DESIGNING A SECURE DATABASE FOR THE ASSIGNMENT DECISION-MAKING FOR TENDERS BASED ON CLOUD COMPUTING

Anhar Khairy Al-deen
Department of MIS, Mosul University, Mosul, Iraq

ABSTRACT

Cloud computing for tenders has been programmed based on the Linux kernel 2.3.6 and the language of PHP code to build desktop applications needed to run the system on the Internet and the system uses protocols http, https, ftp, SSL, the user name and password will be entered for Registration on the cloud computing and used it in the next login. The password encrypt by using MD5 Hash function, then the encrypted password & User Name is storing in cloud database. A Tenders website was designed special for General Directorate for the North Electricity Distribution - Commercial Affairs Department / tenders by using asp.net language , via this site the tenders advertisements is publish and invite to apply to the tender, then the applicant can fill the required information & upload all the required documents on the website voice conference contract by using VOIP technique especial for applicant on tenders to answer their participants questions. K Algorithm(By Weka) was used in order to classify applicants to tender to complete and incomplete and is only allowed the applicants to tender who is complete the requirements(conditions) to lift the profile commercial offer on cloud computing then encrypts the file by using the SHA3 Hash function.*

KEYWORDS: Cloud Computing, cloud Database, *CDBMS*, Web3.0, VOIP, *IP Multicasting*, *Cryptography, MD5, SHA3, K*Classifier, Lazy Classifier.*

I. INTRODUCTION

Became cope with the massive developments in the field of informatics at the moment of the most important concerns of contemporary business organizations.

As I realized these organizations the importance of the use of information and communication technologies and their various applications in the various activities of the organization, as it focused organizations to use these technologies in the construction and infrastructure development for Management information systems of various kinds, as well as building models e-business and the use of these technologies to deal with the external environment in which we find all dealers who are involved in the organization of competitors, Suppliers and customers and other elements of the external environment.

Therefore, it is essential that business organizations based on the broad applications of information and communication technology that evolved after a rapid development in order to meet the needs of organizations and beneficiaries, as well as decision-makers in the organization.

II. TENDERS

Tender : Is a set of statutory procedures, which aims to invite the largest possible number of competitors to submit their bids and their offerings as a prelude to choose the most appropriate, including whether relates to the quality of public to be purchased or prices or the rest of the other conditions of the quantity and processing time and the terms of payment and delivery and other things that may have an impact directly or indirectly, in the performance of this important function of the functions of the organization.

Or

Tender: is a method whereby administration selects the best of those applying for the contracted conditions, both in financial terms and in terms of service to be performed.

And competition phenomenon generally humanitarian and commercial specifically seek means to provide better by others this principle has appeared since the beginning of creation, when man began to address the subject of buying and selling and work.

The freedom of competition within the tendering means freedom in tenders announced by the administration of any open scramble honest in front of all those who wish to participate in the tender, any individual or body find in themselves the ability to perform the operation at hand can submit a bid which may not manage to prevent any who wish to contract in the tender, as long as its conditions are available where and management has the right to deprive some of the contractors and the exclusion of certain bidding competition for the tender announced by the failure to comply with the tender conditions set by the administration may also be excluded for lack of technical competence or financial with the bidder .

III. WEB 3.0

Web 3.0 could be defined as: “Web 3.0, a phrase coined by John Markoff of the New York Times in 2006, refers to a supposed third generation of Internet-based services”.

Web 3.0 enabled by the convergence of several key emerging technology trends :Ubiquitous Connectivity(Broadband adoption, Mobile Internet access, Mobile devices),Network Computing(Software-as-a-service business models, Web services interoperability, Distributed computing (P2P, grid computing, hosted “cloud computing” server farms such as Amazon S3),Open Technologies(Open APIs and protocols, Open data formats, Open-source software platforms, Open data (Creative Commons, Open Data License, etc.),Open Identity(Open identity (OpenID),Open reputation, Portable identity and personal data (for example, the ability to port your user account and search history from one service to another),The Intelligent Web(Semantic Web technologies (RDF, OWL, SWRL, SPARQL, Semantic application platforms, and statement-based data stores such as triple stores, tuple stores and associative databases),Distributed databases or what I call “The World Wide Database”((wide-area distributed database interoperability enabled by Semantic Web technologies),Intelligent applications (natural language processing, machine learning, machine reasoning, autonomous agents).

IV. VOICE OVER INTERNET PROTOCOL (VOIP)

Voice over Internet Protocol (VOIP) is “a form of communication that allows you to make phone calls over a broadband internet connection instead of typical analog telephone lines”. Basic VoIP access usually allows you to call others who are also receiving calls over the internet. Interconnected VOIP services also allow you to make and receive calls to and from traditional landline numbers, usually for a service fee. Some

VOIP services require a computer or a dedicated VOIP phone, while others allow you to use your landline phone to place VoIP calls through a special adapter.

VOIP is becoming an attractive communications option for consumers. Given the trend towards lower fees for basic broadband service and the brisk adoption of even faster internet offerings, VOIP usage should only gain popularity with time. However, as VoIP usage increases, so will the potential threats to the typical user. While VoIP vulnerabilities are typically similar to the ones users face on the internet, new threats, scams, and attacks unique to IP telephony are now emerging [1]

4.1. Services & Applications

VOIP by its nature is primarily concerned with the provision of voice and telephony services on IP networks. Traditional telephony services on VOIP networks today include Long Distance Toll by pass, **Voice Conferencing**, Call Centers, and PBX networking.

In addition to traditional voice services VOIP provides an environment that allows voice to be integrated with other media types both at the transport layer and at the service layer.

New integrated applications are in their infancy and already new service opportunities such as powerful unified messaging, **IP video conferencing & other IP video applications**, IP Phone & PC Soft phone features, multimedia contact centers, collaboration applications, and mobility enabled presence services, can all help to greatly enhance an organization's communication capabilities.

The extent and pace at which more converged services will emerge is not yet totally clear. What is clear however is the quantum leap convergence has brought to voice service creation and data integration compared to the past history of ISDN and Intelligent Networking.

4.2. How does it work?

Many years ago we discovered that sending a signal to a remote destination could have be done also in a digital fashion: before sending it we have to digitalize it with an ADC (analog to digital converter), transmit it, and at the end transform it again in analog format with DAC (digital to analog converter) to use it.

VOIP works like that, digitalizing voice in data packets, sending them and reconverting them in voice at destination.

Digital format can be better controlled: we can compress it, route it, convert it to a new better format, and so on; also we saw that digital signal is more noise tolerant than the analog one

TCP/IP networks are made of IP packets containing a header (to control communication) and a payload to transport data: VOIP use it to go across the network and come to destination. **[2][3][4]**

4.3. VOIP connection[2]

To setup a VOIP communication we need:

1. First the ADC to convert analog voice to digital signals (bits)

2. Now the bits have to be compressed in a good format for transmission:

 there is a number of protocols we'll see after.

3.Here we have to insert our voice packets in data packets using a real−time protocol (typically RTP over UDP over IP)

RTP - Real Time Transport Protocol is an Internet protocol for transmitting real-time data such as audio and video. RTP itself does not guarantee real-time delivery of data, but it does provide mechanisms for sending and receiving applications to support streaming data. Typically, RTP runs on top of the UDP protocol, although the specification is general enough to support other transport protocols that know how Windows supports Real Time Communication.

RTP Header

Real Time Transport Protocol

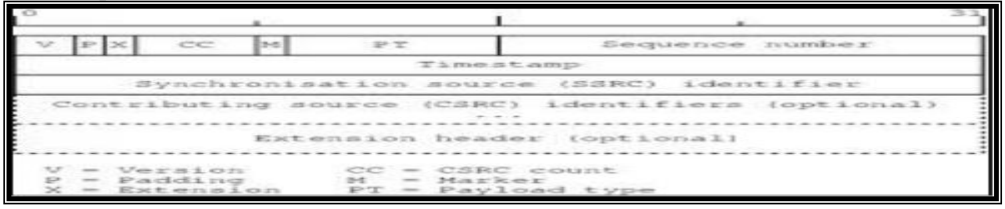

0
31
V
P
X
CC
M
PT
Sequence number
Timestamp
Synchronisation source (SSRC) identifier
Contributing source (CSRC) identifiers (optional)
...
Extension header (optional)
V – Version
P – Padding
X – Extension
CC – CSRC count
M – Marker
PT – Payload type

Fig.1 : Real Time Transport Protocol

4.We need a signaling protocol to call users: ITU−T H323 does that.

5. At RX we have to disassemble packets, extract data, then convert them to analog voice signals and send them to sound card (or phone)

6. All that must be done in a real time fashion cause we cannot waiting for too long for a vocal answer!

4.4. Multicasting Group used to work IP Multicasting

IP multicast means that " one sender is sending data to multiple recipients, but only sending a single copy. It's very useful for streaming media, so let's explore how this works".

Multicast is more efficient than broadcast, because broadcast packets have to be received by everyone on the local link. Each OS takes an interrupt, and passes the packet on for inspection, which normally involves some data copies. In multicast, the network card doesn't listen to these multicast packets unless it has been told to do so. [5]

If we divide the transmitter into groups then you must use IP multicasting in order to be used in the work of multicast group as the majority of software conference rely on it is known as multicasting: he transmitter to a group of users, whether managed by using the client \ server where there is a server in the network and job receive messages from clients group and then send it to the entire group again. Figure(2)

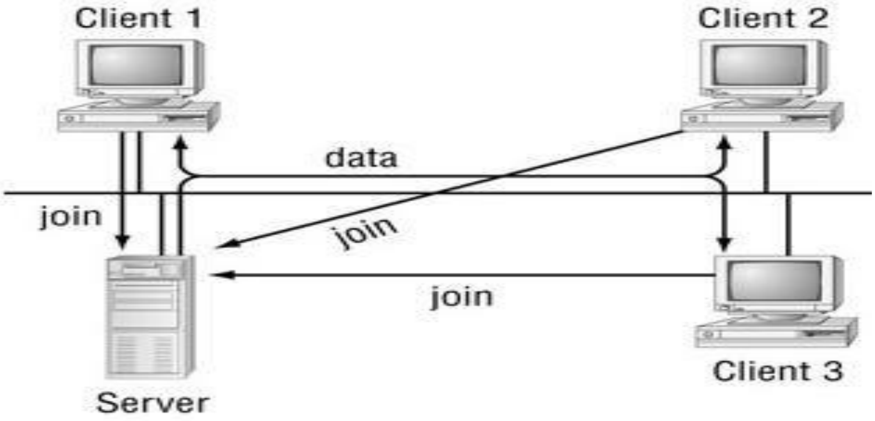


Fig. 2: clients group

We note from the above figure that he can send the request to the group by the clients, and if the server agreed to the demand we put device address to List IP address of its own and each group share the same IP multicast and transmitter to all members of the group, which share the same IP multicast

The second type is called peer-to-peer technique _ unmanaged where each device works like a server and client at the same time and there is no device server central devoted to the process of reception and distribution, where it is to approve the request to join the group automatically and any device in the group has the right to join and then the receiver and transmitter to the entire group.

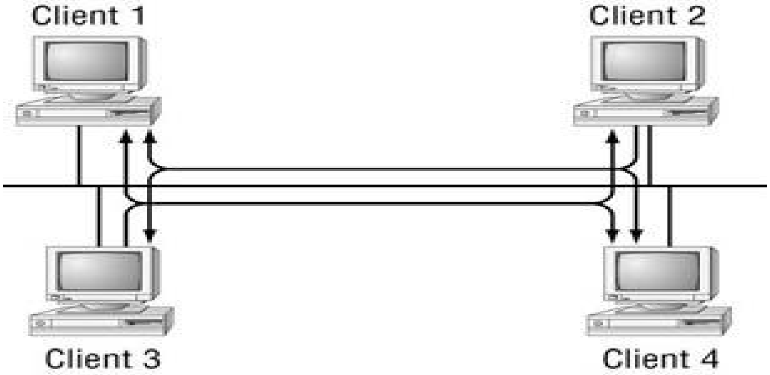


Fig.3 peer-to-peer technique _ unmanaged

Private addresses were allocated to multicast which is called IP multicast Address range from 224.0.0.255 to 224.0.0.0 for local networks.
Address range from 224.0.1.255 to 224.0.1.0 for internetwork
Address range from 224.0.2.0 to 224.0.255.255 for AD-HOC Network block
Multicast can be used in three types of networks, a network of peer-to-peer, where there is no device server and everyone receives and sends to and from the group in which it is. The second type of server based network where they are sending one message on the server and the server distributed to the rest of the devices in the network. The third type are through Router where the transmitter is the process after client's accession to the Group, which owns IP multicast, the client sends a single message to Router where Router distributed setups in the group using the routing table.

V. CLOUD COMPUTING

Cloud computing is one of the majority emerging technologies which plays an momentous role in the next generation architecture of IT project.

It has been vastly accepted because of its ability to reduce costs linked with computing while rising flexibility and scalability for computer processes. In the course of the past few years, cloud computing has developed from being a promising business notion to one of the fastest developing parts of the IT industry. In the cloud computing system, both application program and databases are moved to the big data centers, where the data should not be safe in the hands of suppliers.

Cloud computing has become very public and for a good excuse. The intense motive to lessen operational expenses and IT complexities has fueled a new generation of technologies that deliver program and solutions via the web without needing traditional procurement, licensing, installation, upkeep or administration by inner IT staff [6]

In addition the users can reach their files at anytime, anywhere in the world, because of new advanced servers that are all combined with these servers compel for a cloud computing (http://code.google.com, Google App Engine)

The aim of cloud computing is to allow users to take avail from all of these technologies, without the need for profound knowledge about or expertness with each one of them. The cloud aims to cut costs, and help the users center on their main business instead of being impeded by IT impediments.

Organizations use the Cloud in a variety of various service specimens (SaaS, PaaS, IaaS) and deployment specimens (Private, Public, Hybrid).

5.1. Cloud database

Database accessible to clients from the cloud and presented to users on request through the Internet from a cloud database supplier's servers. Also called as Database-as-a-Service (DBaaS), cloud databases can use cloud computing to achieve optimized scaling, lofty availability, multi-tenancy and efficient resource allocation.

A cloud database is a kind of database service that is built , deployed and presented through a cloud platform. It is primarily a cloud Platform as a Service (PaaS) specimen that allows organizations, end users and their implementations to save, manage and reply data from the cloud. [7]

A cloud database typically works as an exemplary database solution that is generally implemented via the installation of database program on top of a computing/infrastructure cloud. It may be straight accessed via a Web browser or a seller supplied Application programming Interface (API) for application and service completeness. Unlike a standard database, a cloud database may be measured on run time, in which additional cases and resources of storage and computing may be restricted immediately while a cloud database can be a conventional database.

Cloud database inclines to improve supply to optimally use cloud resources and to warrant scalability in addition to availability and constancy

Cloud databases can give significant benefits over their conventional counterparts, containing increased accessibility, automatic unsuccessful over and fast automated improving from failures, automated on the go measuring , fewer investment and upkeep of in house hardware, and potentially skillful performance at the same time, cloud databases have their participating of potential handicaps, containing safety and privacy issues in addition of the probable loss of or unable to access embarrassing data in the case of event a disaster or insolvency of the cloud database service supplier[8]

5.2. Database Management in the Cloud

CDBMS (A Cloud database management system) is a distributed database that surrenders computing as a service in place of a product. It is the participating of resources, programs, and information between multiply equipment's over a network which is majority on the internet. It is anticipated that this number will developed significantly in the future. Cloud applications linking in the *database* that is being run on the cloud and have different degrees of efficiency. Some are manually constituted, some are preconfigured, and some are local.

In spite of the avails presented by cloud basis DBMS, many people still have apprehensions about them. This is most likely because of the different security issues until now not deal with it. These security for that cloud DBMS must be monitor from they often span through multiple hardware codes and servers. Security becomes a serious case with cloud DBMS when there's multiple Virtual Machines that can be able to access a database without setting off any alerts. In this kind of status a parasitical person could access sensitive data or cause serious damage to the structure of a database, putting the entire system in risk[9]

VI. SECURITY IN THE CLOUD

Security is one of the most important issues of the cloud computing. Being completely based on the Internet makes it subject to attacks. All the modern IT systems today are always connected to the Internet. the distributed network in cloud computing is makes it easier for companies to get rid of such attacks [10]

business decision makers and IT as they consider the security issues of cloud computing on their business the most of the security issues fears associated with cloud computing but these issues can be divided into two categories:

- Security issues concerned by cloud providers (organizations supplying programs, platform, or infrastructure as a service through the cloud)
- The security matters faced by their clients.

In most cases, the supplier make sure that their infrastructure, their clients' data and their applications are protected, while the client make sure that the supplier has taken the correctly security measures to protect their information[11]

Companies must be careful, for example, how to protect passwords and changed. The customers are advised to obtain information about those companies which could input their data. [12]

we must consider the following areas when you have a secured Cloud computing ,spread , the cloud computing architecture, Governance , transport and interoperability, conventional security, business continuity and catastrophe recovery, data center operations, incident response, notification and remediation, Application Security,

Typical users who use the cloud computing service for example storing their files on the server to access it anywhere they want via internet, don’t anxious much about the security of their common files that don't need to be secured. But a big companies which have very interesting information, they need to have secured cloud computing system.

6.1. Cryptography

The mathematical techniques is study for all aspects of information security. The transformation of data into a secret symbol for transmission over a general network, which means, the real text is converted into a coded text called "cipher text" via an encryption algorithm. The cipher text is decrypted and turned back into plaintext at the receiving end. Cryptography is carried out by three methods, those are:

i. Symmetric Crypto System
ii. Asymmetric Crypto System
iii. Hash Functions

6.1.1. Cryptographic hash function

First: MD5 [13][14]

Secrecy, Authentication, Nonrepudiation and Integrity control. Secrecy has to do with keeping information out of hands of unauthorized users. Authentication deals with determining whom you are talking to before revealing sensitive information non repudiation deals with signature. Security in networking is based on cryptography[15]

The owner of the website can be attacked as well. Some websites have been defaced; the files that make up the website content have been remotely accessed and modified without authorization.

General Designers Ronald Rivest First published April 1992 Series MD2, MD4 [16], MD5, Detail Digest sizes 128 bit Structure Merkle–Damgård construction Rounds 4 .

MD5 is a type of cryptographic hash function that can be used to store a one-way hash of a password, often with key stretching. Along with other hash functions, it is also used in the field of electronic discovery, in order to provide a unique identifier for each document that is exchanged during the legal discovery process.

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is

1- **padded** so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 264.

2- Appending length

A 64-bit binary representation of the original length of the message is concatenated to the result of step (1).(Least significant byte first). The expanded message at this level will exactly be a multiple of 512-bits. Let the expanded message be represented as a sequence of *L*512-bit blocks *Y0, Y1,..,Yq,..,YL-1* as shown in Figure (6).Note that in the figure, IV and CV represent initial value and chaining variable respectively.

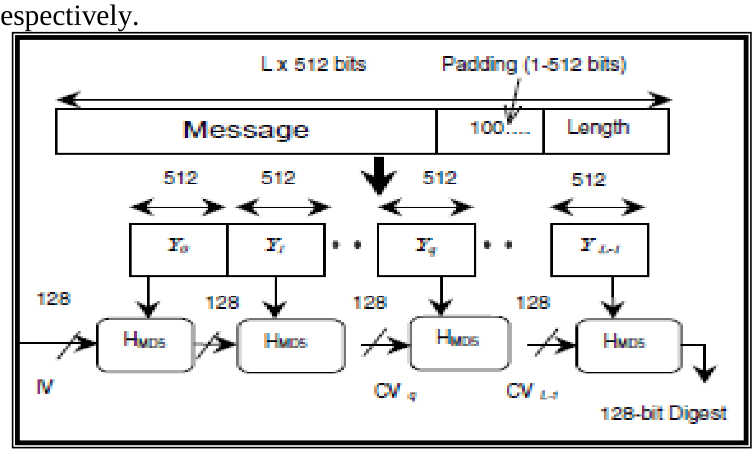


Fig.4:generation of message digest

3-Initialize the MD buffer

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C and D. These are initialized to certain fixed constants.

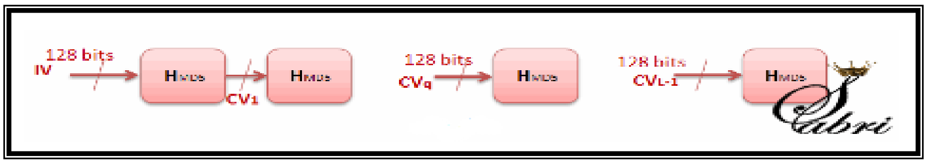


Fig.5:MD5 Buffer

4-Process message in 16-word blocks

The main algorithm then uses each 512-bit message block in turn to modify the state. The processing of a message block consists of four similar stages, termed rounds; as a given in equations (1) and(2). Each round consists of 16 steps and each step uses a 64-element table *T* [1 ... 64] constructed from the sine function. Let*T*[*i*] denote the *i*-th element of the table, which is equal to the integer part of 232 times abs(sin(*i*)), where *i* is in radians. Each round also takes as input the current 512-bit block (*Yq*) and the 128-bit chaining variable (CVq).An array *X* of 32-bit words holds the current 512-bit *Yq*. For the first round the words are used in their original order. The following permutations of the words are defined for rounds 2 through 4:

r2(*i*) = (1+ 5*i*) mod 16
r3(*i*) = (5+ 3*i*) mod 16
r4(*i*) = 7*i* mod 16

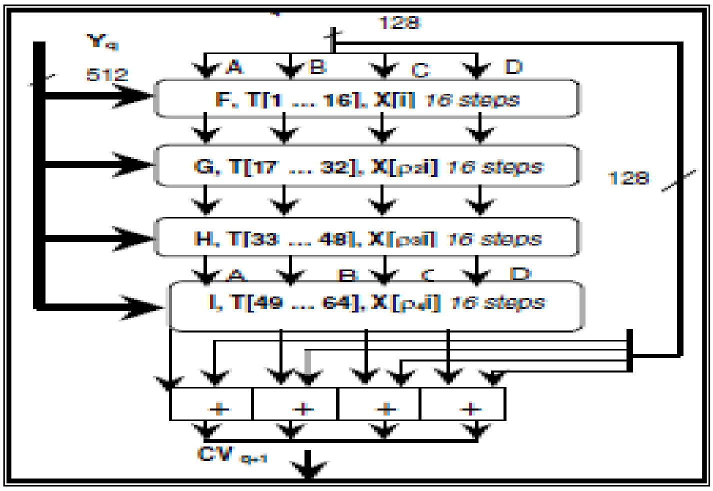

Y_q
512
128
A
B
C
D
F, T[1 ... 16], X[i] 16 steps
G, T[17 ... 32], X[ρ2i] 16 steps
128
H, T[33 ... 48], X[ρ3i] 16 steps
A
B
C
D
I, T[49 ... 64], X[ρ4i] 16 steps
+
+
+
+
CV q+1

Fig.6: Compression function HMD5

There are four possible functions F; a different one is used in each round:

$$A = B + ((A + \mathrm{Func}(B,C,D) + X_j[k] + T[i]) \lll s)$$

$$A \leftarrow D, B \leftarrow A, C \leftarrow B, D \leftarrow C \qquad (1)$$

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D) \qquad (2)$$

$\oplus, \wedge, \vee, \neg$ denote the XOR, AND, OR and NOT operations respectively.
The output of the fourth round is added to the input of the first round (CVq) to produce CVq+1.

5- Output

After all *L* 512-bit blocks have been processed, the output from *L*th stage is the 128-bit message digest. Figure(9) shows the operations involved in a single step. The additions are modulo 232. Four different circular shift amounts(s) are used each round and are different from round to round. Each step is of the following form.

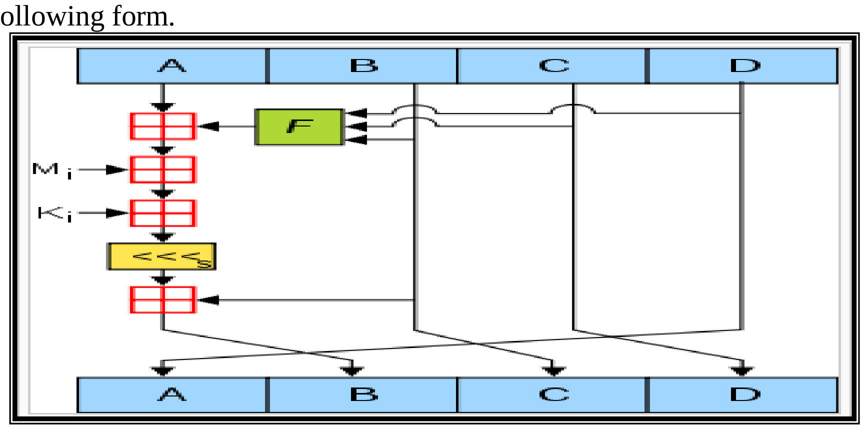


Fig.7:MD5 transform Operation (Operations in a single step of MD5)

<u>Second: SHA-3</u>

Originally known as Keccak is a cryptographic hash function designed by Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche, building upon RadioGatún.

<u>The block permutation</u> [17][18]

This is defined for any power-of-two word size, $w = 2^{\ell}$ bits. The main SHA-3 submission uses 64-bit words, $\ell = 6$.

The state can be considered to be a 5×5×*w* array of bits. Let $a[i][j][k]$ be bit $(i\times5 + j)\times w + k$ of the input, using a little-endian convention. Index arithmetic is performed modulo 5 for the first two dimensions and modulo *w* for the third.

The basic block permutation function consists of 12+2ℓ iterations of five sub-rounds, each individually very simple:

θ

Compute the parity of each of the 5×*w* (320, when *w* = 64) 5-bit columns, and exclusive-or that into two nearby columns in a regular pattern. To be precise, $a[i][j][k]$ ⊕= parity(a[i][j−1][k]) ⊕ parity(a[i][j+1][k−1])

ρ

Bitwise rotate each of the 25 words by a different triangular number 0, 1, 3, 6, 10, 15, ... To be precise, $a[0][0]$ is not rotated, and for all $0 \le t < 24$, $a[i][j][k] = a[i][j][k-(t+1)(t+2)/2]$, where

$$\begin{pmatrix} i \\ j \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 0 \end{pmatrix}^t \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

π

Permute the 25 words in a fixed pattern. $a[j][2i+3j] = a[i][j]$

χ

Bitwise combine along rows, using $a = a \oplus (\neg b \,\&\, c)$. To be precise, $a[i][j][k]$ ⊕= $\neg a[i][j+1][k]$ & $a[i][j+2][k]$. This is the only non-linear operation in SHA-3.

ι

Exclusive-or a round constant into one word of the state. To be precise, in round n, for $0 \le m \le \ell$, $a[0][0][2^m-1]$ is exclusive-OR with bit $m+7n$ of a degree-8 LFSR sequence. This breaks the symmetry that is preserved by the other sub-rounds.

VII. LAZY CLASSIFIER

Lazy learns save the training instances and not work really until classification time. Lazy learning is a learning way in which generalization after the training data is delayed until a query is did to the system . before receiving queries, the training data is generated by the system. The main benefits gained in using a lazy learning method is that the target function will be approximated locally like in the (k nearest neighbor) algorithm.

each query system , the objective function is approximated locally therefor the lazy learning systems can solve many problems, and deal with updates in the problem arena [19]

7.1. K Star Classifier

K *algorithm is used as the classifier, A K Star is a memory based classifier that is the class of a test instance is based upon the class of those training instances similar to it, as determined by some similarity function. The use of entropy as a distance measure has several benefits. Amongst other things it provides a consistent approach to handling of symbolic attributes, real valued attributes and missing values. K* is an instance-based learner which uses measures like entropy[20][21]

Specification of K*[22]

Let I be a (possibly infinite) set of instances and T a finite set of transformations on I. Each t ÎT maps instances to instances: t: I _ I. T contains a distinguished member(the stop symbol) which for completeness maps instances to themselves ((a) = a). Let P be the set of all prefix codes from T* which are terminated by _. Members of T* (and so of P) uniquely define a transformation on I: t(a) = tn (tn-1 (... t1(a) ...)) where t = t1,...tn

A probability function p is defined on T*. It satisfies the following properties:

$$0 \le \frac{p(\overline{tu})}{p(\overline{t})} \le 1$$
$$\sum_{u} p(\overline{tu}) = p(\overline{t})$$
$$p(\Lambda) = 1 \qquad (1)$$

As a consequence it satisfies the following:

$$\sum_{t \in P} p(\overline{t}) = 1 \qquad (2)$$

The probability function P* is defined as the probability of all paths from instance ‘a’ to instance ‘b’:

$$P^*(b|a) = \sum_{\bar{t}\in P:\bar{t}(a)=b} p(\bar{t}) \qquad (3)$$

It is easily proven that P* satisfies the following properties:

$$\sum_b P^*(b|a) = 1$$

$$0 \le P^*(b|a) \le 1 \qquad (4)$$

The K* function is then defined as:

$$K^*(b|a) = -\log_2 P^*(b|a) \qquad (5)$$

K* is not strictly a distance function. For example, K*(a|a) is in general non-zero and the function (as emphasized by the | notation) is not symmetric. Although possibly counter-intuitive the lack of these properties does not interfere with the development of the K* algorithm below. The following properties are provable:

$$K^*(b|a) \ge 0$$

$$K^*(c|b) + K^*(b|a) \ge K^*(c|a) \qquad (6)$$

VIII. Practical Part

Appendix(1) show the mechanism of tender system

8.1. cloud computing

cloud computing special for General Directorate for the North Electricity Distribution - Commercial Affairs Department / tenders has been programmed based on the Linux kernel 2.3.6 and the language of PHP Software to build a desktop with the applications needed to run the system on the Internet, And works on the Internet where you can have access to your files and edit them and see them through custom applications.

"kernel" is a Linux kernel and is responsible for a management operating system, let's say it is a mediator between the applications and programs that are installed on the machine ,cutting device and the external accessories that have been linked to the device, as shown in Fig(8):

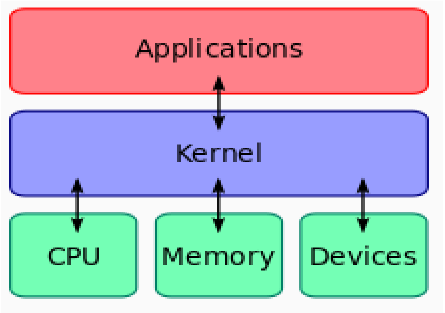


Fig.8: Kernel

System contains memberships where you can share files with your visitors and give them the space allocated to them and working on a web browser.

To upload any file to the system, this is done :

- From the top menu of Cloud computing O.S of the Tender select Application and then choose File Manager to upload a file to the system, as shown in Appendix(2)

The system allows a group powers, determined by the root user is the Director-General of the system which is responsible for all users in the system, as follows

The permition are given by:

-From the top menu select group, and give the name of the group has been pushing to create group then add members as shown in Appendix(5)

System uses protocols http, https, SSL,FTP

System contains memberships where you can share files with your visitors and give them the space allocated to them and working on a web browser.

This system has been programmed based on the Linux kernel and the language of php Software to build a desktop with the applications needed to run the system on the Internet
The demo O.S cloud computing of Tender system has shown in Appendix(2), Appendix(3), Appendix(4) , Appendix(5) .

a. Join interface for system

Appendix (6), shows the face of the registration system, where the applicant is required to fill the following fields:
Full name, Title User name in Arabic or English, Encrypted password by md5 technology, Repeat your password, E-Mail must be true, and then presses the register as shown in Appendix(7)

b. Desktop system

Desktop system as shown in appendix(8) is roughly similar to a desktop windows and accept all of its programs and similar programs System Used for windows

8.2. The mechanism of designing the website

The site of Tenders Directorate General of Electricity Distribution North - Commercial Affairs Department / tenders is designed by using ASP.Net Language

***a. The front page*:** This page represents the main page for the website and it includes the advertisements, the results page that will be activated after the tender being finishing completely tender being completed…etc as shown in Appendix(9).

b. The application form page: After the applicant enters the website and seeing the advertisements of Tender and knowing the needed conditions, The Suppliers can enter the application form page to fill the information. Every information entered is directly stored in its special field in the database as shown in appendix (10), and then filling the needed documents for the Tender, as shown in Appendix(11) and Appendix(12).

c. Voice Conference

voice conference contract by using technique VOIP especial for advanced on tenders to answer their questions according to the following steps:

- ❖ Dealing with the Sound Card for the recording operation from the microphone and dealing with the Wave Format.

<u>**Wave Format:**</u>

This characteristic is used to specify the Wave Format details such a number of Channels, Samples per second and Bits Per Sample, using these information in the operation of transforming the sound waves into bits, so that it can be transmitted throughout the network.

- Managing the Buggering, by splitting the Buffer into two parts, the first one in the process of recording the recorder sound and the second to prepare it in the processing operation such as sending it or compress it.
- Covering the Buffering in the RTP Packet and send it throughout the network into the Multicast RTP Session.

RTP Session:

The RTP Session is basically used in the connection board management operation, in which through it we can send a group of RTP Stream also it is possible to connect with one session a group of users to be connected with more than one RTP Session, therefore each RTP Session is characterized by the Address and the Port, that sent to him.

- On the other side, the joining into the RTP Session will take place then the listening operation starts on the Session, thus performing the Session Event which will be able to receive the incoming data from the sender, thereafter, collecting the Buffer and viewing it.
- After the receiving process, collecting the received bits in the Buffer to perform the decompressing operation, then play it on the sound device.

Channel:

Is the number of the channels, through which recording the sound and play it.

Bits per Sample:

Is the number of the bits needed to transform the Wave Sample from the analogue into the digital system as Shown in Appendix(13), Appendix(14), Appendix(15), Appendix(16)

8.3. Decision making of decision of giving the contracts of Tender

Admin makes the decision on the offer of private commercial applicants to tender and depending on the results of the algorithm If the applicant to tender patchy conditions not allow him upload commercial offer file into the cloud computing system (tenders operating system) and if it allow him to work upload commercial offer file into the cloud computing and before save the commercial offer file , is encrypted it by using sha3 algorithm to protect file from hackers and competitors. (The input variables of Kstar algorithm are: Pay BID, Book of the martyrdom of the tax concerned Directorates ,Similar acts,_The identity of the Chamber of Commerce / identity classification of contractors certificate of Incorporation of the company / office,_Certificate examination of the material processed by the company ,_Certificate of Incorporation of the company / office,Showing technician whose specification is identical to the tender conditions, Type Tend.

❖ Accuracy Classification

The Table(1) show the accuracy measure of classification Kstar. The True Positive rate, F-Measure, Receiver Operating Characteristics (ROC) Area. The TP Rate is the ratio of play cases predicted correctly cases to the total of positive cases. It is a probability corrected measure of agreement between the classifications and the true classes. It is calculated by taking the agreement expected by chance away from the observed agreement and dividing by the maximum possible agreement. F Measure is a way of combining recall and precision scores into a single measure of performance. Recall is the ratio of relevant documents found in the search result to the total of all relevant documents. Precision is the proportion of relevant documents in the results returned. ROC Area is a traditional to plot this same information in a normalized form with 1-false negative rate plotted against the false positive rate**.**

Table1 : Detailed Accuracy By Class

Correctly Classifier Instance	Incorrectly Classified Instance	TP Rate	FP Rate	Precision	Recall	F-Measure	ROC Area	class
95.8333%	4.1667%	1	1	0.958	1	0.979	0.141	Not Complete
		0	0	0	0	0	0.043	Complete

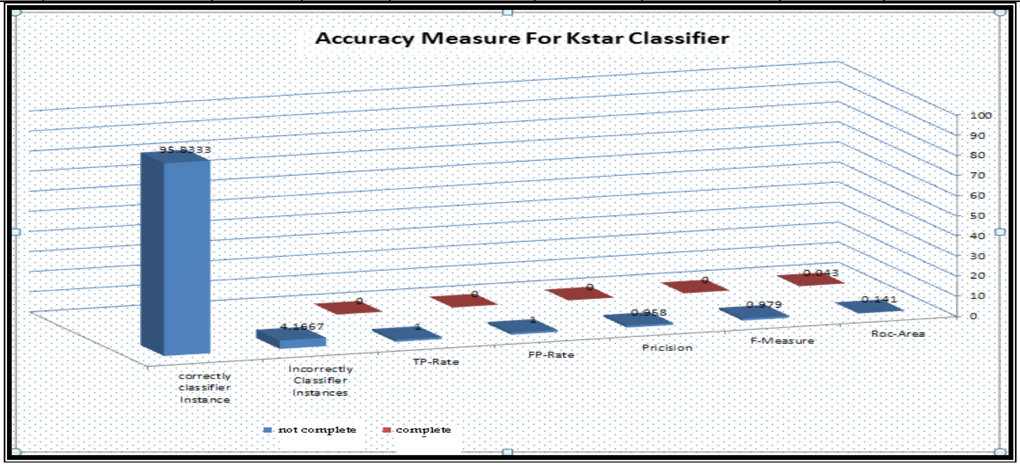


Fig. 9: Accuracy Measure For Kstar classifier

They are the Mean Absolute Error (M.A.E), Root Mean Square Error (R.M.S.E), Relative Absolute Error (R.A.E)and Root Relative Squared Error (R.R.S.E). The mean absolute error (MAE) is defined as the quantity used to measure how close predictions or forecasts are to the eventual outcomes. The root mean square error (RMSE) is defined as frequently used measure of the differences between values predicted by a model or an estimator and the values actually observed. It is a good measure of accuracy, to compare the forecasting errors within a dataset as it is scale-dependent. Relative error is a measure of the uncertainty of measurement compared to the size of the measurement. The root relative squared error is defined as a relative to what it would have been if a simple predictor had been used. More specifically, this predictor is just the average of the actual values.

Table2: Error Rate For Kstar Classifier

Algorithm	MAE	RMSE	RAE	RRSE
Ksatr	0.0575	0.1783	71.8014%	105.0991%

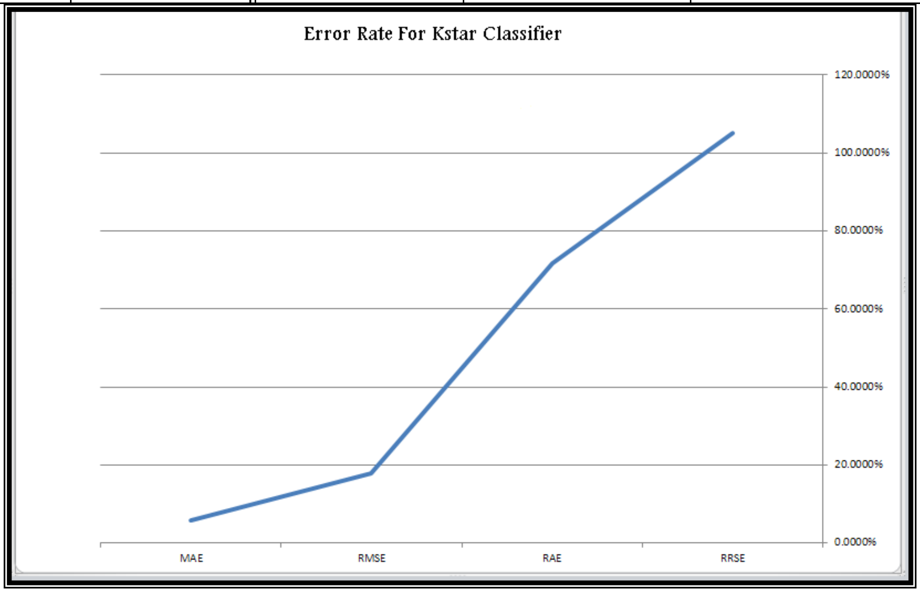


Fig.10:Error Rate For Kstar Classifier

8.4. Upload Commercial Trade File

Uses the protocol FTP to raise the file into the system and participation of all or memberships registered in the system according to the authority given to the file submitted and granted by the Administrator-General of the cloud computing which allows the lifting of the commercial offer file only to those who complete the conditions of the tender by the (K-star algorithm) where The Administrator notice on the e-mails, they complete the conditions of the tender and the possible lifting of commercial offer file on the cloud computing**.**

8.5 SHA3 Hash Function

General of the system which allows the lifting of the commercial offer file only to those who complete tender conditions determined by (K-star algorithm) where the Director shall send notice to the e-mails, they're completing the tender conditions and possible uploading commercial offer file on the cloud computing and is then encrypted by using the (SHA3 algorithm) to store it in a cloud database while giving validity to members for reading file only and download ability on their computer only, without any modification on the file after file decryption
Commercial offer file is encrypted/decrypted by using SHA3 algorithm as shown in appendix(17)

IX. CONCLUSIONS

1- Cloud computing is an Open Source Platform designed to hold a wide variety of Web Applications over it. Cloud computing was thought as a new definition of Operating System, where everything inside it can be accessed from everywhere in a Network. All you need to do is to login into your Cloud computing server with a normal Internet Browser, and access your personal desktop, with your applications, documents, music, movies... just like you left it last time. With the base system you can find a full suite of applications bundled, some for private use, like the file manager, a word processor, calendar, and notepad or contacts manager. There are also some groupware applications, such as a group manager, a file sharing application, a group board and many more.

The manager can have your own private cloud computing server for your establishment, employees and customers, or Web Network, completely free.

Cloud computing is all about removing compatibility issues between applications and operating systems. Sharing resources easily between different work centers of a same company, or working from different places and countries in the same projects.- Enjoying always the same applications with the same open formats, and forgetting the usual compatibility problems between Office suites or traditional operating systems.- Being able to continue working if you have to leave your local computer or it just crashes, without loosing data or time in solving its problems: Just log in to your O.S from another place and continue working. Requirements manager can view the establishment's office from anywhere outside of a friend's house or your house. If you can communicate and deal with the (establishment's files, programs, applications)

2-For enhancing privacy in cloud, we implemented one cryptography algorithms to protect the password of each into cloud .we have implemented MD5 algorithms for each use's password and uploading file(commerce offer) into cloud in secure way by using SHA3 algorithm . From the results we obtained it is proved SHA3 algorithms gives protection for the commercial offer files, which are stored in Cloud. The users can store the file by using SHA3 security application. Even if anyone happens to read the file. Accidentally, the original meaning of the information will not be understood. Also we argued that the importance of security and privacy of data stored and retrieved in the cloud.

3-The classification algorithm namely Lazy classifier is used for classifying applicants to tender. The Lazy algorithm KStar techniques was used. By analyzing the experimental results it is observed that the lazy classifier's Kstar classification performed completely with a classification accuracy of 95.8333%.

4-MD5 hashing for secure communication, password to authenticate users.

5- Conference was held using the technique of the voice VOIP: is to assist applicants in the tender for the tender:

A - find each other without chases telephone.

B - Connecting applicants to tender person Administrator to tender to put up their queries.

C - IP phones help to provide the cost of telephone charges.

D - Facilitates network that combines voice and data processes of installation and management.

E - Lead conferences that are made by the sound to reduce travel costs, especially that security.

Conditions experienced by the country may prevent travel on Advanced tender for the reasons may be a curfew ... etc.

6-Cloud computing system has a four protocols which:

-HTTPS: The HTTP Secure protocol was invented to address the security shortfall of HTTP. Users know when HTTPS is transporting web traffic because the URL in the browser's address bar starts with "https://

-SSL: SSL (*pronounced as separate letters*) is short for ***S****ecure* ***S****ockets* ***L****ayer*.

Uses: Can the SSL protocol to encrypt all communications between the ports immediately and without user intervention, which provides security support for all applications, the Internet, especially e-mail, and protocol Tel Net, and FTP, in addition to the various exchanges that take place on the Web, where it can be protected all through SSL FT

- FTP protocol is used to raise any file to the system

REFERENCES

[1]. DESANTIS, MATTHEW,(2008) Understanding Voice over Internet Protocol (VoIP), US-CERT, a government organization.

[2]. Roberto Arcomano berto,(2002) VOIP How TO,P5

[3]. Federal Communications Commission,(2012) Voice Over Internet Protocol(VoIP), Consumer and Governmental Affairs Bureau Consumer Inquiries and Complaints Division

[4]. www.programming-language.board-idea.com

[5]. Schluting, Charlie,(2006) Networking 101: Understanding Multicast Routing

[6]. Bonnette, Rowena ,(2011) Top Benefits of Database Cloud Computing

[7]. Techopedia.,(2013) cloud database,Janalta Interactive Inc

[8]. ITBUSINESSEDGE,(2013) cloud database, QuinStreet Inc.

[9]. Masayuki Okuhara et al,(2010) "Security Architecture for Cloud Computing", FUJITSU Sci. Tech. J., Vol. 46, No.4, pp. 397-402 .

[10]. Viswanathan, Priya,(2014) The Risks Involved in Cloud Computing,

[11]. Winkler, Vic., (2012) Cloud Computing: Virtual Cloud Security Concerns , Technet Magazine, Microsoft.

[12]. Binning , David,(2009)Top five cloud computing security issues, TechTarge.

[13]. Wikipedia,MD4,(2014) Wikimedia Foundation, Inc., a non-profit organization.

[14]. Al-Marakeby,(2013) “Analysis Of MD5 algorithm safety against Hardware Implementation of Brute Force Attack”, International Journal of Advanced Research in Computer and Communication Engineering ,Vol.2,No.9

[15]. Khushdeep Kaur, Er. Seema,(2012) “ Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com

[16]. Ciampa, Mark (2009) CompTIA Security+ 2008 in depth. Australia ; United States: Course Technology/Cengage Learning. p. 290.

[17]. Cruz, José R. C. ,(2011) Finding the New Encryption Standard, SHA-3

[18]. Perlner, Ray,(2012) Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition, National Institute of Standards and Technology.

[19]. S. Vijayarani1& M. Muthulakshmi(,2013) “ Comparative Analysis of Bayes and Lazy Classification Algorithms, International Journal of Advanced Research in Computer and Communication Engineering”Vol. 2, NO. 8.

[20]. C. Lakshmi Devasena1,(2013) “ Classification of Incomplete Multivariate Datasets using Memory Based Classifiers A Proficiency Evaluation., International Journal of Advanced Trends in Computer Science and Engineering”, Vol.2 , No.1.

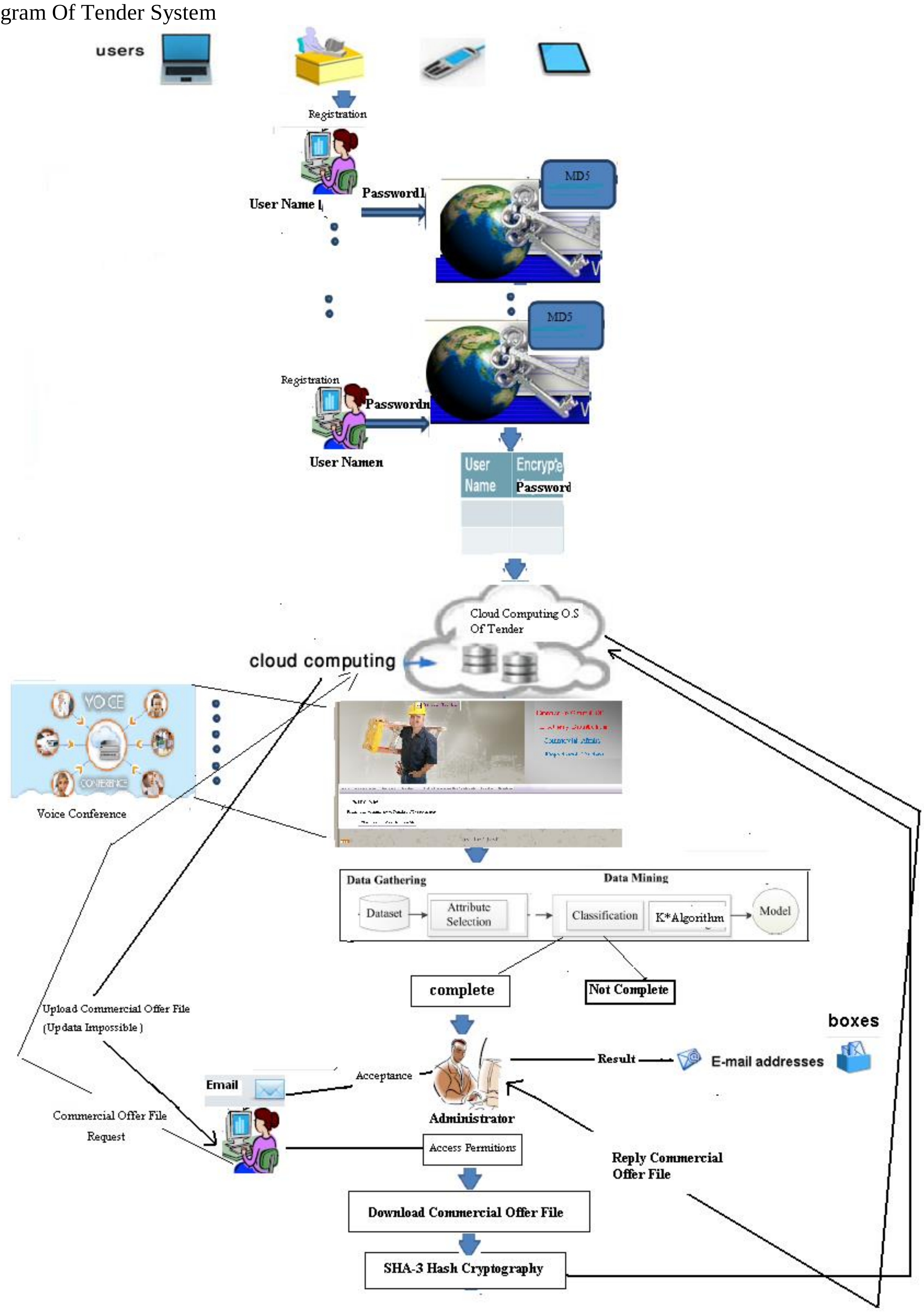
[21]. Anish Bahri, V.Sugumaran & S. Babu Devasenapati,(2013) Misfire Detection in IC Engine using Kstar Algorithm.

[22]. V. Suresh Kumar, M. Aramudhan (2014), "Trust Based Resource Selection and List Scheduling in Cloud Computing", International Journal of Advances in Engineering & Technology, Vol. 6, Issue 6, pp. 2455-2463.

[23]. C. Lakshmi Devasena,(2013) “Classification of Multivariate Data Sets Without Missing Values Using Memory Based Classifiers – An Effectiveness Evaluation”, International Journal of Artificial Intelligence & Applications (IJAIA), Vol.4, No.1, pp 131-132)

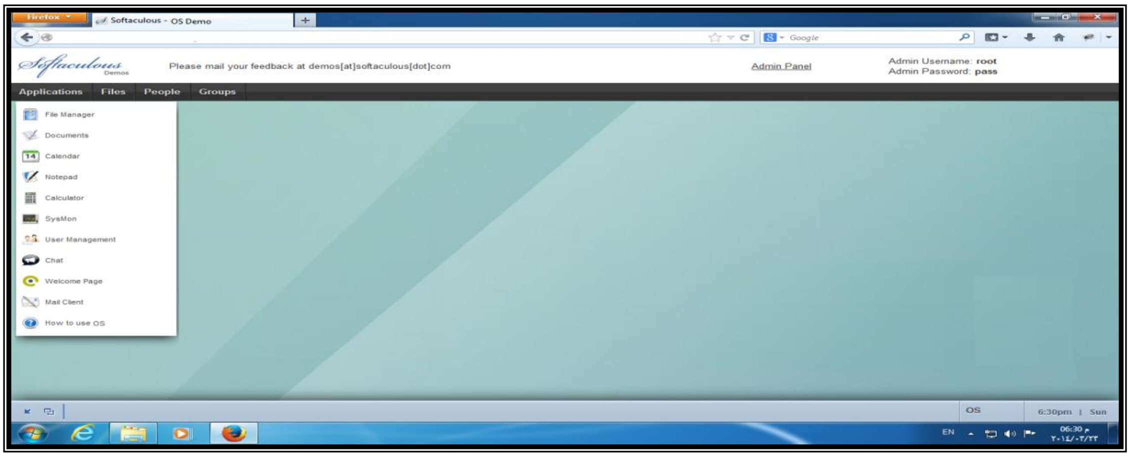
Appendix(1)

Diagram Of Tender System



Appendix(2)

The Application Menu of Cloud Computing

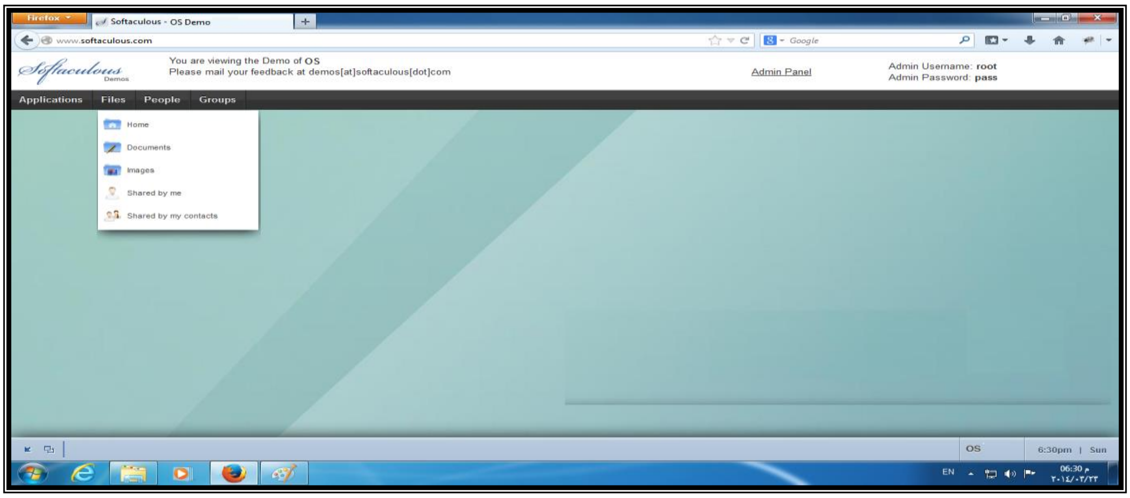


Please mail your feedback at demos[at]softaculous[dot]com

Admin Username: root
Admin Password: pass

Appendix(3)

The File Menu Cloud Computing



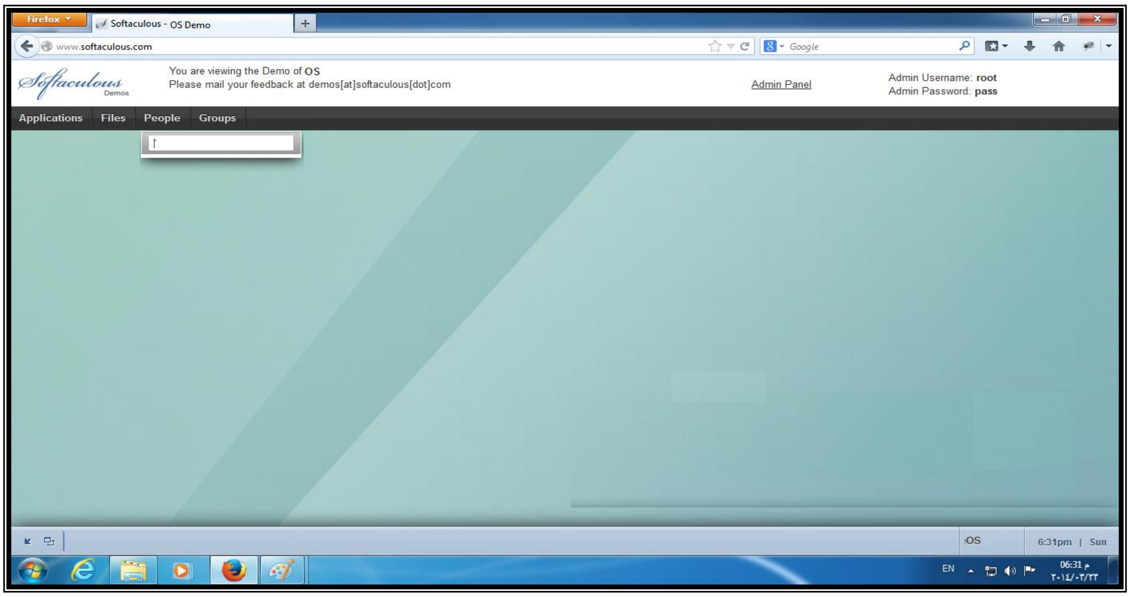
www.softaculous.com

You are viewing the Demo of OS
Please mail your feedback at demos[at]softaculous[dot]com

Admin Username: root
Admin Password: pass

Appendix(4)

The People Menu Cloud Computing



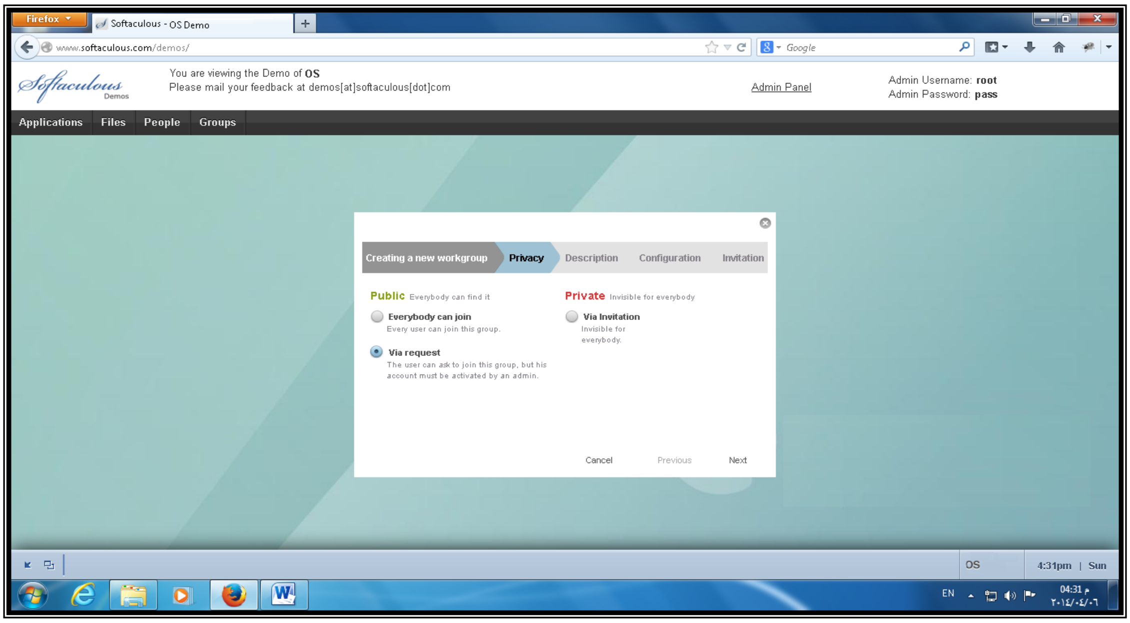
www.softaculous.com

You are viewing the Demo of OS
Please mail your feedback at demos[at]softaculous[dot]com

Admin Username: root
Admin Password: pass

Appendix (5)

The Groups Meue Cloud Computing



You are viewing the Demo of **OS**
Please mail your feedback at demos[at]softaculous[dot]com

Admin Username: **root**
Admin Password: **pass**

Creating a new workgroup | **Privacy** | Description | Configuration | Invitation

Public Everybody can find it

○ Everybody can join
Every user can join this group.

● Via request
The user can ask to join this group, but his account must be activated by an admin.

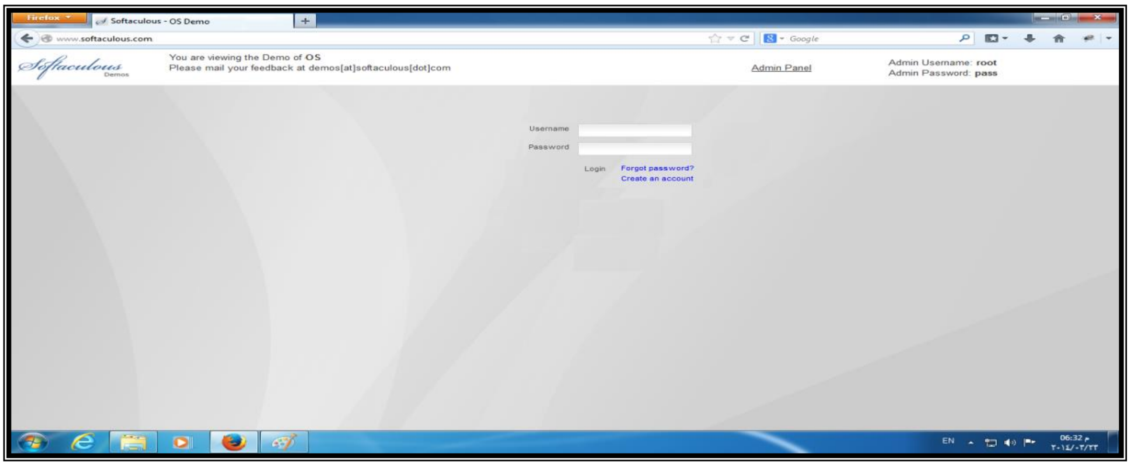
Private Invisible for everybody

○ Via Invitation
Invisible for everybody.

Cancel Previous Next

Appendix(6)

Username & Password form



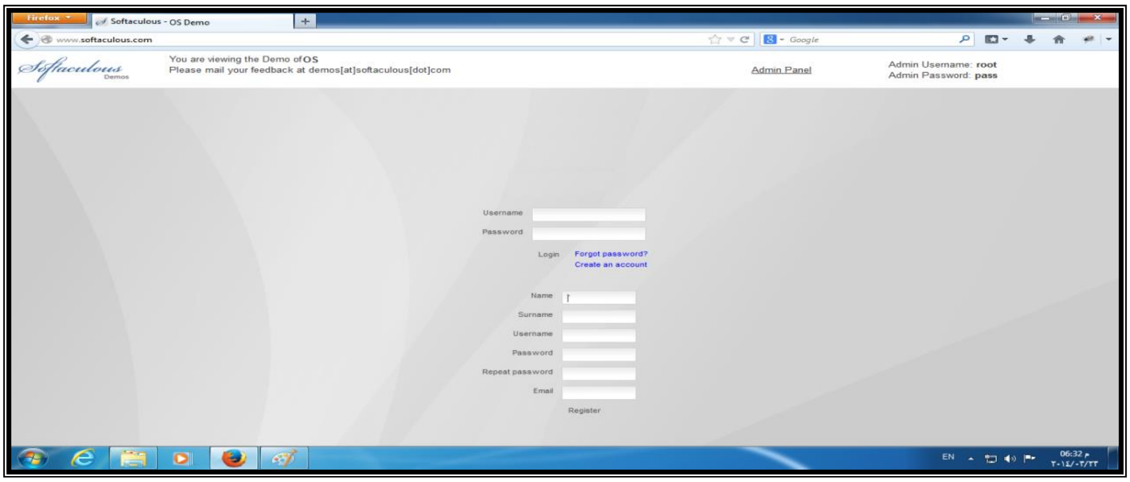
You are viewing the Demo of **OS**
Please mail your feedback at demos[at]softaculous[dot]com

Admin Username: **root**
Admin Password: **pass**

Username
Password
Login Forgot password?
Create an account

Appendix(7)

Join interface for Cloud computing



You are viewing the Demo of **OS**
Please mail your feedback at demos[at]softaculous[dot]com

Admin Username: **root**
Admin Password: **pass**

Username
Password
Login Forgot password?
Create an account

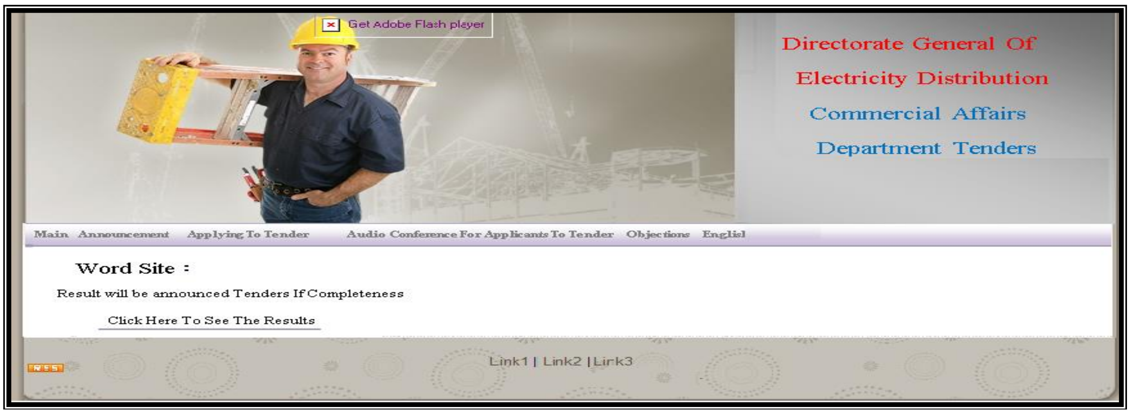
Name
Surname
Username
Password
Repeat password
Email
Register

Appendix(8)

Desktop cloud computing Of Tenders

Appendix(9)

Main form of website


Get Adobe Flash player
Main Announcement Applying To Tender Audio Conference For Applicants To Tender Objections Englisl
Link1 | Link2 | Lirk3
RSS

Directorate General Of
Electricity Distribution
Commercial Affairs
Department Tenders

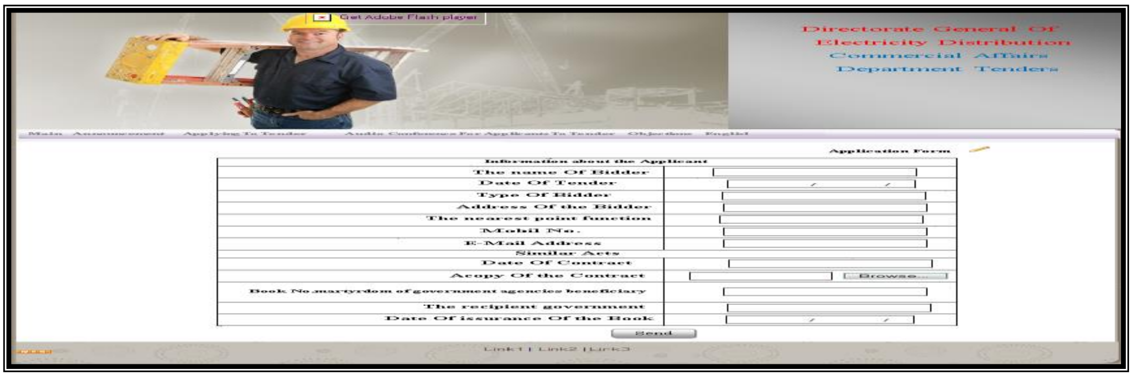
Word Site :

Result will be announced Tenders If Completeness

Click Here To See The Results

Appendix(10)

Applicant form of Tenders Website


Get Adobe Flash player
Main Announcement Applying To Tender Audio Conference For Applicants To Tender Objections Englisl
Browse...
Send
Link1 | Link2 | Lirk3

Directorate General Of
Electricity Distribution
Commercial Affairs
Department Tenders

Application Form

Information about the Applicant

The name Of Bidder

Date Of Tender / /

Type Of Bidder

Address Of the Bidder

The nearest point function

Mobil No.

E-Mail Address

Similar Acts

Date Of Contract

Acopy Of the Contract

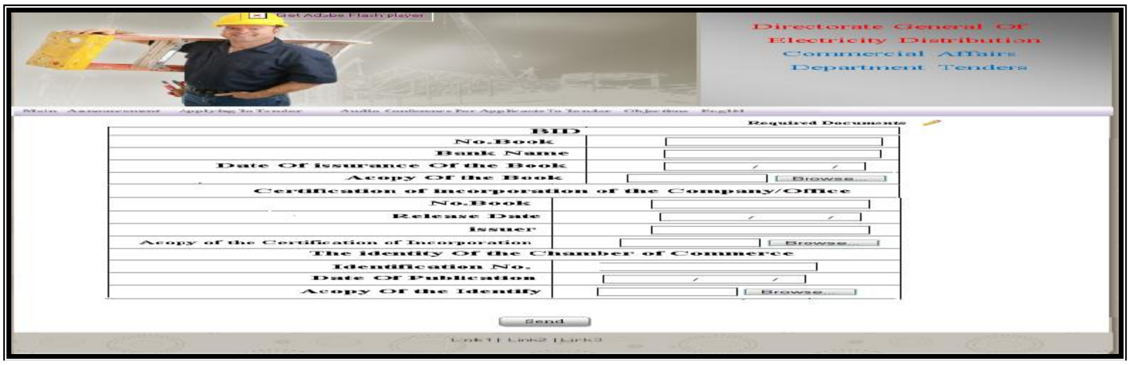
Book No.martyrdom of government agencies beneficiary

The recipient government

Date Of issurance Of the Book / /

Appendix(11)

Required Documents Form 1



Get Adobe Flash player
Main Announcement Applying To Tender Audio Conference For Applicants To Tender Objections English
Link1 | Link2 | Link3

Directorate General Of
Electricity Distribution
Commercial Affairs
Department Tenders

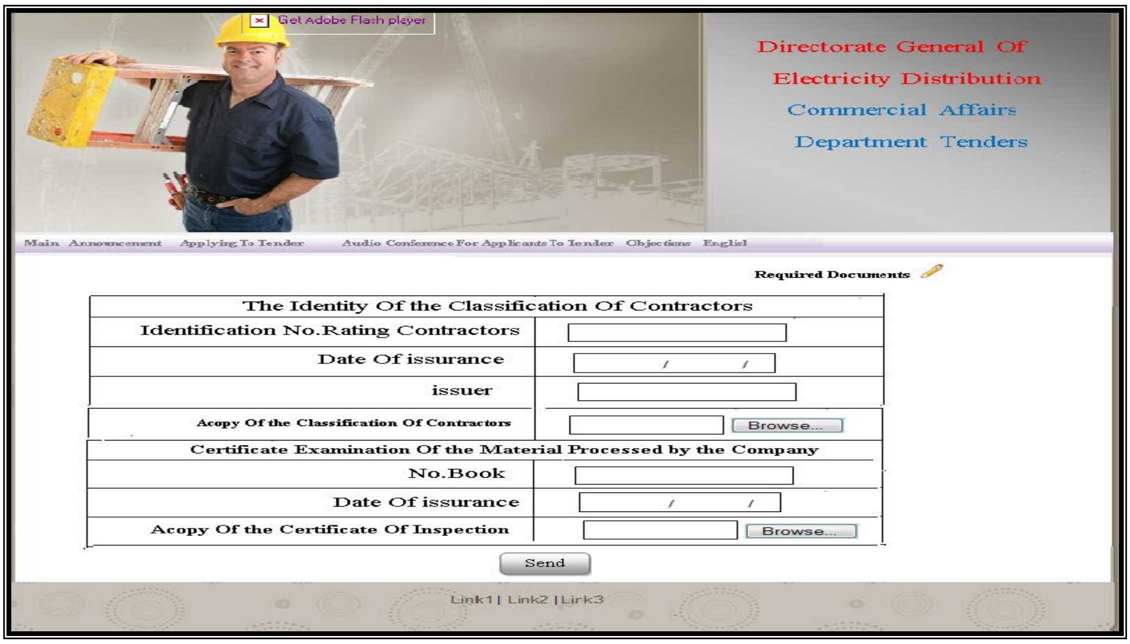
Required Documents

BID	
No.Book	
Bank Name	
Date Of issurance Of the Book	/ /
Acopy Of the Book	Browse...
Certification of incorporation of the Company/Office	
No.Book	
Release Date	/ /
issuer	
Acopy of the Certification of Incorporation	Browse...
The identity Of the Chamber of Commerce	
Identification No.	
Date Of Publication	/ /
Acopy Of the Identify	Browse...

Send

Appendix(12)

Required Documents Form 2



Get Adobe Flash player
Main Announcement Applying To Tender Audio Conference For Applicants To Tender Objections English
Link1 | Link2 | Link3

Directorate General Of
Electricity Distribution
Commercial Affairs
Department Tenders

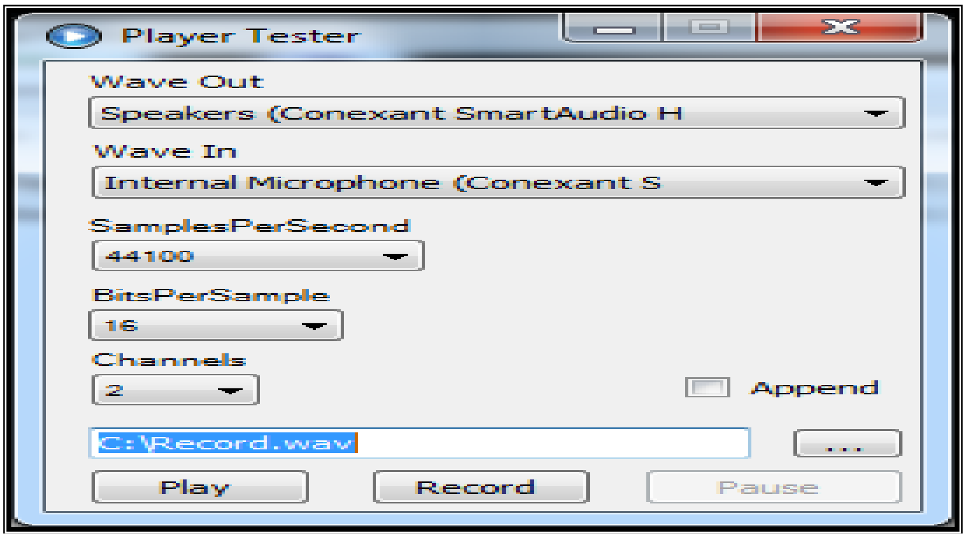
Required Documents

The Identity Of the Classification Of Contractors	
Identification No.Rating Contractors	
Date Of issurance	/ /
issuer	
Acopy Of the Classification Of Contractors	Browse...
Certificate Examination Of the Material Processed by the Company	
No.Book	
Date Of issurance	/ /
Acopy Of the Certificate Of Inspection	Browse...

Send

Appendix(13)

Player Tester



Player Tester

Wave Out
Speakers (Conexant SmartAudio H

Wave In
Internal Microphone (Conexant S

SamplesPerSecond
44100

BitsPerSample
16

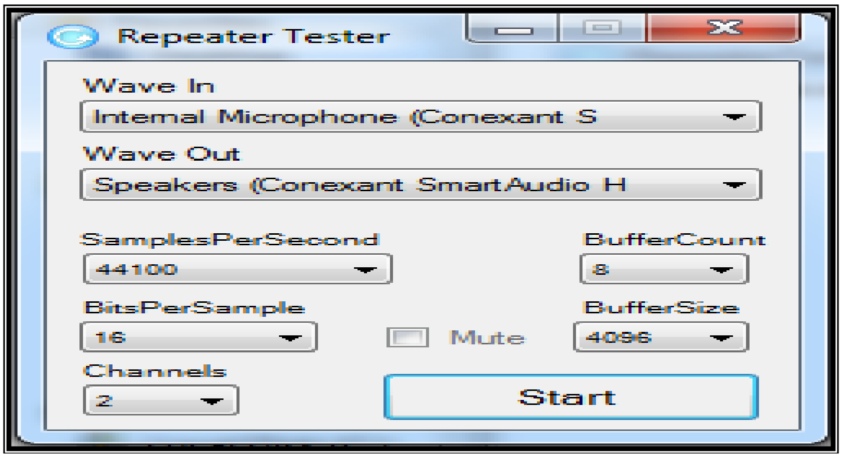
Channels
2

□ Append

C:\Record.wav

Appendix(14)

Repeater Tester



Wave In: Internal Microphone (Conexant S

Wave Out: Speakers (Conexant SmartAudio H

SamplesPerSecond: 44100

BufferCount: 8

BitsPerSample: 16

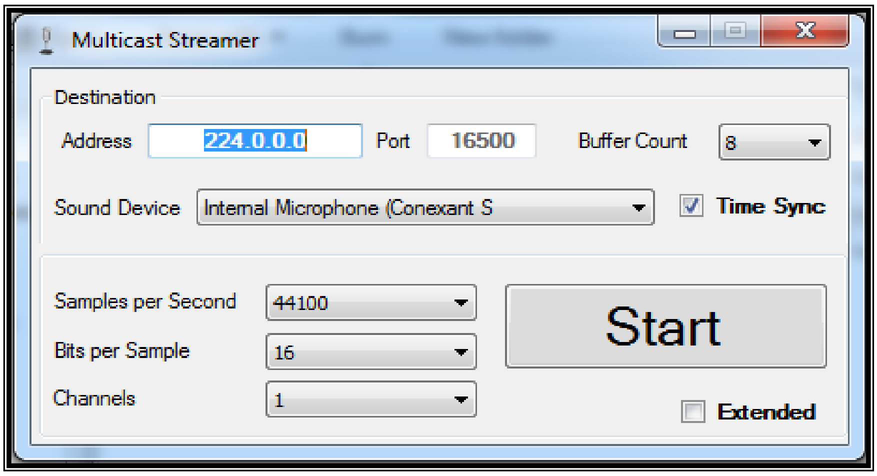
□ Mute

BufferSize: 4096

Channels: 2

Appendix(15)

Multicast Stream



Address: 224.0.0.0 Port: 16500 Buffer Count: 8

Sound Device: Internal Microphone (Conexant S ☑ Time Sync

Samples per Second: 44100

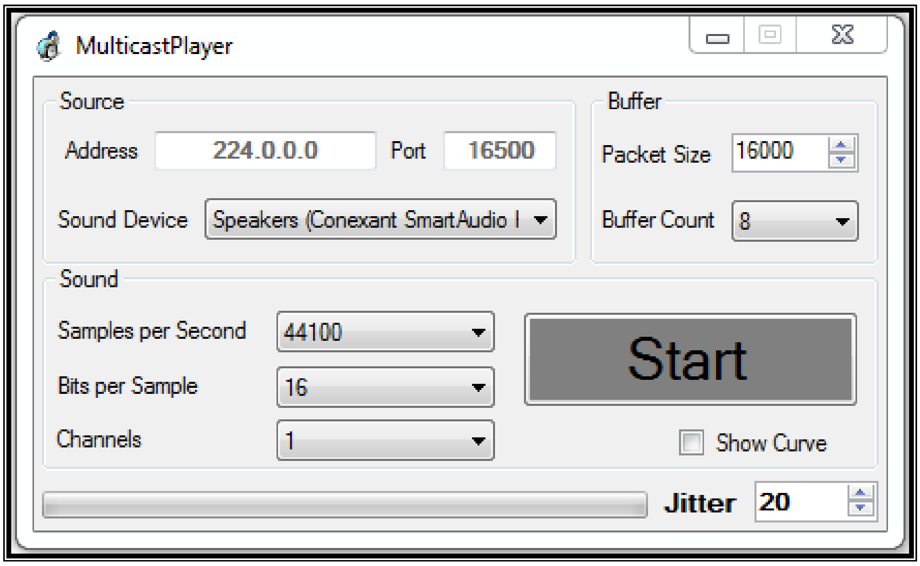
Bits per Sample: 16

Channels: 1

□ Extended

Appendix(16)

Multicast Player



Address: 224.0.0.0 Port: 16500

Sound Device: Speakers (Conexant SmartAudio I

Packet Size: 16000

Buffer Count: 8

Samples per Second: 44100

Bits per Sample: 16

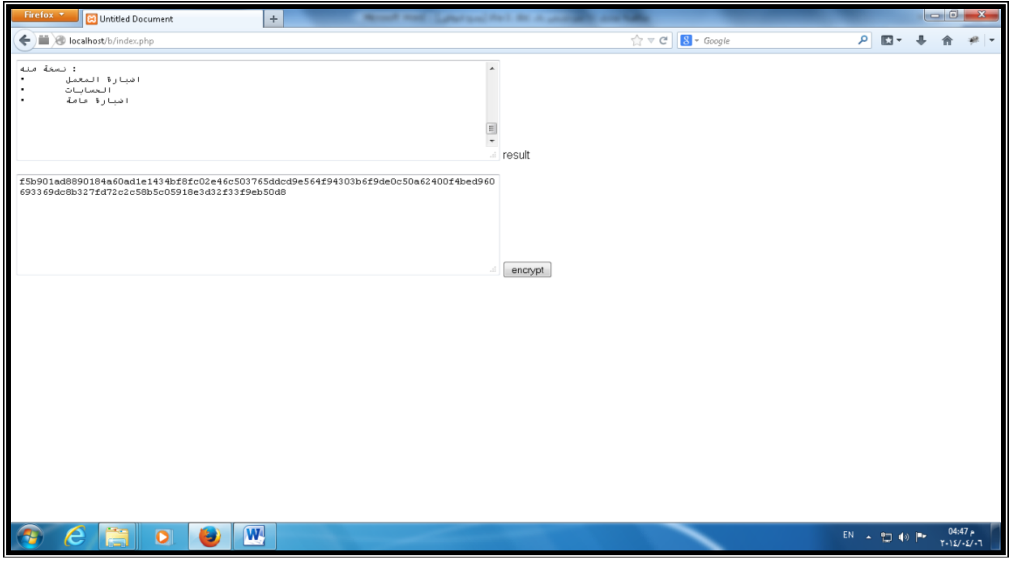
Channels: 1

□ Show Curve

Jitter: 20

Appendix(17)

Encryption / Decryption Commercial offer file By Using SHA3



```
نسخة منه :
•       اضبارة المعمل
•       الحسابات
•       اضبارة عامة
```

```
f5b901ad8890184a60ad1e1434bf8fc02e46c503765ddcd9e564f94303b6f9de0c50a62400f4bed960
693369dc8b327fd72c2c58b5c05918e3d32f33f9eb50d8
```