Provide Privacy of Data and user Authentication using Efficient Encryption Technique

Sattaru Sailaja[1], Chintada Sunil Kumar [2]

Final M.Tech Student[1], Asst.professor[2]
[1,2]Dept of CSE, *Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh*

Abstract: *Security is one of most important issue over the networks and also the smart phones. As a net technology implemented and alternate security threats also appear in the network. By overcome those type of security threats attacks we can implement cryptography techniques. Now days so many cryptography techniques are available in the market for performing encryption and decryption process. Most of the mobile operating system has been added this type of encryption process for protect their customer and mobile data. But implementing these algorithm face the problem of performance issues that discourage users from using them. Most of the time by implementing these encryption and decryption process will take more time. Though these encryption policies quite capable of securing mobile data, due to lack of proper management time, they are not used by users. By overcome these problems we can implement an efficient encryption and decryption process. In this paper we are propose matrix sub parts shifting transpose technique for encryption and decryption of mobile data. By implementing this technique we can overcome time complexity and also consumes less CPU power for encrypt, decrypt the system.*

Keywords: *Cryptography, One time password, privacy, mobile platform, Encryption and Decryption.*

I. INTRODUCTION

Now a day's security of data places an important role for every platform. In a mobile platform to provide security of transferred message through network is an important and also face the problem of authentication. Before providing the security of data each user will be identify by each other, after that we can provide privacy of transferred message. In the security of transferred message we can use the cryptography concepts of encryption and decryption of data. By performing those operations we can implement an efficient encryption and decryption algorithm such Triple Data Encryption Algorithm, Data Encryption Algorithm and Advanced Encryption algorithm. So that most of the existing mobile operation system will use those algorithms for encryption and decryption of transferred message. But these algorithms will have some performance issues for performing encryption and decryption process. By implementing these algorithms it will take time consuming for performing encryption and decryption process. Though these encryption policies are quite capable for provide security of data, due to lack of time management, they are not used by the users. So that to overcome these security issues the researchers will implement an efficient encryption and decryption process. By implementing this process we can overcome time complexity and also provide more security.

In this paper we are implementing one of most efficient encryption and decryption process for encryption and decryption of mobile data. By using this process we can easily reduce time complexity for encryption and decryption of mobile data. Before performing the encryption and decryption of mobile data each user will be identify by them using one time password. The implementation OTP is based on password is entered by the users. By creating OTP we are using password pair base technique for generation of OTP. After generating these OTP we can send that respect mobile number and using that OTP each user verify them. The most significant of this research is that it would allow customers to encourage encryption to prevent major data theft. Most of the popular mobile operating systems have added this encryption as an option to protect their customers' data and privacy. The most significant aspect of this research is that it would allow the customers to encourage using encryption to prevent major data theft. Mobile platforms have limited resources such as battery and computing power. To obtain desired performance, applications written for mobile platforms also have to be efficient. Context provides an insight of relevant user information that can help prioritize important data. We implemented context of user information to decrease the latency of encryption algorithms.

The Remaining of this paper is organized is as follows.

ii. Gives an overview of related work.

iii. it provides implementation procedure of proposed system

iv. gives the conclusions of our proposed system.

II. RELATED WORK

Role-based access control is presented in Sandhu et al.'s seminal paper [1] where the main RBAC components (users, roles, permissions, sessions) are systematically addressed. Using this model, efficiency is gained by associating permissions with roles rather than users. This model greatly simplifies security management for administrators, and many complex security policies can be applied more easily. Bertino et al. [2] presents Temporal RBAC, which supports periodic role enabling and disabling and temporal dependencies among permissions by introducing time into the access control infrastructure. Covington et al. [3] extends the model beyond time by introducing location and system status as constraints. Moyer and Abamad propose generalized RBAC in [4]; GRBAC leverages and extends the power of traditional RBAC by incorporating subject roles, object roles, and environment roles into access control decisions. Georgiadis and Mavridis [5] and Wang [6] both present a team-based access control model that is aware of contextual information associated with activities in applications. Kumar et al. [7] summarizes previous work and formally proposes a context-sensitive RBAC model. Their model enables traditional RBAC to enforce more complicated security policies that are dependent on the context of an attempted operation; however, this model does not provide a mechanism for automatically merging new context types into existing access policies, which limits its application in distributed scenarios. McDaniel [8] gives a more generic view of contexts, suggesting that a context should be defined by its implementation. Neumann and Strembeck [9] and Lei et al. [10] also discuss some research issues in context-related security applications.

There are also some papers on security issues in distributed healthcare systems. Weaver et al. [11,12] propose a federated, secure trust network for distributed healthcare systems, which is the motivation for this paper. Zhang et al. [13] presents a delegation framework that can be used within the security framework of healthcare applications. Wilikens et al. [14] discusses how to apply CBAC to healthcare, but the model is static and not able to handle arbitrary context-dependent authorization policies.

III. PROPOSED SYSTEM

In this section we are describe the implementation process our proposed system. In this paper we are implementing an efficient encryption and decryption algorithm for provide security of mobile data. In this paper we are using matrix sub parts shifting transpose technique for encryption and decryption mobile data. Before performing the encryption and decryption process each user will send request to server for connection. After that the server will accept the connection and generate ids for individual users. Using that id each user will share the information between them. Before performing the encryption and decryption process of users it will enter username and password for login into application. After login the system will generate one time password by using password pair based technique. The implementation process of password pair based technique is as follows.

Password pair based technique:

During registration of each user will submit his password and the length of the password should be eight characters. The eight characters will be called as secret pass and secret pass will contain even number of characters. By using secret pass the system will generate one time password for each user. During login phase user enter his username an interface consisting of grid is displayed. The size of grid is 8*8 and it consists of alphabets and numbers. These are randomly placed in grid and grid will be changed every time.

a	s	d	f	g	h	j	K
q	w	l	e	r	t	y	U
z	x	c	v	i	o	p	B
6	n	8	m	A	Q	Z	S
1	W	X	2	E	D	3	C
R	4	F	V	5	G	T	B
7	Y	H	N	9	U	J	M
I	L	K	P	O	@	#	$

After generating random grid user enter into his secret pass and using that secret pass the system will generate one time password. User has considered his secret pass in terms of for generating one time password. The one time password consists of numbers, alphabets and special symbols. In the secret pass the first letter is used for select the row and second letter is used for the select the column. After select the rows and columns take interaction letter as one time password and repeat this process for complete length of secret pass. After completion of interaction process it will generate four character types of one time password will be generated.

a	s	d	f	g	h	j	K
q	w	l	e	r	t	y	U
z	x	c	v	i	o	p	B
6	n	8	m	A	Q	Z	S
1	W	X	2	E	D	3	C
R	4	F	V	5	G	T	B
7	Y	H	N	9	U	J	M
I	L	K	P	O	@	#	$

The completion of generating one time password that password will sent message to respect mobile. After that the user will get one time password and enter into verification process. The completion of verification process the user enters into encryption process and encrypts the transferred message. Before perform the encryption process the sender or user will enter respect receiver id and performing the encryption process. The implementation of encryption and decryption process is as follows.

Matrix Sub Parts Shifting Transpose Technique:

In this module each user will perform encrypt and decrypt transferred message. Before encrypt the message sender will enter destination user id and encrypt the message. The implementation process of encryption is as follows.

i) Encryption process:

1. The sender will enter transferred message.

2. Take each character from the message and convert into ascii format until completion of message length.

3. Take each ascii of character and extract the 8 bit format.

4. Reverse the each 8 bits of character until completion of message length.

5. Perform XOR operation. Take bit-1 and bit8 and perform XOR operation and stored into position-8. Similarly take bit-2 and bit-7 and XOR those bits and stored into position-7. Repeated this process for the completion of eight bits.

6. After completion of this process take those binary values and stored into 32* 32 matrix format.

7. Sub parts the 32* 32 matrix into 32*16 and take the right side of eight columns of first 32*16 and those sub part will be put into second matrix. Same process will also apply for second matrix of right side eight parts put into first matrix right side.

8. Again take the 32*16 matrix into sub parts of 32*8 and take the right side four columns of first matrix put into the right left side of second matrix. Take the left side of second matrix of four columns put into right side of first matrix. Apply this process for the completion of all sub parts matrixes.

9. Take all sub parts of matrix and again generate 32*32 matrix format.

10. Take that 32*32 matrix perform the transpose operation of rows into columns and columns into rows.

11. After completion of transpose operation take bit format data and convert into ascii values are cipher format.

After getting the cipher format data the sender will send that data to respect receiver. The receiver will retrieve cipher format and perform the decryption process it will get original plain format data. The decryption process of matrix sub parts shifting transpose technique is as follows.

ii) Decryption Process:

1. The receiver will retrieve cipher format and get each ascii values.

2. Take each ascii value and convert into eight bit format.

3. After convert all ascii values bits format and generate 32*32 Matrix format.

4. Take that matrix and sub parts into 8*8 format and take first matrix right sub parts of four columns put into second matrix left side. Take the second matrix left side and put into first matrix right side.

5. After completion of this process take those 32*8 matrixes and again generate 32*16 matrixes. Take the first 32*16 matrix right sub parts of eight columns and put into second matrix right side. Take right side of eight columns of second matrix put into right side of first matrix.

6. Take those 32* 16 matrixes and generate into 32 * 32 matrixes.

7. Take the 8 bits of data from matrix and perform the xor operation.

8. Take bit-1 and bit8 and perform XOR operation and stored into position-8. Similarly take bit-2 and bit-7 and XOR those bits and stored into position-7. Repeated this process for the completion of eight bits.

9. Reverse of eight bit of data until completion of all bits.

10. Get the each eight bit of data and convert into ascii format.

11. Take ascii value and convert into character it will get original plain format data.

By performing the decryption process the receiver will get plain format data. By implementing those concepts we can provide more privacy of transferred data and also reduce cpu power for performing encryption and decryption process.

IV. CONCLUSIONS

In this paper we are describe an efficient encryption algorithm for provide security of transferred data. Before performing the encryption and decryption of data each user will be verified by using password pair based technique. By implementing password pair based technique will be generate one time password with contain four characters. After generating one time password will be sent respect mobile through sms. By using one time password each user will be verified and perform the encryption, decryption process. In this paper we are proposed matrix sub parts shifting transpose technique for encryption and decryption of transferred data. By implementing those concepts we can verify user is authenticated user or not and also provide more security of message. So that by implementing those concepts we can overcome time complexity of encryption and decryption process and also reduce cpu power system.

REFERENCES

[1]Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman, "Role based Access Control Models," IEEE Computer, volume 2, February 1996, pp. 38-47.

[2] Elisa Bertino, Piero Andrea Bonatti and Elena Ferrari, "TRBAC: A Temporal Role-Based Access Control Model," ACM Transactions on Information and System Security, Volume 4, No. 3, August 2001, pp. 191-223.

[3] Michael J. Covington, Wende Long and Srividhya Srinivasan, "Secure Context-Aware Applications Using Environment Roles," Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies, May 2001, Chantilly, Virginia, USA.

[4] M. J. Moyer and M. Abamad, "Generalized RoleBased Access Control," 21st International Conference on Distributed Computing Systems, April 16-19, 2001, Atlanta, GA, USA.

[5] Christos K. Georgiadis, Ioannis Mavridis, George Pangalos and Roshnan K. Thomas, "Flexible Team-Based Access Control Using Contexts," Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies, May 2001, Chantilly, Virginia, USA.

[6] Weigang Wang, "Team-and-Role-Based Organizational Context and Access Control for Cooperative Hypermedia Environments," Proceedings of the Tenth ACM Conference on Hypertext and Hypermedia, February 1999, Darmstadt, Germany.

[7] Arun Kumar, Neeran Karnik, and Girish Chafle, "Context Sensitivity in Role-based Access Control," ACM SIGOPS Operating Systems Review, Volume 36, Issue 3, July 2002.

[8] Patrick McDaniel, "On Context in Authorization Policy," Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies, June 2003, Como, Italy.

[9] Gustaf Neumann and Mark Strembeck, "An Approach to Engineer and Enforce Context Constraints in an RBAC Environment," Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies, June 2003, Como, Italy.

[10] Hui Lei, Daby M. Sow, John S. Davis II, Guruduth Banavar and Maria R. Ebling, "The Design and Applications of a Context Service," ACM SIGMOBILE Mobile Computing and Communications Review, Volume 6, Issue 4, October 2002.

[11].] Alfred C. Weaver, Samuel J. Dwyer III, Andrew M. Snyder, et al., "Federated, Secure Trust Networks for Distributed Healthcare IT Services," IEEE International Conference on Industrial Informatics, August 2003, Banff, Alberta, Canada.

[12] Andrew M. Snyder and Alfred C. Weaver, "The elogistics of Securing Distributed Medical Data," IEEE International Conference on Industrial Informatics, Banff, Alberta, Canada, August 20-25, 2003.

[13] Longhua Zhang, Gail-Joon Ahn and Bei-Tseng Chu, "A Role-Based Delegation Framework for Healthcare Information Systems," Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, June 2002, Monterey, California, USA.

[14]. Marc Wilikens, Simone Feriti, Alberto Sanna and Marcelo Masera, "A Context-Related Authorization and Access Control Method Based on RBAC: A case study from the health care domain," Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, June 2002, Monterey, California, USA.

BIOGRAPHIES:

Sattaru Sailaja is student in M.Tech(CSE) in sarada institute of science technology and management, srikakulam. She has received her B.Tech from Aditya Institute of technology and management, Tekkali,srikakulam. Her interesting areas are network security, data mining.

Chintada Sunil Kumar working as a Asst Professor of CSE in Sarada Institute of Science, Technology and Management (SISTAM), Srikakulam, Andhra Pradesh. He received his **M.Tech** (CSE) from Jntuk, Kakinada. Andhra Pradesh. His interest research areas are Database management systems, Computer Architecture, Image Processing, Computer Networks, Distributed Systems. He published 4 international journals and he was attended number of conferences and workshops.