ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

BY PASS IDENTIFICATION PRESERVATION ADMINISTRATOR

K.Ramakrishna [1], J.Thirupathi[2]
Assistant Professor in Department of Computer Science Engineering and Technology in Samara University ,Samara, Ethopia[1]
Associate Professor in Department of Computer Science Engineering and Technology in Samara University ,Samara, Ethopia[1]

Abstract: This paper we propose the Today you need to remember much identification. You need a identification for the Windows network logon, your e-mail account, your homepage's FTP identification, online identifications (like website member account), etc. etc. etc. The list is endless. Also, you should use different identifications for each account. Because if you use only one identification everywhere and someone get this identification you have a problem. A serious problem to the owner of the id. The thief would have access to your e-mail account, homepage, etc. Unimaginable. This system is a identification administrator, which helps you to manage your identifications in a secure way. You can put all your identifications in one database, which is locked with one master key or a key file. So you only have to remember one single master identification or select the key file to unlock the whole database. The databases are encrypted. A facility to update and change information is provided.

Keywords: Encryption, Decryption, effective identification, Primitive Functions, permutation function, iteration, DES Encryption, Report Generation, Data security.

I.INTRODUCTION

To provide security to highly confidential data such as id's and identifications that may span from PC applications to financial information. Intended for Project Administrators, Developers, End users and Quality Assurance engineers. Suggested reading the document would be overall document description, product based information gathering followed by Infrastructure requirement.

Project Scope:-Provides registration to public in order to access the application. The user can change his identification.

Registered users can store critical and confidential data in a secured form. Unprotect and Retrieve data as and when necessary. The data can be retrieved anytime, from anywhere and any number of times. Preservation provided to the stored data using the Blowfish algorithm In the present scenario every person is associated with some id and identification. It may pertain to accessing the PC, the web, emails, financial institutions, access to credit cards, ATM's etc. Most often a person tries to remember them in order to use it. It is always known that a person or individual confuses between identifications of different ids. Some individuals in order to avoid confusion also adapt to use a common identification for all ids.

Both of the above can either lead to misplaced identification or forgotten identification or easily hacked when the single identification is known. Some individuals even try to save critical information in books or registers or electronic diaries and carry them along. The possibility of this carrier being lost or damaged is high. In the present scenario certain identifications can be recovered after a procedural delay. In some cases the identification cannot be reset easily and the user has to forgo or close the account permanently as in the case of mails. Proposal to maintain a centralized server that, stores critical information and be accessible to the user from anywhere, any time. The server can now remember any amount of .id's and identifications irrespective of even their lengths. Highly useful when data such as a credit card, debit card number etc that have larger number of digits or characters cannot be remembered easily. In order to provide higher level security the data is stored in an unreadable format. To provide this scenario the server implements the Blowfish algorithm using the visual studio. Similarly whenever the data needs to be unprotected and used the decryption ensures that the data is recovered without any loss or alterations.

II.SYSTEM OVERVIEW

Project Scope

Provides registration to public in order to access the website.

The user can change his identification. Registered users can store critical and confidential data in a secured form. Unprotect and Retrieve data as and when necessary. The data can be retrieved from anywhere, any number of times and anytime. Preservation provided to the stored data using the DES algorithm.

MODULES:

(1) Login & Security
(2) ID & Identification Administrator
(3) Encryption
(4) Decryption
(5) Report Generation.

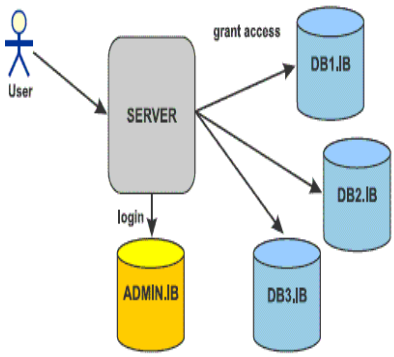
1) Login & Security:

The module deals with authentication of the users using the application. There are basically two types of users – Administrator & the public. Each of the above users are associated with user id and identification. The user id is unique to each user. The users login with the specified id and identification to access their schema information.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Additional facility to change their identification is also provided.



2) Id & Identification Administrator:
This module deals with storing as many id's and correlated identifications into the database. Each user can have more than one id stored. The identification is sent to the Blowfish encryption module to have it encrypted or converted to cipher text before it can be stored in the database. Each id acts as the primary key for that identification. The id is then used to retrieve the associated identification later.

3) Encryption:
DES encrypts and decrypts data in 64-bit blocks, using a 64-bit key (although the effective key strength is only 56 bits, as explained below). It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and a substitution in the algorithm, DES is both a block cipher and a product cipher.DES have 16 rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially.

4) Decryption:
DES encrypts and decrypts data in 64-bit blocks, using a 64-bit key (although the effective key strength is only 56 bits, as explained below). It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and a substitution in the algorithm, DES is both a block cipher and a product cipher.DES has 16 rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially

5) Report Generation:
The module allows the users of the application to view the following reports:-Identification for a particular user id.Tabulated listing of all user account and related identifications

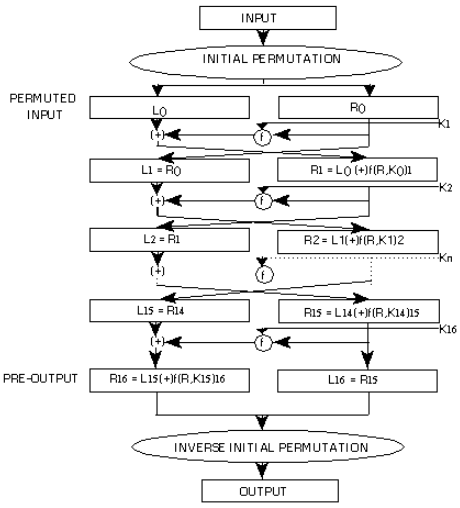
III.THE WORKING PRINCIPLE

The project had two main objectives:
Provide functionality to store a identification in the form of key, that key is stored in some file in an decrypted format, which is stored in database. To provide security to highly confidential data such as id's and identifications that may span from PC applications to financial information

DES Algorithm
Category of Standard**:** Computer Security.
Explanation: The Data Encryption Standard (DES) specifies a FIPS approved cryptographic algorithm as required by FIPS 140-1.

Qualifications: The cryptographic algorithm specified in this standard transforms a 64-bit binary value into a unique 64-bit binary value based on a 56-bit variable. As there are over 70,000,000,000,000,000 (seventy quadrillion) possible keys of 56 bits, the feasibility of deriving a particular key in this way is extremely unlikely in typical threat environments. The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key .A block to be enciphered is subjected to an initial permutation IP and then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP^{-1}.Permutation is an operation performed by a function, which moves an element at place j to the place k.The key-dependent computation can be simply defined in terms of a function f, called the cipher function, and a function KS, called the key schedule. First, a description of the computation. Next, the use of the algorithm for decipherment. Finally, a definition of the cipher function ***f*** that is given in terms of selection function $\mathbf{S}_i$ and permutation function **P**.

LR denotes the block consisting of the bits of L followed by the bits of R. A sketch of the enciphering computation is given in the figure. Sometimes abbreviated as PWD (not to be confused with the pwd command), a identification is a set of secret characters or words utilized to gain access to a computer, network resource, or data. Identifications help ensure that computers and/or data can only be accessed by those who have been granted the right to view or access them.



ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Strong identification - Term used to describe a identification that is an effective identification that would be difficult to break. Often a strong identification has between six and ten characters, numbers and other characters, and upper and lowercase.
Weak identification - A identification that is not an effective identification because it's easy to remember. Examples of a weak identification are names, birth dates, phone numbers, etc.
Initial Permutation of DES:

- Initial Permutation

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

- The permuted input block is then the input to a complex key-dependent computation.
- The output of that computation (preoutput) is then subjected to the next permutation which is the inverse of the initial permutation.

Inverse Initial Permutation of DES

- **IP^{-1}**

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

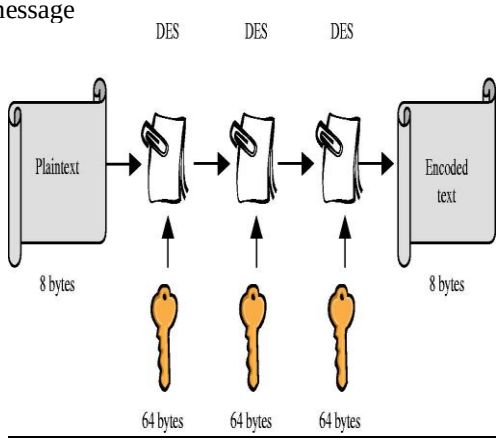
- The computation consists of 16 iterations of a calculation
- The cipher function f operates on two blocks, one of 32 bits and one of 48 bits, and produces a block of 32 bits.
- The input block is then LR, 32 bit block L followed by a 32 bit block R.
- Let K be a block of 48 bits chosen from the 64-bit key. Then the output L'R' of an iteration with input LR is defined by:
  L' = R
  R' = L (+) f (R,K).
- L'R' is the output of the 16th iteration then R'L' is the preoutput block.
- At each iteration a different block K of key bits is chosen from the 64-bit key designated by KEY.
- Let KS be a function which takes an integer n in the range from 1 to 16 and a 64-bit block KEY as input and yields as output a 48-bit block Kn which is a permuted selection of bits from KEY. That is
- Kn = KS (n, KEY)
- Let the permuted input block be LR.
- Finally, let L0 and R0 be respectively L and R and let Ln and Rn be respectively L' and R' when L and R are respectively Ln-1 and Rn-1 and K is Rn; that is, when n is in the range from 1 to 16,
- Ln = Rn-1

Primitive Functions For The Data Encryption Algorithm

- The choice of the primitive functions KS, S1, ..., S8 and P is critical to the strength of an decipherment resulting from the algorithm
- The recommended sets of functions are described as S1... S8 and P in the algorithm.

3DES Algorithm:

- Triple-DES is just DES with two 56-bit keys applied.
- First key is used to DES- encrypt the plaintext message.
- The second key is used to DES-decrypt the encrypted message



IV.IMPLEMENTATION OF SYSTEM

Java was conceived by James Gosling, Patrick Naught on, Chris Warth, Ed Frank and Mike Sheridan at SUN Micro Systems Incorporation in 1991. It took 18 months to develop the first working version. This language was initially called “OAK”, but was renamed “JAVA” in 1995. Before the initial implementation of OAK in 1992 and the public announcement of Java in 1995, many more contributed to the design and evolution of the language.

OVERVIEW OF JAVA:

An Object Oriented Programming Language (OOPL) developed at Sun Microsystems. A Virtual Machine Run Time Environment that can be embedded in web browser (IE, NN). Java is a powerful but lean object oriented programming language. It has generated a lot of excitement because it makes it possible to program for Internet by creating applets, programs that can be embedded in web page.

The context of an applet is limited only by one’s imagination. For example, an applet can be an animation with sound, an interactive game or a ticker tape with constantly updated stock prices. Applets can be serious application like word processor or spreadsheet.But Java is more than a programming language for writing applets. It is being used more and more for writing standalone applications as well. It is becoming so popular that many people believe it will become standard language for both general purpose and Internet programming. There are many buzzwords associated with Java, but because of its

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

spectacular growth in popularity, a new buzzword has appeared ubiquitous. Indeed, all indications are that it will soon be everywhere.

Java is actually a platform consisting of three components:

- Java Programming Language.
- Java Library of Classes and Interfaces.
- Java Virtual Machine.

It also has a Standardized set of Packages (Class, Interfaces):

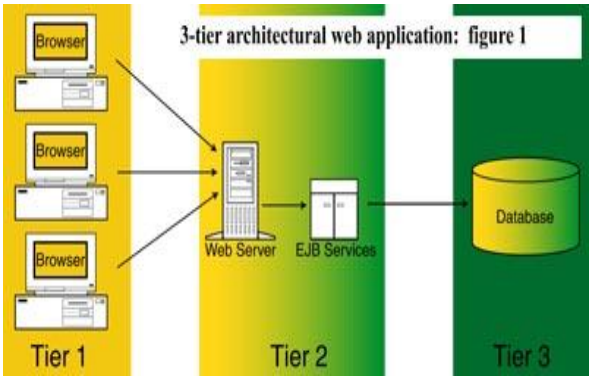
- Creating Graphical User Interfaces
- Controlling Multimedia Data
- Communicating over Network

Java Server Pages (Jsp):
Java Server Pages (JSP's) permit server side Java logic to reside within the requested document. Upon request of a JSP document the server activates the specified JSP. The JSP then becomes responsible for providing an HTML response.

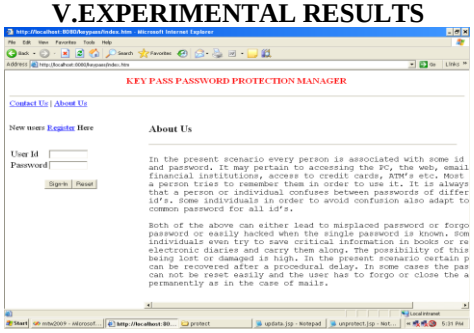
The server side logic within a JSP is written in Java. The Java code segments, referred to as script lets, are generally responsible for providing dynamic HTML content to the JSP's response HTML. The JSP itself is compiled by the server, and is executed as an object that extends the Java Servlet API. As such, the HTTP Servlet request and response objects are available by the scriptlets defined within the JSP.

This document reviews client-server design considerations in respect to the use of JSP's. Implementation options, particularly the use of JSP language extensions and use of Enterprise Java Beans (EJB's) will also be discussed. Focus will be placed on the presentation layer and how the JSP is used to provide a user interface and communicate business logic requests to the supporting system.

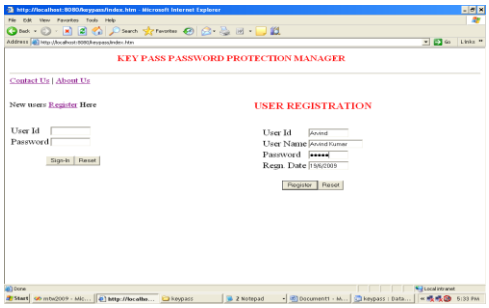
If we consider a 3-tier architectural WEB application, the browser becomes the client side application. The user communicates requests to the WEB/app server via the browser. The presentation layer receives the client requests and prepares the response and server side business functionality is executed. In the context of this example, the JSP engine represents the presentation layer. It is responsible for processing requests and responses. Additional messages may be passed between this layer and that which handles business processes represented below as EJB's.



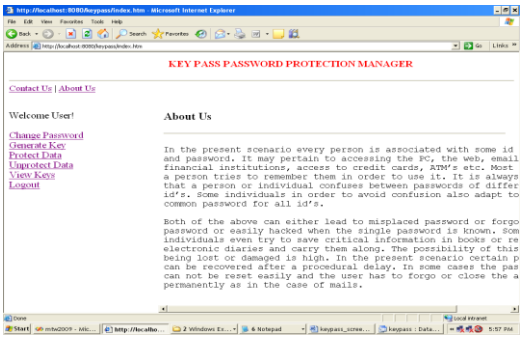
V.EXPERIMENTAL RESULTS



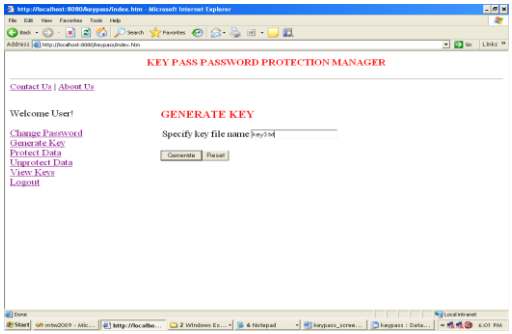
Home page



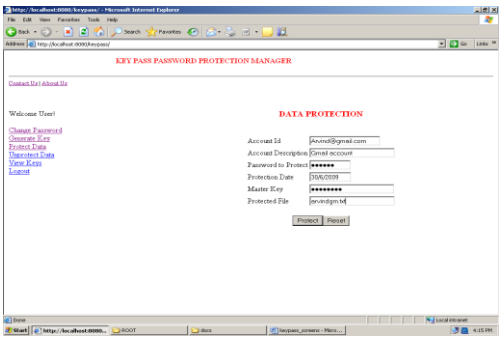
User registration



Change Identification



Generate Keys



Identification protected successfully

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

VI.TESTING

The purpose of testing is to assess product quality. It helps to strengthen and stabilize the architecture early in the development cycle. We can verify through testing, the various interactions, integration of components and the requirements which were implemented. It provides timely feedback to resolve the quality issues, in a timely and cost effective manner. The test workflow involves the following:

Verifying the interactions of components. Verifying the proper integration of components. Verifying that all requirements have been implemented correctly. Identifying and ensuring that all discovered defects are addressed before the software is deployed.

Quality:

The common usage of the term quality refers to a number of things: principally it means the absence of defects, but more importantly, a fitness for a desired purpose. The ultimate goal of testing is to assess the quality of the end product. Quality assessments often consider process quality and organizational factors as well as direct product quality.

Product Quality:

The role of testing is not to assure quality, but to assess it, and to provide timely feedback so that quality issues can be resolved in a timely and cost-effective manner.

Testing In the Iterative Lifecycle:

Testing is not a single activity, nor is it a phase in the project during which we assess quality. If developers are to obtain timely feedback on evolving product quality, testing must occur throughout the lifecycle: we can test the broad functionality of early prototypes: we can test the stability, coverage and performance of the architecture while there is still an opportunity to fix it; and we can test the final product to assess its readiness for delivery to customers.

VII. CONCLUSION

To provide security to highly confidential data such as id's and identifications that may span from PC applications to financial information. Too many identifications cannot be remembered by a single person as it leads to confusion. Maintaining a single identification to all his accounts leads to insecurity. When maintaining critical information in electronic diaries or books, there is a possibility of information being damaged or lost. Provide functionality to store a identification in the form of key, that key is stored in some file in a decrypted format, which is stored in database

REFERENCES

[1] Y. Gu, Y. Tian, and E. Ekici, "Real-Time Multimedia Processing inVideo Sensor Networks," Signal Processing: Image CommunicationJournal (Elsevier), vol. 22, no. 3, pp. 237–251, March 2007.
[2] "Advanced Video Coding for Generic Audiovisual Services," ITU-TRecommendation H.264.
[3] T. Wiegand, G. J. Sullivan, G. Bjntegaard, and A. Luthra"Overview of the H.264/AVC video coding standard," IEEE Trans. on Circuits andSystems for Video Technology, vol. 13, no. 7, pp. 560–576, July 2003.
[4] J. Ostermann, J. Bormans, P. List, D. Marpe, M. Narroschke, F. Pereira,T. Stockhammar, and T.Wedi, "Video coding with H.264/AVC: Tools,performance, and complexity," IEEE Circuits and System Magazine,vol. 4, no. 1, pp. 7–28, April 2004.
[5] http://www.networkcomputing.com

Mr. K.Ramakrishna, post graduated in (CSE-SE) M.Tech from JNTUH and graduated in (IT) B.Tech from kakatiya university, Warangal ,AP, INDIA, he is has 5+ experience, He is working presently as an Asst.Professor in Department of computer science engineering and technology in Samara University ,Samara, ETHIOPIA, his research interests include mobile ad-hoc networks ,information security and communaction

Mr. Thirupathi J, post graduated in (CSE-) M.Tech from JNTUH and graduated in (CSE) B.Tech from JNTUH,AP,INDIA,he is has 8+ experience, He is working presently as an Assoc. Professor in Department of computer science engineering and technology in Samara University ,Samara, ETHIOPIA, his research interests include, cloud computing and information security .