IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue, 6, March 2019 E-ISSN: 2347-2693

Study on Securely Digitalizing Crime Records by using RSA Algorithm

M. Nagaraju Naik[1*], S.Muni Kumar[2], J.S. Ananda Kumar[3]

[1]Dept. of Computer Science, S.V. University, Tirupati, India
[2, 3]KMM Institute of P.G Studies, Tirupati, India

Corresponding Author: nagarajubank@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si6.167169 | Available online at: www.ijcseonline.org

***Abstract*—**Crime Records are exists in Police Stations. Crime Records are enable to find crimes and their involved criminals. In the existing system they are using a FIR for maintain the crime and criminal details. It contain a less security and easy to perform fraud. The record has been updated manually every time. The main objective of this system is providing security to data, by using the RSA algorithm. It contain the two keys based security. In this, crime and involved criminal details are stored in database in the form of encrypted data. Criminal details such as (name, address, etc,) are stored in the Ciphertext format. So that we can speed up investigation process as soon as possible. Highly impossible to decrypt data who are unauthorized to access crime data. Through the using this system witnesses can easy to access and generate the reports. We can providing a security to witnesses data by using RSA algorithm. If any person performing misleading activities to on crime data they can't access plain text and difficult to change cipher text to plain text.

***Keywords*—**RSA, Encrypt, Decrypt, Ciphertext, Crime, Criminlas.

I. INTRODUCTION

In Crime Record Management System every police station have a police officer(writer) for write FIR (First Information Report) it is very difficult to maintain records. In the proposed system we can avoid all the difficulty in the system. The main aim of this proposed project is providing security to a data. In this system all the criminal and their involved crimes data will be processing encryption (i.e., converting the plain text into a cipher text). After we can store the data into database

If witnesses need to give report for any crime based information they need to consult near police station. Through the using this system witnesses can easily providing information. By using RSA algorithm to protect data about witnesses and they provided information. RSA is asymmetric key based algorithm it contain public key and private key. For encrypt the data we can using the public key, decrypt the data based on using private key. Public key act as shared key.

Crime Investigator can access the data form database using their authentication credentials. Investigator can access the reports, are generated by the witnesses and police officer(writer). Investigator have authority to modify the data (i.e., update, delete and etc.,) this data is helps to investigator to speed up their investigation process and identify the criminals easily.

Securing Digital Crime Records Using RSA Algorithm is web based application that organise the data and various information about the criminals and their crimes. For the easy retrieval data from database, that are stored in various levels. By performing less efficiency to gathering information about particular crime. Providing user friendliness and helps to investigators to find the criminal in rapid manor. It refers suggestion form for providing ideas to investigators.

The main purpose of choosing RSA algorithm is, that contain 1024-bit key and also algorithm processing using asymmetric key, it exists two key to encrypt and decrypt the data. It have a less throughput than the DES and also low confidentiality.

II. RELATED WORK

Anu Sharma, [1] suggested a system that crime records can be stored in database. It can replacement of files.The potency of the Police andthe effectiveness with that it tackles crime relyon what quality of knowledge it will derive from itsexisting records and the way quick it will have access toit. Limitation of this is they can't providing security to a data(i.e., they can store actual data into database).

Richard Adderley, [2] suggested a crime analysis and investigated using the computer. By comparing two different crimes is easy to done to analysis then providing information of those crimes. He can apply an artificial intelligence technique to identifying the difference and tracking crime rate in the society. He performing mining techniques to automatic detect patterns in crime reports. Through using various algorithms, to mining data then

performing comparison with other crimes. Finding relation between the current occur crime with old recorded crime details.

Ms. Pooja.Bahule, [3] author proposed e-police mechanism To increase the efficiency for accessing the crime record securely. e-police follows centric approach when service is delivered. It provides accuracy and alert notification about case details. By managing secure crime record as time complexity will reduce to solve the cases. By giving the awareness about the consequences of crime , it reduce crime ratio.

Sandeep D, [4] suggestedglobel criminal record it is useful to police to access information of criminals. He proposed scanning based system to identify the criminals. Through the using scanner for scanning fingerprints to identify criminals. It can performing searching criminals matching criminal files. It overcome the heavily maintain of records. Fingerprint scanner can done two tasks; copy the image of fingerprint and compare fingerprint with available fingerprint in database

Nentawe Y. Goshwe, [5] suggested data protection in application running over network. Using public key method on RSA algorithm it convert actual information or data into not understandable(cipher text) before decryption. Describe using two key system it contain one key for encryption and another key is used for decryption. This algorithm is used to key exchange and digital signatures. The graphical user interface is designed to user friendly, to encryption and decryption data using GUI interface.

M. Preetha, [6] suggested difference between various cryptography algorithms. Provided information as in RSA contain two types of methodologies if public key and private act as same key then this methodology is called symmetric key encryption. If public key is differ as private key them this methodology called as a asymmetric key encryption. He provided information about AES as based on substation-permutation. It as fixed block size. BLOW FISH is symmetric key cipher.it is an alternative to the DES and associated easy to other algorithms. DES (Data Encryption Standard) provide a standard method for protecting important
and commercial data. It performing only two operations bit shifting and bit substitution.

III. METHODOLOGY

There are many ways to done cryptography process. We can classified based on keys number to processing encryption and decryption. The two common types of algorithms are:

A. Secret Key Cryptography :

The secret key cryptography used single for both encryption and decryption. It can generated two types of cipher text they are stream cipher and block cipher. Stream cipher performing(operate) single bit at a time and block cipher operate one block of data at a time
The main drawback of secret key cryptography is propagation error because a distorted bit in transmission.

B. Public Key Cryptography:

Public Key Cryptography schema uses one key for encryption and another key for decryption.. In public key encryption, one of the keys is generated public it will advertising all the world another key is generated private key it never wants other.RSA is implemented first and still using this public key cryptography.

RSA algorithm worked based on asymmetric crypto algorithm. In this algorithm contain two keys they are public key and private key. The name itself signifying that public key is given to everyone and private key need to maintain private. For example of asymmetric cryptography a client sends its public key to server then perform request data from server. The server will perform encryption through using user provided public key and sends the encrypted data to user. By using private key to decrypt data.

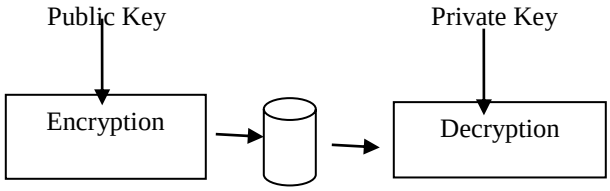

Figure 1: RSA Encryption and Decryption Process

Like banking applications, transaction are not done in safely manner, for such applications RSA is work more efficient. The RSA algorithm is very difficult to factor large numbers. If very large numbers are used as a prime numbers it will generating result double length of the given number. Attacker needed a long time period for break the code.

1) Algorithm

Police Officer/ witnesses

Key Generating

Step1: Choose two prime numbers suppose p and q
Step2: finding public key
Step2.1: public key (n) = p*q
Step2.2: choose one small exponent e
But must e as

- Integer
- Not factor of n

- 1<e<pie(n)

Step2.3 public key is generated of n and e
Step3: finding Private key
Step3.1: find pie(n):
Pie(n) = (p-1)*(q-1)
Step3.2: cal private key as d:
d = (k*pie(n)+1) / e

Encryption Data

Stpe1: convert letters as numbers
Step2: encrypted data c = $\mathbf{actual\ data^{e}\ mod\ n.}$

Decryption Data

Step1: access encrypted data
Step2:decrypted data=$\mathbf{encrypted\ data^{d}\ mod\ n.}$

IV. PROPOSED SYSTEM

Securing Digital Crime Records Using RSA we can performing encryption and decryption operations. This system access plain text or actual data from the user it performing encryption then the data is stored into database. Authorized person(s) can access only actual information, unauthorized person(s) try access information they get only cipher text. If person have public key not possible to decrypt the data

In this paper it provides core level information about previous crime information details and how to protect data and how to access data securely. It allows to implements new ideas in this system as a result it is easy to track crime information. It provide guidelines and ability to give the feedback with effective graphical interface. It have to compatible to use same software in another system so that it is migratable.
First we can gather the information from police officer and peoples in the form of a plain text. In the background process using public key it was generating the cipher text by using server to store cipher text in database. If the investigator need data from database it will performing authentication first. If he/she is authorized person they performing the decryption using private key(Authorize person have the private key)

V. CONCLUSION AND FUTURE SCOPE

In this paper the study of existing Crime Record Management System and disadvantages of the system. It contain a solutions for those drawbacks. Though the using this system police officers, common peoples and investigators work pressure is reduced. It providing user friendly nature and easy to understand the non technical persons. The main use of this system is protecting the information using RSA algorithm. If any attacker performing attack on server they get only cipher text it is highly impossible to decrypt the data. Using this system investigator rapidly performing their investigation process.

REFERENCES

[1] Anu Sharma 1 ,Mohd. Shahnawaz 2, *" Crime Record Management System*", 3rdInternational Conference on System Modeling & Advancement in Research Trends (SMART) College of Computing Sciences and Information Technology (CCSIT) ,TeerthankerMahaveer University , Moradabad , page **6-9**, October **2016.**

[2] Richard Adderley, *"Police Crime Recording and Investigation System",* Policing An International Journal Of Police Strategies And Management, **24(1):100-114**, March **2001**.

[3] Ms. Pooja.Bahule, Ms. Nisha Maria Abraham, *"E-Police System"* , International Journal of Engineering Research & Management Technology, Volume **2**, Issue-**1**, January- **2015**.

[4] Sandeep D. Nawale, Ms. Poonam C. Songra*, "Online Criminal Record"*, Global Journal of Computer Science and Technology, Volume **12**, Issue **8**, April **2012**.

[5] NentaweY .Goshwe ,*"Data Encryption and Decryption Using RSA Algorithm in a Network Environment"*, International Journal of Computer Science and Network Security, VOL.**13** No.**7**, July **2013.**

[6] M. Preetha1 , M. Nithya2 *, "A Study And Performance Analysis Of Rsa Algorithm"*, International Journal of Computer Science and Mobile Computing , Vol. **2**, Issue. **6,** June **2013**.

