CHAPTER 20

A novel approach for securing e-health application in a cloud environment

Dipesh Kumar[a], **Nirupama Mandal**[a], **and Yugal Kumar**[b]

Department of ECE, IIT(ISM), Dhanbad, India[a] *Department of CSE & IT, JUIT, Solan, Himachal Pradesh, India*[b]

Chapter outline

1 Introduction

With the rapid increase in convergence technologies, the world is able to get lot of information through the portable mobile devices (Mumrez et al., 2019). Due to development of internet and its users across the world, there is a demand of centralized healthcare information system. Rapid increase in chronic diseases and various disease aspects, disease prevention, and various government policies of providing a better healthcare facility to its citizens steadily increased the demand for intelligent and portable mobile-based services (Sravani et al., 2017). In the past one decade, the use of smart phones has increased and the same can be utilized for e-Health services and can be used for providing personal health record (PHR), disease-related information and other self-heathcare facilities (Jung and Chung, 2016).

In the current scenario, the use of Information Communication Technologies (ICT)-based intelligent system such as smart mobile devices gives ample opportunity for the growth and development of e-Health services. Irrespective of geographical barriers, the use of ICT helps to deliver mobile-based e-Health services to its users. Nowadays, the mobile health (m-health) applications directly address the

Machine Learning, Big Data, and IoT for Medical Informatics. https://doi.org/10.1016/B978-0-12-821777-1.00018-5

problems of sudden rise in chronic diseases and help patients and their families for self-care (Xiong, 2019; Chung et al., 2015).

ICT-based intelligent system can be seen as a combination of person device assistant (PDA) (such as mobile phones, electronic/smart watches, and i-pad) with the application of IoT and Cloud computing services (Mumrez et al., 2019; Vishwakarma et al., 2019). Intelligent personal devices (IPD) are software agents that help the users in doing their day-to-day work (such as shopping, online bill payments, making appointments, and attending meetings) with ease of simplicity. Now, with the advancement and inclusion of IoT and cloud computing with IPD, the capabilities and demands of such devices are increasing at an alarming rate. Researchers have created many dynamic and static gateways to enable portable/personal devices to work with IoT or Cloud-based intelligent systems (Nanayakkara et al., 2019).

The emergence of Internet of Things (IoT) has made all the addressable devices/objects to communicate and cooperate with each other in order to further increase the capabilities of IPD. By providing an easy gateway path, we can easily extend the accessibility of intelligent devices on different dynamic scenarios. Further, building of smart cities, homes, transportation, and healthcare services are some applications where IoT can be used along with the IPD (Atzori et al., 2010).

The convergence of cloud computing with mobile devices and other computing technologies has allowed us to build an intelligent system for providing a better e-Healthcare services (Selvaraj and Sundaravaradhan, 2020). The innovative idea of cloud technology, which came up with a new and extended infrastructure facilities, has made intelligent system like portable computing/mobile devices to provide more reliable services to its end users. As mentioned earlier, like other technologies, cloud computing can help in empowering the healthcare services in the most efficient way. It offers a fast, reliable, and cost-effective infrastructure and application. The concept of cloud can help in management of data-centric health facilities and can help in removing the complexity involved in storing and retrieval of health-related data. Only challenges that cloud technologies currently facing are security, confidentiality, and trust issue. Weak security factor in cloud hinders its complete application in health industry. Further, measures were taken to remove security challenges for cloud to enable its application in healthcare industry (Malhotra et al., 2019).

As stated earlier, with the rapid increase in chronic diseases and intelligent devices to monitor those diseases, there is a need to develop systems for monitoring personal healthcare record (PHR) using cloud computing techniques (Kadhim et al., 2020). To provide continuous healthcare facility to an individual, a tool known as PHR needs to be created which can monitor and manage health-related information. It may also help us to maintain and view medical information that can be needed while a patient visits hospitals for treatment. This development of PHR is only possible when we have an intelligent system for recording and monitoring healthcare information of an individual in a convenient way. Apart from intelligent system, many hospitals also maintain a centralized cloud-based system to record day-to-day information of their patient situated at distant places (Silva et al., 2015; Santos et al., 2016; Kaur and Chana, 2014; Kanrar and Mandal, 2017).

A PHR or e-Health application utilizes patient's clinical data. Security of clinical data is an important concern while sending it to cloud environment. Data can be secured using https protocol using ciphers. Cipher is used to encrypt and decrypt data using encryption and decryption algorithm. While sending patient's clinical data to the cloud server, data should be encrypted. Encryption of data hides the actual message and converts it to hypothetical text so that the data are not easily read by hackers. At destination, i.e., cloud server, the encrypted data are decrypted by using decryption algorithm to fetch the actual data.

With increasing technology usage, various steps have been taken to secure the data in transport layer, and also various technologies have been developed by hackers to decode the secured data to get the original message. The PHR's or e-Health application stores very sensitive data. The data include patient's clinical information, patient's medical history, bank account details used for transactions with hospitals, etc. These data are very private and can cause major impact if it is hacked by any hacker and can be used for any unusual activities. So, there is a need to implement new ciphers as the already existing ciphers can be decoded by hackers. So, existing ciphers must be updated, and new ciphers must be developed with course of time. The proposed work includes introduction of new improved cipher for encrypting the message at the senders' end and decrypting the message at the receivers' end to allow end-to-end secured connectivity and transmission of message securely for an e-Health application. In the proposed work, an improved reverse transposition cipher is proposed which provides new improved encryption and decryption algorithm.

1.1 Contribution

The major contribution of the proposed work is to develop new algorithm to be used in cipher to encrypt the message at the senders' end and decrypt the message at the receivers' end to retrieve the original message. The proposed algorithm allows to develop new cipher to be used in digital certificates in e-Health application and cloud servers. The proposed cipher will be effective to secure the messages and prevent any unauthorized access by hackers. In the proposed work, the improved reverse transposition cipher will provide encryption of messages at the senders' end and decryption of messages at the receivers' end to retrieve the original message.

2 Motivation

The increase in the growth of e-services between users and enterprises is one of the most interesting and considerable topics for researchers. In the current scenario, the diseases are being transformed from acute stage to chronic stage in a quick span of time due to rapid increase in population, lack of knowledge, etc. It has been studied in the literature (Mumrez et al., 2019; Sravani et al., 2017; Jung and Chung, 2016; Xiong, 2019; Chung et al., 2015; Vishwakarma et al., 2019; Nanayakkara et al., 2019; Atzori et al., 2010; Selvaraj and Sundaravaradhan, 2020; Malhotra et al., 2019; Kadhim et al., 2020; Silva et al., 2015) that many healthcare intelligent system use cloud and IoT-based applications for providing e-Health services. However, both cloud and IoT is inefficient to handle, store, and process health-related data due to its complex structure, hardware capacity limitations, and -security-related issues (Shin et al., 2016). A reliable healthcare system is the need of the hour which can be used to manage and monitor public health and can provide suitable treatment as and when required. The motivation behind this work is to develop an intelligent system-based platform that provides an uninterrupted and scalable cloud service interface, which can easily provide healthcare facilities to its users. The interface between portable devices and cloud technologies often faces the problem related to security and privacy. In the proposed work, we have developed a uniform platform to centralize user data that can be shared and accessed across various platforms by preserving the security and privacy of user personal data (Lee and Kim, 2014).

2.1 Related works

With increase in the uses of mobile phones, e-Health care becomes one of the most important factors in today's growing life. In the past few years, the world has witnessed a rapid increase in population and because of this, it is hard to provide a smooth and better healthcare facilities to all the individuals situated at different remote locations. Therefore, there is a need to provide medical facilities and healthcare services via mobile technologies. In the current era of mobile revolution, it is easier to develop a mobile-based online application which can easily be accessed through personal smart mobile phones or portable devices where a user can maintain and update their health-related information and the same can also be accessed and managed by maintaining a centralized database through cloud or IoT-based application (Santos et al., 2015).

It has been observed that ICT-based e-Health services are gaining popularity among its user and medical practitioners across the world (Ogasawara, 2006). ICT-based intelligent devices have the potential to provide high-quality, low-cost and error-free healthcare facility to all its user in a convenient and efficient way. But, still, these intelligent devices lack in providing some basic services due to data complexity, storage limitation, less infrastructure and proper coordination of distributed databases. In the studies cited herein (Shojania et al., 2009; Deutsch et al., 2004; Wang et al., 2009) different solutions have been suggested to overcome this limitation. Due to increase in the use of smart mobile phones or other portable devices, many healthcare applications (Patients Like Me (Wicks et al., 2010), Sugar Stats (Sugarstats, 2019), Cure Together (Curetogether, 2020), TU Diabetes (Tudiabetes, 2019)) are available where users can maintain their own health data and can seek medical advices as and when required.

It has been seen in the literature (Mumrez et al., 2019; Sravani et al., 2017; Jung and Chung, 2016; Xiong, 2019; Chung et al., 2015; Vishwakarma et al., 2019; Nanayakkara et al., 2019; Atzori et al., 2010; Selvaraj and Sundaravaradhan, 2020; Malhotra et al., 2019; Kadhim et al., 2020; Silva et al., 2015; Santos et al., 2016; Kaur and Chana, 2014; Kanrar and Mandal, 2017; Shin et al., 2016; Lee and Kim, 2014; Santos et al., 2015; Ogasawara, 2006; Shojania et al., 2009; Deutsch et al., 2004; Wang et al., 2009; Wicks et al., 2010; Sugarstats, 2019; Curetogether, 2020; Tudiabetes, 2019; Apple Siri Webpage, 2015; Google Now Webpage, 2015; Samsung, 2015; Microsoft, 2015; Rodrigues et al., 2013; Komninos and Stamou, 2006) that ICT-based intelligent devices can easily be interfaced with other applications to assist patients, doctors, and hospitals. Further, many applications such as Apple's Siri (Apple Siri Webpage, 2015), Google Now (Google Now Webpage, 2015), Samsung's S Voice (Samsung, 2015), and Microsoft's Cortana (Microsoft, 2015) are currently being used to monitor personal healthcare information which includes medicine reminder, day-to-day change in health condition, monitoring heart beat and blood pressure, etc. Authors in the referred study here (Rodrigues et al., 2013) presented a similar kind of mobile-based health application where patient's weight is getting monitored to prevent obesity. Apart from maintaining weight information, the application also keeps record of body mass index, health meal planning, and basal metabolic rate. As we are considering the use of intelligent devices, authors in the referred study here (Komninos and Stamou, 2006) made an application where peripheral device such as thermometer interact with PDA of the patient and a notification of the temperature will be sent to the doctor or the care taken if there is any variation in patient body temperature beyond the prescribed limit (Santos et al., 2016).

As we have seen in literature and in the above paragraph, cloud technology will help in developing an intelligent portable platform to perform the exchange of healthcare services to its service providers.

Further, authors in the referred study here (Pandey et al., 2012) used data mining technique to build an intelligent system with a strong focus on the quality of services with respect to cost, infrastructure, and security. The same strategy is followed by the authors in the study cited herein (Kuo, 2011) which use cloud computing techniques to provide the services suggested in the other study (Pandey et al., 2012).

As stated earlier in this chapter, there is a need to look upon the security requirements of cloud applications. In this view, Xie et al. (Xie et al., 2019) presented an approach for the security aspect of cloud technology, which consists of prospective threats and the preventative measure need to be followed in the deployment of cloud application. Before using cloud application for healthcare industry, we should have a complete knowledge of the work being done in the same field. Avancha et al. (Avancha et al., 2012) provided a complete review of the application of cloud in healthcare industry and also presented a privacy framework for e-Health sector. Ibrahim et al. (Ibrahim and Singhal, 2016) provided a secure sharing on e-Health data with different service providers using cloud computing. Along the line, Abbas and Khan (2014) presented related studies which aim to contrast the privacy-preserving approaches employed in e-Health clouds.

Authors in the studies referred herein (Ferna'ndez et al., 2013; Dong et al., 2012; Metri and Sarote, 2011; Seol et al., 2018) also presented various security-related issues and mechanism to overcome the same for e-Health cloud environment. We introduce the summary of the most existing technique that is commonly being adopted by various health sectors for cloud environment. With reference to the various literature studies (Chenthara et al., 2019; Abbas and Khan, 2014; Wang et al., 2019; Zhang et al., 2018; Ayofe et al., 2019), there is no inclusive survey available independently at a point of concentration on confidentiality issues of e-Health cloud. As per the survey, it is clearly indicated that privacy and security of the personal health and medical related data are very much important. Various authors (Dong et al., 2012; Metri and Sarote, 2011; Seol et al., 2018; Chenthara et al., 2019; Abbas and Khan, 2014) introduced the architectural view of cloud for handling applications related to biomedical with respect to security and privacy issues.

2.2 Challenges

The major challenge in e-Health application is to maintain confidentiality and integrity of the data retrieved from IoT device which is continuously monitoring a patient. There are multiple ways to breach data by hackers. Transport layer is very prone to attack by hackers the reason why data encryption is a very challenging task. Various ciphers are available in today's world, but hackers' attacks are also increasing day by day. To avoid such kind of attacks, proper steps need to be taken for securing the data. With the advancement of technology, attackers use new techniques to steal or hack data. So, there is a need to introduce new improved encryption and decryption technique which provides an efficient solution to save data from various types of security threats and attacks. In the upcoming section, a new approach to secure e-Health application using improved reverse transposition cipher is discussed.

3 Proposed system

In this section, a new approach to secure e-Health application using improved reverse transposition cipher is proposed. In the architecture shown in Fig. 1, the IoT device with MP5700AP pressure sensor to record patients' blood pressure is used, which records and sends data to e-Health mobile application.

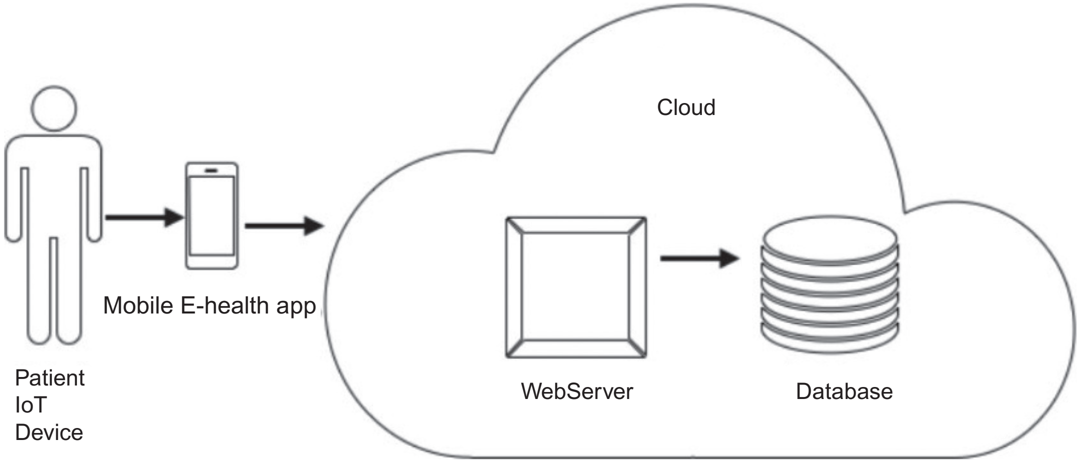


FIG. 1

IoT-based mobile e-Health architecture.

The e-Health mobile application is developed to interact and receive data from IoT sensor and send it to web server in cloud environment securely with https protocol using cipher. The e-Health mobile application is developed using android studio version 3.6.3 in 64 bit windows platform which supports Android version jelly beans and above android versions. After receiving the data from e-Health mobile application, the web server sends the data to the app server and the app server sends that data to cloud database. The web server is apache Tomcat and the database is Microsoft SQL Server. In Fig. 1, patient's clinical data are sent to web server by e-Health mobile application using https protocol. The https protocol requires ciphers to encrypt data while sending and to decrypt data after receiving it.

The improved reverse transposition cipher provides encryption algorithm to encrypt the data while sending it from e-Health mobile application to web server. Also, it provides decryption algorithm to decrypt the received data at the web server end. The encryption and decryption technique is explained in detail in the next section.

Improved reverse transposition Cipher:

Improved reverse transposition cipher is explained in the following sections:

Encryption of message:

The data recorded by the IoT device is encrypted by using the below encryption algorithm while sending to the cloud web server:

- Select a key value of any length say N.
- Create a two dimensional table with column length N and row length depends on the length of message to be encrypted.
- Assign each alphabet (including blank spaces) of the message to each cell of the table.
- Create a new empty table of size same as the original table.
- Move the elements of last column of the table and first column of new table vertically.

- Repeat this until all the elements of the original table are moved to new table in the reverse order.
- Note down the elements of first two columns of new table. Then jump by two columns and note down elements of 5th and 6th columns of the table and again jump by two columns and repeat the process.
- If there is no column further left in the table. Then end the loop and note the elements of 3rd and 4th columns and again jump 2 places and note the elements of next two columns and continue the same process till all the columns are covered.
- Place all the elements together to obtain the encrypted message.

The above encryption algorithm is explained in detail below:

Let us assume that below message is recorded by IoT device and sent to e-Health application for saving it securely in cloud database.

Recorded message:

"***Systolic blood pressure:120, Diastolic blood pressure:80***".

Step 1: Let us assume we have selected a key value as 10.

Step 2: Create two-dimensional table with column length as 10 and assign each alphabets to each cell (Fig. 2)

Step 3: Create a new empty table. Move all the elements of last column of the table shown in Fig. 1 to the first column of new table. Then, move all the elements of the second last column of the old table to the second column to the new table. Repeat this step until all the elements of old table are assigned to the new table in reverse order. This step is explained in Fig. 3. After assigning all the elements of the old table to the new table in reverse order, name the columns of the new table as C1, C2, … C10 as shown in Fig. 3.

Step 4: In this step, note down all the alphabets (including space for empty cells) from C1 and C2. Jump two columns and note down all the alphabets (including space for empty cell) from C5 and from C6. Again, jump two columns and note down all the alphabets (including space for empty cell) from C9 and C10. This step is explained in Fig. 4.

Below message is obtained from this step:

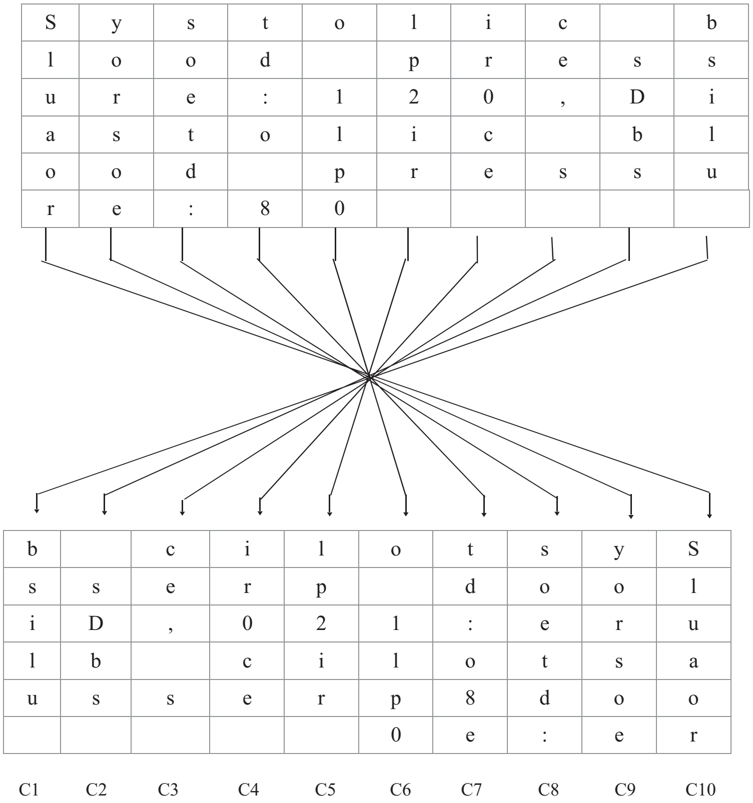
bsilu sobs lp2ir o 1lp0yorsoesluaor.

When the execution reaches the last column, then, stop the iteration and go back and note the alphabets (space for empty cell) from C3 and from C4. Again jump two columns and note down all the

S	y	s	t	o	l	i	c		b
l	o	o	d		p	r	e	s	s
u	r	e	:	1	2	0	,	D	i
a	s	t	o	l	i	c		b	l
o	o	d		p	r	e	s	s	u
r	e	:	8	0					

FIG. 2

Received messages assigned row-wise to create a table.



S	y	s	t	o	l	i	c		b
l	o	o	d		p	r	e	s	s
u	r	e	:	1	2	0	,	D	i
a	s	t	o	l	i	c		b	l
o	o	d		p	r	e	s	s	u
r	e	:	8	0					

b		c	i	l	o	t	s	y	S
s	s	e	r	p		d	o	o	l
i	D	,	0	2	1	:	e	r	u
l	b		c	i	l	o	t	s	a
u	s	s	e	r	p	8	d	o	o
					0	e	:	e	r
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10

FIG. 3

Mapping process to create new table with elements in reverse order.

alphabets (space for empty cell) from C7 and from C8. Since there is no column after this to jump the iteration, the execution will be stopped.

The below message is obtained from this step:

ce, s ir0ce td:o 8soetd:

Now, combine these two messages to obtain the final encrypted message as below:

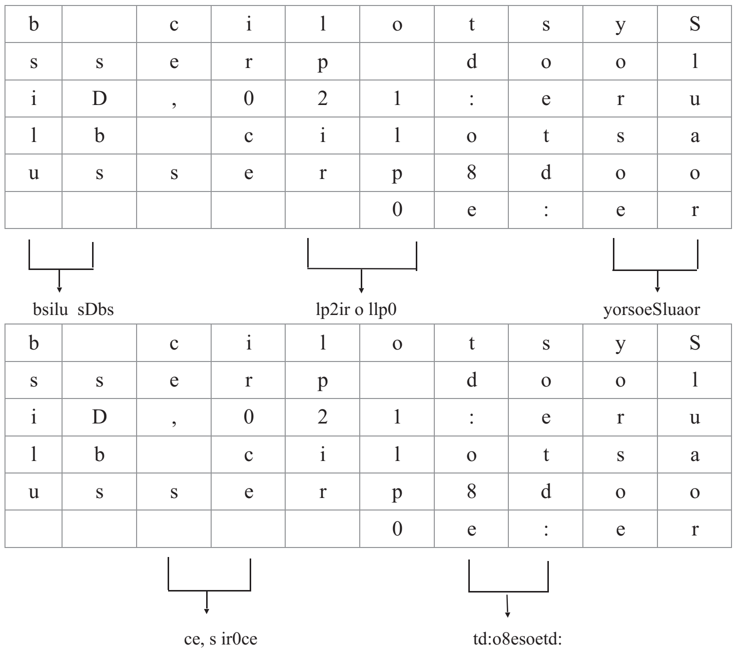
bsilu sDbs lp2ir o 1lp0yorsoesluaorce, s ir0ce td:o 8soetd:

The encryption process is explained in flowchart (Fig. 5) below:

Decryption of received message:

The encrypted message received at the server's end in cloud environment is decrypted by using the decryption algorithm shown here:

- Count the total number of alphabets in the received encrypted message (including blank spaces).
- Divide the total count by key value N to get K.
- Create a table with row size as K and column size as N.



b		c	i	l	o	t	s	y	S
s	s	e	r	p		d	o	o	l
i	D	,	0	2	1	:	e	r	u
l	b		c	i	l	o	t	s	a
u	s	s	e	r	p	8	d	o	o
					0	e	:	e	r

b		c	i	l	o	t	s	y	S
s	s	e	r	p		d	o	o	l
i	D	,	0	2	1	:	e	r	u
l	b		c	i	l	o	t	s	a
u	s	s	e	r	p	8	d	o	o
					0	e	:	e	r

FIG. 4

Reverse transposition method to encrypt message.

- Fill first two column of the table with alphabet from encrypted message received. Once all the cells of first two columns got filled, then leave the two columns empty and jump to 5th columns and fill cells of the next two columns with alphabets. After filling the 5th and 6th columns, again leave two columns blank and jump to the 9th column and fill the alphabets from encrypted message to the 9th and 10th columns. After this, return back to the 3rd column which was left empty and fill the cells of the 3rd and 4th columns with alphabets and jump to the 7th column and fill the cells of 7th and 8th columns.
- Create a new table. Starting from last column, move all the elements of the last column of old table to the first column of the new table. Continue this process to make sure that all the elements of old table are moved to the new table in reverse order.
- Place the alphabets of this table row wise to get the decrypted message.

The decryption algorithm is explained below:

Below is the message received at the server's end:

bsilu sDbs lp2ir o 1lp0yorsoesluaorce, s ir0ce td:o 8soetd:

Step 1: Count the length of received encrypted message.

Length of encrypted message is 60 (including blank spaces).

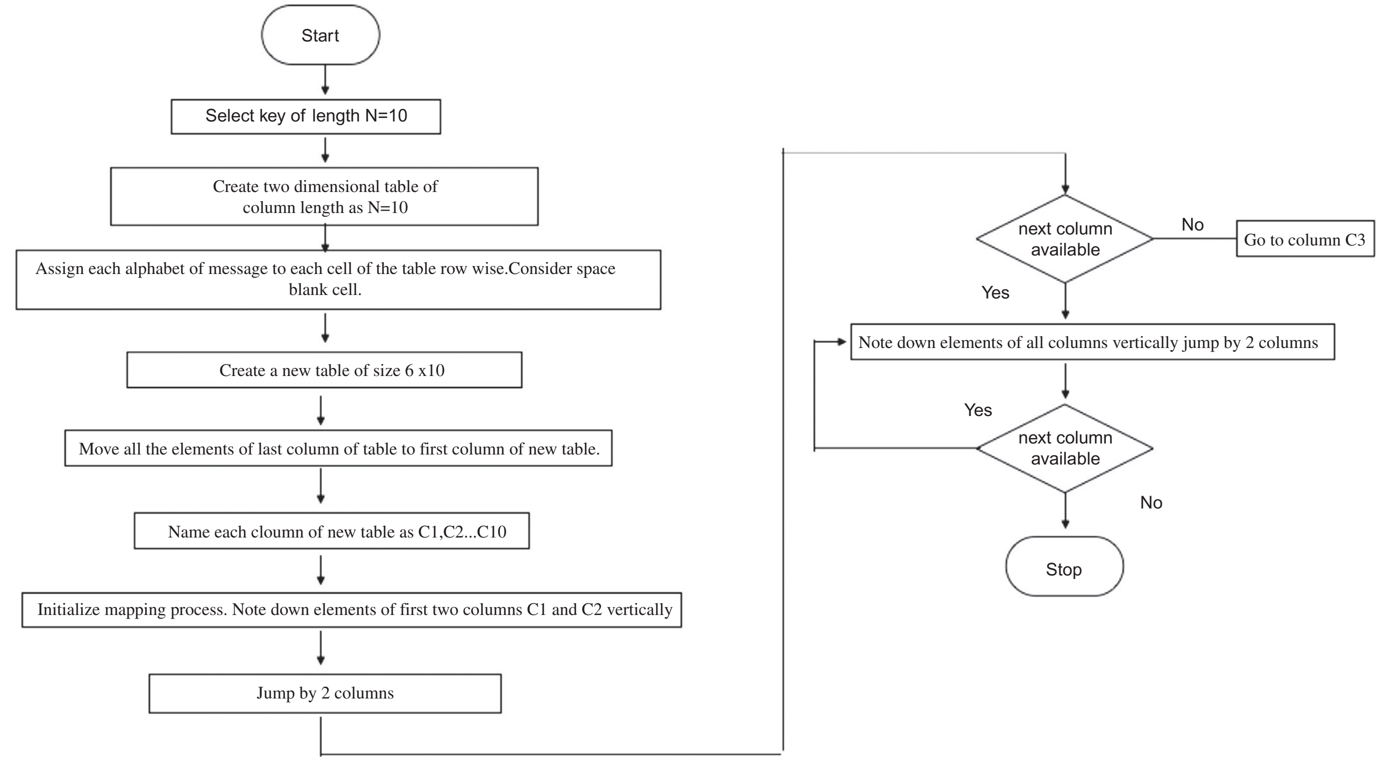

Start
Select key of length N=10
Create two dimensional table of column length as N=10
Assign each alphabet of message to each cell of the table row wise.Consider space blank cell.
Create a new table of size 6 x10
Move all the elements of last column of table to first column of new table.
Name each cloumn of new table as C1,C2...C10
Initialize mapping process. Note down elements of first two columns C1 and C2 vertically
Jump by 2 columns
next column available
No
Go to column C3
Yes
Note down elements of all columns vertically jump by 2 columns
Yes
next column available
No
Stop

FIG. 5

Flowchart of encryption process using improved reverse transposition method.

Step 2: Calculate N.

$$N = \text{Message length}/K$$
$$N = 60/10$$
$$N = 6$$

Step 3: Create a table of row length as N, i.e., 6 and assign the first 12 letters in the first two columns C1 and C2 vertically. Then skip two columns and assign another 12 letters in the next two columns C5 and C6. Again skip two columns and assign another 12 letters in the next two columns, i.e., C9 and C10, respectively.

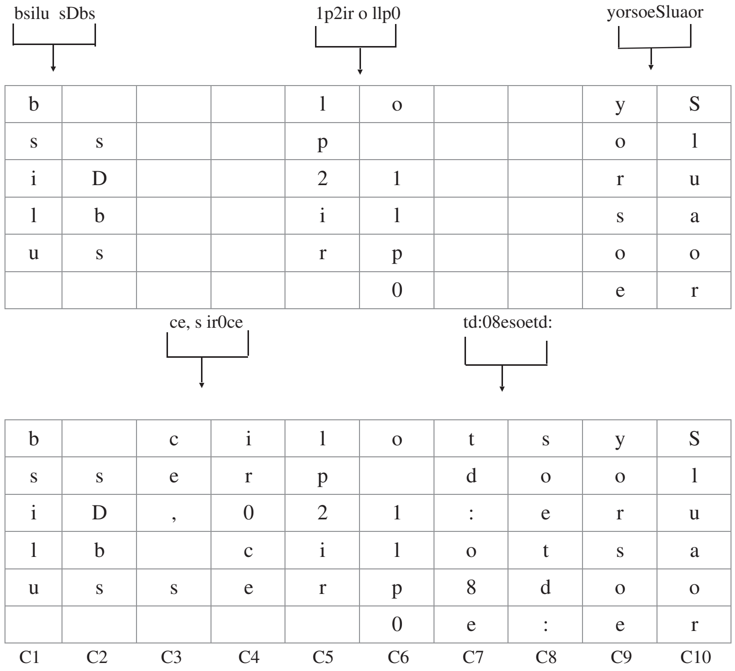
When all the columns get filled, then return back to the 3rd column C3 and fill letters in two consecutive columns, i.e., C3 and C4. Jump two times to columns C7 and C8 and fill the cells of C7 and C8 with remaining letters as shown in the table below to create a table.

Step 4: Create a new table. In Fig. 6, starting from the last column, i.e., C10, move all the elements of column C10 to the first column of the new table. Repeat this process so that all the elements of the above table get assigned to the new table in reverse order vertically as shown in Fig. 7.

Step 5: Note all elements from each cell row wise as shown in Fig. 8.

Combine all the elements got from the table and retrieve original message as below: ***"Systolic blood pressure: 120, Diastolic blood pressure: 80".***

The Decryption process is explained in the flowchart (Fig. 9).

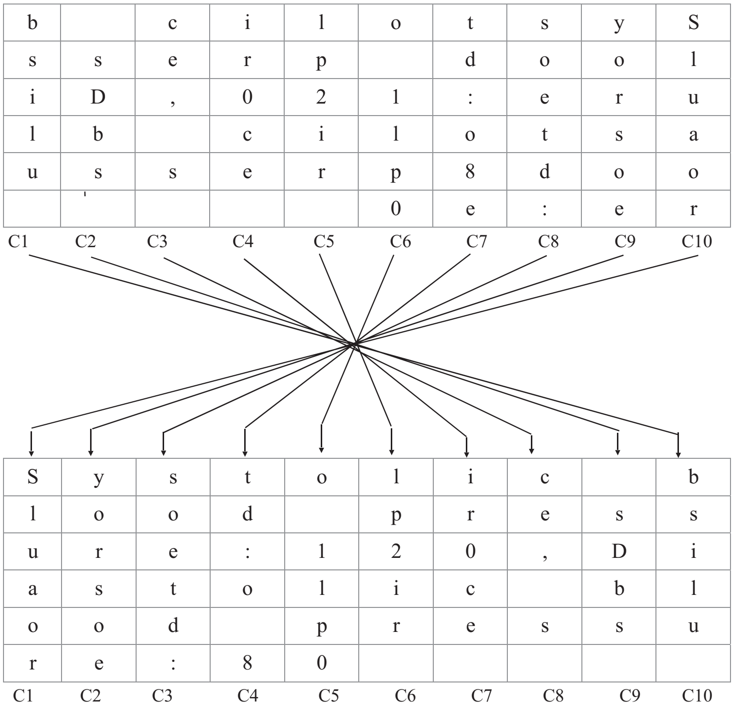


b				l	o			y	S
s	s			p				o	l
i	D			2	1			r	u
l	b			i	l			s	a
u	s			r	p			o	o
					0			e	r

b		c	i	l	o	t	s	y	S
s	s	e	r	p		d	o	o	l
i	D	,	0	2	1	:	e	r	u
l	b		c	i	l	o	t	s	a
u	s	s	e	r	p	8	d	o	o
					0	e	:	e	r
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10

FIG. 6

Inverse transposition method to decrypt message.

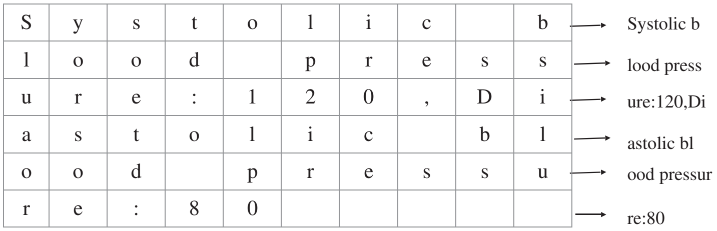


b		c	i	l	o	t	s	y	S
s	s	e	r	p		d	o	o	l
i	D	,	0	2	1	:	e	r	u
l	b		c	i	l	o	t	s	a
u	s	s	e	r	p	8	d	o	o
					0	e	:	e	r
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10

S	y	s	t	o	l	i	c		b
l	o	o	d		p	r	e	s	s
u	r	e	:	1	2	0	,	D	i
a	s	t	o	l	i	c		b	l
o	o	d		p	r	e	s	s	u
r	e	:	8	0					
C1	C2	C3	C4	C5	C6	C7	C8	C9	C10

FIG. 7

Mapping process.



S	y	s	t	o	l	i	c		b	→ Systolic b
l	o	o	d		p	r	e	s	s	→ lood press
u	r	e	:	1	2	0	,	D	i	→ ure:120,Di
a	s	t	o	l	i	c		b	l	→ astolic bl
o	o	d		p	r	e	s	s	u	→ ood pressur
r	e	:	8	0						→ re:80

FIG. 8

Fetching original message from the table.

4 Conclusion

The development of e-Health mobile application using cloud environment has proved to be very useful in monitoring and managing patient's clinical data. The security of patient's data using e- Health mobile application is an important area of concern. The e-Health mobile application interacts with cloud environment to save patients' critical health data in cloud database securely. The study in this paper

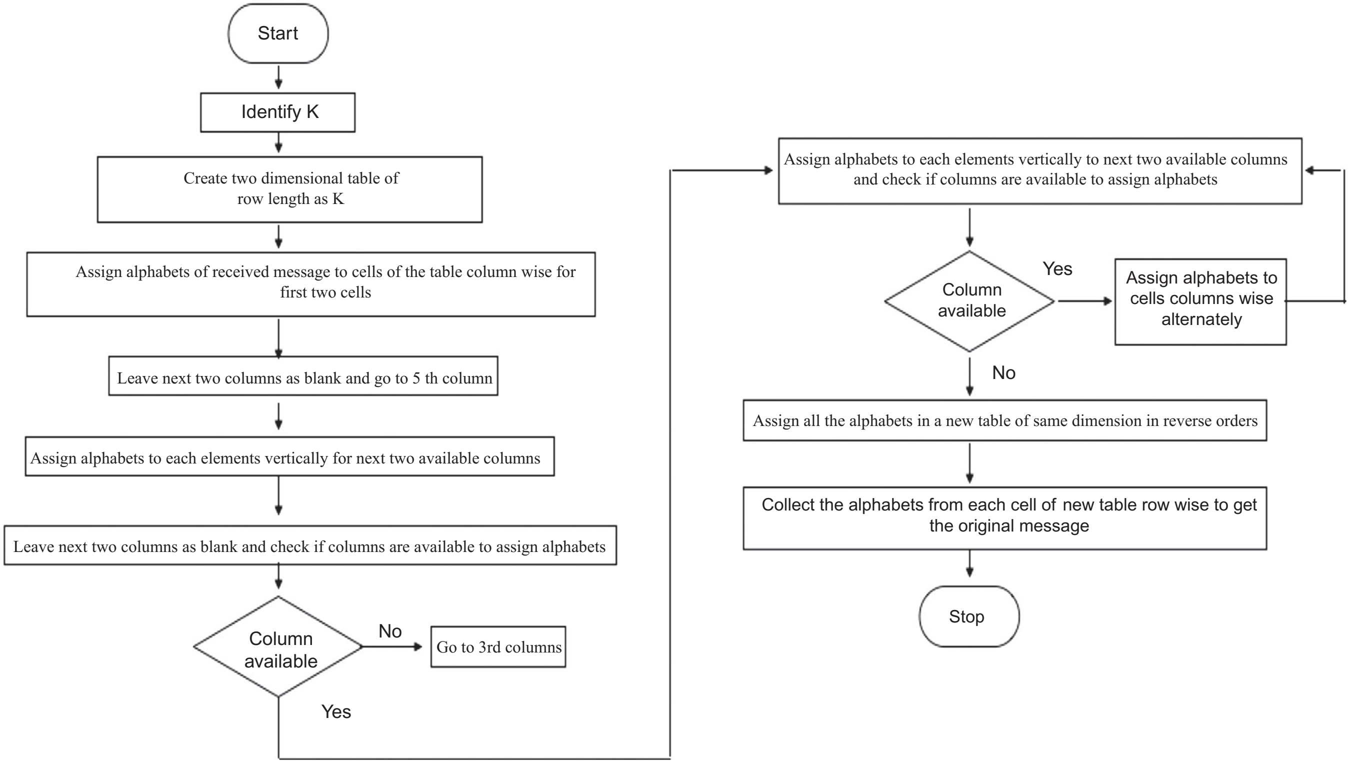

Start
Identify K
Create two dimensional table of row length as K
Assign alphabets of received message to cells of the table column wise for first two cells
Leave next two columns as blank and go to 5 th column
Assign alphabets to each elements vertically for next two available columns
Leave next two columns as blank and check if columns are available to assign alphabets
Column available
No
Go to 3rd columns
Yes
Assign alphabets to each elements vertically to next two available columns and check if columns are available to assign alphabets
Column available
Yes
Assign alphabets to cells columns wise alternately
No
Assign all the alphabets in a new table of same dimension in reverse orders
Collect the alphabets from each cell of new table row wise to get the original message
Stop

FIG. 9

Flowchart of decryption process using improved reverse transposition method.

shows that the connectivity between e-Health mobile application and cloud web server can be secured using ciphers. The reverse transposition cipher can be used to secure data in cloud environment. The effectiveness of encryption and decryption technique depends on the difficulty level it presents to hackers to decode the original message. The improved reverse transposition cipher has suggested an effective technique to encrypt and decrypt data. In further studies, this cipher can be compared with other ciphers available in today's world in terms of efficiency. The proposed improved transposition cipher can be used for performing encryption, decryption, hashing, or digital signatures. The proposed cipher can be used in digital certificates used in e-Health application and cloud server for authentication and handshaking to initiate https connectivity between the client and the server.

References

Abbas, A., Khan, S.U., 2014. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE J. Biomed. Health Inform. 18 (4), 1431–1441.

Apple Siri Webpage, 2015. "Apple Siri Webpage." [Online]. Available: https://www.apple.com/ios/siri/.

Atzori, L., Iera, A., Morabito, G., October 2010. The internet of things: a survey. Comput. Netw. 54 (15), 2787–2805.

Avancha, S., Baxi, A., Kotz, D., 2012. Privacy in mobile technology for personal healthcare. ACM Comput. Surv. 45 (1), 1–54.

Ayofe, N., Charles, A., Vyver, V., 2019. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egypt. Inform. J. 20 (2), 97–108.

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., 2019. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access 7.

Chung, K., Kim, J.C., Park, R.C., 2015. Knowledge based health service considering user convenience using hybrid Wi-Fi P2P. Inf. Technol. Manag. https://doi.org/10.1007/s10799-015-0241-5.

Curetogether, 2020. http://curetogether.com/.

Deutsch, T., Gergely, T., Trunov, V., 2004. A computer system for interpreting blood glucose data. Comput. Methods Programs Biomed. 76, 41–51.

Dong, N., Hugo, J., Pang, J., 2012. Challenges in e-Health: From enabling to enforcing privacy. In: Foundations of Health Informatics Engineering and System. Springer, Berlin, Germany, pp. 195–206.

Ferna'ndez, A.J.L., Senõr, I.C., Lozoya, P.Á.O., Toval, A., 2013. Security and privacy in electronic health records: a systematic literature review. J. Biomed. Inform. 46, 541–562.

Google Now Webpage, 2015. "Google Now Webpage." [Online]. Available: http://www.google.com/landing/now/.

Ibrahim, B.M., Singhal, M., 2016. A secure framework for sharing electronic health records over clouds. In: IEEE International Conference on Serious Games and Applications for Health (SeGAH), Kyoto, Japan, pp. 1–8.

Jung, H., Chung, K., 2016. PHR based life health index mobile service using decision support model. Wirel. Pers. Commun. 86, 315–332. https://doi.org/10.1007/s11277-015-3069-8.

Kadhim, K.T., Alsahlany, A.M., Wadi, S.M., Kadhum, H.T., 2020. An overview of patient's health status monitoring system based on internet of things (IoT). Wirel. Pers. Commun. 114, 2235–2262.

Kanrar, S., Mandal, P.K., 2017. E-health monitoring system enhancement with Gaussian mixture model. Multimed. Tools Appl. 76, 10801–10823.

Kaur, P.D., Chana, I., 2014. Cloud based intelligent system for delivering health care as a service. Comput. Methods Programs Biomed. 113, 346–359.

Komninos, A., Stamou, S., 2006. HealthPal: an intelligent personal medical assistant for supporting the self-monitoring of healthcare in the ageing society. In: 4th International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications (UbiComp 2006), California, USA, September 17-21.

Kuo, A.M., 2011. Opportunities, challenges of cloud computing to improve health care services. J. Med. Internet Res. 13 (3), e67.

Lee, E., Kim, C., 2014. An intelligent green Service in Internet of things. J. Converg. 5 (3), 4–8.

Malhotra, A., Som, S., Khatri, S.K., 2019, February. IoT based predictive model for cloud seeding. In: 2019 Amity International Conference on Artificial Intelligence (AICAI). IEEE, pp. 669–773.

Metri, P., Sarote, G., 2011. Privacy issues and challenges in cloud computing. Int. J. Adv. Eng. Sci. Technol. 5 (1), 001–006.

Microsoft, 2015. “Microsoft Cortana Webpage.” [Online]. Available: http://www.windowsphone.com/en-us/how-to/wp8/cortana/meetcortana.

Mumrez, A., Tariq, H., Ajmal, U., Abrar, M., 2019. IOT-based framework for E-health monitoring system. In: International Conference on Green and Human Information Technology (ICGHIT).

Nanayakkara, N., Halgamuge, M., Syed, A., 2019. Security and Privacy of Internet of Medical Things (IoMT) Based Healthcare Applications: A Review. International Conference on Advances in Business Management and Information Technology, Istanbul, Turkey.

Ogasawara, A., 2006. Energy issues confronting the ICT sector. Sci. Technol. Trends 21. Quarterly Review No. 20.

Pandey, S., Voorsluys, W., Niu, S., Khandoker, A., Buyya, R., 2012. An autonomic cloud environment for hosting ECG data analysis services. Futur. Gener. Comput. Syst. 28, 147–154.

Rodrigues, J.J.P.C., Lopes, I.M.C., Silva, B.M.C., La Torre, I.D., 2013. A new mobile ubiquitous computing application to control obesity. SapoFit. Inform. Health Soc. Care 38 (1), 37–53.

Samsung, 2015. “Samsung S Voice Webpage.” [Online]. Available: http://www.samsung.com/global/galaxys3/svoice.html.

Santos, P., Varandas, L., Alves, T., Romeiro, C., Casal, J., Lourenço, S., Santos, J., 2015. A pervasive system architecture for smart environments in internet of things context. In: ICMI 2015: XVII International Conference on Multimodal Interaction, London, United Kingdom, January 19–20.

Santos, J., Rodrigues, J.J.P.C., Silva, B.M.C., Casal, J., Saleem, K., Denisov, V., 2016. An IoT-based mobile gateway for intelligent personal assistants on mobile health environments. J. Netw. Comput. Appl. 71, 194–204. https://doi.org/10.1016/j.jnca.2016.03.014.

Selvaraj, S., Sundaravaradhan, S., 2020. Challenges and opportunities in IoT healthcare systems: a systematic review. SN Appl. Sci. 2 (1), 139.

Seol, Y.-G., Kim, E.L., Seo, Y.-D., Baik, D.-K., 2018. Privacy-preserving attribute-based access control model for XML-based electronic health record system. IEEE Access 6, 9114–9128.

Shin, D., Shin, D., Shin, D., 2016. Health: Ubiquitous healthcare platform for chronic patients. In: International Conference on Platform Technology and Service (PlatCon).

Shojania, K.G., Jennings, A., Mayhew, A., Ramsay, C.R., Eccles, M.P., Grimshaw, J., 2009. The effects of on-screen, point of care computer computer reminders on processes and outcomes of care. Cochrane Database Syst. Rev. https://doi.org/10.1002/14651858.CD001096.pub2, CD001096.

Silva, B.M.C., Rodrigues, J.J.P.C., de la Torre Díez, I., López-Coronado, M., Saleem, K., 2015. Mobile-health: a review of current state in 2015. J. Biomed. Inform. 56, 265–272.

Sravani, D., Vinod Nayak, B., Ravindra Babu, J., 2017. IoT based patient health monitoring system. Int. J. Sci. Eng. Technol. Res. 5 (35), 7327–7330.

Sugarstats, 2019. https://sugarstats.com/.

Tudiabetes, 2019. http://www.tudiabetes.org/.

Vishwakarma, S.K., Upadhyaya, P., Kumari, B., Mishra, A.K., 2019, April. Smart energy efficient home automation system using IoT. In: 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). IEEE, pp. 1–4.

Wang, T., Shao, K., Chu, Q., et al., 2009. Automics: an integrated platform for NMR-based metabonomics spectral processing and data analysis. BMC Bioinform. 10, 83.

Wang, F., Shi, T., Li, S., 2019. Authorization of searchable CP-ABE scheme with attribute revocation in cloud computing. In: IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC).

Wicks, P., et al., 2010. Sharing health data for better outcomes on patients like me. J. Med. Internet Res. 12 (2), e19.

Xie, Y., Wen, H., Wu, B., Jiang, Y., Meng, J., 2019. A modified hierarchical attribute-based encryption access control method for mobile cloud computing. IEEE Trans. Cloud Comput. 7 (2).

Xiong, N., 2019. Application of artificial intelligence technology in decision support software. In: International Conference on Virtual Reality and Intelligent Systems (ICVRIS) IEEE.

Zhang, C., Zhu, L., Xu, C., Lu, R., 2018. PPDP: an efficient and privacy-preserving disease prediction scheme in cloud-based e-healthcare system. Futur. Gener. Comput. Syst. 79, 16–25.