IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 15, Issue 3 Ver. II (May-June. 2020), PP 64-73
www.iosrjournals.org

The Behavior of Databases in Maintaining the Security of Data Transferred Between Two Communication Points

Mohini Prasad Mishra[1], Haripriya Mishra[2]
1(Department Of Computer Science & Engineering ,Gandhi Engineering College, India)
2(Department Of Computer Science & Engineering ,Gandhi Institute For Technology ,India)

Abstract: *Keeping and controlling the security and secrecy of database data is significant in the cutting edge time as long as there are a ton of methods for entrance, surveillance, and access to information on the Internet. The significance of database security is a higher priority than the significance of information to be ensured. There are numerous available resources of security that help keep up the security of data and encryption to the level that meets the prerequisites of database security. It is notable that every office or division has its own strategy to shield its information from robbery or harm in relation to the size and sort of information notwithstanding the hand that works on such information and that the data security circumstance is in accordance with the foundation of the database.*
Key Words: *Information systems, data exchange, data classification, data encryption, ports.*

I. Introduction

Modern technologies for computers and networks have revolutionized and continue to revolutionize the world of use, dissemination, and transmission of information. The standards of behavior that databases use in the transfer and linking of databases around the world must force users to respect rights and responsibilities.
We can consider information to be a source of strength, and it is the key to prosperity for users who have access to it.

Do not forget that the information is a treasure to the hackers of the computer must be protected from Pirates of information, Do not forget that the information is a treasure to the hackers of the computer must be protected from them, the data and information must be protected whether stored in the database or transmitted directly through the channel connection on both ends of computers, one of them sent to data and other data receiver.

The electronic systems should reach the majority of international institutions, companies, workplaces and private life. Therefore, new ethical and legal decisions must be made to achieve balance and guarantee the rights of all.

II. The Ethical Issue Of Electronic Information Systems

The ethical issue is the accepted standards of behavior and the rules governing members of the profession, including information control, access, privacy and misuse of data. These extend to electronic networks and electronic databases, and more specifically, electronic information systems[1].

2.1. Electronic Copyright Law

The ease with which information is being pumped increasingly on networks is causing confusion and how copyright and intellectual property rights can be applied to electronic files. With the growing growth of networks, especially social networks, and the dissemination of information on them and the ease of sharing and use of information published without reference to the His idea, It became necessary to provide explanations on how to use electronic files, the ease with which the distribution of electronic files and the nature of some electronic information create problems under the law of copyright and intellectual property rights.

2.2. Unintended Consequences of Data Exchange

The consequences of data exchange are quite complex and point to many problems. Therefore, the database administrator must balance the security required for the data set with access to it by designing information systems carefully to prevent inappropriate access to all data or part of the data While at the same time allowing access to information exchange.

However, many basic problems arise with how information is handled, stored and manipulated in digital formats.

For us not to forget to point out here the unintended consequences of data exchange are the dissemination of errors, errors can reach the database in an unintended way shortening an employee or intentional way by pirating information and penetrating sites and publishing specific, intended and targeted data

to a specific person or institution, Published errors can at the moment create endless complications in the life of someone or cause the bankruptcy of an institution at least

2.3. Use of unauthorized Applications

Use of unauthorized applications on business networks It can put sensitive companies and applied information Staff at risk.

Email at my discretion is the most common unauthorized application to access from the work network. Online banking, online billing, shopping and instant messaging via internet applications and other applications, all pose a serious risk of data loss by the employee or data theft By pirates because they are often not controlled and do not use security standards.

In the report of the company Anzikshres Research[2].

- (78% of employees use personal email access on their computers)
- And ((63% of employees admit that they use the computer at work for personal use))
- And ((83% admit to using your computer at work for personal use))

Here we refer to it 70% of IT professionals confirm that the use of unauthorized software has resulted in half of data loss incidents in their companies.

2.4. Prevent Data Leaks

Evolve Threats to data security, The professions that are growing daily are piracy of electronic information, Pirates have become collaborators in the field of electronic penetration. Electronic piracy is a profitable project.

The risk of piracy comes largely through the Internet, which today is a vital component of all modern life magazines, from infrastructure to all life attachments.

In a risky Internet environment, data are leaking around the world despite the best efforts of IT engineers to protect data.

With ignorance, challenge and lack of simple care playing the key roles in leaking employees' data, it is very clear there is no magic solution to secure corporate data, especially "with companies and data that are more mobile and operate with virtual rather than physical boundaries.

Many companies, institutions, and even people make mistakes by placing a lot of confidence in technology alone, their trust in a security program and not updated with technology raids makes them more vulnerable to piracy and data theft.

Companies should assess employee behavior and associated risks based on several factors example (geographic location, vulnerabilities, protection of programs, security programs, etc.).

Information security must be part of the business culture of IT infrastructure, one of the steps to be taken to prevent information leaks:

- Know your private data and manage it well.
- The creation of tools and processes suitable for the movement of data and protect and facilitate the process of storage and access to and use.
- Diagnose data that needs a unique protection system inside or outside the company's firewall. The protection system here is not only electronic, but some data must provide the building protection it has.
- Use new and updated security approaches that keep up with evolution.
- Use special protection for application systems using only approved access methods.
- To protect the hardness of mobile devices by keeping them in the possession of only one person and securing them at all times, and not to use the equipment load of work for personal activities.
- Log off applications and systems when you go away from the devices and even had a few steps, to prevent unauthorized access to data.
- Speak quietly while discussing confidential information in public.
- Conduct daily business activities related to information security in accordance with the organization's rules of conduct.
- Dealing with different levels of confidentiality of documents and data, it is necessary to distinguish between (public data), (confidential data), (highly confidential data), (restricted data).

2.5. Training Staff and Employees Training Staff and Employees

To understand the challenge of protecting sensitive information, employees and data workers must be educated and trained, because data here represents money for businesses and people.

Despite the policies, procedures and security measures in place, employees around the world are involved in risky behaviors and thus expose data to danger, IT professionals must educate, and train staff and data workers on:

Avoiding security errors by highlighting and identifying vulnerable areas and reporting those responsible.
- Optimal use of systems and data protection.
- Identify computer security incidents and how to report them.
- Training employees on new data protection systems.

Assign a paragraph to the security awareness of the data when interviewing the recruitment.
Training employees about physical security concerns ((allowing staff only with their badges to enter buildings and rooms where important data is stored)).

III. Data Classification

It is necessary to have a classification of data, by identifying the most valuable data, this classification reduces the voltage and time to secure the data, it is impossible to secure and manage all data equally.
The labels differ in ways of categorizing information and data around the world.
In these papers, We use a classification and label the largest category of institutions Table
(1) This description shows.

Table 1 Classification and label

Unclassified	**Restricted**	**Secrecy**	**Highly confidential**	**Sensitive**
Data that can be shared with others	Data that is officially traded within the organization only, the disclosure of which have undesirable effects.	Data that must comply with confidentiality requirements. Their disclosure leads to damage to the institution.	Data took the effort and the cost of the in assembled. Detecting leads to serious damage.	State security data.

IV. Behavior Of Databases

A large percentage of enterprises and companies currently rely on the management of database systems in their activities and daily programs, as a result of the development in modern electronic technology, which still fascinates us every day with its development and speed of communication and data transmission and verify the authenticity of data from its original center , As well as the speed of storage and retrieval, The databases helped to complete things and accomplish the work as quickly as possible, and reduce the cadres and time and without errors and documented data. It is possible to refer to this data and to search for any record of the database records at any time without the need to record data in the papers or archives for that. You should not have access to an easy database or any person up to the unauthorized people only authorized persons to have access to the data.

There are people who are only allowed to view the data (such as publishing student results, students can only see the result without changing or affecting it), and there are people who are allowed to change and update data such as (teachers, change grades And add new degrees)[4].

4.1. The Functions of the Database Manager

- Data Definition Language (DDL).
- Storage Structure and Access-Method Definition.
- Schema and Physical-Organization modification.
- Granting of authorization for Data Access.
- Maintenance of the database.

4.2. Security Databases

The most important points that should be available when creating a database to protect or improve the required security level[7]: -

- Data availability.
- Data Integrity.
- Determining the number of attempts to access the database which may be a maximum of three attempts.
- Disable network (ping), which is in the Internet control message protocol (ICMP) and not allowing the device server that contains a database in response to the requests of this command.

V. Encrypts Data Transferred Between Two Touch Points

One of the latest developments in the field of computers used in data and information communication systems and methods of storage and processed such as emails and email and database systems and information and digital image processing audio recognition and processing systems, Where computers have become an important part of the components of communication networks through which most of the data and information networks, which require a mechanism to transfer and protect this data and information[8].

5.1. Data Security

The means and methods of security data for many information and active finally, data encryption systems that contain different types of traditional and modern codes, where traditional encryption systems, regular blades compensatory and blades The modern encryption systems standard encryption for data encryption and streamlined user and key systems[9].

Encipher Operation is designed to disguise important information in such a way that the meaning of this information becomes unclear to the unauthorized person. The information you want to hide before the encryption process is called Plaintext. The encoder is called Encipher, Ciphertext encryption or Cryptogram.

The set of steps used by the Crypto Wizard to encrypt clear text is known as the Encryption Algorithm. The algorithm's work depends on the key crypto key that enters with clear text to the algorithm[10]. This key is defined by the recipient and can retrieve the clear text from the encrypted text. The process of retrieving clear text from encrypted text using a decryption key.

Mathematically express the Encryption process in relation
C=FE(P,K)
Where C encoded text, FE cryptographic algorithm, P clear text, K encryption key.
P=FD(C,K)
Where P is clear text, FD decoding algorithm, C encoded text, K key decoded.

An encryption system is ideal when it has the ability to encrypt clear text to produce more than one understandable message when the message is decrypted by the objector. The objector does not have sufficient information to decide which understandable messages were sent. This encryption system is said to be unbreakable.

There are many cryptographic systems that can be used when transmitting live data between and among contact points:

- Encryption way napsack.
- polynomial Encryption system.
- Collective Encryption system.
- Encryption system Beating.

5.2. Port

The port can be considered as a device connecting the processor with the outside world. Through the port receives the signal from the input device and sends other signals to the output device.

Ports are defined by their addresses and are located between 0H-3FFH and a different address. These addresses are completely different from traditional memory addresses and are used only with OUT and IN to charge input and output from ports directly.

5.3. Live Data Encryption System

The design and construction of a software system for the transmission and protection of data transmitted through a communication channel on both ends of the two devices, one of which is sent and the other receiver, as any of the computers T1 or T2 are sent and other receptor data.

Both the sending and receiving computers contain the low-level software for the chosen port. The parallel port has been consistently selected for the ease of providing the physical tools to be applied in a practical way, but it can be changed to any other type. This is to use the dynamic method of selecting the port type after determining the value of its address. The two computers also contain the software protection system that contains the main interface, which contains only two options, the Close option, which closes the system and return to the operating system, and the Next option, which allows you to enter the system and to select the encryption and decryption window.

If you want to send the text in this case, the option will choose to encrypt data that unlocks the selection window encryption methods, which contains five options, the first four of which are encryption methods that have been remembered in this research which is the first choice (Encryption way napsack) and second choice (polynomial Encryption system) and the third choice (Collective Encryption system) and the fourth selection (Encryption system Beating) The choice is the fifth (Close) came out of the window And return to the encryption and decryption window.

If you want to receive text and decoding blade in this case decoded, which takes you to the selection window mode decryption that contains five options also, the first four of which option is you will need ways of decoding methods used encryption in the system, which is the first choice (Decode napsack) second choice (Decode polynomial) and the third choice (Decode Collective) and the fourth selection (Decode Beating) The fifth choice it is to close the window and return to the previous window[8].

VI. The Proposed Technique

6.1. Design of encryption algorithm for transferred data

The algorithm adopted in this study combined the two methods of encryption together, Symmetric encryption method and Asymmetric encryption method.

We have a complex encryption algorithm with a high level of confidentiality that provides data protection, As well as the protection of distributed and shared encryption keys between the two ends of the network.

Implemented encryption algorithm consists of three partial encryption algorithms, namely:

- The RSA Algorithm RSA.
- International Data Encryption Algorithm IDEA.
- Generate Key Algorithm.

6.1.1. The RSA Algorithm RSA

Is a public key algorithm that is based on the principle of its work as follows:

Divide the message into blocks, so that each block has a binary value smaller than the number N Encryption and decryption are as follows:

Encrypted text C = Me mod N

Unencrypted text M = Cd mod N = (Me)d mod N = Med mod N

Where M is the number assigned to the symbol. The keys are as follows:

public key Ku = {e, n}:

The private key Kr = {d, n}:

We get these keys as follows:

1. We select an odd number e which is part of the public key
2. We select two primary numbers p, q so that the number 1- (1-q) (1-p) is divided by e
3. where n is calculated n = p.q

Where n as we mentioned the first part of both keys.

4. where d is calculated d = (p-1) (q-1) (e-1) +1 / e It is the second part of the private key.

This algorithm is illustrated by the following example:

- We choose the individual number e=3
- We select two primary numbers p = 5 q =11 where: (q - 1) (p - 1) - 1 = 39 on the division accepts e -We calculate n = q. p = 55
- We calculate d = (p-1) (q-1) (e-1) +1 / e = 27

We have it Ku = {3, 55} Kr = {27, 55} Assuming we have 7 = M then have: Encryption C = Me mod n = 73 mod 55 = 13 encoder decoding M = Cd mod n = 1327 mod 55 = 7

In order to increase confidentiality and eliminate the problem of the distribution of keys for this algorithm, Each node of the network nodes has its own key that generates it secretly, and hence on each node, publish the public key and keep your private key and build it on there is no one, the need to devise any secret method to exchange these keys is the responsibility of securing the key on each node in isolation from the other nodes. The network contract is agreed upon, A special strategy is to change the keys which can be cyclical or when In order to raise the level of confidentiality of the approved encryption method.

6.1.2. International Data Encryption Algorithm IDEA

Is a traditional encryption algorithm called Oriented-Block that encrypts blocks of 64-bit length messages using a 128-bit key.

This algorithm works on the principle that each bit affects both the original and every bit Key in each bit in the encoded text. This is achieved by using three different processes.

Each process takes 16 bit Two entrances and produces one output of bit 16. These processes are:

- Operation XOR bit to bit.
- Collecting and taking the rest of the total divided by 216 (A + B mod 216).
- The process of taking the rest of the division to 1 + 216 (a * b mod 1 + 216).

Stage	Encryption			Decryption
	Key numbers Partial	Key numbers derived from the key	Partial keys	Derivative for
Repetition 1	Z1z2z3z4z5z6	Z{1..96}	U1u2u3u4u5u6	Z49-1-z50-z51-z52-1 Z47z48
Repetition 2	Z7z8z9z10z11z12	Z{97..128;26..89}	U7u8u9u10u11u12	Z43-1-z45-z44z46-1 z41 z42
Repetition 3	Z13z14z15z16z17z18	Z{90..128;1..25;51..82}	U13u14u15u16u17u18	Z37-1 –z39 –z38 z40-1 Z35 z36
Repetition 4	Z19z20z21z22z23z24	Z{83..128;1..50}	U19u20u21u22u23u24	Z31-1 –z33-z32 z34-1 Z29 z30
Repetition 5	Z25z26z27z28z29z30	Z{76..128;1..43}	U25u26u27u28u29u30	Z25-1 –z27-z26 z28-1 Z23 z24
Repetition 6	Z31z32z33z34z35z36	Z{44..75;101..128;1..36}	U31u32u33u34u35u36	Z19-1 –z21 -z20- z22-1 Z17 z18
Repetition 7	Z37z38z39z40z41z42	Z{37..100;126..128;1..29}	U37u38u39u40u41u42	Z13-1 –z15-z14z16-1 Z11 z12
Repetition 8	Z43z44z45z46z47z48	Z{30..125}	U43u44u45u46u47u48	Z7-1 –z9-z8 z10-1 z5 z6
Final conversion	Z49z50z51z52	Z{23..86}	U49u50u51u52	Z1-1 –z2 –z3 z4-1

6.1.3. Generate Key Algorithm

Is an algorithm entered by a statement of the number of bytes taken optionally from a generation file the keys (is a file size byte M 1 is randomly generated and sent to all network nodes , Using the RSA algorithm)based on this optional number of bytes This algorithm generates a 128-bit key that is used as the encryption key in the IDEA algorithm.

As an example of this algorithm we review the following principle of action:

- After taking the number of byte n from the generate key,a1, a2, a3...an. we increase the number from zeros to the end of this string so that the number becomes divisible by 16 and done as follows:
  - The algorithm calculates the value I=16-(n mod 16).
  - We add I zero to the end of the string where the number of bits becomes divisible by 16 : (n + I) mod 16 = 0.

- We divide this series of bytes into a partial string K where K=(n+I) div 16
- each partial string consists of byte 16.
- We generate from these strings 16 partial keys length byte 1 as follows:

o We take the first byte of the first partial string and we process it with XOR the first bytes of each partial string we get the first partial key, and the same applies to the rest of the bytes we get 16 keys in part of which 1byte consists of the sum of these keys constitutes the total key author of 128 bit.

o This particular algorithm can add to it some additions either in design or Implementation making it a privacy algorithm because the secret encryption algorithm lies in the key encryption.

6.2. Key Generator

The 128-bit key is generated by:

- Generate Key Algorithm.
- File generation keys.

The method of work:

From the key generation file we take a set of bits optionally according to the value of the displacement and a specified length is sent encoded within the letterhead of each message where the displacement is indicated on the first byte number that will be taken from the file generating keys as the length is Fidel on number of selected bytes.

Example:

If the

Displacement = 150

And

Length = 225

- This means that the key generation algorithm takes as an input its starting bytes from Byte 150 and up to 374 bytes. So we can choose probabilities of bytes as an input to the key generation algorithm and then get the number the same huge variety of keys are used in the IDEA encryption algorithm.
- It should be noted that a pointer with the message must be an indication of the integrity of the information the message and its contents did not change during the transfer process, whether the change was intentional or this indicator can be labeled as the message imprint. This fingerprint is calculated the sending party sends it with the encrypted message and is counted at the receiving end for confirmation of the message arrives correctly. The letter impression is calculated according to a single mathematical process the trend converts the entire encrypted message information to a short frame of information we call it as we mentioned the message footprint. Changing a single bit in a message leads to getting her different fingerprint. The message imputation algorithm is of a type so that if a fingerprint is known it is not possible to retrieve the message the footprint is not less than 16 byte.

6.3. The level of confidentiality of the encryption algorithm

All cryptographic algorithms that are mathematically generated are theoretically breakable. But what distinguishes them from some are the time of coverage (the time required for the fracture) that is the time of energy and the importance of information with time. But when trying to break encryption should consider the following:

- The cost of decryption does not exceed the value of encrypted information.
- The decoding time does not exceed the useful time of the information or the lifetime of the information. Consequently, as the computational power of the computers evolved, this led to a reduction in time coverage also varies according to the method of analysis used which can be:

o Random style.

o Parallel processing.

Assuming that the same key will be used to encrypt all text. An attacker can the random style is used to break the encoder, ie the experiment and the error and in this case it is the number of possibilities to try is (2^{128}) Try where is the key length of 128 try approximately user in our algorithm and this is equal to 10^{38} * 4.3.

If the attacker can experience a key for every 1 microsecond, to experience all the keys he needs 10^{25} years.
If parallel processing is used using several processors, all of them are processed

The problem is the one chip that can handle one key every nanosecond ((If possible)), it is possible to experiment with a key (10^{14}) of 1 day (10^{24} chip) to experience all the switches, which means that we need about 10^{24} chip working parallel to this rate until the detection is accomplished within one day and of course completion such a machine is not easy if it was not impossible.

The complexities mentioned were for one key used to encrypt many messages, In this algorithm, the key changes permanently and random, According to the selected value of the key generation file where the key can be changed in each message, which means that each message has its own key, So even if an attacker can detect a cryptographic key for a message, that does not mean that the encryption algorithm has been broken.

Knowing that even a person able to detect the content of the message should be:

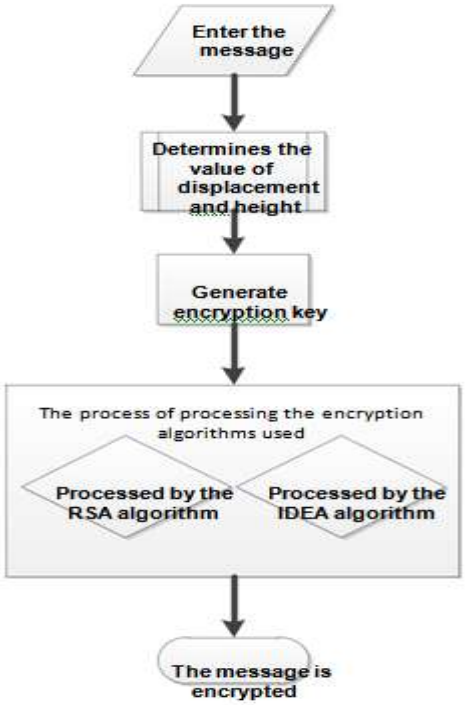
- Get file generation keys and decryption.
- He must know the values of the length and displacement-encoded by the RSA algorithm and the two topics in the header of the message.
- Break the key generation algorithm.
- Break the encryption algorithm IDEA.
- If it is very difficult to succeed in one of those steps, how can succeed in all steps and break all the algorithms together.

6.4. Stages of implementation of the proposed program for encryption

Before we start encrypting the messages by executing the algorithm we distribute the key generation file which is randomly generated as we mentioned, we distribute it on all branches of the network encrypted using the RSA algorithm in order to avoid detection of this file. This file is distributed once unless we want to change it from one time to another, We will generate another random file and send it in the same way. We can resize this file because its size does not affect the generation of keys. The encryption process is as follows:

- Determine the value of displacement and length necessary to generate the encryption key.
- The key generation algorithm Working on the key generation file, the displacement values and the length of the 128-bit random key generation will be used in the IDEA algorithm.
- The clear message is encrypted by the IDEA encryption algorithm that uses the previously generated encryption key.
- The value of displacement and length is encoded by the RSA algorithm.
- The encrypted value for both the offset and the length is added to the encrypted message header.
- In the end, the message is sent encrypted to the intended destination.

The Behavior of Databases in Maintaining the Security of Data Transferred Between Two Communication Points



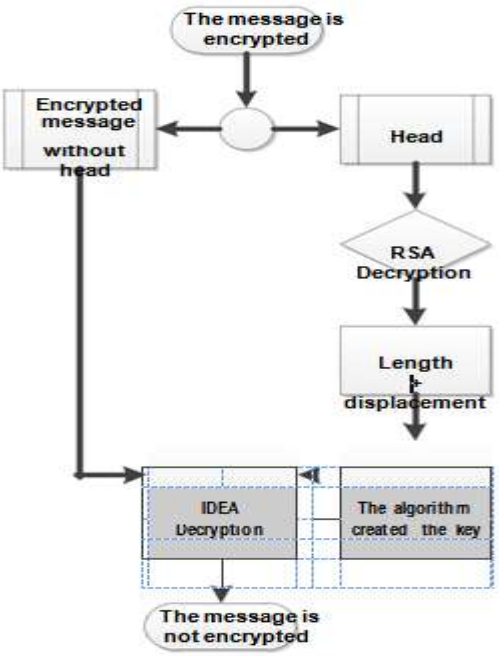
The behavior of the encryption program

6.5. The Decryption

After the encryption process is complete and the data is sent in the encrypted message, and received by the future, the algorithm performs the decryption process unlike the encryption process in the following stages:

- Separate the header from the message and make sure it is correct with the message footprint.
- The head part containing the length and displacement is decoded by the RSA algorithm.
- The key generating algorithm and depending on the values of length and displacement generates key 128 bit.

Enter the encrypted message on an IDEA algorithm that uses the 128-bit key to obtain the unencrypted message



Behavior of the decoding algorithm

VII. Results

For the future of security and to prevent the diversion of data that is a challenge at this time for most institutions and people A working structure that can be programmed with the creation of a database to measure the security of the transferred data.

The ultimate goal of this research is to secure all data whether transferred or stored in a database and achieve a secure environment for data and manage it comfortably and effectively without losing or manipulating it.

The integrity of the database is intended to preserve all data and information from damage, manipulation or unauthorized access by unauthorized persons. Data must be secure at all times, either in storage or in transit, and always available to users who are authorized to access the database.

It is important to note that power outages should not affect the information inside the data room or peripherals to ensure continuity of data flow.

References

[1]. Margaret Lynch, "Ethical Issues in Electronic Information Systems",Thesis, the University of Texas at Austin, 2015.
[2]. http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html
[3]. Catherine Paquet, " Network Security Concepts and Policies ",
[4]. Chapter of Cisco Press, Feb 5, 2013. http://www.ciscopress.com/articles/article.asp?p=1998559
[5]. Sabah Mohamed Fayyad, "Behavioral Databases in Preserving Data Stored", Journal of Babylon University, Issue 3, 2013.
[6]. Abraham Silberschatz and Henry F . Korth and S.sudarshan "Database System Concepts", Fifth Edition 2006.
[7]. Nick Snowdon,"Oracle Programming With Visual Basic ", First Indian Edition Reprinted 2002.
[8]. E. Bertino and R. Sandhu, "Database Security—Concepts, Approaches, and Challenges", IEEE Transactions on Dependable and Secure Computing, vol. 2, No. 1, Jan 2005.
[9]. Ali Hadi Hassan, "Encrypted Data Transfer", Journal of the University of Babylon / Pure and Applied Sciences, No. 1, Volume 24, 2016.
[10]. Beker and Piper, "Cipher System (The Protection of Communications)", Printed and Bound in Great Britain Ltd, Edinburgh and London;1982.
[11]. Tarish A. H, "Digital Image Cryptography", M. Sc. Thesis, University of Technology Malaysia (UTM), 2000.
[12]. T.K. S ivakumar and Dr. T. Sheela, A Novel Approach to Increase the Strength of the Round Keys Using Initialization Value (IV) with Key Forward Method in Enhanced Secure Data Encryption Standard (ES - DES) . International Journal of Civil Engineering and Technology, 8(11), 2017, pp. 561 – 568 .
[13]. R. Murugavel, Information Systems Software Quality: An Overview, International Journal of Mechanical Engineering and Technology 8(9), 2017, pp. 205 – 225