Secured Database Using Encryption Methods

Mr Sathisha G[1], Mehaboob Pasha[2]
[1]Asst,Prof.,Dept of Computer Science & Engineering
[2]Dept of Computer Science & Engineering
[1, 2] Atria Institute of Technology, Bangalore

Abstract- *Security of Data is the most significant undertaking in the present world. Throughout the years different encryption plans have been created so as to shield the database from different assaults by the gate crashers. This paper disks the significance of database encryption and makes an inside and out survey of different database encryption systems and analyse them on premise of their benefits and negative marks.*

Keywords- Database Security, Encryption methods, Cryptography,Hashing algorithms, Security breach, Data encryption.

I. INTRODUCTION

Right now, innovation, all our work is finished by the PCs. From talking with companions on person to person communication sites, to making on the web instalments through Net banking everything is being done online through computers. Since these offices are effective and make our work simple, we use them in one way or the other. This way to utilize these online administrations we are putting away the entirety of our own and delicate information in the databases of these sites and applications. which in fact make this information inclined to different security threats. So, insurance of this significant client information is one of the major priorities, in request to dodge any abuse of information. Approval and Authentication are two factors that are utilized to shield the information from the f Side) that is being gotten to by the client, which implies whether an individual has the options to access while validation implies distinguishing there by and large done by the utilization of username/password.Another significant method for ensuring and encoding the information being spared in the sites. Right now, will examine the encryption plans proposed by various study their benefits and negative marks of these plans

II. ENCRYPTION OF DATA IS NEEDED

The need of scrambling the information before sparing it in a database is that by confining the entrance through approval and verification of information can help to a specific cut-off, yet imagine a scenario in which the interloper some way or another gets to the database. He has all the information of database and can abuse it as he like of information before sparing it in database becomes an integral factor. On the off chance that the information is encoded before sparing it in the database, even with access to the database the interloper can't abuse this information. Fig 1,show how the gate crasher can get to the substance of database

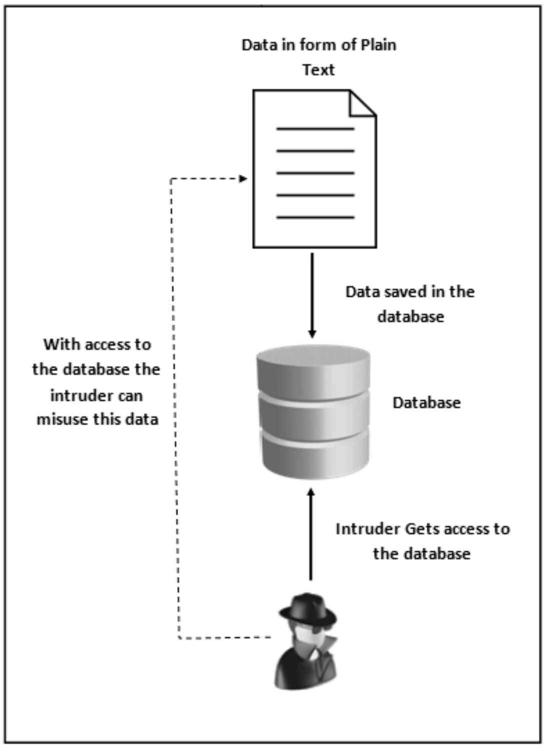

Data in form of Plain Text
Data saved in the database
With access to the database the intruder can misuse this data
Database
Intruder Gets access to the database

Fig 1.Intruder accessing the content of database

III. DATABASE ENCRYPTION

Database Encryption is a procedure of scrambling the information in the database. It is a key technique to secure the substance of information inside the database. The fundamental thought behind this is in-case the interloper some way or another can get to the database of the framework because of encryption he ought to have the option to abuse the information in the database.

Fig 2. shows essential working of the database encryption also, decoding process. The plain content/information to be spared in the database is first changed over into figure content utilizing a fitting calculation and a particular key. At that point this figure content is spared into the database. At the point when the client needs to separate the information from the database, the figure content is changed over back to plain content utilizing the unscrambling calculation and a similar key utilized in encryption. This will restore the plain content to the client, when mentioned

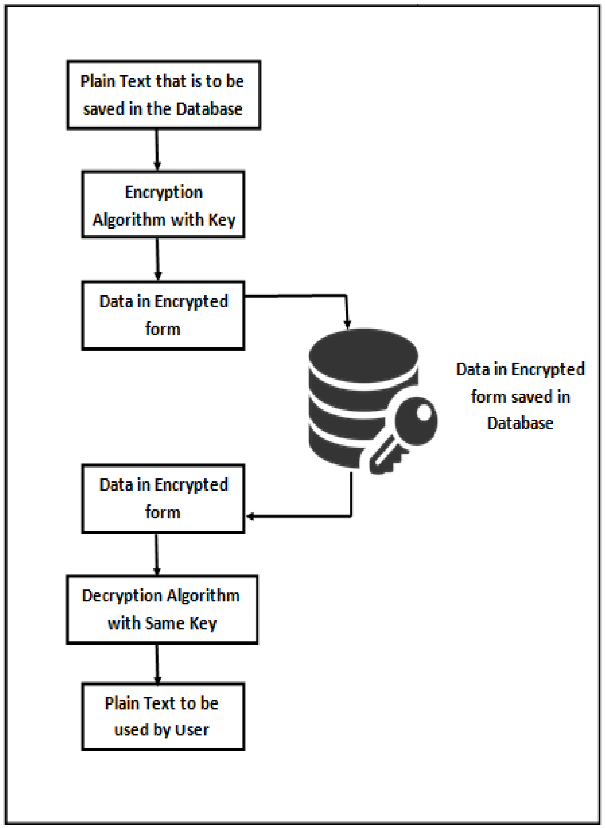

Plain Text that is to be saved in the Database
Encryption Algorithm with Key
Data in Encrypted form
Data in Encrypted form saved in Database
Data in Encrypted form
Decryption Algorithm with Same Key
Plain Text to be used by User

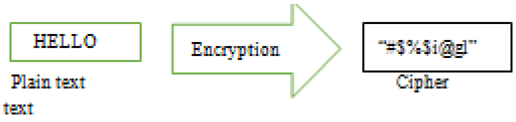
Fig 2. Database Encryption and decryption Process

IV. ENCRYPTION METHODS

Encryption can be done in two possible ways.

A.Cryptographic Encryption
B. Hashing

Encryption: Encryption is a procedure that encodes a message or document with the goal that it tends to be just be perused by specific individuals. Encryption utilizes a calculation to scramble, or encode, information and afterward utilizes a key for the accepting party to unscramble, or decode, the data. The message contained in an encoded message is alluded to as plaintext. In its encoded, garbled structure it is alluded to as ciphertext.



Despite the fact that encoded information seems irregular, encryption continues in a coherent, unsurprising way, with the goal that a gathering getting the scrambled information and possessing the key used to encode the information can unscramble the information, transforming it again into plaintext. Really secure encryption will be perplexing enough that an outsider is profoundly far-fetched to decode the ciphertext by animal power – at the end of the day, by speculating.

Encryption Techniques

1. Symmetric Cipher Model
2. Substitution Techniques
3. Transposition Techniques

A1. Symmetric Cipher Model: A symmetric encryption plot has five fixings. Plaintext, EncryptionAlgorithm, Secrete key, Ciphertext, Decryption algorithm. Simplified structure explained by fallowing Fig 3.

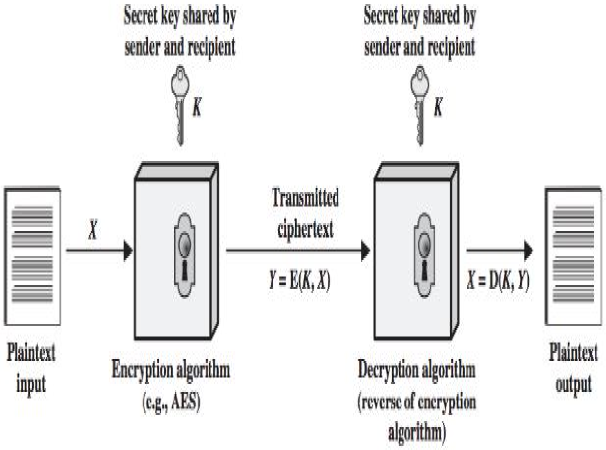

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig3: Simplified view of ConventionalEncryption

Most commonly used encryption algorithms are DES,RC2, RC4,RSA, AES_128, AES_256 etc.

For example: AES encryption and decoding clarified through square chart. Fig 4.

The Rijndael proposition for AES characterized a figure in which the square length and the key length can be autonomously determined to be 128, 192, or 256 bits. The AES particular uses a similar three key size 2options yet restricts the square length to 128 bits

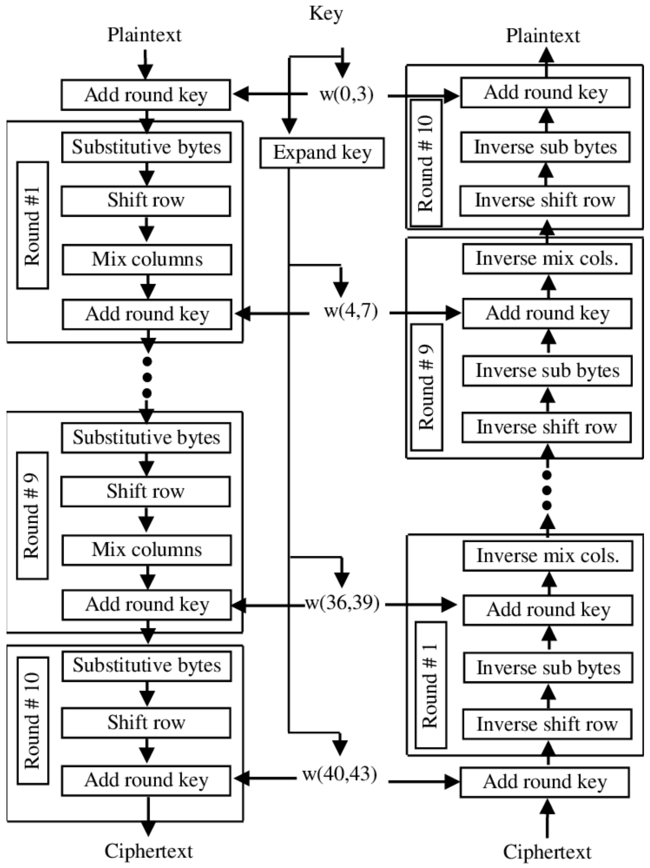


Fig 4: AES encryption & decryption Block diagram

A2. Substitution Technique:

A substitution method is one in which the letters of plaintext are supplanted by different letters or by numbers or images.

On the off chance that the plaintext is seen as a succession of bits, at that point substitution includes supplanting plaintext bit designs with ciphertext bit designs.

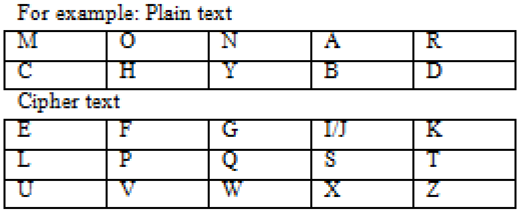
- Caesar cipher
- Mono/Poly alphabetic ciphers
- Playfair cipher
- Hill cipher
- One-time pad
- Rotor machines
- Steganography

Caesar cipher: The Caesar figure includes supplanting each letter of the letters in order with the letter standing three places further down the letter set.

For instance,

Plain text:	MEET	ME	AGAIN
Cipher text:	PHHW	PH	DJDLQ

Playfair cipher: The most popular numerous letter encryption figure is the Playfair, which treats diagrams in the plaintext as single units and makes an interpretation of these units into ciphertext diagrams. The Playfair calculation depends on the utilization of a 5 x 5 lattice of letters developed utilizing a catchphrase.



For example: Plain text

M	O	N	A	R
C	H	Y	B	D

Cipher text

E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Hill Cipher: The encryption calculation takes m progressive plaintext letters and substitutes for them m ciphertext letters. The substitution is controlled by m straight conditions in which each character is appointed a numerical worth (a = 0, b = 1 ... z = 25).

As a rule, terms, the Hill framework can be communicated as follows:

$$C = E (K, P) = KP \bmod 26$$
$$P = D (K, P) = K1C \bmod 26 = K1KP = P$$

As with Playfair, the quality of the Hill figure is that it totally shrouds single-letter frequencies. Indeed, with Hill, the utilization of a bigger grid conceals more recurrence data. Along these lines a 3 x 3 Hill figure conceals single-letter as well as two-letter recurrence data.

Mono/Poly alphabetic cipher: Another approach to enhance the straightforward monoalphabetic method is to utilize diverse monoalphabetic substitutions as one continues through the plaintext message. The general name for this methodology is polyalphabetic substitution figure. Every one of these systems share the accompanying highlights for all intents and purpose:

1. A lot of related monoalphabetic substitution rules is utilized.
2. A key figures out which specific principle is picked for a given change

For example:

key:	deceptivedeceptivedecep
Plaintext:	werwdiscoveredsaveyour
Ciphertext:	ZICVTWQNGRZGVTWA

One-Time Pad: Each new message requires another key of the equivalent length as the new message. Such a plan, known as a one-time pad, is unbreakable. It produces irregular yield that bears no factual relationship to the plaintext. Since the ciphertext contains no data at about the plaintext, there is just no real way to break the code.
For example:

ciphertext: ANKYODKYUREPFJBYOJDSPLRE
key: pxlmvmsydofuyrvzwctnlebnecvgdupa
plaintext: mr mustard with the candlestick in hall

A3. Transposition techniques:

All the procedures inspected so far include the substitution of a ciphertext image for a plaintext symbol. A totally different sort of mapping is accomplished by playing out a type of stage on the plaintext letters. This system is alluded to as a transposition cipher. The least complex such figure is the rail fence method, in which the plaintext is recorded as a grouping of diagonals and afterward read off as an arrangement of lines. For instance, to encipher the message "meet me after the robe party" with a rail fence of profundity 2, we compose the accompanying
The encrypted message is:

MEMATRHTGPRYETEFETEOAAT

An unadulterated transposition figure is handily perceived on the grounds that it has a similar letter frequency as the first plaintext. For the kind of columnar transposition just appeared, cryptanalysis is genuinely clear and includes spreading out the ciphertext in a lattice and messing with section positions. Diagram and trigram recurrence tables can be valuable. The transposition figure can be made altogether more secure by performing more than one phase of transposition. The outcome is a progressively mind-boggling stage that isn't effectively reproduced.

For example.

Key: 4 3 1 2 5 6 7
Input: t t n a a p t
m t s u o a o
d w c o i x k
n l y p e t z

output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

A4. ROTOR MACHINES:

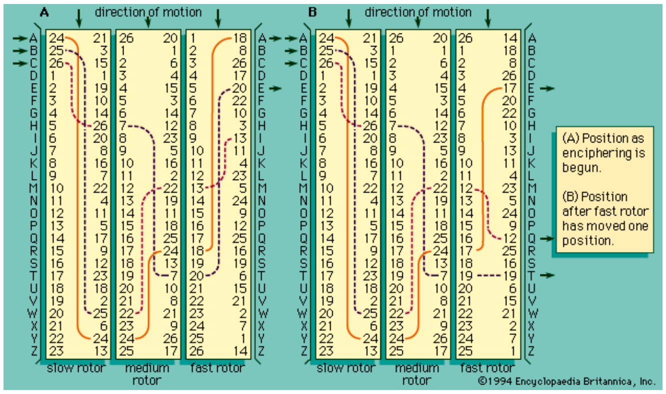

A
direction of motion
B
direction of motion
slow rotor
medium rotor
fast rotor
(A) Position as enciphering is begun.
(B) Position after fast rotor has moved one position.
©1994 Encyclopaedia Britannica, Inc.

Fig 5. Rotor machines.

The fundamental guideline of the rotor machine is delineated in Figure 4 The machine comprises of a lot of freely pivoting chambers through which electrical heartbeats can stream. Every chamber has 26 information pins furthermore, 26 yield pins, with interior wiring that associates each info pin to a remarkable yield pin. For straightforwardness, just three of the inner associations in every chamber are appeared.

A5. Steganography:

A straightforward type of steganography, yet one that is tedious to develop, is one in which a game plan of words or letters inside an evidently harmless book illuminates the genuine message. For instance, the grouping of first letters of each expression of the general message illuminates the concealed message.

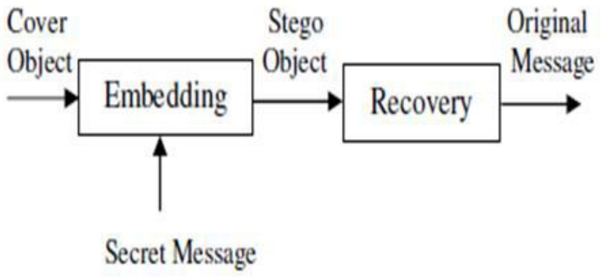


Fig 6: Steganography model

B. HASHING:

A hash work is any capacity that can be utilized to delineate of discretionary size to fixed-size qualities. The qualities returned by a hash work are called hash esteems, hash codes, digests, or essentially hashes. The qualities are utilized to record a fixed-size table called a hash table. Utilization of a hash capacity to record a hash table is called hashing or dissipate capacity tending to. Hash capacities and their related hash tables are utilized in information stockpiling and recovery applications to get to information in a little and about consistent time per recovery, and extra room just partially more noteworthy than the all-out space required for the information or records themselves. Hashing is a computationally and extra room effective type of information get to which maintains a strategic distance from the non-straight access time of requested and unordered records and organized trees, and the frequently exponential stockpiling prerequisites of direct access of state spaces of huge or variable-length keys. Utilization of hash capacities depends on factual properties of key and capacity collaboration: most pessimistic scenario conduct is deplorably terrible with a vanishingly little likelihood, and normal case conduct can be about ideal (insignificant collisions).Hash capacities are identified with (and regularly mistook for) checksums, check digits, fingerprints, lossy pressure, randomization capacities, blunder remedying codes, and figures. In spite of the fact that the ideas cover somewhat, everyone has its own uses and necessities and is structured and advanced in an unexpected way

V. LITRATURE SURVEY

Numerous scientists/researches took a shot at database encryption strategies, calculations, procedures. Right now some of them are clarified in the fallowing.

IqraBasharat National University of Sciences and Technology (NUST), H-12, Islamabad, PakistanTook study on database encryption and security distributed paper with fallowing content. Considered CIA factor to expound security of a database. CIA Which represents secrecy, Integrity, accessibility. At that point Examined about database security dangers, Encryption at various database levels. Given time for near just as observational investigation.

D. Maheshwari, A. Kaushika, A. Jenifer, Published paper on database encryption and unscrambling utilizing Hill figure calculation. They made a point by point concentrate on HILL CIPHER calculation in encryption and decoding process. They additionally referenced cryptography in detail, clarified calculation in stepwise way utilizing model in nitty gritty way.

Erez Shmueli, Yuval Elovici, Chanan Glezer, deutsche Telekom labs took a shot at database encryption and review contemporary challenges with structure contemplations. They thought about database security and assault models, while covering a wide range of encryption they referenced File framework encryption, dbms level encryption, application level, client-side encryption, and coached key administration, ordered encryption. Meanwhile they inspected chance identified with the work

VI. RESULT

This undertaking brought about improvement of a respectable dare to guarantee security in database of any organisation. The primary procedure utilized right now is encryption in which we encode the information to defeat dangers. This guarantees staggered security components of the information. This task cleared a chance to build up an application which is useful to the general public.

VII. CONCLUSION

Information to any association is a most important property. Security of touchy information is constantly a major test for an association at any level. In the present innovative world, database is helpless against hosts of assaults. Right now encryption strategies are talked about that can assist with decreasing the assaults chances and ensure the delicate information. It has been presumed that encryption gives classification. Utilizing solid encryption calculations one can decrease various level dangers. The future work could be done make encryption progressively powerful and effective.

REFERENCES

[1] https://en.wikipedia.org/wiki/Database_security 16-04-2020 10:49am

[2] Iqra Basharat, Farooq Azam, Abdul Wahab, MuzaffarNational University of Sciences and Technology (NUST)H-12, Islamabad, Pakistan, DATABASE SECURITY AND ENCRYPTION: A SURVEY STUDY. June 2012.

[3] D. Maheshwari,A. Kaushika,A. Jenifer, departmentof mathematics, sri Krishna arts and science college. A STUDY ON DATA ENCRYPTIONAND DECRYPTION USING HILL CIPHER ALG ORITHM, March 2018.

[4] Aquila G Palathingal, Anmy George, Blessy AnnThomasAnn Rija Paul, Sahrdaya College of EngineeringTechnology, Kerala, IndiaEnhanced Cloud Data Security using CombinedEncyption Steganography, March-2018.

[5] Ahmad Baraani-Dastjerdi; Josef Pieprzyk; BaraanidastjerdiJosef Pieprzyk ;ReihanedSafavi-Naini, SecurityIn Databases: A Survey Study, 1996

[6] Amichai Shulman; Top Ten Database Security Threats,How to Mitigate the Most Significant DatabaseVulnerabilities, 2006 White Paper.

[7] Tanya Bacca; Making Database Security an IT SecurityPriority A SANS Whitepaper – November 2009

[8] http://www.freetechexams.com/computerstips.computertips/database-security.html

[9] Kadhem, H.; Amagasa, T.; Kitagawa, H.; A NovelFramework for Database Security based on MixedCryptography; Internet and Web Applications andServices, 2009. ICIW '09. Fourth InternationalConference on;Publication Year: 2009, Page(s): 163 170

[10] Luc Bouganim; Yanli GUO; Database Encryption;Encyclopedia of Cryptography and Security, S. Jajodiaand H. van Tilborg (Ed.) 2009, page(s):) 1-9