ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 6.047

Volume 5, Issue 8, August 2017

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Adoption of Crypto Encryption Techniques in Different Scenario

K. Berlin[1]
Ph.D. Research Scholar,
Dept. of Computer Science,
Alagappa University, Karaikudi – India

S. S. Dhenakaran[2]
Professor,
Dept. of Computer Science,
Alagappa University, Karaikudi – India

Abstract: ***Today's high-tech world fully depends on the technological gadgets. To speed up the functionalities of the devices, people want high speed online communications. Particularly customers mostly prefer online banking transactions for their purchases which are relying upon the secured technological transactions. To provide guarantee and confidentiality, mostly cryptography is used as a backbone of the internet based transactions. A lot of professional cryptographic techniques are functioning well to maintain secret transactions in both criteria (Symmetric and Asymmetric) such as AES, DES, Triple DES, Blowfish, RC4, RSA, etc. Even though the need of security is increasing, lose of secrets is also happening due to the hackers involvement. This paper provides the discussion of encryption techniques available for secrets. The wrangling analysis also included in social networks and real time applications to identify the tools, purpose which is helping customers to choose a better encryption mechanism satisfying their requirements.***

Keywords: Cryptography, Encryption, Confidentiality, Communication, Real time Applications, Secret Transaction.

I. INTRODUCTION

In this business world, electrical equipment is used in our everyday activities. Varieties of electronic systems are used for transaction purpose. Without the human intervention, plenty of transactions are automated by keeping confidential secret data. This is possible by making customers do their transactions without the fear of hackers.

A. Need of Encryption

In the present scenario, PM of India tries to convert our country into digital India. To make digital India successful, government of India wanted to transform India into a digitally society and knowledge economy. For, every information is digitally available. Say for banking transaction every citizen of India must have a bank account through which money transaction should happen. Similarly all sales and purchases are to be done through digital computer regarding, so that up-to-date information may be available to everyone.

Cryptography makes sure to provide the good confidentially of every transaction through the End-to-End encryption. Cryptography is used in satellite mechanism too to process the cable TV transactions. The time stamping concept also applicable in cryptography to maintains the destination delivering time.

This paper is organized as numbered below; first section is comprised the introduction part of the crypto system, the second section covers related research works, the third section displays the importance of text encryption in today's' environment, the fourth section describes the uses of text encryption mechanisms among various applications and concluded in the last section.

© 2017, IJARCSMS All Rights Reserved

II. Related Research Work

Yashpalsingh Rajput and Dnyaneshwar Naik [1] et al, authors designed algorithm for text encryption that was named as "An Improved Cryptographic Technique to Encrypt Text using Double Encryption ". In this method, input text file was encrypted twice using two different algorithms such algorithms are: 1. Substitution approach 2. Poly-alphabetic cipher technique. The authors said that their algorithm was provided good security with the help of double encryption. Through this double encryption, the authors provided a strong security against the cryptanalysis.

One efficient cryptographic scheme was designed to secure the text files by Abhishek Joshi, Mohammad Wazid et al [2]. The name of the efficient scheme is An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attack. This technique was designed for required most crucial application. The new key was generated for every new message to fulfil the encryption part. The authors maintains the good time complexity while encrypt data of proposed efficient scheme.

Ajay Kushwahaa, Hari Ram Sharmab et al, authors contributed the encryption technique for text data as selective significant data encryption, name of these designed system is A Novel Selective Encryption method for Securing Text over Mobile Ad hoc Network[3]. For the purpose of reduce the encryption time and enhance the performance, authors select the significant data to perform the encryption from the whole data. here for encryption, BLOWFISH Symmetric key algorithm used.

Nishtha Mathur, Rajesh Bansode et al, proposed hybrid encryption scheme for text data with the name of AES Based Text Encryption using 12 Rounds with Dynamic Key Selection[4]. Here authors combined the both symmetric and asymmetric crypto systems, which means they are used two algorithms such as Advanced Encryption Standard and Elliptic Curve Cryptography. Using AES 192 bit sizes of key length and 12 numbers of iterations are used for the purpose of increase the competency.

A novel data encryption algorithm designed to protect the outsourced sensitive data on the cloud system. Prakash G, Dr. Manish Prateek et al [5], the authors provided the data security in the name of "Data Encryption and Decryption Algorithm using Key Rotations for Data Security in Cloud System". Here block level data encryption was taken placed and the rotation of 256-bit key used for encrypt the data before keep it into the cloud system. Thus the authors said that their proposed method is highly efficient than the existing systems.

III. The Importance of Encryption Today

In the digital world, many sectors used encryption to manage the electronic transactions without fail. Because encryption has made people to trust the web security. Cryptography provides strong key to regulate better online commercial transactions. After the creation of RSA, people are making their communication secretly and also it achieves great secured transaction that is online based purchases. For website security, encryption plays a big role to preserve the secrets between the server and clients. Encryption gives more confidence to people who are interested to place their transactions in web. The following web based sectors are using text encryption, which are mobile devices, business purpose, banking sectors and firewalls like securing web connections.

A) Security in Mobile devices

Today people run their life with the handset to communicating with each other. Strong security is needed here for every handset to avoid problems like information hacking. Lot of mobile devices is launched in the market by different companies. Security is one of the essential things of mobile devices. So before purchasing, the customers should check out whether the handset is having the capability of adopting security technology. Strong password security is required here to increase the data security. Two different kinds of encryption methods are considered for smart phone devices,

© 2017, IJARCSMS All Rights Reserved

1. End-to-End Encryption
2. Encryption of stored data

Both kind of encryption were designed to avoid unauthorized access. Here End-to-End encryption provides strong security service; it restrains the secret messages from the third party even it may be phone designers or app designers. After the execution of end-to-end encryption, third party like a group of terrorist and hackers have difficulty to access the message through decryption. Apple's messaging App has offered this kind of end-to-end encryption and decryption; no one can take. Second type of encryption is made by the encrypted software which encrypts the messages keys here on devices itself. This kind of mobile phone encryption is designed for law enforcement calls, which means to catch terrorist, kidnapers. Google and Apple companies have offered such kind of encryption to obey the order of law enforcement.

B) Security in Business

The U.S National Cyber Security [6] says that, 60 percent of mid-level companies are affected by different group of hackers which takes months of time to recover the cost. Physically small companies need $6, 90,000 and mid-level corporate companies need $1million to release from cyber-attack problems. So they need to do the following task to prevent their secret data from hackers.

1. Should maintain the company network with proper security software - Need to protect the system with updated version of anti-virus software, operating systems.
2. Eliminate nonessential links- which means; through the small links hackers abduct the secrets. So avoid unwanted links from e-mail, online post etc.
3. Achieve the Encryption on secrets- based on the key to safe the secrets is called as encryption. Two methods of encryption are there, first one is hardware based and second one is software based. Hardware based encryption is safe the data through the processors, in software encryption, software is installed to encrypt secret. Compare the both, hardware encryption is faster.
4. Scan before use of USB- through the external devices, virus and worms easily infect the informative systems. So scan properly with the malware detector.\

C) Companies losing their business by hacking

Hackers contribute their innovations through out of every secret; most of the top companies are lost their money and client's secret information. Some companies are listed here, that are: Sony, RSA Security, Citigroup, some of the government websites, etc. The table below depicts the hacking report of companies to understand the type of hacking.

TABLE I Companies affected

S.No	Name of the Company	Who hack the details	Date of Hacking	Amount Loosed	Loss of information
1.	Sony	LulzSec	April – June 2011	$171 million	77 million accounts
2.	Citigroup	Basic online Vulnerability	June 2011	$2.7 million	Stole A/C information of 200,000
3.	Stratfor	Anonymous members	Nov-Dec 2011	$2 million	90,000 credit cards, stolen secrets of 4,000 clients.
4.	FBI partner InfraGard	Cyber attack	June 2011	Not mentioned	180 user name and passwords are stolen
5.	eBay	Through the credentials of three employees	May 2014	Not mentioned	Information including encrypted passwords of 145 million users.
6.	Anthem subsidiary	Click a link of phishing e-mail	February 2015	Exceed $100 million	78.8 million records of customer were stolen
7.	LinkedIn	Peace	June 2016	Not mentioned	167 million user accounts were stolen

© 2017, IJARCSMS All Rights Reserved

8.	MySpace	Peace	June 2016	Not mentioned	360 million data stolen

IV. APPLICATIONS OF ENCRYPTION

The means of encryption is to convert the customer's message into unreadable format using mathematical techniques. Applications that are frequently used by the people are listed below: WhatsApp, Facebook Messenger, Line, Telegram, Viber, Hangouts, Google Allo, WeChat, IM+, Signal, Snapchat etc. Few of them are discussed below:

TABLE II Frequently used Apps

Name of the Messenger	No of Users	Usage cost	Name of Encryption	Designed For	Cross-Platform
WhatsApp	1 billion	Free	End-to-End Encryption	Text,photos,videos,documents,location,voice calls	Yes
Telegram	100 million	Open source	End-to-End Encryption for secret chats	Messages, photos, videos,files of any type	Yes
Line	170 million	Freeware	Letter Sealing Mechanism	Photos,videos,voice messages,contact,location information	Yes
Signal	3.62 million	Open Source	Validated Cryptographic Algorithm	Text, Voice, Video Chat	Yes
WeChat	963 million	Free	Client to server and server to client Encryption made	Text, Voice and video calls, moments, photo sharing, games	Yes
FaceBook Messenger	900 million	Free	Combination of End-to-End Encryption and message countdown clock	Text, photos, videos, free calls	Yes

A) Encryption Mechanism in WhatsApp

The team of WhatsApp done a great job to increase the security is known as End-to-End Encryption. Here with this technology, intruder can't able to do the intake of secrets other than the senders and receivers. TextSecure is an open source application for encrypted messaging that was designed by Open Whisper System. TextSecure application is used in WhatsApp to establish end-to-end encryption. Use of the end-to-end encryption technology, message is encrypted between user's device and WhatsApp Servers before being decrypted.

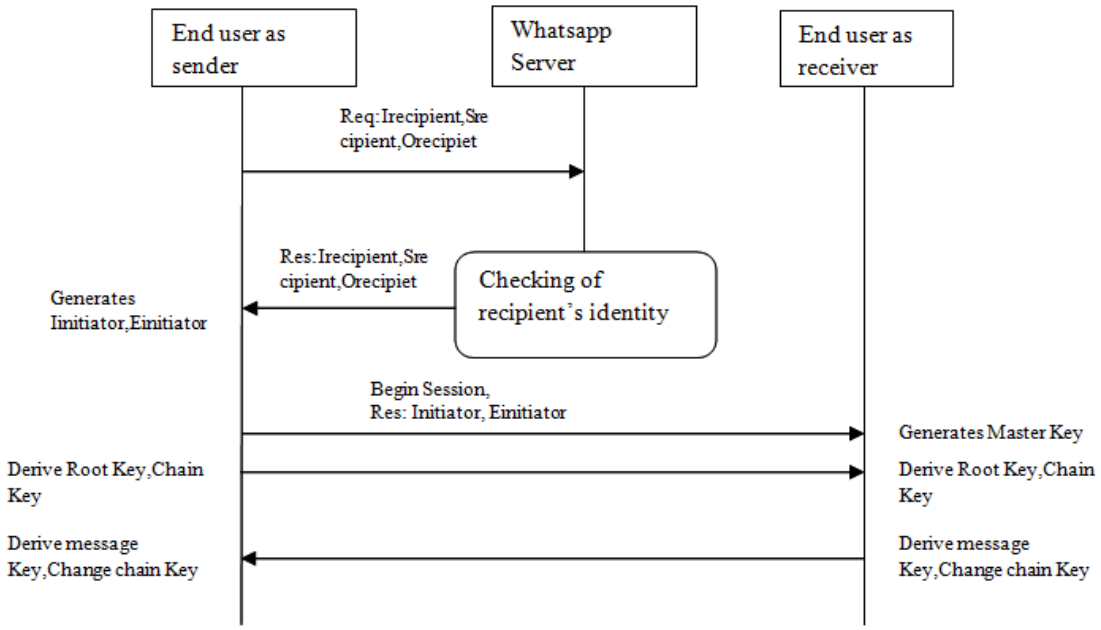

Fig. 3 WhatsApp end-to-end Encryption

The diagrammatic representation of Fig1 clearly depicts the flow of end-to-end Encryption that is used by the WhatsApp App. The initiator requests the identity key, signed pre key, one-time pre key in public for recipient [7]. Name of the identity key is Irecipient, the Srecipient key is working as signed pre key and the key term Orecipient is used as one-time pre key.

B) Encryption Mechanism in LINE

LINE has provided Letter sealing mechanism to ensure the security among secrets with multiple platforms and multiple data devices. This letter sealing mechanism is used to encrypt data of both text and multimedia. Each client of LINE application should have a public key given by LINE server to initiate the messaging while install the LINE app. The client's messages encrypted within the client device before entered into the LINE server and decryption is done by the appropriate receiver[10]. Three standard cryptographic algorithms are used in LINE to establish the security for secrets among the senders and receivers that are:

1. ECDH – Elliptic Curve Diffie – Hellman for the purpose of exchanging the key.
2. AES - 256 – Advanced Encryption Standard is a symmetric key Encryption mechanism, 256 bit key of AES algorithm is used to encrypt the messages.
3. SHA - 256 – 256 bit of message hashing algorithm works here to establish the shared secret key which are generated for the message encryption using AES-256.

C) Companies Permitting Customers Secrets

Huge amount of companies have offered messaging App to achieve the secret communication among users. At the same time they are also providing security mechanisms to protect their customer's secrets. However some Multinational Companies contribute strong security even can't open by itself. On the other hand, officially some company captures and maintains the secrets on their main servers for the purpose of solving problems of the customers.

TABLE III: list of Secured Apps

Name of the Company	Can Read secrets	Can't Read the secrets
Apple iMessage		✓
Kik	✓	
Facebook Messenger	✓	
WhatsApp		✓
Telegram	✓	
Signal		✓
Google	✓	
Snapchat	✓	
Line		✓
Cyber Dust		✓
Twitter	✓	
Skype	✓	

From the table it is being that the companies Apple, WhatsApp, Signal, Line, and Cyber Dust have been provided the better secrecy and confidentiality to their end users.

D) List of Encryption Technique

TABLE IV: Encryption Techniques of different Apps

S. No	Encryption Technique	Application	Hacking details
1.	AES-256 bit key	iMessage	Not hacked
2.	RC4	Twitter	Logic Captured
3.	AES-256bit,Diffie-Hellman,SHA1[8]	Telegram	Not hacked
4.	Signal Protocol using ECDH key agreement scheme.	WhatsApp	Not hacked
5.	3-DH,AES-256bit key,HMAC-SHA 256[9].	Signal	Not hacked
6.	ECDH and AES-256 bit key,SHA-256[10]	Line	Not hacked

© 2017, IJARCSMS All Rights Reserved

7.	Signal protocol [11]	Facebook Messenger	Not hacked
8.	Signal Protocol[12]	Google Allo	Not hacked

The above table shows encryption techniques that have been used by different Apps. Eight discrete Apps are listed above, appropriate crypto techniques also classified. Both symmetric and asymmetric encryption mechanisms are taken place. Mostly Apps designer prefer three techniques which are AES-256, ECDH and SHA. For crake RSA-256, brute force attack need to compute 2^{256} combinations. Even by the super computer, hackers require 33.86×2^{50} mathematic calculations per second. So exactly, hackers need to spend 9.63×10^{52} years to break. The combination of Elliptic Curve and Diffie Hellman also still working good in security aspects. SHA is a top most hashing algorithm used by lot of Applications to defense the secrets. Twitter has been using RC4, in the march 2015, RC4 cracked within 312 to 776 hours by the password recovery attack. So it is not suited for security provisions. FaceBook messenger and Google Allo have been using signal protocol to secure their customer's secrets. This protocol combines four crypto mechanisms to fulfill security perspective. Those are trible Diffie Hellman, curve25519, AES-256, HMAC-SHA 256.

V. CONCLUSION

In our society, encryption is needed for every transmission. Recently details of some of the companies and organizations were hacked by Ransomware malware and hackers needed more money to place the data again . So people should have aware of these malicious software types. In this paper, the role of encryption is covered entirely in different aspects. The encryption mechanisms that are used by the banking sector, business, social networks and Apps have analyzed clearly. Different encryption techniques evaluated based on the security aspects. Finally, this paper suggests best security mechanisms for ongoing use that are AES-256 is for encryption, Diffie Hellman and Elliptic Curve is for key exchange.

References

1. Yashpalsingh Rajput, Dnyaneshwar Naik, Charudatt Mane, "An Improved Cryptographic Technique to Encrypt Text using Double Encryption", International Journal of Computer Applications, Vol.86, No.6, pp: 24 – 28, January 2014.
2. Abhishek Joshi, Mohammad Wazid, R. H. Goudar, "An Efficient Cryptographic Scheme for Text Message Protection against Brute Force and Cryptanalytic Attacks", in International Conference on Intelligent Computing, Communication and Convergence (ICCC- 2015), Procedia Computer Science 48(2015), pp: 360-366.
3. Ajay Kushwaha, Hari Ram Sharma, Asha Ambhaikar, "A Novel Selective Encryption Method for Securing Text Over Mobile Ad Hoc Network", in 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79(2016), pp: 16-23.
4. Nishtha Mathur, Rajesh Bansode, "AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection", in 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79 (2016), pp: 1036 – 1043.
5. Prakash G L, Dr. Manish Prateek and Dr. Inder Singh, "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System", International Journal Of Engineering And Computer Science, Vol. 3, Issue. 4, April 2014, pp. 5215-5223.
6. Available: http://www.denverpost.com
7. Nidhi Rastogi, James Hendler, "WhatsApp security and role of metadata in preserving privacy", by Rensselaer Polytechnic Institute, Troy, NY, USA.
8. Available at: https://core.telegram.org/api/end-to-end.
9. Available at: https://en.wikipedia.org/wiki/Signal_(software)#Encryption_protocols.
10. Technical White Paper on "Line Encryption Overview" September 29,2016. Available at: https://scdn.line-apps.com/stf/linecorp/en/csr/line-encryption-whitepaper-ver1.0.pdf.
11. Technical White Paper on "Messenger Secret Conversations" July 8, 2016. Available at: https://fbnewsroomus.files.wordpress.com/2016/07/secret_conversations_whitepaper-1.pdf.
12. Available at https://en.wikipedia.org/wiki/Signal_Protocol.

AUTHOR(S) PROFILE

K. Berlin, received her M.Phil degree in Alagappa University, Tamil Nadu. Now she is pursuing her Ph.D (Computer Science) research in the same university. The field of her research is data security in cryptography. Four Research papers are published in Journals and Conferences.

S. S. Dhenakaran, a faculty member is working in the Department of Computer Science, Alagappa University, Tamil Nadu, India. He has acquired a doctoral degree in Computer Science and Engineering during 2008. Completed post graduation in mathematics during 1984, PG degree in computing during 2003. To his credit, he has more than 95 articles in international journal and conference. His field of research is Data Security using Cryptography. His familiar research fields are Optimization Techniques, Algorithms and Data mining.

© 2017, IJARCSMS All Rights Reserved