A REVIEW ON DATA ENCRYPTION TECHNIQUES USED FOR SOCIAL MEDIA ON INTERNET

1NEHA SHARMA, 2SURENDRA YADAV, 3BRAHMDUTT BOHRA

1M.Tech Scholar, Dept. of Computer Science, Maharishi Arvind College of Engineering & Research Center, Jaipur
2Head, Dept. of Computer Science, Maharishi Arvind College of Engineering & Research Center, Jaipur
3Asst. Prof, Dept. of Computer Science, Maharishi Arvind College of Engineering & Research Center, Jaipur
E-mail: 1nsharma.13111992@gmail.com, 2syadav66@yahoo.in, 3brahmdutt.bohra@gmail.com

Abstract— In today’s scientific world the demand of new technologies based on software is increasing rapidly and on a large scale. These technologies are therefore used and implemented in computers and smart phones or any other such electronic device. With the advancement of computing environment there is an immense need of protecting it as well. We all know that today most of the people have their accounts on Google, facebook, whatsapp and other means of social media. But the question at the same time arises that how much secure our personal information is on these social media sites. In order to protect ourselves from any kind of unauthorized or malicious attacks we need to protect our data as much as we can. For data protection we need to encrypt it. In this paper we shall study some of the conventional encryption methods, importance of encryption, encryption used on social media and phones and the growing need of encryption with time.

Keywords— Cryptography, Symmetric Encryption, Asymmetric Encryption, Public key, Private Key.

I. INTRODUCTION

Every user wants to secure their data and personal information from hackers and any other harmful attacks on their social media accounts. For doing this there occurs a crucial need of a special technique called Cryptography. Cryptography is generally cited as “the learning of private”[1]. Cryptography helps securing the data storage and transmission with the goal that only intended user can see it. It keeps the data completely hidden from the third party who is actually present at the same time. It is about analyzing the protocols which are associated to knowledge safety for instance information secrecy, access control, data reliability and validation.

Cryptography includes following important terms:
- **Plain Text** - It is the original text on sender’s side.
- **Cipher Text** - It is the encoded text of the main text.
- **Encryption or Enciphering** - The procedure of transforming clear text to encrypted text is Encryption.
- **Decryption** - The method of changing secret message code back into ordinary readable form of message is Decryption.

1. Types of Encryption

1.1 Symmetric Encryption- In this method identical keys are used on sender side for encoding of plain text as well as on receiver’s side for decryption of cipher text.

1.2 Asymmetric Encryption-In this method two different keys are used i.e. public key is used on sender’s side or encryption and on the other hand private key is used by receiver for decryption where Receiver has the public key of the sender. Public key is shared by everyone whereas Private key is kept secret by the only user who owns it.

Figure 1: Diagram showing Symmetric Encryption

Figure 2: Diagram showing Asymmetric Encryption

II CONVENTIONAL ENCRYPTION METHODS INTRODUCTION

2.1 Triple DES

The cipher key size of original DES was sufficient when the innovation of that algorithm took place but with the enhancement of computational power the scope of growing Brute Force attacks increased with time. Triple DES is just an advancement of DES with increased key size with a motive of preventing it from any kind of such attack, without a requirement to build a fully innovative block cipher design. The concept of Triple DES algorithm includes a bundle of key which contains 3 DES Keys namely K₁, K₂ & K₃. Each key is of 56 bits(apart from parity bits). Triple DES consisting of three dissimilar keys contains a key length of 168 bits. It has three keys each of 56 bit key length but because of meet in middle attack it provides a protection of only 112 bits. Another version called 2-Key TDES uses K₁=K₃
thus reducing key size to 112 bits and storage length to 128 bits. The major limitation of this algorithm is its slow performance in software. Triple DES algorithm is valuable in its own way, reason being its unique key length, which is longer than most key lengths affiliated with other encryption modes [4].

2.2 IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM)

2.2.1 Introduction

It has been a covert key encoding algorithm and is applicable in marketable and monetary applications. International Data Encryption algorithm is an enciphering algorithm for chunk code planned by Xuejia Lai and James L and it was first portrayed in 1991[5]. It is a trivial extended version of a former secret message, PES (Proposed Encryption Standard). IDEA was initially called IPES (Improved PES). The new algorithm was applied as the uniform code in premature class of the Pretty Good Privacy cryptosystem. It keeps away from the uses of any come upon tables or X-Boxes.

Explanation of IDEA

This chunk code algorithm works with 64-bit clear text and secret code blocks. It is managed by a key containing 128 bits. The basic idea for designing it is the use of actions from three different arithmetical groups. The replacement trunks and the connected table research used in the lump cipher obtainable up to now have been totally averted. The configuration of the algorithm is selected such that, with the exclusion that diverse key sub-blocks are used, the encipher method is similar to decode method.

Advantages of IDEA algorithm:

- It provides a high level of security
- It is easily understandable and fully specified
- It is easily available.
- It can be used efficiently
- It may be exported worldwide

2.3 Blowfish

A proportional lump cipher which can be adequately applied for enciphering and defending of raw facts is termed as BLOWFISH. It was established by Bruce Schneie and was first disclosed in the year 1993[6]. It fashioned as a quick and free option to accessible predictable encipher method. It is license-free and non-proprietary and is obtainable universally for all. It is a Fiested set-up performing iteration around straightforward enciphering action 16 times. The block size is 64 bits, and the key-length can be up-to 448 bits. Actual encryption of data has its own significance in large microprocessors. It works quicker than the majority of encipher methods when executed on 32-bit circuitry with huge cache. Blowfish operates with a large number of sub-keys. It is the most important task to pre-compute these sub-keys before operating on any data enciphering or deciphering methods.

2.4 CAST-128

It is a planned process for proportional encryption algorithm designed by Carlisle Adams and Stafford Tavares. It consists of a classic Fiested set-up which operates in 16 rounds in order to convert 64 bit plaintext to 64 bits of cipher text. The size of key is variable ranging from 40 bits to 128 bits in 8-bit augmentation. For encryption of data, first the plaintext block is partitioned as left-half and right-half segments. The algorithm consists of 8 rounds. In every round the right half segment is joined with certain key matter using function f. This material is then XORed with left half segment to figure the new right half. The initial right half becomes the new lefthalf. Following 8 rounds, the two halves are joined to form the cipher text.

2.5 RC2

It is an algorithm which has variable key size and it was designed by Ron Rivest. It consists of a volatile sized key of 64 bit block cipher formed to be a restoration of DES. This methodology has a key of flexible length ranging from 0 bytes to the maximal length that the computer organization ropes. Its velocity of encryption is free of its key size.

III ENCRYPTION USED ON SOCIAL MEDIA AND PHONES

Both concepts cryptography and Steganography have a safe method – AES algorithm is a very safe and sound technique for these two phenomenons, which are helpful for regularity sphere of influence, and are highly protected [3]. Communication between two parties on social media is done through various messaging apps such as Whatsapp, facebook messenger, snap chat etc. There needs to be a law in order to encrypt the messages that are sent on net. Encryption provides secure data communication and transmission over internet. Various efforts in the field of encryption used by social media companies to mid-2013, with the fallout from the revelations of Snowden is a turn. Some Applications like Telegram were designed so as to Provide end-to-end encryption following the announcements and applications like whatsapp pursued the trend, partially to hold market share and partially because it would not let them answer to the law enforcement agencies for their requests of data and other information which they actually wanted. In shared media applications, the meaning of E2EE encryption states that the encrypted data can be read only by sender and receiver as the solution to decipher the information is kept only with the user who concludes it. None of the other party has the capacity to decrypt data even when it travels through server. Where some apps may use encryption not all of the apps on net use end to end encryption.
In certain mobile applications like messenger of Facebook, process of encryption is employed only to
the figures in transfer whereas functions like snap
chat encode only facts in transit whereas messages
once read by the receiver are then deleted from the
server. Two types of encryption i.e Symmetric as well
as asymmetric encryption are used on Social media.

IV. NEED OF ENCRYPTION

Due to accelerated growth in both computer
technologies and Internet, the safety measures of
information are considered as one of the most
significant factors of Information Technology and
Intelligence [2]. With the invent of social media on
internet the means of communication also grew with
time. Earlier there were email lists and bulletin
boards which allowed the people to collect and share
the information across the globe. But today we have
much advanced applications on internet though which
we can communicate with each other and can
exchange our information all around the world. But
with this advancement there is a drawback that the
data is not secure on social media as we can share
almost everything like text, pictures, video, audio etc.
Even if we try to keep our information safe by doing
personal settings in privacy, our information will be
kept hidden only by the persons whom we don’t want
to show it. Rather all the information is collected by
the owner of the site. It is the procedure of
transforming normal information (called plaintext)
into muddled text (called cipher-text) [7]. So if we
work with shared grid services it is vital to know the
confidentiality and safety issues that they lift. Prior to
working on any public networking site it becomes
crucial to realize how they compose us exposed and
further take initiatives to defend ourselves and public
we do job with. Hence there raises a need of
encryption of data to make ourselves free from any
kind of malicious attacks as much as we can.

V RECENT TECHNIQUES USED ON SOCIAL
MEDIA FOR ENCRYPTION

5.1 Facebook

This social media site has developed various complex
systems which work in the back end so as to keep the
user absolutely secure from attacks. Facebook has
even created some advanced features by which user
can protect them such as Distant Logout and OTP
(One Time Passwords). Such attributes are helpful
when one is not sure about the security of the network
or computer systems. Two such features that are new
in technology are:

5.1.1 A Secured Connection

Whenever the user does online shopping or accesses
ebanking, he/she could have noted a “security device”
sign that appears in the address block or that the
address block turns green. It reveals that the portal the
user is using is completely protected link (“HTTPS”) to
converse with the site and ensures that the message
one sends persists as confidential. The application
Facebook at present uses (“HTTPS”) when secret
code of user is delivered to it.

But now Facebook provides the user the facility to get
familiar to facebook completely over HTTPS. User
should think about empowering this choice if he/she
commonly uses facebook form anywhere like public
places or at home. The alternative exists as a element
of superior safety attributes which user can discover
in “Account Security” segment of the Account
Settings page. It is very important to make the user
account secure on facebook because once it is
hacked, the personal information of user can be
retrieved by the hacker and he can misuse it to a large
extent. Facebook provides ample number of options
to make user account safe from various malicious
attacks. Various spams can also affect user account in
many ways which is really very harmful. Concept of
HTTPS works really well and is very crucial for
safeguarding data and personal information of user.

There are a few things one should keep in knowledge
and should be aware previous to determining to
facilitate HTTPS. Enciphered pages take a very long
time to load, as a result user gets to know that
Facebook is lazy using HTTPS. In totaling certain attributes counting various
third party functions are not presently backed in
HTTPS. Facebook ensures to solve these remaining
issues in the near future.

5.1.1 Social Authentication

Facebook has intended to place citizens at the
midpoint of all its stuffs and to devise each
occurrence the user keeps on the website to be
societal. Facebook wants to bring social design to an
extended level where user may get more safety.
Public verification is the most recent attempt towards this objective. People using Facebook on large scale do not often have security problems. However if Facebook notices doubtful movement on the account of any user like if one has logged in from California at day time and after few hours from Australia, then Facebook may enquire the user about his/her individuality so that Facebook can make sure that account of user hasn’t been bargained. Facebook including various other social sections use a confront reply check termed as Captcha in their listing or procuring stream. The objective of this experiment is to make sure that the one operating is a mortal and not a computer betting the organization. Conventional Captchas have massive shortcomings sometimes difficult to decode and because they are only intended to protect against outbreaks by computers which are vulnerable to computer operators.

**Figure 5: Figure showing Captcha on Facebook**

Sometimes instead of showing traditional captchas Facebook may test the user in another way, where it may ask about the identity of the user’s friends by showing them their pictures. In this way we can ensure that even if might know user’s password but he would never know user’s friends identity.

### 5.2 Whatsapp

Facebook’s forecasting service Whatsapp intended to enlarge its sheltered messaging service as a result of which, tone calls are also eniphered adding to its accessible isolation attributes. The assistance has near about one billion monthly users. This messaging app has been providing powerful encoding to the people who use it since 2014, creating it very tricky for the establishment to discover the messages of its service. This matter is private for the creator Jan Koum who was born in Soviet-era Ukraine. Whatsapp already offers IPhone and Android users encrypted messaging. It has also planned to provide users encrypted voice calls, group messages etc. That would make Whatsapp very difficult to be tapped by authorities. Whatsapp also has planned to announce officially about its extended encoded aids. Whatsapp encryption code is basically planted on rules designed by a famous retreated missionary Moxie Marlinspike whose protected messaging app is worn by safety belligerents.

#### 5.2.1 What is the Concept of Whatsapp web?

Whatsapp can also be accessed through computers by its service messaging app known as Whatsapp web. This service uses QR code to verify user’s identity instead of email id and user name. It does-not even need any password. User’s smart-phone is his key to use whatsapp web. QR code is a 2 dimensional bar code that can work much efficiently and can store more information than a 1dimensional bar code. The information can be retrieved simply by scanning QR code with user’s smart-phone application. QR codes are now available for marketing, inventory and other related purposes.

#### 5.2.2 How does the QR CODE works?

When user first creates a whatsapp account, he/she only needs to enter the phone number and verify it. Now since whatsapp is allowing users to access their account via computers it needs to verify the user’s account properly and authenticate them. Steps that the user needs to follow are as follows:

1. Go to web.whatsapp.com on your browser on computer. Important point is whatsapp web only supports Mozilla Firefox, Google Chrome or open browsers.
2. On the main screen user will view a QR code. It is dynamic in nature i.e. it will change every moment or in a few seconds.
3. Open whatsapp on your smart-phone. Important point is whatsapp mesh is accessible for Blackberry, Windows phone 8.0 and 8.1, Android, i-phones and other Smart phones.
4. Click on ‘More Options’ and click on whatsapp web.
5. Open whatsapp on your smart-phone. Important point is whatsapp web is available for Blackberry, Android, Windows phone 8.0 and 8.1, Nokia S60, Nokia S40 Single SIM EVO, iphones, BB10 Smart-phones.

**Figure 6: Figure showing QR Code on Whatsapp Web**

6. Open whatsapp on your smart-phone.
7. Click on ‘More Options’ and click on whatsapp web.
8. From the screen click on ‘+’ symbol on the top right corner to open the scanner.
9. Using this scanner, scan the QR Code on your browser screen to complete the authentication process.
10. Now you will be able to view your whatsapp chats on your computer screen as well. Important thing is you need a fast and secure internet
A Review on Data Encryption Techniques Used For Social Media on Internet

5.3 Amazon
Data protection refers to protecting data when it is in transmission phase and at rest. Data in transmission phase can be protected using SSL client side encryption. One has following options for securing stationary data in Amazon S3.

5.3.1 Server Side Encryption
User can demand Amazon S3 to encode his/her entity prior to discounting it on disc and decode it when user has to download the object.

5.3.2 Client Side Encryption
Users can encode data on the side of client and can transfer the encoded data to Amazon S3. Here user can administer encoded keys, encryption procedure and its devices. Amazon encrypts user data using 256 bit AES encryption also known as AES-256. User can apply encrypt the data stored using Amazon S3’s set or Condensed Repetition cache choices. The whole process of encoding, managing key and decoding searched and checked privately in frequent intervals of time as a part of Amazon’s existing audit process.

CONCLUSION
In this paper existing conventional encryption methods have been studied and analyzed. It is also analyzed that all techniques are crucial for real time encryption. We have also studied current encryption done on social media and phones and the urging need of encryption in the social world on internet. Every day innovative encoding system is developing and hence conformist enciphering tools will always exercise at a faster and high rate of security.

REFERENCES

★★★