045	0,111	0,470	0,0679	0,538
4	0,067	0,046	0,113	0,512	0,0694	0,581
5	0,071	0,05	0,121	0,524	0,0700	0,594
6	0,085	0,061	0,146	0,588	0,0787	0,667
7	0,086	0,082	0,168	0,650	0,0905	0,741
8	0,090	0,099	0,189	0,697	0,1012	0,798

Figure 9 shows a comparison of the evaluation of execution time performance with and without using the ECDSA digital signature algorithm. It can be shown when our system adds the ECDSA algorithm, in the ECDSA encryption process it takes more than 0.3 to 0.6 seconds longer than without ECDSA which only requires around 0.06 to 0.08 seconds. Then, when the decryption process with ECDSA around 0.06 to 0.1 seconds while decryption without ECDSA was only 0.04 to 0.09 seconds. From the results of this measurement, the calculation of encryption time and the decryption algorithm increases when a digital signature was added, this processing increases linearly when the number of access policies were added.

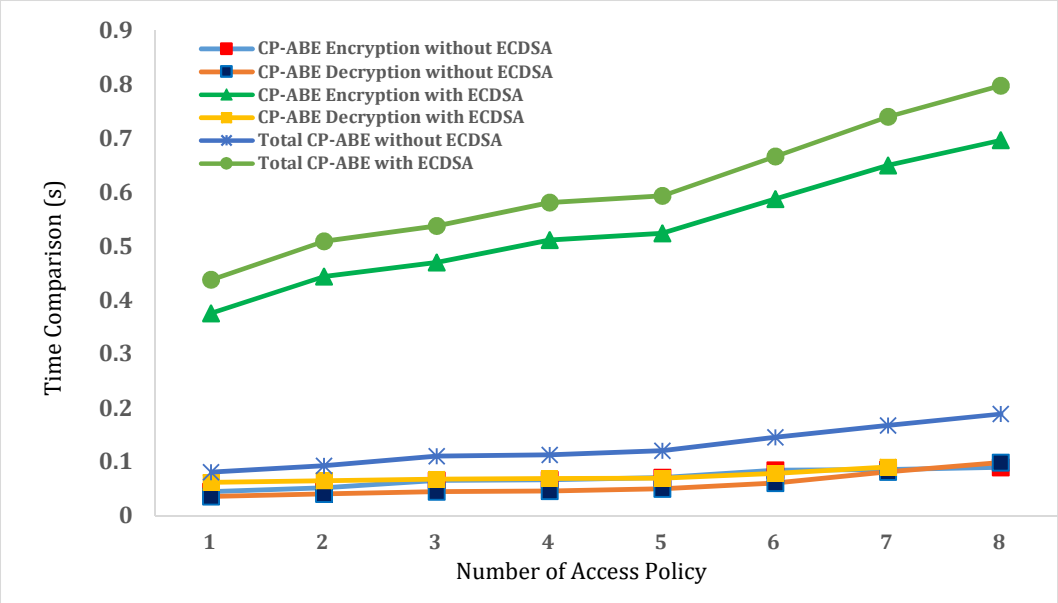


Figure 9. Comparison of performance evaluation of execution time with and without the use of a digital signature algorithm ECDSA

The results of the total processing time when the system uses the CP-ABE algorithm without ECDSA 0.1 seconds and with ECDSA 0.6 seconds. The system we propose provides a longer computation time than without the signing process. From the results of security testing using the CP-ABE method, it was found that when the system was added to the ECDSA method, the time needed to encrypt messages had a performance increase of up to 84%. And when the process of decrypting ciphertext has a performance increase of 2%. The presentation of this increase is obtained at the final value when the CP-ABE algorithm is added by the ECDSA method (with ECDSA) minus the initial time before the addition of a signature (without ECDSA). The results obtained will be divided by the final value so that there will be a presentation of the increase in system performance. Although the increase in encryption time on our proposal is greater, this does not reduce performance because the advantages of this addition provide a higher level of security than without

using signatures. Then the other benefits obtained are that the decryption process experiences a slight increase in time when the signing method is added so that the system security we propose will be more efficient.

Table 3. Increased processing time with CP-ABE access policy and ECDSA digital Signature

Number of access policy	Sign Time (s)	Verify Time (s)	Transmission Time to data center (s)	Transmission Time to user (s)	Processing Time (s)		Total Time (s)
					Encrypt	Decrypt	
1	0,046	0,114	0,0010	0,0014	0,376	0,0620	0,600
2	0,053	0,132	0,0009	0,0250	0,444	0,0654	0,701
3	0,065	0,135	0,0013	0,0029	0,470	0,0679	0,746
4	0,071	0,163	0,0013	0,0030	0,512	0,0694	0,820
5	0,074	0,169	0,0013	0,0042	0,524	0,0700	0,869
6	0,084	0,222	0,0014	0,0057	0,588	0,0787	0,980
7	0,097	0,252	0,0014	0,0065	0,650	0,0905	1,097
8	0,115	0,282	0,0015	0,0082	0,697	0,1012	1,205

Table 3 shows the results of the processing time to sign and verify files using ECDSA algorithm based on the amount of access policy. We measure time transmission when data are sent to the data center and data sent to the user. Figure 9, computing time increases due to the addition of a number of access policies, for signing the ciphertext takes 0.04-0.1 s and verify digital signatures 0.1 to 0.3 s shown in figure 10 (a). Transmission time is relatively stable when the data sent to the data center 0.001 s and when sent to the users from the results of 0,005 s shown in figure 10 (b). Transmission time is taken by calculating the time when the file was created when the output file is read, so the process of sending CT time with S.

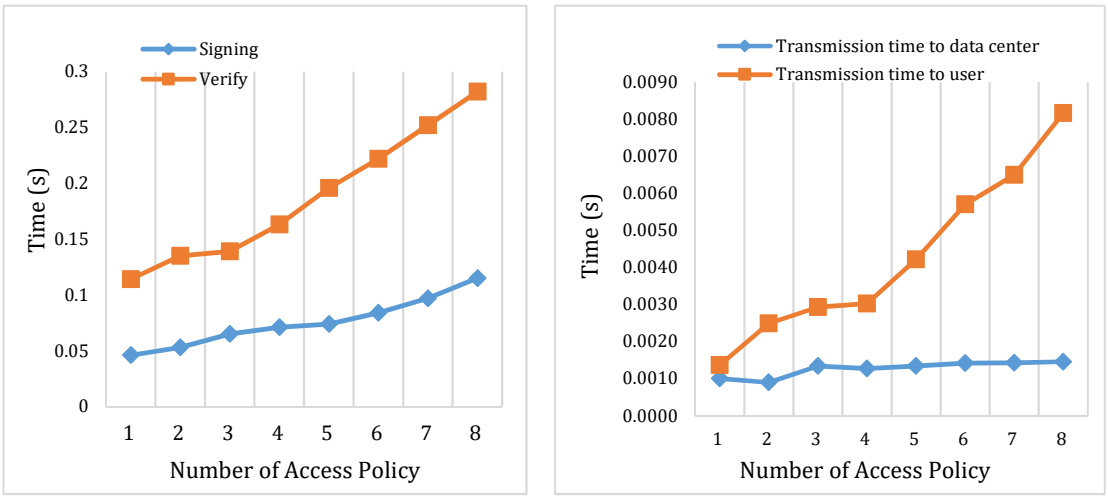


Figure 10. Performance evaluation of execution time for signing and verify the signature (a), transmission time to the center and user (b) using ECDSA

Next experiment in this study compared the results of measurements by including all access policy rules, such as gynecology department, internist department, child health department, and dental and mouth department for the process of encryption, decryption, signing and verification of customers. In this section, we have made a comparison of the proposed scheme with another schema approach [12] in evaluating computational performance and time. In the scheme, the revocation and digital signatures are added. The measurement results are averaged to get the end result of computing time which is 0.4 seconds in the encryption process can be seen in Figure 11. However, our scheme has decryption 0.07 seconds time faster than the previous scheme of around 0.08 seconds. Schema [12] is efficient for adding user revocation but failed to give a short execution time when the decryption process. We calculate the decryption time after the digital signature verification process.

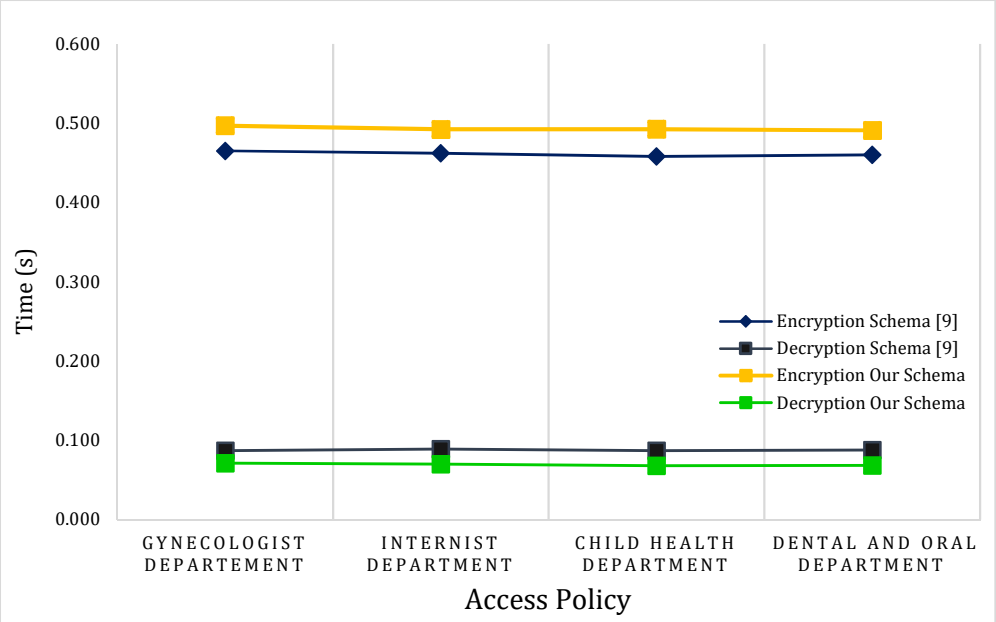


Figure 11. Computational costs of our scheme under different comparison access policy

7. SECURITY TEST

In this section, we discuss the security assessment on systems based on three main features of the system such as confidentiality, integrity and availability. The web application server is vulnerable to attacks such as session exploitation, cross-site scripting, SQL injection etc [24]. Testing of the system as a step to identifying security flaws given CPABE and ECDSA algorithms in the process of sending medical records to a data center and then when envy data to the destination user. This process will use Kali Linux because this operating system offers advantages with a variety of tools for vulnerability and penetration assessment that are best identified in this study.

In general, there are 4 main categories of security assessments used, namely penetration test, footprinting, modeling treatments, and vulnerability analysis. In the study using the penetration test [25] by attempting to attack a computer system, network or web server application so that vulnerabilities can be found so that attackers can exploit security weaknesses to gain access to the database. Penetration test scenario in which an attacker exploit to attack targets data centers with IP address 192.168.10.2 port 22 to find a weakness web browser. Attacking vulnerability security using metasploit framework, vega, and using SQLmap to detect and exploit SQL injection bugs so that attackers can find out weaknesses and take over the database server. Illustration of this scenario shown in Figure 12.

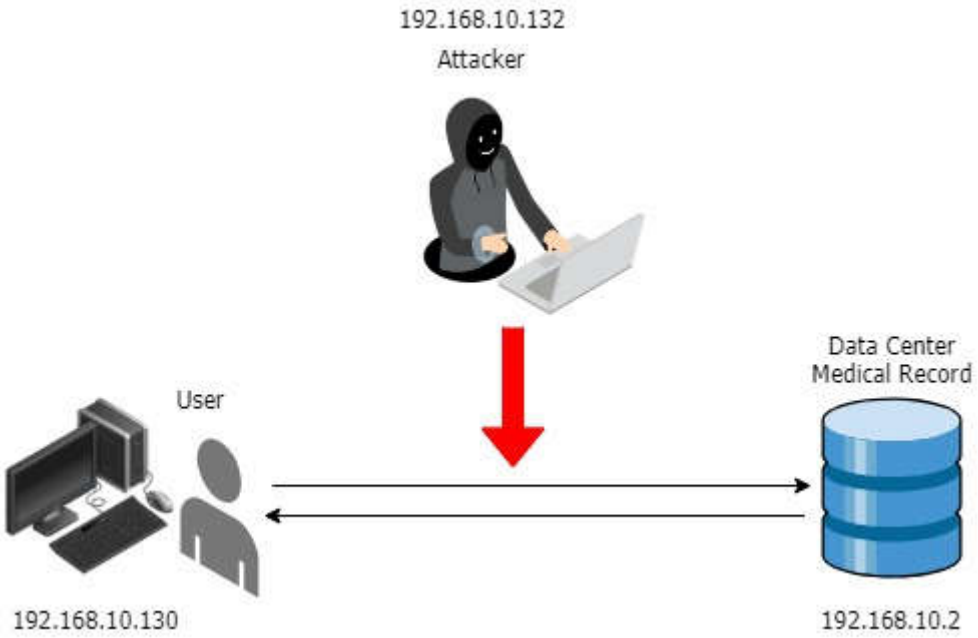


Figure 12. Illustration of penetration test scenario

SQL attacks can occur if the web server was not given security before data is sent to the database. In this case, this type of testing was where the tester will play the attacker's role and try to enter the system to find related security bugs. SQL injection will authenticate before forwarding to the SQL query. It can deliver malicious attacks by removing and modify the data on the server, transmit the virus and take your email and password information user.

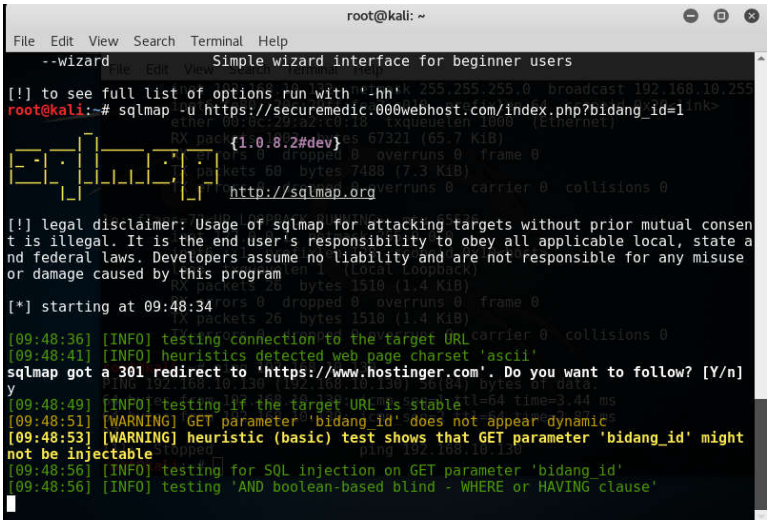


Figure 13. SQLMap for SQL injection to hack website and database

Figure 13 display results from SQLMap for SQL injection to websites and databases. When running a Mapper using a web server URL, the attacker only knows the target database was MySQL but cannot exploit the 'field_id'

parameter. So that the attacker was not given the opportunity to view and retrieve tables available in the database. SQLMap will easily find the hash password from the SQL Database table for illegal actions. Penetration testing is very important for web applications to check if confidential data is stored safely without modification.

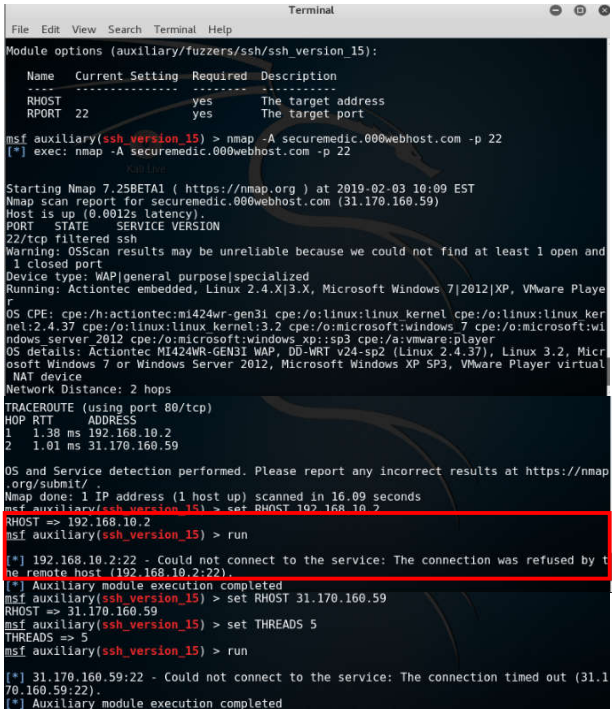


Figure 14. Exploit the weaknesses of a system using the metasploit framework

Figure 14 shows the exploitation of system weaknesses using the Metasploit Framework. Each exploit has a series of options that configured for remote hosts. If metasploit successfully exploits a vulnerability, it will provide an opportunity for attackers to find important data stored. Our test was successful because the attacker could not connect to the service when trying to enter through the target IP address.

6. CONCLUSION

In this study, it has been proven that our scheme is safe against possible attackers because we have tested the system security using Kali Linux. The results obtained also indicate that the database cannot be connected and injected. We also ensure that the proposed access policy is more complex to avoid illegal access such as the encryption process and then add the process of signing the ciphertext before the file download process must pass the verification process first if it is valid then the file can be decrypted. The implementation of the CP-ABE method and the addition of the ECDSA method result in greater computation time because there are an additional signing and

verify process so that execution time also has an effect, but this will provide a higher level of security than before the addition. Even though there was an increase in time to encrypt the system we found a lower decryption time of 0.1 seconds no more than 1 second. The process of signing and verification also does not significantly affect system performance when ECDSA is added. The study also carried out a comparison of the systems proposed in previous studies. The proposed results show that computational time provides an efficient solution when decryption is around 0.06 seconds. The total time in the system that we propose requires around 0.6 seconds. In the future, this research method will continue to use cloud servers to create safer medical data storage systems and facilitate synchronization between hospitals during patient referrals.

Acknowledgment
This research was supported in part by Ministry of Research, Technology and Higher Education of Indonesia, under scheme 'Penelitian Terapan Unggulan Perguruan Tinggi (PTUPT)', Grant No. T/140/E3/RA.00/2019.

REFERENCES

[1] B Eswara Reddy, Gandikota Ramu, **A Secure Framework for Ensuring EHR's Integrity Using Fine-Grained Auditing and CP-ABE**, In *Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), IEEE 2nd International Conference on* (pp. 85-89). IEEE. 2016

[2] Nihayatus Saádah, I Gede Puja Astawa, and Amang Sudarsono, **Trusted Data Transmission Using Data Scrambling Security Method with Asymmetric Key Algorithm for Sychronization**, *EMITTER International Journal of Engineering Technology*, Vol. 6, No. 2, 217-235 , 2018

[3] Yinghui Zhang, Dong Zheng, and Robert H. Deng, **Security and Privacy in Smart Health : Efficient Policy-Hiding Attribute-Based Access Control**, *IEEE Internet of Things Journal.* vol. 3, no. 1, pp. 1–15, 2018.

[4] Entao Luo, Md Zakirul Alam Bhuiyan, Guojun Wang, Md Arafatur Rahman, Jie Wu, and Mohammed Atiquzzaman, **PrivacyProtector : Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems**, *IEEE Communications Magazine*, *56*(2), February, pp. 163–168, 2018.

[5] Kwangsoo Seol, Young-Gab Kim, Euijong Lee, Young-Duk Seo, and Doo-Kwon Baik, **Privacy-Preserving Attribute-Based Access Control Model for XML-Based Electronic Health Record System**, *IEEE Access vol. 6*, pp. 9114-9128. 2018.

[6] Ho Hui Chung, Peter Shaojui Wang, Te-Wei Ho, Hsu-Chun Hsiao, and

Feipei Lai, **A Secure Authorization System in PHR based on CP-ABE**, *E-Health and Bioengineering Conference (EHB),* pp. 1-4. IEEE. 2015.

[7] Ahmed Lounis, Abdelkrim. Hadjidj el al. "**Secure and Scalable Cloud-based Architecture for e-Health Wireless Sensor Networks.** *International Conference on Computer Communications and Networks (ICCCN),* pp. 1-7,IEEE, 2012 21st.

[8] Samsul Huda, Amang Sudarsono, and Tri Harsono, **Secure Communication and Information Exchange using Authenticated Ciphertext Policy Attribute-Based Encyrption in Mobile Ad-hoc Network**, *EMITTER International Journal of Engineering Technology*, Vol.4, No.1, 115-140, 2016.

[9] Novi Aryani Fitri, Udin Harun Al Rasyi, and Amang Sudarsono, **Secure Attribute-Based Encryption With Access Control to Data Medical Records**. *2018 International Electronics Symposium on Knowledge Creation and Intelligent Computing (IES-KCIC),* pp. 105-111. 2018.

[10] Muhammad Arif Mughal, Xiong Luo, Ata Ullah Subhan Ullah, and Zahid Mahmood, **A Lightweight Digital Signature Based Security Scheme for Human-Centered Internet of Things**, *IEEE Access*, pp. 31630 - 31643. 2018.

[11] B. Sindhu and Dr. R. M. Noorullah, **Secure Elliptic Curve Digital Signature Algorithm for Internet of Things**, *Global Journal of Computer Science and Technology*, vol. 1, no. 3, 2016.

[12] Munsyi, Amang Sudarsono, and Udin Harun Al Rasyi. **Secure Data Sensor In Environmental Monitoring Sistem Using Attribute-Based Encryption With Revocation**. *International Journal on Advanced Science, Engineering and Information Technology*, vol. *7*(2), pp. 609-624. 2017

[13] Jie Zhang, Nian Xue , and Xin Huang. **A Secure System For Pervasive Social Network-based Healthcare.** *IEEE Access*, *4*,pp. 9239-9250. 2016.

[14] Wei Li, Bonnie M. Liu, Dongxi Liu, Ren Ping Liu, Peishun Wang, Shoushan Luo, and Wei Ni, **Unified Fine-grained Access Control for Personal Health Records in Cloud Computing**. *IEEE journal of biomedical and health informatics*, pp. 1 - 1 2018

[15] Young Sil Lee, Esko Alasaarela, and HoonJae Lee, "**Secure key management scheme based on ECC algorithm for patient's medical information in healthcare sistem**, *The International Conference on Information Networking 2014 (ICOIN2014),* February, pp. 453-457. 2014.

[16] Al Imem Ali, "**Comparison and Evaluation of Digital Signature Schemes Employes in NDN Network**, *Internattional Journal of Embedded systems and Application (IJESA),* Vol.5, No.2_ 2015

[17] J. Bethencourt, A. Sahai, and B. Waters, **Ciphertext-Policy AttributeBased Encryption**, IEEE Symposium on Security and Privacy, pp. 321-334, 2007.

[18] Bhanu Panjwani**, Scalable and parameterized hardware implementation of Elliptic Curve Digital Signature Algorithm over**

Prime Fields, *Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference,* pp. 211-218. IEEE, 2017.

[19] Don Johnson, Alfred Menezes, and Scott Vanstone, **The Elliptic Curve Digital Signature Algorithm (ECDSA)**, *International journal of information security*, *1*(1), pp. 36-63. 2001.

[20] Muhammad Haikal Azaim, Dodi Wisaksono Sudiharto, and Erwid Musthofa Jadied, **Design and Implementation of Encrypted SMS on Android Smartphone Combining ECDSA - ECDH and AES**, *Multimedia and Broadcasting (APMediaCast), 2016 Asia Pacific Conference,* pp. 18-23. IEEE, 2016.

[21] Ravi Kishore Kodali, **Implementation of ECDSA in WSN**, *International Conference on Control Communication and Computing (ICCC).* pp. 310-314. IEEE. 2013

[22] Abdessalem Abidi, Belgacem Bouallegue, and Fatma Kahri, **Implementation of elliptic curve digital signature algorithm (ECDSA)**, *Global Summit Computer & Information Technology (GSCIT),* pp. 1-6. IEEE , 2014.

[23] Cameron F. Kerry, **Digital Signature Standard (DSS),** *Federal Information Processing Standards Publication (FIPSP)*, Ed. 3, 2013.

[24] Prof. Sangeeta Nagpure, and Sonal Kurkure. **Vulnerability Assessment and Penetration Testing of Web Application.** *International Conference on Computing, Communication, Control and Automation (ICCUBEA)*. Pp.1-6. IEEE. 2017

[25] Petar Cisar, Sanja Maravic Cisar, and Igor Furstner, **Security Assessment with Kali Linux***, Bánki Közlemények*, 1(1), pp. 49-52, 2018