International Journal of Engineering and Technology Innovation, vol. 9, no. 1, 2019, pp. 49 - 60

Enhancing Security Levels at ISP Server Using Multiple Security Techniques with Proposed Crypo Application

Suraj U. Rasal[1,*], Varsha S. Rasal[2], Shraddha T. Shelar[3]

[1] Department of Computer Engineering, Bharati Vidyapeeth Deemed to be University College of Engineering, Pune, India

[2] Department of Computer Engineering, Sinhgad Academy of Engineering, Pune, India

[3]Department of Information technology, D Y Patil College of Engineering Akurdi, Pune, India

Received 18 April 2017; received in revised form 27 July 2017; accepted 08 January 2018

Abstract

The internet is widely used in computing. Security is an important aspect when the quality of service is evaluated and current security possesses high level encryption techniques. However, due to high data saturation and complexity, it is not enough for, only to rely on the common security techniques. In this paper, proposed application named Crypo is installed at both ends, including user and Internet Service Provider (ISP). User can connect to the public internet through providing credentials. Both ends work with same cryptographic techniques and logics. Crypo includes the existing security techniques with proposed logics. Attribute Based Encryption (ABE) is applied to user credentials. Cipher policy applies to data exchange between user and Internet Service Provider (ISP) to form a combined cipher data. Proposed logic is further applied to the binary formatted cipher data. According to proposed logic, the final encrypted binary formatted data are further applied with Advanced Encryption Standard (AES) to deliver it to the ISP. Decryption is done by the same logic applied to the sender side or vice versa. When data is retrieved by ISP from its end user, it is decrypted by the ISP after which is delivered to the public network in normal format. Four level security keeps the data and user credentials confidential. Intruders or hackers can't reach to the end user without decrypting the secured data at ISP. While delivering encrypted data, applied logic name is also delivered so that end users can decrypt data using the same logic. By using proposed application Crypo, a secure connection is established between the end user and the ISP. An outsider cannot cause threat to the ISP's users. Proposed multilevel cryptographic approach enhances the security.

Keywords: attribute based encryption (ABE), advanced encryption standard (AES), american standard code for information interchange (ASCII), cipher policy, crypo - proposed application name, internet service provider (ISP).

1. Introduction

The existing security techniques are applied to proposed 'Crypo' system and it also played a vital role in internet security. Security techniques are used and implemented in different aspects and approaches. Logical part varies from the usage of security. Security techniques are upgraded according to its importance in recent cryptographic trends.

The existing security techniques are developed by using multiple cryptographic techniques and trends. These cryptographic techniques are applied directly or with different cryptographic techniques, for example, a Cipher policy with Attribute Based Encryption, and a cipher policy with multiple authorities or decentralized approach. Multiple combinations of

* Corresponding author. E-mail address surasal@bvucoep.edu.in
Tel.: +918793000079

cryptographic techniques enhance the level of security. The quality of security can be maintained by reducing the efficiency and performance of multiple processes. The proposed approach is applied to some cryptographic techniques like cipher policy, Attribute Based Encryption (ABE) and Advanced Encryption Standard (AES) with proposed cryptographic logic. Security of internet service provider is an important factor that the customers rely on. Proposed logic is applied between end user and ISP network to enhance the security level.

2. Existing Security Techniques in Computing

The existing security techniques are invented to overcome the sensitive data loss problems. Traditional and current cryptographic trends rely on the update of cryptographic techniques and innovations in existing security techniques. Computing is upgraded in every domain like Internet of Things, cloud computing, and so on. These trends need high level security because computing is widely used by the society in daily life. Proposed paper shows how security level can be enhanced by applying own logic with existing cryptographic techniques.

2.1. Ciphertext policy

Ciphertext policy is the traditional approach to encrypt the secret data by applying secrete logic. On recent cryptographic trends, cipher text policy is updated and high leveled logics are applied [1]. Cipher policy is one of the best cryptographic policies; the data can't be decrypted without understanding the cipher logic applied behind the encryption process. Cipher policy is not limited to the type of Unicode values like characters, symbols and others.

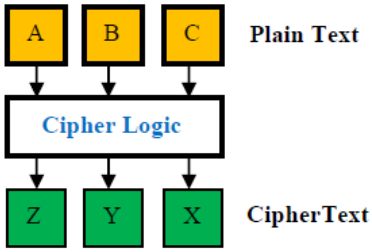

Fig. 1 Ciphertext generation

It can be applied to anything based on logic. For instance, if 'A' character is allocated with cipher value as 'z' or if set 'A7B' allocated to cipher value '$' and so on [2]. As shown in Fig.1, the cipher logic block includes the logical part where logic is set as, replace all alphabets with the reverse order of alphabets from A to Z. For A= Z, B=Y, C=X and so on. Cipher policy plays a vital role in the encryption of secrete or personal information exchange. Further cipher policy is combined with other cryptographic techniques like Attribute Based Encryption (ABE) and others.

2.2. Attribute based encryption

When compared with the indirect structure, the direct data access in not secure enough. Indirect access structure methods are applied to a database where security techniques are applied like Attribute Based Encryption. Actual data is referenced by attributes allocated or through keys allocated. Key policy based on ABE is developed further. Actual character data are allocated with some cipher value. This cipher value is allocated with attributes which are used to refer the required cipher value. In the database management, different data access structures are used for which keys are allocated. These keys define the required data based on access structure [3]. In the proposed approach, Attribute Based Encryption is mainly focused to enhance the encryption level. Furthermore, it is improved by allocating attributes to the user credentials. The attributes are stored in other parties rather than storing them to the connected systems. Due to this policy, important data can be decrypted, even when the database or parties are not been secured [4]. Decentralized Cipher Text Policy Attribute Based Encryption (DCP-ABE) is developed to overcome the database access structure problems related to security. If understand the logical approach applied, the intruder can track or reach to the central database. DCP-ABE with Monotone Access Structure (MAS) defines the multi

locality storage approach which doesn't require or use central authority. The database access structure is distributed among registered authorities with MAS. Therefore, even when any authority is damaged or attacked by an intruder, the database access structure won't be affected, and the important data is preserved. Important data is preserved. In the same approach, ABE is also applied to where the attributes are referred to access the data or values [5-6]. In current computing, efficiency is important to maintain the quality of service in information technology. Levels of encryption, decrease the efficiency problem due to high levels and complexity in algorithm solving. To overcome with the problem, Minimal Authorization Sets are used to decrease the cipher text which becomes linear with bilinear pairings in the decryption process [7]. All these ABE based on techniques are applied to the proposed approach with the additional logical approach.

2.3. Advanced encryption standard

Specific encryption is defined based on the cipher policy and a set of rules is applied to form Advanced Encryption Based standard (AES) data. A byte is the basic unit in AES, and each byte value represents a binary value. All American Standard Code for Information Interchange (ASCII) character set is defined by some binary values. Element in ASCII set is considered as a character or a set of characteristics. For example, if 79 is the element, then the byte value is separate to '7' and '9' and its binary value is {00110111 00111001}. Bit pattern is defined by the type of applied level of the bits like 4bit, 8bit, 128bits,256bits and so on [8-9].

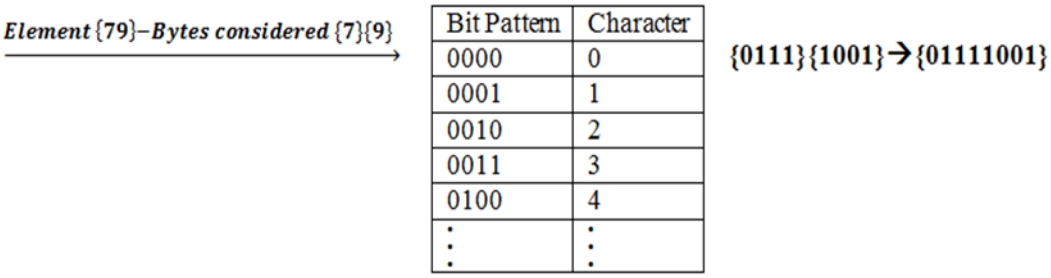

Fig. 2 Element to byte conversion and combination [10]

Single value is referred with byte. Arrays of bytes are created to store the element values. Sub bytes are considered and allocated according to defined logic. New formed sub bytes array set is further applied to shifting rows and to generate the new array set table. While performing an action, elements of sub byte table are used. As shown in Fig. 2, bit values are selected according to the combined character value. While accessing bytes, decryption needs to be applied to get the required data [10].

2.4. Multiple authorities cipher policy ABE

In Cipher policy attribute based encryption, cipher policy with multi key sharing approach is applied to enhance the encryption level [11]. Cipher policy is applied to generate the encrypted data using security logic. Encrypted data are divided into multiple segments, and these segments are delivered to the multiple authorities. These authorities are unknown to other contributor authorities. Multiple authorities are registered in the security system. Without all participated authority's key, encrypted data cannot be decrypted. During the central authority, encryption process, trustworthy authorities are being selected randomly. In the Decentralized ABE scheme, attributes are randomly allocated to generate trusted authority keys. The main secret key is formed by using Trusted Authority keys. Central authority manages all cryptographic processes related to multiple authorities CP-ABE [12]. This system has a drawback as, failure to the central authority can down all systems. However, there's a drawback of the system, all systems may collapse due to the failure of the central authority.

2.5. Decentralized cipher policy ABE

In decentralized cipher policy Attribute Based Encryption, multiple authorities become a member of the security system. In this approach, there is no any available central authority. All authorities work independently. Decentralized environment is established where all authorities participate in the security access. Due to it, the security level has enhanced and the central authority failure problem is overcome. Attribute based encryption is applied to multiple authorities approach. This system is

invented to overcome the central authority failure. In this approach, if any, authority collapses, then randomly select another authority to do the job. Decryption is done with the help of all participated trusted authority keys [13]. As shown in Fig.3, A_1,A_2,A_3,A_4,…..,A_n are multiple authorities participated in decentralized environment and U_1,U_2,…,U_n are respective users.

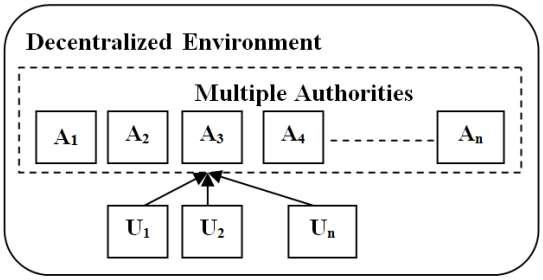

Fig. 3 Decentralized cipher policy attribute based encryption [14]

2.6. Decentralized cipher policy- attribute based encryption with a mediator

In DCP-ABE-M approach, the mediator is considering to participate in the encryption process. The Mediator is allocated to the normal logic process, so as to manage the credential security and system access. After entering into DCP-ABE-M system, the mediator is randomly assigned to allocate authorities to complete the task. The assigned mediator in charge for the referee in the DCP-ABE-M system. System identified and understands to Mediator, rather than the actual user [14].

3. Proposed System

Internet works with protocols, standards and technologies. The user directly or indirectly interacts with each other through the internet. Users depend on the service and product which were provided by the companies or organizations. All service providers and organizations try to maintain security. Quality of service depends on security, and the security depends on the levels and complexity of cryptographic algorithms. In previous proposed approaches, database access structure methods are applied with security techniques, including ABE with One Time Password (OTP) in various appliances, like internet banking [15]. In the proposed approach, new concept with existing cryptographic techniques is considered. Internet Service Provider (ISP) is the most important component in the internet access and usage. Algorithmic approaches and cryptographic techniques must be updated and be fine tuned to maintain the security. Further web browser and firewall of the user's system plays vital role in the security aspects. Internet of Things (IoT) segregates almost all computing and multidisciplinary domains. Security approaches and are applied to IoT access structure [16]. In the proposed approach, four level encryption is being applied to the web browser based application.

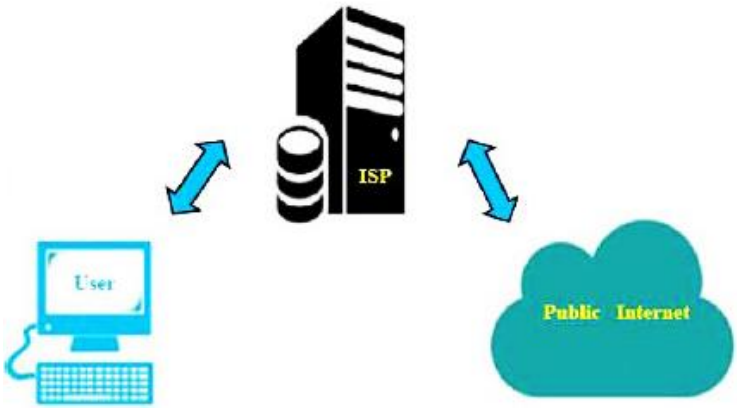

Fig. 4 Proposed 'Crypo' application

What's more, web browser and firewall of the user's system plays vital role in the security aspects. Proposed logic is based on existing security techniques including Attribute Based Encryption (ABE) and Cipher policy. Also Advanced Encryption

Standard (AES) is considered in encryption and decryption process. Source code is loaded into a web browser, after the output is displayed and the required operations and actions are performed. Source code is considered as sensitive data to deliver. Proposed application named 'Crypo' whose logic based on ABE, Cipher policy and AES cryptographic techniques is been considered. 'Crypo' is installed at the two ends of the system. End users and ISP are the systems where 'Crypo' is installed , only by the system can the users access the public internet. As shown in Fig. 4, information is transferred through the ISP. Protocol conversion suite manages the internet standards of 'Crypo' between the users and the server.

For example, if the user wants to use the internet, they have to log in to 'Crypo' and only they can connect to ISP and the public internet. Proposed cryptographic algorithms are applied to 'Crypo's logical and mathematical model to provide high level security.

3.1. Attribute Based Encryption in 'Crypo' application

User credentials are required to identify as a registered user. While registering user towards ISP, attributes are randomly allocated. These attributes are referred further rather than referencing credentials directly. While traveling along the internet, the original message will be converted to encrypted format which can be decrypted by 'Crypo' only. Similar logics are applied for encryption and decryption.

Table 1 'Crypo' database table with ABE, Cipher & AES data

Credentials	Attributes Stored	Message / Data	Cipher	AES Key	AES Data
surasal	AB_9X	Hello there	X@!!*1 #Wq~+	surasal	,Ž¼¹W¡-L8t)öˆuR›O¬□wÈu♀@QNýq^X÷ÞÞ³‡¨äÏb• æ|j íP+
vrasal	DE_7Y	Hello	%$wwQ	vrasal	¢œ 5úâ¼ ±½ ½ g G&{□3ãWh¢+¾ • ^\«Ð À (˜ pèSíc:© @tŸ XþÏ• ê
sshelar	XX_1Z	Hi	*$	sshelar	W*ô0&:ûXÎªP'Ö?»ä:† (§~,¯,{ïoYÀCQÉž Å ÌøÕ Ú (P+¾
:	:	:	:	:	:
srasal	YX_97	Hey	%#@	srasal	Þ³£=?™ñ«´Q+¾ W—*ô0&:ûXÎªP'Ö?»ä:† (§~,¯,{. .

User credentials like user name, password and other details are stored according to Attribute Based Encryption (ABE). Table 1 includes credentials related to attributes allocation. While referring credentials, attributes are referred rather than actual values. This security level is applied to enhance the security level in database storage and access methods. Cipher policy with the proposed logical approach is further applied for data encryption.

3.2. Cipher Policy on 'Crypo' application

Table 2 'Crypo's cipher table

ASCII Set	**T_1**	**T_2**	**T_3**	**……**	**T_N**
A	@	®	©	……	*
B	~	©	╡	……	¤
C	$	¤	*	……	●
D	^	╝	@	……	£
E	#	µ	^	……	*
F	§	Ý	~	……	§
. . .	. . .	. . .	. . .	……	. . .

There is a cipher table in Crypo's secured system, which all American Standard Code for Information Interchange (ASCII) set values are allocated with special symbols. Randomly allocated symbols are cipher values. Table 2 includes all details of cipher values allocated. For more security approach, time constraint T_X is been considered. Cipher values are allocated according to T_X, and only. T_X retrieves the value according to current time components, including hours, minute and date.

These components are read according to session functionality, for example, when a user is accessing the service. In Table 2, T1, T_2, T_3,….., T_N are time constraints out of which single constraint is selected based on current time constraint components. If T_1 time constraint is selected, then cipher values from T_1 column will be allocated to ASCII set. Like A will be replaced by cipher value @, B by ~ , C by $ and so on. Binary value will be selected from Table 3.

Table 3 ASCII to Cipher binary conversion

ASCII Set	**Binary Value**		**T_1**	**Binary Value**	……
A	01000001		@	01000000	……
B	01000010		~	01111110	……
C	01000011		$	00100100	……
D	01000100	→	^	01011110	……
E	01000101		#	00100011	……
F	01000110		§	10100111	……
.	.		.	.	……
.	.		.	.	
.	.		.	.	

3.3. Combined approach and binary value

Based on a time constraint, logic A_L will be selected from Table 4; based on T_X, A_L is applied to the complete data C_D. Complete data are in the binary format. C_D is binary formatted data of ABE and cipher values based data. All logics work and behave in different manners, like A_1 will generate different binary value than A_2.

Table 4 Logic (A_L) selection with respect to time constraint (T_X)

Time Constraint (T_X)	A_L Logics set					
T_1	A_1	A_6	A_8	A_2	…	A_N
T_2	A_3	A_2	A_9	A_7	…	A_N
T_3	A_7	A_1	A_2	A_{13}	…	A_N
T_4	A_N	A_4	A_3	A_{19}	…	A_N
:	:	:	:	:	:	:
T_N	A_2	A_N	A_1	A_{24}	…	A_N

Consider the example given in Table.4, User credentials is “surasal” and data D_C is “Hello there”. Total data are considered as D_T with @ symbol so as to combine them.

$$\begin{aligned} T_D &= 19{:}08{:}21||24{:}04{:}2017 \\ T_X &= T_5 \\ D_T &= A_D + @ + D_C \\ D_T &= surasal@Hello\ there \end{aligned} \tag{1}$$

Attributes are allocated as AB_9X to the user credentials “surasal”. Attribute formed user credential data is A_D. Time constraint T_X is selected based on current time and date. While accessing service through ‘Crypo’, the current time component is 19:08:21 and date components is 24:04:2016. The total time of constraint data T_D is, 19:08:21||24:04:2017. The time constraint value T_7 is selected based on time constraint data. Based on the selection, respective cipher values are allocated to the ASCII values. D_C is newly generated cipher data based on T_7 from data “Hello there”. Total cipher data formed from attributes and cipher policy is C_D. Furthermore, C_D is converted to binary format.

3.4. Proposed time based randomized selection function R_Z

Randomized function $R_Z$is proposed and implemented to successfully select an element randomly from providing elements set , but don't allow the user to input. In proposing research manuscript, the proposed randomized selection function is applied to select A_L and T_X values randomly from their elements set. The following are the respective element sets with respective values.

$$T_X = \{T_1, T_2, T_3, T_4, \ldots, T_N\} \quad (2)$$

$$A_L = \{A_1, A_2, A_3, A_4, \ldots, A_N\} \quad (3)$$

$$T_X \xrightarrow{R_Z} T_S \quad (4)$$

$$A_L \xrightarrow{R_Z} A_S \quad (5)$$

Where T_S and A_S are time constraint and selected logic values, respectively. R_Z is suitable to input the received A_L from the system or users. Array_rand ( ) function is used to select an element randomly from elements set or array set in PHP programming [17]. According to functional syntax, some input integer has to pass to the function. In proposing randomized function R_Z, current time is considered with respect to time components as HOUR::MINUTE::SECOND. 'SECOND'. Time component S_S is used as input required for array_rand ( ). If the current time is 07:58:14 then S_S value will be 14. In this manner input value for array_rand( ) is provided.

array_rand($array_name, $input); //syntax

$T_D = date ("h:i:s"); // To select the current system time

$S_S = date ("s"); // To select the second value only

Our array sets are A_L and T_X.

array_rand($T_X, $S_S); //For array set T_X selecting a value randomly

array_rand($A_L, $S_S); //For array set A_L selecting a value randomly

array_rand( ) will select T_S and A_S values randomly from T_X and A_L array sets respectively.

T_5 and A_{14} are selected by applying array_rand( ) function.

$$A_L \xrightarrow{R_Z} A_{14} \quad (6)$$

$$D_T \xrightarrow{ABE+Cipher\ policy} C_D \quad (7)$$

$$C_D = \$AB\_9X\$@\ X@!!*1\#Wq\sim+ \quad (8)$$

$$C_D \xrightarrow{Binary\ value} 0010010001000001010000100101111100111001010110000010010001000000001000000101100001000000001000010010000100101010001100010010001101010111011100010111111000101011 \quad (9)$$

3.5. Proposed mathematical and logical approach

Table 5 Logical description

Logic	Description	Bits set operations
A_1	P_1= Multiple of odd positioned bits in sequential order P_2= Remaining bits of P_1 in sequential order	$P=P_1+P_2$
:	:	:
A_{14}	P_1= Multiple of 3 positioned bits in sequential order P_2= Remaining bits of P_1 in sequential order	$P=P_1+P_2$
:	:	:
A_N	P_1= Multiples of 2 positioned bits in sequential order P_2= Remaining bits of P_1 in sequential order	$P=P_2+P_1$

Based on T_X, A_L applies to the C_D. Each time constraint (T_X) contains the numbers of logics, like A_1, A_2, A_3, A_4,..., A_N in a random order. From Table 5, single logic is selected by applying randomized selection algorithm R_Z to T_X. Where, T_7 has

logics, set as A_1, A_4, A_9,…., A_N. In considered example, A_9 is selected from T_7 by applying R_Z logic. According to A_9,multiple of 3 positioned bits in the sequential order are considered to be separated. All separated bits are gathered together as P_1 in a sequential order and the remaining bits are gathered together as P_2 in a sequential order. Final encrypted bits set is considered as P where P_1 and P_2 are added to form the final bits set. It will be considered as final encrypted user data. This final encrypted data are further delivered by applying Advanced Encryption Standard (AES). Delivered encrypted data is E_A.

Table 6 Bits set generation and binary values

Bits set	Binary value
$C_D \xrightarrow{Binary\ value} T_7 + A_{14}$	0010010001000001010000100101111100111001010110000010010001000000001000000101100001 0000000010000100100001001010100011000100100011010101110111000101111 111000101011
$P_1 \rightarrow$	1100010001010110110000000000000110001001100111011100
$P_2 \rightarrow$	0000001000100001011111011010010000000100000100001110010000010000000010110001100000011100111011000111001101
$P \rightarrow$	1100010001010110110000000000000110001001100111011100100000010001000010111110110100100000001000001000011100100000100000000101100011000000111001101100011111001101010000100000100001110010000010000000010110001100000011100110110001111001101
$A_{14} \rightarrow$	0100000100111001
$E_D \rightarrow$	1100010001010110110000000000000110001001100111011100100000010001000010111110110100100000001000001000011100100000100000000101100011000000111001101100011111001101010000100111001
$E_A \rightarrow$	1011111010000001010111100101110010101011110100001100000000101000100110000111000011010000101001111101101011000110011101010100101000000011101001001111101011000111110111011111001000011101010000111000101000111111100110011111000110101011101101000101000101000001010111111001100111110001101010111011010001010001010000 00101011

$$P = P_1 + P_2 \tag{10}$$

$$E_D = \{P, A_L\} \tag{11}$$

$$E_D = \{P, A_{14}\} \tag{12}$$

ASCII value of E_D is,

$$E_D = \text{\textbf{\textit{}}}V\text{\textbf{\textit{}}}C\text{\textbf{\textit{}}}@,`sc\text{\textbf{\textit{}}}A14 \tag{13}$$

E_D 's ASCII value is considered to apply AES with its key. In this approach, the key is considered as stored credentials. In considered example, a credential is "surasal". Hence "surasal" is the AES key to encrypt it again. For conversion, Electronic Code Book (ECB) is considered. Table 6 shows the respective binary values.

$$E_A = ,\check{Z}¼'W¡\text{-}L8t)ö\hat{}uR›O¬\boxed{w}\grave{E}u♀@QNýq\hat{}X÷ÞP³‡¨äÏbæ|jíP+ \tag{14}$$

After applying AES, above ASCII text value is retrieved from an encrypted format of E_A. Its binary value is finally delivered to ISP. After retrieving the binary value, due to same logical approach towards both ends; ISP will automatically understand the actual data behind the encrypted data. Logic will be upgraded timely due to the security reasons.

$$E_A \xrightarrow{\textbf{\textit{Binary value}}} \tag{15}$$

1011111010000001010111100101110010101011110100001100000000101000100110000111000011010000101001111101101011000110011101010100101000000011101001001111101011000111101110111100100001110101000011000100000010100010100111000011010111111010111000101011110010111000111101111011110111100100001110101000011000100000010100010100111000011010111111010111000101011110010111000111101111011110111100100001110101000011000100000010100010100111000011010111111010111000101011110010111000111101111011110111100100001110101000011000

0010100011111111001100111110001101010111011010001010001010000000101011

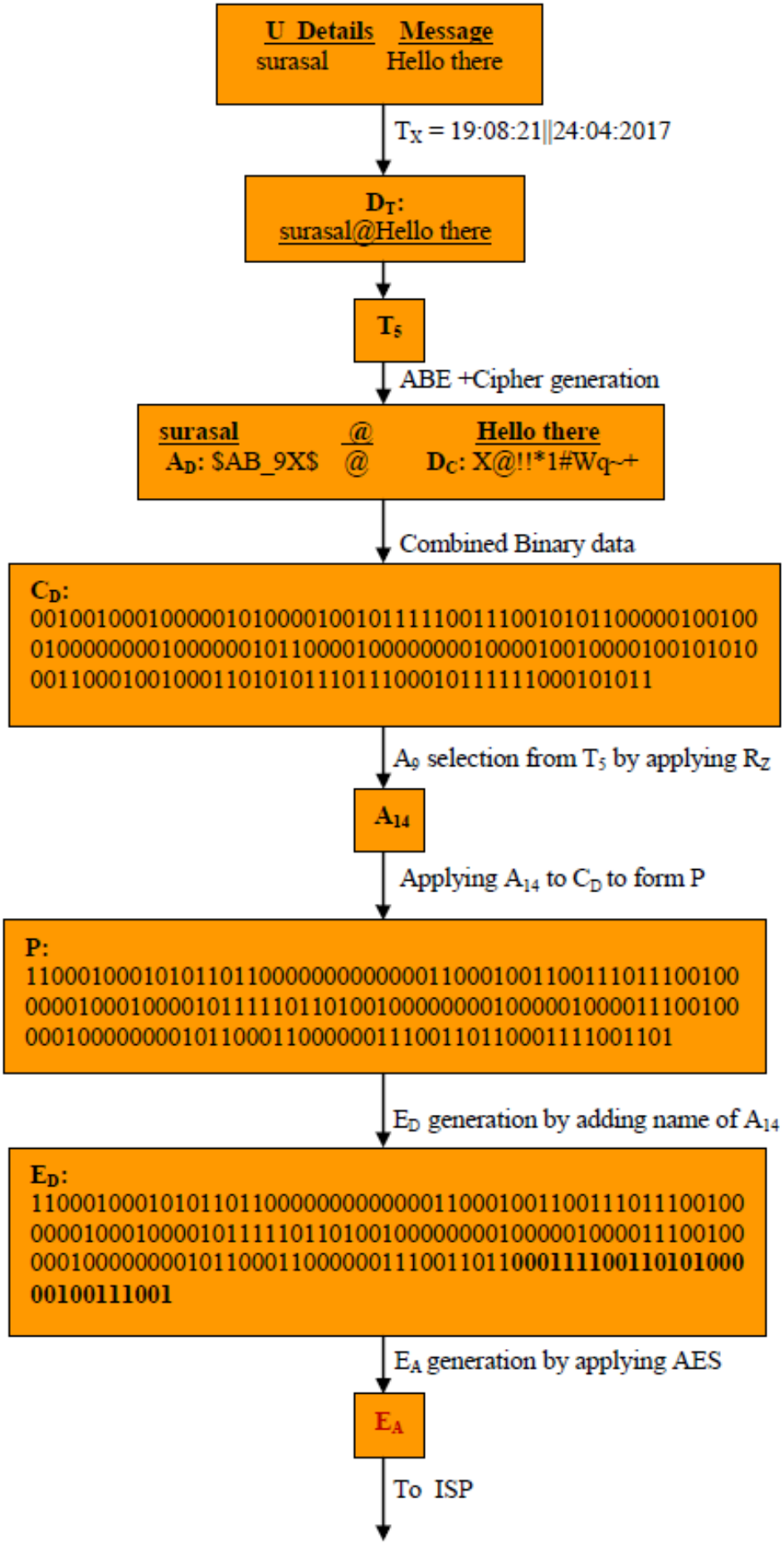

Fig. 5 Cryptographic steps in ‘Crypo’ application

$$E_D \xrightarrow{AES} E_A \rightarrow \boxed{ISP} \tag{16}$$

The same logic applies to decrypt the data. Fig. 5 shows step by step approach to generate E_A. While carrying encrypted data, the applied logic A_L is included in the delivered data. Unless the selected logic has been known, 'Crypo' can't decrypt it. While selecting the logic, current time constraint components are selected.

3.6. Decryption in Crypos application

In this point decryption heading is given, but in actual way hash values are generated and be matched with the existing hash values, so as to confirm the applied logic. According to SHA standards, hash values can't decrypt back to the original values. In considered example, generated hash value is used to check which logic (A_S) and time constraints (T_S) has been selected. Based on a time constraint, respective hash value is generated and it is matched form crypo's hash values table. At the other end, generated hash value is matched and respective logic is selected for generating the required decrypted data. Based on R_Z, time constraints and logics are selected. These selected values are considered as single data S_D. Selected logics are kept inside round brackets, separated by '+'. On the whole (T_S + A_S) data, SHA-256 is applied to generate a hash value which is considered as key S_E [18].

$$S_D = T_S + A_S \tag{17}$$

T_E and A_E are hash values of T_S and A_S respectively which are generated using SHA-256.

$$T_S \xrightarrow{SHA-256} \tag{18}$$

$$A_S \xrightarrow{SHA-256} A_E \tag{19}$$

Hence final encrypted key will be delivered as S_E.

$$S_E = T_E + surasal + A_E \tag{20}$$

Here, +surasal+ is separator used to separate two hash values of T_S and A_S. In executed example T_5 and A_{14} are selected,

$$S_D = T_5 + A_{14} \tag{21}$$

PHP Code to generate SHA-256 value:

```
<?php
$Te=hash('SHA256', 'T5');
$Ae=hash('SHA256', 'A14');
echo "<font color='blue' size='5'>Secrete key 'SE' is: </font>".$Te."<font color='red' size='3'>+surasal+</font>".$Ae."<br>";
?>
```

Output:

Secrete key 'SE' is:
020d01e5b92677a3996c6d0e9fde6322095a0b486b7fbee5252d5e4915317bf4+surasal+cc1e22142e7d545252f349a1d1dd84100e4441043f7485de6eeeb2f9eaea9e14

$T_5 \xrightarrow{SHA-256} T_E$ → 020d01e5b92677a3996c6d0e9fde6322095a0b486b7fbee5252d5e4915317bf4

$A_{14} \xrightarrow{SHA-256} A_E$ → cc1e22142e7d545252f349a1d1dd84100e4441043f7485de6eeeb2f9eaea9e14

S_E=020d01e5b92677a3996c6d0e9fde6322095a0b486b7fbee5252d5e4915317bf4+surasal+ cc1e22142e7d545252f349a1d1dd84100e4441043f7485de6eeeb2f9eaea9e14

S_E will be delivered after delivering encrypted data as a secret key to understand which logic set is used from Table.4.

When S_E is delivered, its two hash values T_E and A_E are separated by separator '+surasal+'. Those separated hash values are been searched in the hash table of the end device. By matching their values, respective values of T_S and A_S are selected and logics are applied to decrypt the data. Once respective logics are retrieved, 'Crypo' decrypts the encrypted data, using T_S and A_S logics. In Table.7, received SHA-256 values are checked to retrieve the applied T_S and A_S values.

Table 7 Hash values table

T_S	SHA-256	A_S	SHA-256
T_1	1f93603db53bfad5c92390f735d0cbb8617b 4ab8214ae91c5664a3d1e9b009c8	A_1	16a36e86f6fed5d465ff332511a0ce1a863b55 d364b25a7cdaa25db19abf9648
⋮	⋮	⋮	⋮
T_5	020d01e5b92677a3996c6d0e9fde6322095a 0b486b7fbee5252d5e4915317bf4	A_5	ea644b359f0b0abde72ab7dbdc03c7d630537 bdd0fd7ca1bbb99d41e7f446eea
⋮	⋮	⋮	⋮
T_{14}	7fe51a276aa44f3983c157d4a98f6b5aa257d ad74b5ab8f9253fb0798d19217e	A_{14}	cc1e22142e7d545252f349a1d1dd84100e444 1043f7485de6eeeb2f9eaea9e14
⋮	⋮	⋮	⋮
T_N	⋮	A_N	⋮

When T_S and A_S values are selected, the decryption part can be done based on applied logic to encrypt it in reverse order. In a similar way, other logics are applied when it gets selected, based on a time constraint and randomized selection algorithm. In the above examples, separator '+surasal+' separates the T_5 and A_{14} which will be matched with hash values table. After matching hash values, T_S and A_S value has been applied will be confirmed. For decryption, same values will be applied to decrypt the content. In Fig. 5 the flow chart shows that the working of Crypo's algorithmic and mathematical approach can be understood. Flowchart shows how Crypo's approach is applied step by step to generate the required output of considered an example. Protocol conversion suite manages all protocols, standards and logics applied at both ends that are at the client and servers as ISP. Internet Service Providers are looking for high level security techniques. Compared to current internet saturation in the globe, even the proxy servers are not secured. 'Crypo' can support ISP's to establish secure protocol between their clients. Clients can access and connect to the internet through ISP. ISP can prevent internet attacks through proposed 'Crypo' based application. Same kind of proposed approach can be applied at multiple internet components like proxy servers, routers, firewalls and others. The main aim behind the proposed 'Crypo' application is to establish the secure and personal, crypto-logic based system.

4. Conclusion

Proposed application establishes a secured network between Internet Service Provider and end users through secured platform to access the public network. Security level is enhanced by applying multiple security techniques including Attribute Based Encryption (ABE), Cipher policy, Advanced Encryption Standard (AES) and proposed logic. SHA-256 hash function is used to encrypt the key data. SHA-256 hash value is used to select the applied logics. The Actual data are not travelling through the internet between ISP and end users. Encrypted data are travelling through the internet whose meaning can be understood by decrypting it through applied security techniques and logics only. The combinational security approach makes cryptography more complex due to which security levels are increased. Proposed Crypo logic is developed according to private security. Its logic is known to the end user and ISP only after the successful authentication. It will be updated and synchronized

timing through internet. Hence multiple security techniques and proposed logic improve the security of the Internet Service Provider due to which end users can access the public network safely and securely.

References

[1] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded cipher text policy attribute based encryption," Automata, Languages and Programming, pp. 579-591, 2008.
[2] A. A. Bruen and M. A. Forcinito, Cryptography, information theory, and error-correction: a handbook for the 21st Century, 1st ed. New Jersey: John Wiley & Sons, 2011.
[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proceedings of The 13th ACM Conference on Computer and Communications Security, Oct. 2006, pp. 89-98.
[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption in security and privacy," IEEE Symposium, May 2007, pp. 321-334.
[5] M. S. Rahman, A. Basu, and S. Kiyomoto, "Decentralized ciphertext-policy attribute-based encryption from learning with errors over rings," Trustcom/BigDataSE/I SPA IEEE, Aug. 2016, pp. 1759-1764.
[6] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, "Multi-authority ciphertext-policy attribute-based encryption with accountability," Proceedings of The 6th ACM Symposium on Information, Computer and Communications Security, March 2011, pp. 386-390.
[7] Y. S. Rao and R. Dutta, "Decentralized ciphertext-policy attribute-based encryption scheme with fast decryption," IFIP International Conference on Communications and Multimedia Security, Springer Berlin Heidelberg, Sept. 2013, pp. 66-81.
[8] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of applied cryptography, 1st ed. New York: CRC Press, 1996.
[9] C. P. Pfleeger and S. L. Pfleeger, Security in computing, 1st ed. New Jersey: Prentice Hall Professional, 2003.
[10] C. P. Pfleeger, Security in computing, 5th ed. New Delhi: Pearson Education, 2006.
[11] B. Waters, "iphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization," International Workshop on Public Key Cryptography, Springer Berlin Heidelberg, March 2011, pp. 53-70.
[12] J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, " Multi-authority ciphertext-policy attribute-based encryption with accountability, " Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM, 2011, pp. 386-390.
[13] A. Lewko and B. Waters, "Decentralizing attribute-based encryption, " Annual International Conference on The Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, 2011, pp. 568-588.
[14] V. T. Mulik, K. Saritha, and S. U. Rasal, "Privacy preserving through mediator in decentralized ciphertext policy attribute based encryption, " IJRET: International Journal of Research in Engineering and Technology, vol. 5, pp. 535-540, June 2016.
[15] S. U. Rasal, S. T. Shelar, and V. S. Rasal, "Securing internet banking using multiple attributes scheme and OTP," The IIOAB Journal, vol. 7, pp. 26-30, Oct. 2016.
[16] S. U. Rasal, R. Agarwal, V. S Rasal, and S. T. Shelar, "IOT appliance access structure using ABE based OTP technique," The IIOAB Journal, vol. 7, pp. 180-186, Sept. 2016.
[17] S. Prettyman, PHP arrays, 1st ed. New York: Apress, 2017.
[18] S. Holzner, PHP: the complete reference. New York: McGraw-Hill Education, 2007.