 ISBN: 978-81-931039-3-7

A NOVEL APPROACH FOR MULTI-KEYWORD SEARCH WITH ANONYMOUS ID ASSIGNMENT OVER ENCRYPTED CLOUD DATA

U.Pandi Priya[1], R.Padma Priya[2]

[1]Research Scholar, Department of Computer Science and Information Technology,
Nadar Saraswathi College of Arts and Science, (India)
[2]Assistant Professor, Department of Computer Application,
Nadar Saraswathi College of Arts and Science, (India)

ABSTRACT

The advancement in cloud computing has motivated the data owners to outsource their data management systems from local sites to commercial public cloud for great flexibility and economic savings. But people can enjoy full benefit of cloud computing if we are able to address very real privacy and security concerns that come with storing sensitive personal information. For real privacy, user identity should remain hidden from CSP (Cloud service provider) and to protect privacy of data, data which is sensitive is to be encrypted before outsourcing. Thus, enabling an encrypted cloud data search service is of great importance. By considering the large number of data users, documents in the cloud, it is important for the search service to allow multikeyword query and provide result similarity ranking to meet the effective need of data retrieval search and not often differentiate the search results. In this system, we define and solve the challenging problem of privacy-preserving multikeyword ranked search over encrypted cloud data (MRSE), and establish a set of strict privacy requirements for such a secure cloud data utilization system to be implemented in real.

We first propose a basic idea for the Multi-keyword Ranked Search over Encrypted cloud data (MRSE) based on secure inner product computation and efficient similarity measure of coordinate matching, i.e., as many matches as possible, in order to capture the relevance of data documents to the search query, then we give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Assignment of anonymous ID to the user to provide more security to the data on cloud server is done. To improve the search experience of the data search service, further extension of the two schemes to support more search semantics is done.

Keywords: Cloud Computing, Keyword Search, Mrse, Privacy Preserving, Ranked Search Anonymization, Searchable Encryption,

I. INTRODUCTION

Cloud computing is the long dreamed vision of computing as a utility, where cloud customers remotely store their data into the cloud so as to enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources. Its great flexibility and economic savings are motivating both individuals and enterprises to outsource their local complex data management system into the cloud. To protect privacy of

Data and oppose unsolicited accesses in the cloud and beyond it, sensitive data, for instance, e-mails, personalhealth records, photo albums, tax documents, and so on, may have to be encrypted by data owners before Outsourcing to the commercial public cloud; this, however, obsoletes the traditional data utilization service based on plaintext keyword search. The insignificant solution of downloading all the data and decrypting locally is clearly impractical, due to the large amount of bandwidth cost in cloud scale systems. Images also contain useful and important information, so proposed system also provides image tagging in MRSE scheme [1]. Moreover, aside from eliminating the local storage management, storing data into the cloud doesn't serve any purpose unless they can be easily searched and utilized. Hence, exploring privacy preserving and effective search service over encrypted cloud data is of great importance. Considering potentially huge number of on-demand data users and large amount of outsourced data documents in the cloud, this problem is particularly challenging as it is extremely difficult to meet also the requirements of performance, system usability, and scalability. Document ranking is provided for fast search, but the priorities of all the data documents is kept same so that the cloud service provider and third party remains unaware of the important documents, thus, maintaining privacy of data. Ranked search can also elegantly eliminate unnecessary network traffic by sending back only the most relevant data, which is highly desirable in the "pay-as-you-use" cloud paradigm. For privacy protection, such ranking operation, however, should not leak any keyword related information. Besides, to improve search result accuracy as well as to enhance the user searching experience, it is also necessary for such ranking system to support multiple keyword searches, as single keyword search often yields far too coarse results. As a common practice indicated by today's web search engines (ex. Google search), data users may tend to provide a set of keywords instead of only one as the indicator of their search interest to retrieve the most relevant data. Along with the privacy of data and efficient searching schemes, real privacy is obtained only if the user's identity remains hidden from the Cloud Service Provider (CSP) as well as the third party user on the cloud server.

II. MODELS

2.1 System Model

Considering a cloud data hosting service involving three different entities, the data owner, the data user, and the cloud server. The data owner has a collection of data documents *F* to be outsourced to the cloud server in the encrypted form *C*. To enable the searching capability over *C* for effective data utilization, the data owner, before outsourcing, will first build an encrypted searchable index *I* from *F*, and then outsource both the index *I* and the encrypted document collection *C* to the cloud server. To search the document collection for *t* given keywords, an authorized user acquires a corresponding trapdoor *T* through search control Mechanisms, e.g., broadcast encryption. Upon receiving *T* from a data user, the cloud server is responsible to search the index *I* and return the corresponding set of encrypted documents. To improve the document retrieval accuracy, the search result should be ranked by the cloud server according to some ranking criteria (e.g., coordinate matching, as will be introduced shortly). Moreover, to reduce the communication cost, the data user may send an optional number *k* along with the trapdoor *T* so that the cloud server only sends back top-*k* documents that are most relevant to the search query. Finally, the access control mechanism is employed to manage decryption capabilities given to users.

2.2 Threat Model

The cloud server is considered as "honest-but-curious" in our model, which is consistent with related works on cloud security [24], [25]. Specifically, the cloud server acts in an "honest" fashion and correctly follows the designated protocol specification. However, it is "curious" to infer and analyze data (including index) in its storage and message flows received during the protocol so as to learn additional information. Based on what information the cloud server knows, we consider two threat models with different attack capabilities as follows.
Known Cipher text Model. In this model, the cloud server is supposed to only know encrypted dataset *C* and searchable index *I*, both of which are outsourced from the data owner. Known Background Model In this stronger model, the cloud server is supposed to possess more knowledge than what can be accessed in the Known Cipher text Model. Such information may include the correlation relationship of given search requests (trapdoors), as well as the dataset related statistical information. As an instance of possible attacks in
This case, the cloud server could use the known trapdoor information combined with document/keyword frequency to deduce/identify certain keywords in the query.

2.3. Design Goals

To enable ranked search for effective utilization of outsourced cloud data under the aforementioned model, our System design should simultaneously achieve security and performance guarantees as follows.
• Multi-keyword Ranked Search: To design search schemes which allow multi-keyword query and provide Result similarity ranking for effective data retrieval, instead of returning undifferentiated results.
• Privacy-Preserving: To prevent the cloud server from learning additional information from the dataset and the index, and to meet privacy requirements.
• Efficiency**:** Above goals on functionality and privacy should be achieved with low communication and computation overhead.

2.4 Preliminary on Coordinate Matching

As a hybrid of conjunctive search and disjunctive search, "coordinate matching" [4] is an intermediate similarity measure which uses the number of query keywords appearing in the document to quantify the relevance of that document to the query. When users know the exact subset of the dataset to be retrieved, Boolean queries perform well with the precise search requirement specified by the user. In cloud computing, however, this is not the practical case, given the huge amount of outsourced data. Therefore, it is more flexible for users to
Specify a list of keywords indicating their interest and retrieve the most relevant documents with a rank order.

III. FRAMEWORK AND PRIVACY REQUIREMENTS FOR MRSE

In this section, we define the framework of multi-keyword ranked search over encrypted cloud data (MRSE) and establish various strict system-wise privacy requirements for such a secure cloud data utilization system.

3.1MRSE Framework

For easy presentation, operations on the data documents are not shown in the framework since the data owner could easily employ the traditional symmetric key cryptography to encrypt and then outsource data. With focus on the index and query, the MRSE system consists of four algorithms as follows.
• **Setup (1*ℓ*)** Taking a security parameter ℓ as input, the data owner outputs a symmetric key as SK.

• **Build Index (*F, SK*)** Based on the dataset F, the data owner builds a searchable index I which is encrypted by The symmetric key SK and then outsourced to the cloud server. After the index construction, the document collection can be independently encrypted and outsourced.

• **Trapdoor (f*W*)** with t keywords of interest in fW as input, this algorithm generates a corresponding trapdoor TfW.

• **Query(*TfW, k, I*)** When the cloud server receives a query request as (TfW, k), it performs the ranked search on the index I with the help of trapdoor TfW, and finally returns FfW, the ranked id list of top-k documents sorted by their similarity with fW.

Neither the search control nor the access control is within the scope of this paper. While the former is to regulate how authorized users acquire trapdoors, the later is to manage users' access to outsourced documents.

3.2. Privacy Requirements for MRSE

The representative privacy guarantee in the related literature, such as searchable encryption, is that the server should learn nothing but search results. With this general privacy description, we explore and establish a set of strict privacy requirements specifically for the MRSE framework. As for the *data privacy*, the data owner can resort to the traditional symmetric key cryptography to encrypt the data before outsourcing, and successfully prevent the cloud server from prying into the outsourced data. With respect to the *index privacy*, if the cloud server deduces any association between keywords and encrypted documents from index, it may learn the major subject of a document, even the content of a short document. Therefore, the searchable index should

Be constructed to prevent the cloud server from performing such kind of association attack. While data and index privacy guarantees are demanded by default in the related literature, various *search privacy* requirements involved in the query procedure are more complex and difficult to tackle as follows.

IV. PROPOSED ALGORITHM

4.1Homo Morphic Token Pre-computation

Homomorphism encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. This is sometimes a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption.

4.2 Algorithm

1: **procedure**

2: Choose parameters l, n and function f;

3: Choose the number t of tokens;

4: Choose the number r of indices per

Verification;

5: Generate master key

6: **for** vector G(j), j ← 1, n **do**

7: **for** round i← 1, t **do**

8: Derive _i = fkchal (i) and k(i) prp
from KPRP .
9: Compute v (j)
i =Pr
q=1 * G(j)[_k(i)prp (q)]
10: **end for**
11: **end for**
12: Store all the vis locally.
13: **end procedure**

V. PROPOSED SYSTEM

Considering a cloud data hosting service involving three different entities, the data owner, the data user along with his ID, and the cloud server. The data owner first registers on cloud using anonymity algorithm for cloud computing services. Before saving user registration information to database present on cloud anonymous algorithm process the data and then anonymous data is saved to registration database. The data owner has a collection of data documents F to be outsourced to the cloud server in the encrypted form C. To enable searching capability over C for effective data utilization, the data owner, will first build an encrypted searchable index I from F before outsourcing , and then outsource both the index I and the encrypted document collection C to the cloud server. The work deals with efficient algorithms for assigning identifiers (IDs) to the users on the cloud in such a way that the IDs are anonymous using a distributed computation with no central authority. Given are N nodes, this assignment is essentially a permutation of the integers {1….N} with each ID being known only to the node to which it is assigned. Our main algorithm is based on a method for anonymously sharing Simple data and results in methods for efficient sharing of complex data. To search the document collection for given keywords, an authorized user having an ID acquires a corresponding trapdoor T through search control Mechanisms, for example, broadcast encryption. On receiving T from a data user, cloud server is responsible to Search the index I and then returns the corresponding set of encrypted documents. In order to improve the document retrieval accuracy, the search result should be ranked by the cloud server according to some ranking criteria (e.g., coordinate matching) and assigning anonymous ID to the user on cloud in order to make the data on cloud more secure. Moreover, to reduce the cost of communication the data user may send an optional number k along with the trapdoor T so that the cloud server only sends back top-k documents that are most relevant to the search query. At last, the access control mechanism is employed in order to manage decryption capabilities given to users and the data collection can be updated in terms of inserting new documents, updating existing ones, and deleting the existing documents.

VI. CONCLUSION

The previous work mainly focused on providing privacy to the data on cloud in which using multi-keyword ranked search. In this paper, for the first time we define and solve the problem of multi-keyword ranked search over encrypted cloud data using Homomorphism token Pre-Computation and establish a variety of privacy requirements. There was a need to provide more real privacy which this paper presents. In this system, stringent privacy is provided by assigning the cloud user a unique ID. This user ID is kept hidden from the cloud service

provider as well as the third party user in order to protect the user's data on cloud from the CSP and the third party user. Thus, by hiding the user's identity, the confidentiality of user's data is maintained.

REFERENCES

[1] Ankatha Samuyelu Raja Vasanthi ," Secured Multi keyword Ranked Search over Encrypted Cloud Data", 2012

[2] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.

[3] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptograpy and Data Security, Jan.2010.

[4] Y. Prasanna, Ramesh . "Efficient and Secure Multi-Keyword Searchon Encrypted Cloud Data", 2012.

[5] Jain Wang, Yan Zhao , Shuo Jaing, and Jaijin Le, "Providing Privacy Preserving in Cloud Computing",2010.

[6] Larry A. Dunning, Ray Kresman ," Privacy Preserving Data Sharing With Anonymous ID ssignment",2013.

[7] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010.

[8] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, pp. 693-701, 2012.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, 2010.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, 2010.

[11] N. Cao, Z. Yang, C. Wang, K. Ren, and W. Lou, "Privacy preserving Query over Encrypted Graph-Structured Data in Cloud Computing," Proc. Distributed Computing Systems (ICDCS), pp. 393-402, June,2011. Shiba Sampat Kale et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7093-7096 www.ijcsit.

 ISBN: 978-81-931039-3-7

STUDY OF VARIOUS NETWORK TYPE SECURITY PROTOCOLS

Sudhakar Singh[1], P.K. Khare[2], Prashant Mor[3]

[1] Research Scholar, [2] Professor and Head, [3] Scientific Officer,

Department of Physics and Electronic, RDVV, Jabalpur (M.P.),(India)

ABSTRACT

In information technology, a protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols specify interactions between the communicating entities. Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. In the standard model known as Open Systems Interconnection (OSI), there are one or more protocols at each layer in the telecommunication exchange that both ends of the exchange must recognize and observe. In recent years, wireless networks have gained rapid popularity. Wireless networks are inexpensive and provides mobility but they are prone to a variety of threats like denial of service, replay attacks, eavesdropping and data modification. A security protocol or cryptographic protocol or encryption protocol is an abstract or concrete protocol that performs a security related function and applies cryptographic methods, often as sequences of cryptographic primitives. A protocol describes how the algorithms should be used. A sufficiently detailed protocol includes details about data structures and representations at which point it can be used to implement multiple, interoperable versions of a program. Cryptographic protocols are widely used for secure application level data transport. This paper presents the various network types and its related security protocols architecture and applications.

Keywords- TCP/IP, Wi-Fi, Bluetooth, Sensor Network, SPINS

I. INTRODUCTION

The Internet protocols are the world's most popular open-system protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications. The Internet protocols consist of a suite of communication protocols of which the two best known are the Transmission Control Protocol (TCP) and the Internet Protocol (IP). The Internet protocol suite not only includes lower layer protocols (such as TCP and IP), but it also specifies common applications such as electronic mail, terminal emulation and file transfer. Internet protocols were first developed in the mid 1970s, when the Defense Advanced Research Projects Agency (DARPA) became interested in establishing a packet switched network that would facilitate communication between dissimilar computer systems at research institutions. With the goal of heterogeneous connectivity in mind, DARPA funded research by Stanford University and Bolt, Beranek and Newman (BBN). The result of this development effort was the Internet protocol suite, completed in the late 1970s. TCP/IP later was included with Berkeley Software Distribution (BSD) UNIX and has since become the foundation on which the Internet and the World Wide Web (WWW) are based**[1]**.

When computers talk over the Internet, the language they speak is the TCP/IP. It is also the protocol of choice for most medium and large-sized networks. Novell Netware, UNIX and Window NT networks can all implement TCP/IP, particularly on growing networks and on ones that use client/server or web-based applications. TCP/IP is one of the oldest protocols and is proven technology that is used by millions of computer users around the globe. Its broad acceptance, reliable history and extensive capabilities make it a good choice for most LAN-to-WAN installations. The TCP/IP protocol suite, used in the Internet, was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not match exactly with those in the OSI model. The TCP/IP protocol suite is made of five layers.

- Application layer
- Transport layer
- Internet layer
- Network access layer
- Physical layer

The first four layers provide physical standards, network interface, Internet working and transport functions that correspond to the first four layers of the OSI model. The three top most layers in OSI model however are represented in TCP/IP by a single layer called the application layer Figure 1**[1-2]**. A number of applications have been standardized to operate on top of TCP. We define three of the most common here.

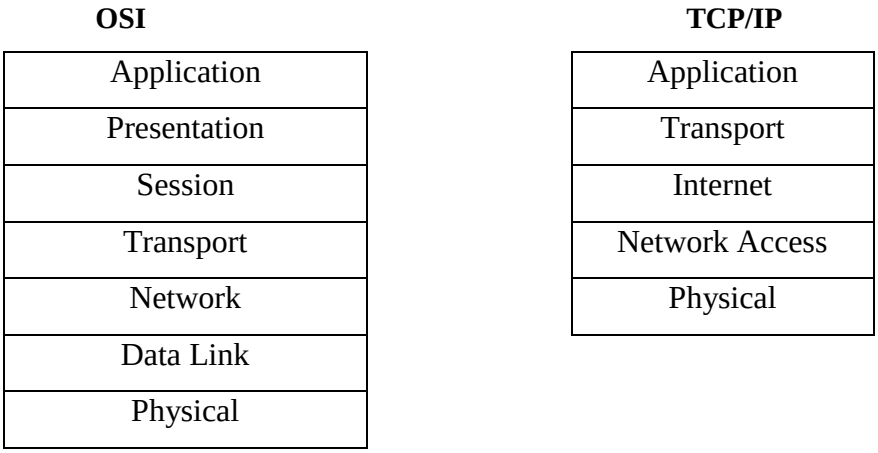


Figure 1: Comparison of OSI and TCP/IP Model

1.3 Simple Mail Transfer Protocol (Smtp)

SMTP provides a basic electronic mail facility. It provides a mechanism for transferring messages among separate hosts. Features of SMTP include mailing lists, return receipts and forwarding. Once a message is created, SMTP accepts the message and makes use of TCP to send it to an SMTP module on another host. The target SMTP module will make use of local electronic mail package to store the incoming message in user's mailbox.

1.2 File Transfer Protocol (Ftp)

FTP is used to send files from one system to another under user command. Both text and binary files are accommodated and the protocol provides features for controlling user access. When a user wishes to engage in file transfer, FTP sets up a TCP connection to the target system for the exchange of control messages. This connection allows user ID and password to be transmitted and allows the user a file transfer is approved a second TCP connection is set-up for the data transfer. The file is transferred over the data connection, without

the overhead of any headers of control information at the application level. When the transfer is complete, the control connection is used to single the completion and to accept new file transfer commands.

1.3 Telnet (Terminal Network)

The main task of the Internet and its TCP/IP protocol suite is to provide services for users. For example, users want to be able to run different application programs at a remote site and create results that can be transferred to their local site. One way to satisfy these demands is to create different client-server application programs for each desired service. Program such as file transfer programs (FTP), e-mail (SMTP) and so on are already available. But it would be impossible to write a specific client-server program for each demand.

The better solution is a general purpose client-server program that lets user access any application program on a remote computer, in other words, allow the user to log on to a remote computer. After logging on, a user can use the services available on the remote computer and transfer the results back to the local computer. TELNET is an abbreviation of Terminal Network. Client-server application program is called TELNET.

II. SECUTITY PROTOCOLS

Security is becoming more and more crucial as the volume of data being exchanged on the Internet increases. Various protocols have been developed to measure security, which can be applied to the application layer and IP layer.

2.1 Secure Socket Layer

Secure sockets Layer (SSL) is the Internet security protocol for point-to-point connection. With the growth of the Internet, many applications need to securely transmit data to remote applications and computers. SSL was designed to solve this problem. Many popular web browsers like Netscape communication and Internet Explorer use SSL to protect again eavesdropping, tampering, and forgery. In SSL, when clients and servers make connections they authenticate each other. Once authenticated a “secure pipe” is established and data can be securely exchanged as shown in Figure 2**[1-3]**. SSL uses the strong encryption technologies from RSA Data Security. Some practical application of SSL is.

- Client/Server systems: Securing database access
- Financial: Remote banking programs
- Information systems: Remote access and administration application
- Travel industry: Create online reservation systems and secure information transfer

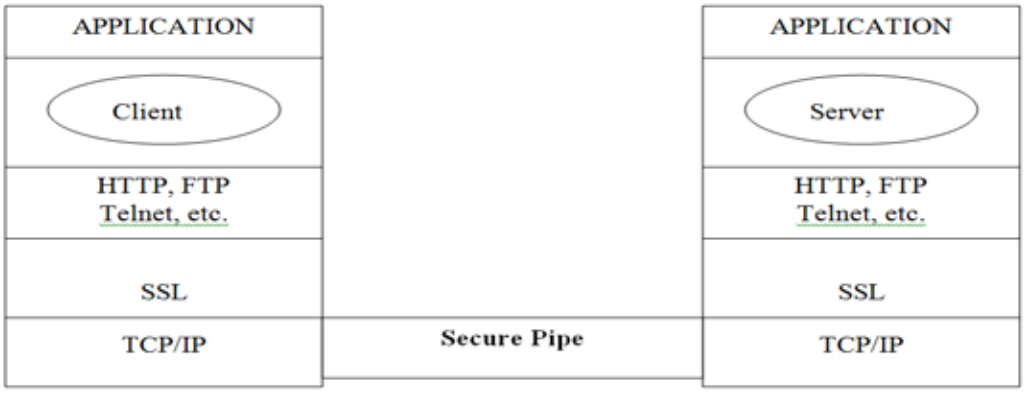
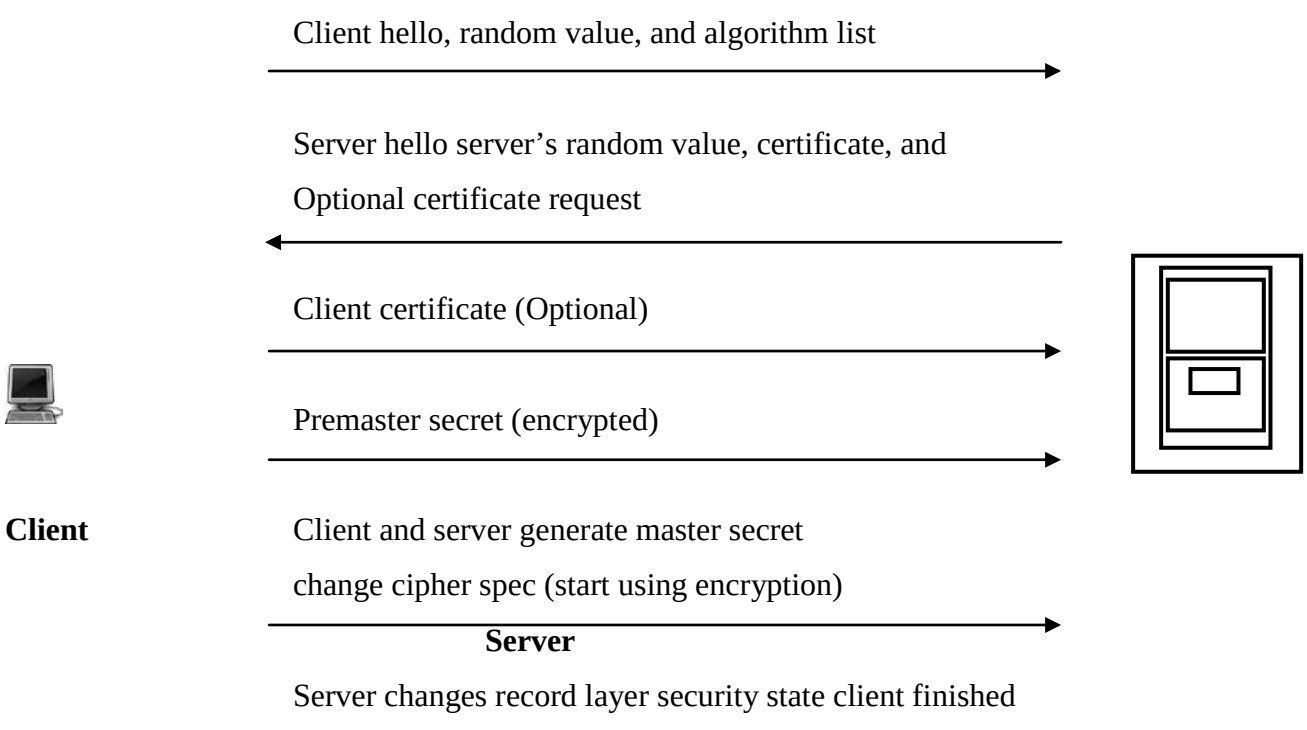


Figure: 2 Secure Socket Layer

2.2 Transport Layer Security

The IETF established the TLS working group in 1996 to develop a standard transport security protocol. The working group began with SSL version 3, as its basis and released RFC 2246, TLS protocol version 1.0 in 1999 as a proposed standard. The working group also published RFC 2712, "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)" as a proposed standard, and two RFCs on the use of TLS with HITP. Like its predecessor, TLS is a protocol that ensures privacy between communicating applications and their uses on Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. Transport Layer Security (TLS) is composed of two parts. The TLS Record Protocol and the TLS Handshake protocol. The TLS Record Protocol provides connection security by using supported encryption methods, such as the data encryption standard (DES). The TLS Record protocol can also be used without encryption. The TLS Handshake protocol allows the server and the client to authenticate each other and to negotiate a session encryption algorithm and cryptographic keys before data is exchanged.

Though TLS is based on SSL and is sometimes referred to as SSL, They are not interoperable. However, the TLS protocol does contain a mechanism that allows a TLS implementation to back down to SSL 3.0. The difference between the two is in the way they perform key expansion and message authentication computation. TLS uses the MD5 and SHA (Secure Hash Algorithm) algorithms together to determine the session key. Though SSL also uses both hashing algorithms, SSL is considered less secure because the way it uses them forces a reliance on MD5 rather than SHA. The TLS Record Protocol is a layered protocol. At each layer, message may include fields for length, description and content. The record protocol takes messages to be transmitted, fragments the data into manageable blocks, optionally compressed the data, applied a message authentication code (MAC) to the data, encrypt it and transmits the result. Received data decrypted verified, decompressed and reassembled and then delivered to higher-level clients. The TLS Handshake protocol involves the following steps, which are summarized in Figure 3**[1-2,5]**.



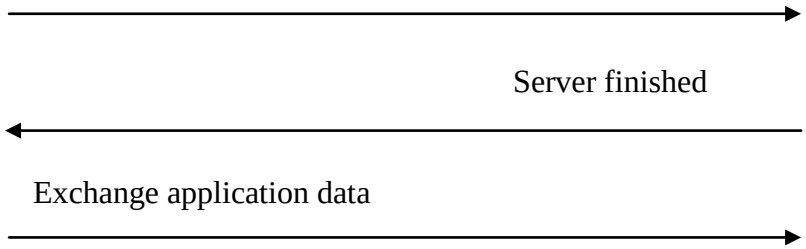


Figure 3: TLS Handshake Protocol

Step 1: Exchange hello messages to agree on algorithms, exchange random values and check for session resumption.

Step 2: Exchange the necessary cryptographic parameters to allow the client and server to agree on a per-master secret.

Step 3: Exchange certificates and cryptographic information to allow the client and server to authenticate them selves.

Step 4: Generate a master secret from the premaster secret and exchanged random values.

Step 5: Provide security parameters to the record layer.

Step 6: Allow the client and server to verify that their peer has calculated the same security parameters and that the handshake occurred without tempering by an attacker.

Though it has been designed to minimize this risk, TLS still has potential vulnerabilities to a man in the middle attack. A highly-spilled and well-placed attacker can force TLS to operate at lower security levels. Regardless, through the use of validated and trusted certificates, a secure cipher suit can be selected for the exchange of data. Once established, a TLS session remains active as long as data is being exchanged. If sufficient inactive time has elapsed for the secure connection to time out, it can be reinitiated.

2.3 IPsec

Internet protocol security (IPSec), a set of protocols developed by the Internet Engineering Task Force (IETF) for encryption and authentication of TCP/IP traffic, is the leading standard for cryptographically-based authentication, integrity and privacy services. At the IP layer, computers on a network communicate by routing datagram packets that contain data, destination addresses, source addresses and other information. In a corporate LAN or the Internet where packet datagram's are transmitted "as is" unencrypted a corporate attacker could hijack, forge or modify them. IPSec secures the network packets to create a secure network of computers over insecure channels. It enables users to communicate securely with a remote hast over the Internet via VPNs. Where SSL authentication and encrypts communication between clients and servers at the application layers, IPSec secures the underlying network layers. IPSec provides the capability to secure communication across a LAN, across private and public WAN's and across the Internet. Some practical applications of IPSec are.

(i) A company can build a secure virtual private network over the internet or over a public WAN. This enables a business to rely heavily on the internet and reduce its need for private networks, saving costs and network management overhead.

(ii) An end user whose system is equipped with IP security protocols can make a local call to an internet service provider (ISP) and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecomputers.

(iii) IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

The principle feature of IPSec that enables it to support these varied applications is that I can encrypt and/or authenticate all traffic at the IP level. Thus all distributed applications, including remote login, client/server, email, file transfer, web access and so on, can secured. Following are benefits of IPSec **[1]**:

(i) When IPSec is implemented is a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

(ii) IPSec in a firewall is a resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the internet into the organization.

(iii) IPSec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPSec is implemented in the firewall or router. Even if IPSec is implemented in end systems, upper-layer software, including applications is not affected.

(iv) IPSec can be transparent to the end users. There is no need to train users on security mechanisms issue keying material on a per user basis, or revoke keying material when users leave the organization.

(v) IPSec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual sub network within an organization for sensitive applications.

IPSec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s) and put in place any cryptographic keys required to provide the requested services. Two protocols are used to provide security: an authentication protocol designed by the header of the protocol, Authentication Header (AH); and a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP). The services are provided by the AH and ESP protocol which are shown in Table1**[1,4]**.

Table 1: IPSec services

Services	AH	ESP (Encryption Only)	ESP (Encryption plus Authentication)
Access control	√	√	√
Connectionless integrity	√		√
Data origin authentication	√		√
Rejection of replayed packets	√	√	√
Confidentiality (encryption)		√	√
Limited traffic flow confidentiality		√	√

A key concept that appears in both the authentication and confidentiality mechanisms for IP is the security association (SA). In any IP packet, the security association is uniquely identified by the destination address in the IPv 4 or IPv 6 header.

2.4 Authentication Header (Ah)

The Authentication Header provides connectionless integrity and data origin authentication for IP datagram's. It also optionally provides protection against replays. The AH header is shown in figure 4**[1,5]**. It is either follows the IPv4 header or is an IPv6 extension header, depending on which version of IP it is used with.

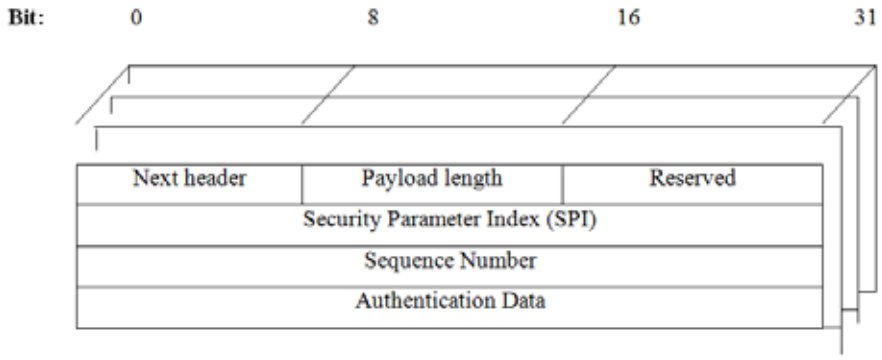


Figure 4 IPSec Authentication Header

The next header field identifies the type of the next payload after the Authentication Header. The payload length field specifies the length of the AH in 32-bit words (4-byte units), minus 2. The reserved field is reserved for future use; it is set to zero for now. The security parameter index (SPI) field is an arbitrary 32-bit value that, in combination with the destination IP address, uniquely identifies the security association for this datagram. The sequence number field contains a monotonically increasing counter or sequence number. This field is used to protect against replay, but it is present even if the receiver does not elect to enable the anti replay service for a specific SA (Security Association). The sender counter and the receiver's counter are initialized to 0 when an SA is established. If anti replay is enabled, which is the default, the transmitted sequence number must never be allowed to cycle. Thus the sender's counter and the receiver's counter must be reset by establishing a new SA and thus a new key prior to transmitting the $2^{32\ nd}$ packet on an SA. Finally, Authentication Data is a variable length field that contains the message integrity code for this packet. The field must be an integral multiple of 32 bits in length. All does not prescribe a specific message digest algorithm. DES and MD5 among others can be used.

2.5 Encapsulation Security Payload (Esp)

The Encapsulating security payload provides confidentiality services, including confidentiality of message contents and limited traffic flow confidentially. As an optional feature, ESP can also provide the same authentication services as AH. ESP header is designed to provide a mix of security services in IPv4 and IPv6. ESP may be applied alone, or in combination with AH. The ESP header is inserted after the IP header and before the upper-layer protocol header (when used between a pairs of hosts) or before an encapsulated IP header when used to tunnel between a pair of security gateways. Like AH, the ESP header either follows the IPv4 header or is an IPv6 extension header. Its format is shown in Figure 5**[1-4]**. The security parameter index (SPI) field has the same function as in the AH. It helps the receiving host identify the security association to which the packet belongs.

Similarly, the sequence number field protects against replay attacks. The packets payload Data contains the data described by the next header field. If confidentiality is selected, then the data is encrypted by whatever encryption algorithm was associated with the security Association. Padding is sometimes necessary, for

example, because the encryption algorithm requires the plaintext to be a multiple of some number of bytes or to ensure that the resulting cipher text terminates on a 4-bytes boundary. The pad length field records how much padding was added to the data. Finally, the Authentication Data Carrier Variable Field (must be an integral number of 32-bit words) that contains the integrity check value computed over the ESP packet minus the Authentication Data Field.

One of the most popular ways to use the ESP is to build an "IPSec tunnel" between two routers. For example, a corporation wanting to link two sites using the Internet could configure a tunnel from a router at one site to a router at the other site. This tunnel may also be configured to use the ESP with confidentiality and authentication, thus preventing unauthorized access to the data that traverses this virtual link and ensuring that no spurious data is received at the far end of the tunnel.

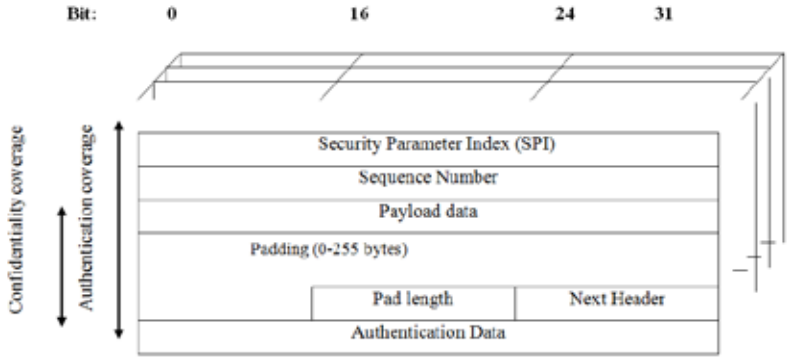


Figure 5: IPSec ESP Header

2.6 S/Mime (Secure/Multipurpose Internet Mail Extension)

S/MIME is the electronic standard that protects messages from unauthorized interception and forgery. S/MIME user public-key encryption technology to secure transmission, storage, authentication and forwarding of secret data, where SSL secures a connection between a client and a server over an insecure network, S/MIME is used to secure users, applications and computers. S/MIME is a security enhancement to the MIME (Multipurpose Internet Mail Extension) Internet e-mail format standard based on technology from RSA data security. To define MIME, we need first to have a general understanding of the underlying e-mail format that it uses, namely MIME. MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP (Simple Mail Transfer protocol)**[1,4]**.

- SMTP cannot transmit executable file or other binary objects. A number of schemes are in use for converting binary files into a text form that can be used by SMTP mail systems.
- SMTP cannot transmit text data that includes national language characters because these are represented by 8-bit codes with values of 128 decimal or higher and SMTP is limited to 7-bit ASCII.
- SMTP servers may reject message over a certain size.
- SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problem.

MIME is intended to resolve these problems in a manner that is compatible with existing RFC822 implementation. The MIME specification includes the following elements.

1. Five new message header fields are defined, which may be included in an RFC 822 header. These fields provide information about the body of the message.

2. A number of content formats are defined, thus standardizing representations that support multimedia electronic mail.
3. Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alternation by the mail system.

In terms of general functionality, S/MIME is very similar to PGP. Both offer the ability to sign and/or encrypt messages. S/MIME provides the following functions.

Enveloped data: This consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.

Signed data: A digital signature is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer. The content plus signature are then encoded using base 64 encoding. A signed data message can only be viewed by a recipient with S/MIME capability.

Clear-signed data: As with signed data, a digital signature of the content is formed. However, in this case, only the digital signature is encoded using base 64. As a result, recipients without S/MIME capability can view the message content, although they cannot verify the signature.

Signed and enveloped data: Signed-only and encrypted-only entities may be nested, so that encrypted data may be signed and signed data or clear-signed data may be encrypted. Some practical applications of S/MIME are.

- Electronic data exchange: Digital signatures on contracts
- Financial messaging: Store and transfer bank statements
- Content delivery: Electronic bill payment
- Health care: Secure patient records and health claims

Like SSL, IPSec and S/MIME is based on RSA algorithm for digital signature and digital envelopes as shown in Table 2**[1,2,5]**.

Table 2: Security Protocols Overview

Protocol	Summary
SSL (**Secure Socket Layer**)	Allows a "Secure Pipe" between any two application for transfer of data and mutual authentication
IPSec (**IP Security Protocol**)	Standard for Cryptographically-based authentication, integrity and confidentiality services at the IP datagram layer
S/MIME (**Secure MIME**)	Guarantees the secure communication, storage, authentication and forwarding of secret data at the application level

In virtually all distributed environments, electronic mail is the most heavily used network-based application. It is also the only distributed application that is widely used across all architectures and vendor platforms. Users expect to be able to and do, send mail to others who are connected directly or indirectly to the Internet, regardless of host operating system of communications suite.

With the explosively growing reliance or electronic mail for every conceivable purpose, there grows a demand for authentication and confidentiality services. Two schemes standout as approaches that are likely to enjoy widespread use in the next few years: pretty good privacy (PGP) and S/MIME.

III. ADDITIONAL NETWORK TYPE SECURITY PROTOCOLS

3.1 Wireless Security Protocols

Various wireless security protocols were developed to protect home wireless networks. These wireless security protocols include WEP, WPA and WPA2 each with their own strengths and weaknesses. In addition to preventing uninvited guests from connecting to your wireless network, wireless security protocols encrypt your private data as it is being transmitted over the airwaves. Wireless networks are inherently insecure. In the early days of wireless networking, manufacturers tried to make it as easy as possible for end users. The out-of-the-box configuration for most wireless networking equipment provided easy (but insecure) access to a wireless network. Although many of these issues have since been addressed, wireless networks are generally not as secure as wired networks. Wired networks, at their most basic level, send data between two points, A and B, which are connected by a network cable. Wireless networks, on the other hand, broadcast data in every direction to every device that happens to be listening, within a limited range. Following are descriptions of the WEP, WPA and WPA2 wireless security protocols**[6]**.

3.1.1 Wired Equivalent Privacy (Wep)

The original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks. However, WEP has many well known security flaws, is difficult to configure and is easily broken.

3.1.2 Wi-Fi Protected Access (Wpa)

Introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Most current WPA implementations use a pre shared key (PSK), commonly referred to as WPA Personal and the Temporal Key Integrity Protocol (TKIP) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates.

3.1.3 Wi-Fi Protected Access Version 2 (Wpa2)

Based on the 802.11i wireless security standard, which was finalized in 2004. The most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. The security provided by AES is sufficient (and approved) for use by the U.S. government to encrypt information classified as top secret it's probably good enough to protect your secrets as well.

3.2 Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances (using short wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz from fixed and mobile devices and building personal area networks (PAN). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops and PDA. These networks are termed "ad hoc" because of their shifting network topologies. Bluetooth is defined as a layer protocol architecture consisting of core protocols, cable replacement protocols, telephony control protocols and adopted protocols. Mandatory protocols for all Bluetooth stacks are: LMP, L2CAP and SDP. In addition devices that communicate with Bluetooth almost universally can use these protocols, HCI and RFCOMM **[7]**.

3.2.1 LMP

The Link Management Protocol (LMP) is used for set-up and control of the radio link between two devices. Implemented on the controller.

3.2.2 L2CAP

The Logical Link Control and Adaptation Protocol (L2CAP) used to multiplex multiple logical connections between two devices using different higher level protocols. Provides segmentation and reassembly of on-air packets.

3.2.3 SDP

The Service Discovery Protocol (SDP) allows a device to discover services offered by other devices and their associated parameters. For example when you use a mobile phone with a Bluetooth headset the phone uses SDP to determine which Bluetooth profiles the headset can use (Headset Profile, Hands Free Profile, Advanced Audio Distribution Profile (A2DP)etc.) and the protocol multiplexer settings needed for the phone to connect to the headset using each of them. Each service is identified by a Universally Unique Identifier (UUID) with official services (Bluetooth profiles) assigned a short form UUID (16 bits rather than the full 128).

3.2.4 RFCOMM

Radio Frequency Communications (RFCOMM) is a cable replacement protocol used to generate a virtual serial data stream. RFCOMM provides for binary data transport and emulates EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer, i.e. it is serial port emulation. RFCOMM provides a simple reliable data stream to the user, similar to TCP. It is used directly by many telephony related profiles as a carrier for AT commands, as well as being a transport layer for OBEX over Bluetooth. Many Bluetooth applications use RFCOMM because of its widespread support and publicly available API on most operating systems. Additionally, applications that used a serial port to communicate can be quickly ported to use RFCOMM.

3.3 Bluetooth Vs Wi-Fi (IEEE 802.11)

Bluetooth and Wi-Fi (The brand name for products using IEEE 802.11 standards) have some similar applications: setting up networks, printing or transferring files. Wi-Fi is intended as a replacement for high speed cabling for general local area network access in work areas. This category of applications is sometimes called wireless local area networks (WLAN). Bluetooth was intended for portable equipment and its applications. The category of applications is outlined as the wireless personal area network (WPAN). Bluetooth is a replacement for cabling in a variety of personally carried applications in any setting and also works for fixed location applications such as smart energy functionality in the home (thermostats, etc.). Wi-Fi and Bluetooth are to some extent complementary in their applications and usage. Wi-Fi is usually access point-centered, with an asymmetrical client-server connection with all traffic routed through the access point, while Bluetooth is usually symmetrical, between two Bluetooth devices. Bluetooth serves well in simple applications where two devices need to connect with minimal configuration like a button press, as in headsets and remote controls, while Wi-Fi suits better in applications where some degree of client configuration is possible and high speeds are required, especially for network access through an access node. However, Bluetooth access points do exist and ad-hoc connections are possible with Wi-Fi though not as simply as with Bluetooth**[8].** Wi-Fi Direct was recently developed to add a more Bluetooth like ad-hoc functionality to Wi-Fi.

3.4 Wireless Sensor Networks

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks (i) SNEP (ii) µTESLA. SNEP includes data confidentiality, two-party data authentication and evidence of data freshness. µTESLA provides authenticated broadcast for severely resource-constrained environments**[9]**.

A wireless sensor network (WSN), sometimes called a wireless sensor and actor network (WSAN) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance, today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring and so on. The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one or sometimes several sensors. Each such sensor network node has typically several parts i.e. a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network.

IV. CONCLUSSION

Protocols are sets of standards that define operations and how they will be done. Without protocols there would be much confusion and there would be no standard to allow computers to communicate. Protocols are a set of defined reactions to given events. When a traffic light turns red, the defined reaction should be to stop. This is a simple form of a protocol. Protocols are used for various purposes in the computer field. Protocols are mainly used to define networking standards. When dealing with networking then term network model and network layer used often. Network models define a set of network layers and how they interact. There are several different network models the most important two are: (1) TCP/IP Model - This model is sometimes called the DOD model since it was designed for the department of defense. It is also called the internet model because TCP/IP is the protocol used on the internet. (2) OSI Network Model - The International Standards Organization (ISO) has defined a standard called the Open Systems Interconnection (OSI) reference model. Currently there are many types of network available to establish communication between different types of devices. These networks uses different types of security protocols. While protocols can vary greatly in purpose and sophistication, most specify one or more of the following properties.

(i) Detection of the underlying physical connection (wired or wireless) or the existence of the other endpoint or node

(ii) Handshaking (dynamically setting parameters of a communications channel)

(iii) Negotiation of various connection characteristics

(iv) How to start and end a message

(v) How to format a message

(vi) What to do with corrupted or improperly formatted messages (error correction)

(vii) How to detect unexpected loss of the connection and what to do next

(viii) Termination of the session and or connection.

REFERENCES

[1]. Singh Brijendra., "Network Security and Management", Prentice Hall of India Private Limited, New Delhi-110001, Published in 2007.

[2]. Stalling, William. "Network Security Essentials application and standards", Third Edition, Pearson Prentice Hall, Published in 2008.

[3]. Silberschatz Abraham, Galvin Peter B., Gange Greg, "Operating System Concepts", 8th Edition, Wiley India Private Limited, New Delhi, Published in 2010.

[4]. Basandra Suresh Kumar," Computer Today", Galgotia publication Pvt. Ltd, New Delhi, Revised Edition 2008.

[5]. Stalling, William "Cryptography and Network Security", Fourth Edition, Pearson Prentice Hall, Published in 2006.

[6]. http://www.dummies.com/how-to/content/wireless-security-protocols-wep-wpa-and-wpa2.html; Retrieved on dated 18 March 2015.

[7]. http://en.wikipedia.org/wiki/Bluetooth; Retrieved on dated 07 April 2015.

[8]. http://en.wikibooks.org/wiki/Network_Plus_Certification/Technologies/Common_Protocols; Retrieved on dated 12 April 2015.

[9]. http://en.wikipedia.org/wiki/Wireless_sensor_network; Retrieved on dated 15 April 2015.

HUMAN MACHINE INTERACTION

Ritu Gautam[1], Poonam Singh[2]

[1,2] Lecturer, Dav Institute of Management, Faridabad, (India)

ABSTRACT

Human Machine Interaction, or more commonly Human Computer Interaction, is the study of interaction between people and computers. Whether its waking up in the morning to our digital radio alarm clocks, travelling to work in a car or train, using a laptop or desktop computer in our work place, or communicating to friends and family through mobile phones, it is safe to say that computer systems are everywhere in today society and human interact it with it. Human Machine Interaction (HMI) as a field has made great strides towards understanding and improving our interaction with computer based technologies.

Throughout the past two decades HMI researchers have been analyzing and designing specific user interface technologies, studying and improving the processes of technology development and evaluating new applications of technology with the aim of producing software and hardware that are useful, usable and artistic. This led to development of a body of technical knowledge and methodology

The intention of this paper is to provide an overview on the subject of Human-machine Interaction. The overview includes the basic definitions and terminology, a survey of existing technologies and recent advances in the field and challenges which are faced by human computer interaction.

Keywords: Human Computer Interaction, User Interfaces, Interaction Techniques.

I. HUMAN MACHINE INTERACTION: DEFINITION AND TERMINOLOGY

Human computer interaction means the point where the human can tell the computer what to do. A point where the computer displays the requested information. A human usually has 5 senses: Sight, Hearing, Touch, Taste, Smell, A computer hasn't any senses as such, it is machinery, with electrons running around in and out of component devices. The basic goal of HMI is to improve the interaction between user s and computers more usable and receptive to the user's need.

HMI Sometimes called as Man-Machine Interaction or Interfacing, concept of Human-Computer Interaction/Interfacing (HCI) was automatically represented with the emerging of computer, or more generally machine, itself. The reason, in fact, is clear: most sophisticated machines are worthless unless they can be used properly by men. Why a system is actually designed can ultimately be defined by what the system can do i.e. how the functions of a system can help towards the achievement of the purpose of the system

1.1 This Basic Argument Simply Presents the Main Terms that Should be Considered in the Design of HCI

- **Functionality:** of a system is defined by the set of actions or services that it provides to its users. However, the value of functionality is visible only when it becomes possible to be efficiently utilized by the user.
- **Usability:** *Usability* of a system with a certain functionality is the range and degree by which the system can be used efficiently and adequately to accomplish certain goals for certain users.

1.2 The User Activity has Three Different Levels

- **Physical :** The physical aspect determines the mechanics of interaction between human and computer
- **Cognitive :** the cognitive aspect deals with ways that users can understand the system and interact with it
- **Affective :** The affective aspect is a more recent issue and it tries not only to make the interaction a pleasurable experience for the user but also to affect the user in a way that make user continue to use the machine by changing attitudes and emotions toward the user

The recent methods and technologies in HMI are now trying to combine former methods of interaction together and with other advancing technologies such as networking and animation.

1.3 These New Advances Can be Categorized in Three Sections

- Wearable devices
- Wireless devices
- Virtual devices

II. HCI SYSTEMS ARCHITECTURE

Most important factor of a HCI design is its configuration. In fact, any given interface is generally defined by the number and diversity of inputs and outputs it provides. Architecture of a HCI system shows what these inputs and outputs are and how they work together. Following sections explain different configurations and designs upon which an interface is based.

2.1 Unimodal HCI Systems

A system that is based on only one modality is called *unimodal*. Based on the nature of different modalities, they can be divided into three categories:

1. Visual-Based
2. Audio-Based
3. Sensor-Based

2.1.1 Visual-Based HCI

The visual based human computer interaction is probably the most widespread area in HCI research. Considering the extent of applications and variety of open problems and approaches,
researchers tried to tackle different aspects of human responses which can be recognized as a visual signal. Some of the main research areas in this section are as follow:

• Facial Expression Analysis
• Body Movement Tracking (Large-scale)
• Gesture Recognition
• Gaze Detection (Eyes Movement Tracking)

2.1.2 Audio-Based HCI

The audio based interaction between a computer and a human is another important area of HCI systems. This area deals with information acquired by different audio signals. While the nature of audio signals may not be as variable as visual signals but the information gathered from audio signals can be more trustable, helpful, and is some cases unique providers of information. Research areas in this section can be divided to the following parts:

• Speech Recognition

• Speaker Recognition

• Auditory Emotion Analysis

• Human-Made Noise/Sign Detections (Gasp, Sigh, Laugh, Cry, etc.)

• Musical Interaction

2.1.3 Sensor-Based HCI

This section is a combination of variety of areas with a wide range of applications. The commonality of these different areas is that at least one physical sensor is used between user and machine to provide the interaction. These sensors as shown below can be very primitive or very sophisticated.

1. Pen-Based Interaction
2. Mouse & Keyboard
3. Joysticks
4. Motion Tracking Sensors and Digitizers
5. Haptic Sensors
6. Pressure Sensors
7. Taste/Smell Sensors

2.2 Multimodal HCI Systems

The term multimodal refers to combination of multiple modalities. In MMHCI systems, these modalities mostly refer to the ways that the system responds to the inputs, i.e. communication channels. The definition of these channels is inherited from human types of communication which are basically his senses: Sight, Hearing, Touch, Smell, and Taste. The possibilities for interaction with a machine include but are not limited to these types.

Therefore, a multimodal interface acts as a facilitator of human-computer interaction via two or more modes of input that go beyond the traditional keyboard and mouse. The exact number of supported input modes, their types and the way in which they work together may vary widely from one multimodal system to another. Multimodal interfaces incorporate different combinations of speech, gesture, gaze, facial expressions and other non-conventional modes of input. One of the most commonly supported combinations of input methods is that of gesture and speech.

The reason is that the open problems in each area are yet to be perfected meaning that there is still work to be done to acquire a reliable tool for each sub-area. Moreover, roles of different modalities and their share in interplay are not scientifically known. “Yet, people convey multimodal communicative signals in a complementary and redundant manner. Therefore, in order to accomplish a human-like multimodal analysis of multiple input signals acquired by different sensors, the signals cannot be considered mutually independently and cannot be combined in a context-free manner at the end of the intended analysis but, on the contrary, the input data should be processed in a joint feature space and according to a context-dependent model. In practice, however, besides the problems of context sensing and developing context-dependent models for combining multisensory information, one should cope with the size of the required joint feature space. Problems include large dimensionality, differing feature formats, and time-alignment.”

2.2.1 Few Examples of Applications of Multimodal Systems are Listed Below

· Smart Video Conferencing

· Intelligent Homes/Offices

- Driver Monitoring
- Intelligent Games
- E-Commerce
- Helping People with Disabilities
- Multimodal Systems for Disabled people
- Multimodal Human-Robot Interface Applications

III. HUMAN MACHINE INTERACTION GOAL

Develop usable products

– Easy to learn

– Effective to use

– Provide an enjoyable experience

• Involve users in the design process

A basic goal of HCI is to improve the interactions between users and computers by making computers more usable and receptive to the user's needs. Specifically, HCI is concerned with:

- methodologies and processes for designing interfaces (i.e., given a task and a class of users, design the best possible interface within given constraints, optimizing for a desired property such as learn ability or efficiency of use)
- methods for implementing interfaces (e.g. software toolkits and libraries; efficient algorithms)
- techniques for evaluating and comparing interfaces
- developing new interfaces and interaction techniques
- developing descriptive and predictive models and theories of interaction
- Decreasing hardware costs leading to larger memory and faster systems
- Miniaturization of hardware leading to portability
- Reduction in power requirements leading to portability
- New display technologies leading to the packaging of computational devices in new forms
- Specialized hardware leading to new functions
- Increased development of network communication and distributed computing
- Increasingly widespread use of computers, especially by people who are outside of the computing profession
- Increasing innovation in input techniques (i.e., voice, gesture, pen), combined with lowering cost, leading to rapid computerization by people previously left out of the "computer revolution."
- Wider social concerns leading to improved access to computers by currently disadvantaged groups
- The challenge of personal computing became manifest at an opportune time

All these threads of development in computer science pointed to the same conclusion: The way forward for computing entailed understanding and better empowering users

IV. FACTOR WHICH MUST BE CONSIDER WHEN WE TALK ABOUT HMI

1. Basic design considerations – designing for general usability and the evaluating of usability (usability engineering).
2. How people interact with and through systems (Computer-Supported Cooperative work).
3. How individuals differ in their capabilities and how that affects the human-computer interface (individual differences and tailorability).
4. The role of HCI in next-generation architectures (ubiquitous computing, pervasive computing).

V. RECENT ADVANCES IN HCI

5.1 Advanced Information Visualization/Visual Analytics

"Visual analytics is the science of analytical reasoning facilitated by interactive visual interfaces" .Visual Analytics is going through a significant growth. It will also be a technology of choice in the military intelligence world as analysts must digest vast amounts of collected data and make sense of them, identify patterns and trends.

5.2 Context Sensitive / Adaptive User Interfaces

Adaptive user interfaces are also good to overcome the information overload problem by focusing on the required information and processes. Eye-tracking could be used to observe where the user is looking at and customize accordingly the user interface.

5.3 Advanced Interface Widgets

A widget is an element of a graphical user interface that displays an information arrangement changeable by the user, such as a window or a text box, and enabling direct manipulation of a given kind of data. Interface widgets can significantly facilitate the task of a user.

5.4 Mixed Media

Commercial systems can handle images, voice, sounds, video, text, formatted data. These are exchangeable over communication links among users. The separate worlds of consumer electronics (e.g., stereo sets, VCRs, televisions) and computers are partially merging. Computer and print worlds are expected to cross-assimilate each other.

5.5 Large and thin Displays

New display technologies are finally maturing, enabling very large displays and displays that are thin, lightweight, and low in power consumption. This is having large effects on portability and will likely enable the development of paper-like, pen-based computer interaction systems very different in feel from desktop workstations of the present.

VI. CONCLUSION

Human-Computer Interaction is an important part of systems design. Quality of system depends on how it is represented and used by users. Therefore, enormous amount of attention has been paid to better designs of HCI.

The new direction of research is to replace common regular methods of interaction with intelligent, adaptive, multimodal, natural methods.

Virtual reality is also an advancing field of HCI which can be the common interface of the future. This paper attempted to give an overview on these issues and provide a survey of existing research through a comprehensive reference list.

REFERENCES

[1] ENEA,C.R,casacia(1999),"human machine interaction

[2] Ft. Lauderdale, Florida, USA • (April 5-10, 2003)," Design-oriented Human— Computer Interaction"

[3] M. Pantic, A. Pentland, A. Nijholt and T. Huang,(2006) "Human computing and machine understanding of human behavior: a survey".

[4] www.ICT-Teacher.com

[5] Fakhreddine Karray, Milad Alemzadeh(2008) Human-Computer Interaction: Overview on State of the Art.

[6] en.wikipedia.org/wiki/human-computer-interaction

[7] research.microsoft.com/hci2020/being human_a3.pdf

[8] Baecker, R., et al., "A Historical and Intellectual Perspective," in Readings in Human-Computer Interaction: Toward the Year 2000, Second Edition, R. Baecker, et al., Editors. 1995, Morgan Kaufmann Publishers, Inc.: San Francisco. pp. 35-47.

[9] International general on smart sensing and intelligent systems vol1,No1,March 2008

 ISBN: 978-81-931039-3-7

DETECTING MOVEMENTS OF A TARGET USING FACE TRACKING IN WIRELESS SENSOR NETWORKS

M.Chandhraleka[1], Dr.M.Pushparani[2]

[1]M.C.A, [2]Professor and Head, Department of Computer Science, Mother Teresa Women's University, (India)

ABSTRACT

Target tracking is one of the key applications of wireless sensor networks (WSNs). Existing work mostly requires organizing groups of sensor nodes with measurements of a target's movements or accurate distance measurements from the nodes to the target, and predicting those movements. These are, however, often difficult to accurately achieve in practice, especially in the case of unpredictable environments, sensor faults, etc. In this paper, we propose a new tracking framework, called Face Track, which employs the nodes of a spatial region surrounding a target, called a face. Instead of predicting the target location separately in a face, we estimate the target's moving toward another face. We introduce an edge detection algorithm to generate each face further in such a way that the nodes can prepare ahead of the target's moving, which greatly helps tracking the target in a timely fashion and recovering from special cases, e.g., sensor fault, loss of tracking. Also, we develop an optimal selection algorithm to select which sensors of faces to query and to forward the tracking data. Simulation results, compared with existing work, show that Face Track achieves better tracking accuracy and energy efficiency.

Keywords: Mobile Network, Topology, Routing Protocol, Wireless Sensor Network, Ad Hoc Network.

I. INTRODUCTION

A wireless sensor network (WSN) consists of a large number of sensors which are densely deployed over a large area. Each sensor monitors a physical environment and communicates via wireless signals. With the advancements in hardware miniaturization and wireless communication technologies, WSNs have been used in various applications such as education, warfare, and traffic monitoring. Regardless of the applications, extending the network lifetime is a critical issue in WSNs. This is because the sensors are battery-powered and generally difficult to be recharged. One of the main objectives. Unlike detection, a target tracking system is often required to ensure continuous monitoring, i.e., there always exist nodes that can detect the target along its trajectory. In target tracking applications, idle listening is a major source of energy waste. In this project, we propose Face Track, a framework to detect movements of a target using face tracking in a WSN, which does not fall into existing categories and is, to the best of our knowledge, the first of its kind. The concept of Face Track is depicted in Fig. 1, and is inspired by computational geometry, geographic routing, and face routing, in particular.

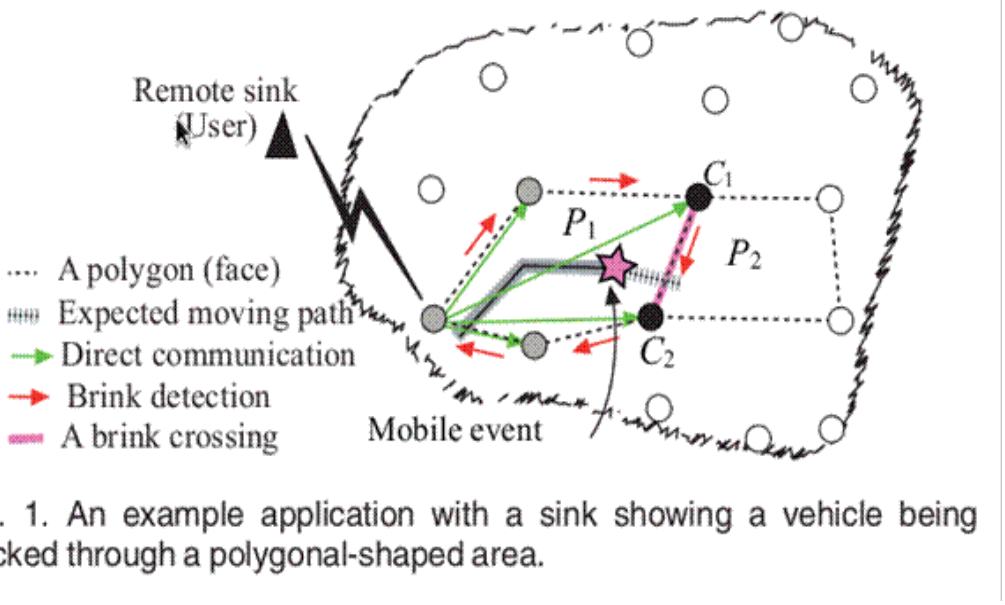


Fig. 1. An example application with a sink showing a vehicle being tracked through a polygonal-shaped area.

Fig. 1 Illustrates a Typical Scenario of an Enemy Vehicle Tracking Application. Sensor Nodes are Informed When the Vehicle Under Surveillance is Discovered, While Some Nodes (Such as Black Nodes) Detect the Vehicle and Send a Vigilance Message to the Nodes on the Vehicle's Expected Moving Path, So as to Wake Them Up. Thus, the Nodes (Such As Grey Nodes) in the Vehicle's Moving Path Can Prepare in Advance and Remain Vigilant in Front of it as it Moves.

II. REVIEW OF LITERATURE

Target tracking is one of the key applications of wireless sensor networks (WSNs). Existing work mostly requires organizing groups of sensor nodes with measurements of a target's movements or accurate distance measurements from the nodes to the target, and predicting those movements. These are, however, often difficult to accurately achieve in practice, especially in the case of unpredictable environments, sensor faults, etc. In this paper, we propose a new tracking framework, called FaceTrack, which employs the nodes of a spatial region surrounding a target, called a face. Instead of predicting the target location separately in a face, we estimate the target's moving toward another face. We introduce an edge detection algorithm to generate each face further in such a way that the nodes can prepare ahead of the target's moving, which greatly helps tracking the target in a timely fashion and recovering from special cases, e.g., sensor fault, loss of tracking. Also, we develop an optimal selection algorithm to select which sensors of faces to query and to forward the tracking data. Simulation results, compared with existing work, show that FaceTrack achieves better tracking accuracy and energy efficiency. We also validate its effectiveness via a proof-of-concept system of the Imote2 sensor platform**.[1]**

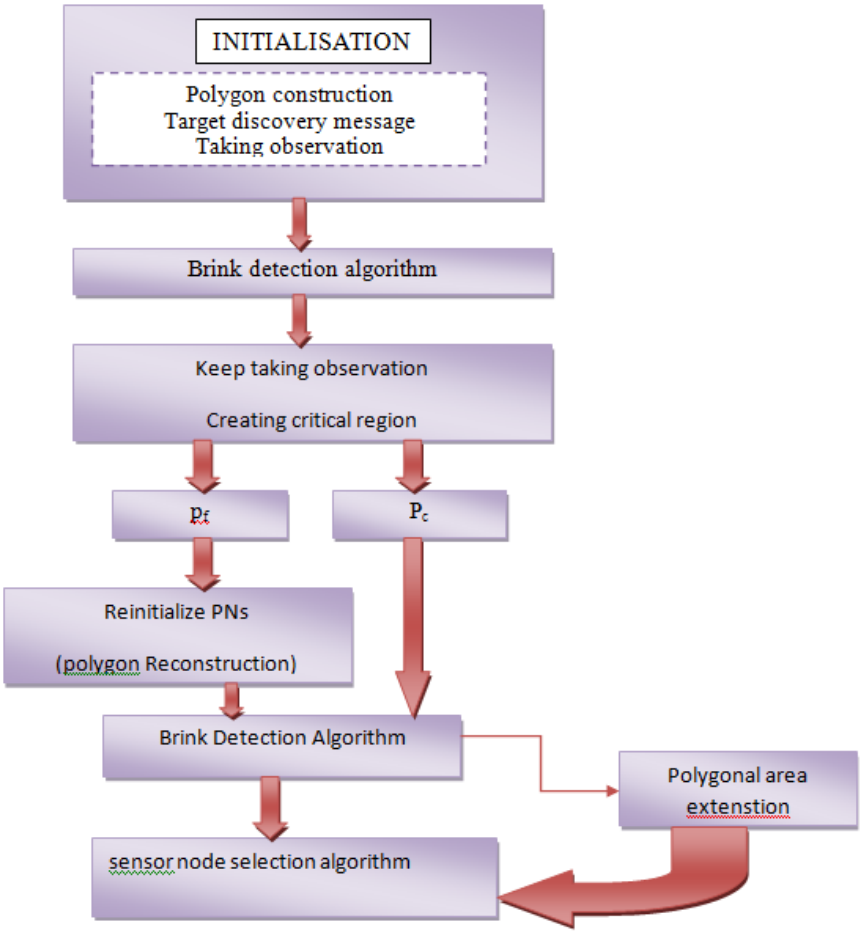
The distinctive features of mobile ad hoc networks (MANETs), including dynamic topology and open wireless medium, may lead MANETs suffering from many security vulnerabilities. In this paper, using recent advances in uncertain reasoning originated from artificial intelligence community, we propose a unified trust management scheme that enhances the security in MANETs. In the proposed trust management scheme, the trust model has two components: trust from direct observation and trust from indirect observation. With direct observation from

an observer node, the trust value is derived using Bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation, also called secondhand information that is obtained from neighbor nodes of the observer node, the trust value is derived using the Dempster-Shafer theory, which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method. Combining these two components in the trust model, we can obtain more accurate trust values of the observed nodes in MANETs. We then evaluate our scheme under the scenario of MANET routing. Extensive simulation results show the effectiveness of the proposed scheme. Specifically, throughput and packet delivery ratio can be improved significantly with slightly increased average endto- end delay and overhead of messages**.[2]**

Mobility-assisted data collection in sensor networks creates a new dimension to reduce and balance the energy consumption for sensor nodes. However, it also introduces extra latency in the data collection process due to the limited mobility of mobile elements. Therefore, how to schedule the movement of mobile elements throughout the field is of ultimate importance. In this paper, the on-demand scenario where data collection requests arrive at the mobile element progressively is investigated, and the data collection process is modelled as anM=G=1=c-NJN queuing system with an intuitive service discipline of nearest-job-next (NJN). Based on this model, the performance of data collection is evaluated through both theoretical analysis and extensive simulation. NJN is further extended by considering the possible requests combination (NJNC). The simulation results validate our models and offer more insights when compared with the first-come-first-serve (FCFS) discipline. In contrary to the conventional wisdom of the starvation problem, we reveal that NJN and NJNC have better performance than FCFS, in both the average and more importantly the worst cases, which offers the much needed assurance to adopt NJN and NJNC in the design of more sophisticated data collection schemes, as well as other similar scheduling scenarios**.[3]**

Recently, the research focus on geographic routing, a promising routing scheme in wireless sensor networks (WSNs), is shifting toward duty-cycled WSNs in which sensors are sleep scheduled to reduce energy consumption. However, except the connected-*k* neighborhood (CKN) sleep scheduling algorithm and the geographic routing oriented sleep scheduling (GSS) algorithm, nearly all research work about geographic routing in duty-cycled WSNs has focused on the geographic forwarding mechanism; further, most of the existing work has ignored the fact that sensors can be mobile. In this paper, we focus on sleep scheduling for geographic routing in duty-cycled WSNs with mobile sensors and propose two geographic-distance-based connected-*k* neighborhood (GCKN) sleep scheduling algorithms. The first one is the *geographic-distance-based connected-kneighborhood for first path* (GCKNF) sleep scheduling algorithm. The second one is the *geographic-distance-based connected*-k*neighborhood for all paths* (GCKNA) sleep scheduling algorithm. By theoretical analysis and simulations, we show that when there are mobile sensors, geographic routing can achieve much shorter average lengths for the first transmission path explored in WSNs employing GCKNF sleep scheduling and all transmission paths searched inWSNs employing GCKNA sleep scheduling compared with those in WSNs employing CKN and GSS sleep scheduling**.[4]**

3. Methodology



3.1 Initialization

The system initialization, including initial polygon construction in the plane. A node has all of the corresponding polygons' information after the WSN planarization. Initially, all nodes in the WSN are in a low-power mode and wake up at a predefined period to carry out the sensing for a short time. We presume that a sensor node has three different states of operation, namely, active (when a node is in a vigilant manner and participates in tracking the target), awakening (when a node awakes for a short period of time), and inactive (when a node is in a sleeping state). We consider that a sensor should be kept awake so long as its participation is needed for a given task. In the beginning, when a target is detected by some nodes, that communicate to all of its adjacent neighbors with their detection information, and reconstruct the polygon.[1]

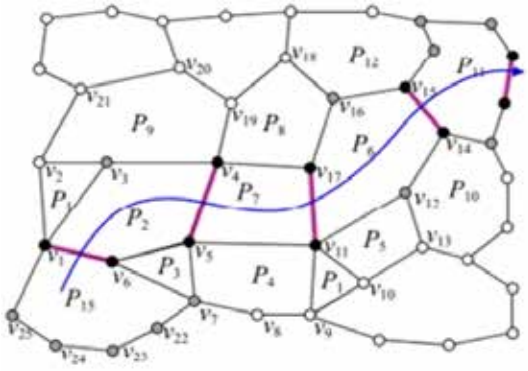


Fig 2. Detecting Target's Movements through Polygons

Fig. 2 illustrates the target movement detection through the polygons. The target is initially detected by sensors v1 and v6 (shaded black to indicate the CNs) in the polygon P15 , and the rest of the corresponding nodes (shaded grey) in P15 are in the vigilant manner, and the rest of the nodes in the sensor network are in the inactive state when the target is in P15 . As shown in Fig. 2, the target travels through the polygons.[1]

3.2 Brink Detection Algorithm

We introduce an edge detection algorithm, which is used to reconstruct another conceptual polygon, called a critical region, by generating an edge, called a brink, to the active polygon, Pc. As the brink is generated on the boundary of In this algorithm, the edges of Pc are mapped by the brinks. As the target moves to a brink, the target is focused on a spot, called a follow spot. In the follow spot, a brink between CNs can be similar to an 'automatic door.' Often found at supermarket entrances and exits, an automatic door will swing open when it senses that a person is approaching the door. The door has a sensor pad in front to detect the presence of a person about to walk through the doorway. Therefore, the door can be called an entrance door or entrance brink.[1][2]

3.3 Methods for Face Tracking

1. Topology Formation.
2. Predicting the target and creating Local Active environment.
3. Face Tracking
4. Modified Face Tracking protocol.

3.3.1 Topology Formation

All sensors are deployed initially. Each sensor updates their information to its neighbor sensor. This is called Initial Neighbor Discovery.[1][4]

3.3.2 Predicting the Target and Creating Local Active Environment

All sensors communicate with each other and updates the routing information once object is detected creates a Local Active environment predicts the Target movement and sends the information to base station. .[1][4]

3.3.3 Face Tracking

Once Target is detected creates an Awake region and based on the prediction results assigns Sleep scheduling to individual sensors at synchronized time and the graph is plotted for Energy efficiency in comparison with the Existing concept along with Throughput, Packet Delivery ratio. .[1][4]

3.3.4 Modified Face Tracking Protocol

In this phase we are synchronizing the proposed PPSS protocol, i.e., Local Active environment with Boundary selection nodes in which the sensors along the boundary of the field region are activated, thus the Mobile target that comes from different directions are detected, once it detects the Moving object along the boundaries, it will start sending the information about the mobile target to the base station, so we are enhancing the proposed concept to detect multiple target along with improved power efficiency.

IV. NETWORK COMPONENTS

The root of the hierarchy is the TclObject class that is the super class of all OTcl library objects (scheduler, network components, timers and the other objects including NAM related ones). As an ancestor class of

TclObject, NsObject class is the super class of all basic network component objects that handle packets, which may compose compound network objects such as nodes and links.

The basic network components are further divided into two subclasses, Connector and Classifier, based on the number of the possible output DATA paths. The basic network and objects that have only one output DATA path are under the Connector class, and switching objects that have possible multiple output DATA paths are under the Classifier class.[3]

V. INVOKING OTCL PROCEDURES

There are four different methods to invoke an OTcl command through the instance, tcl. They differ essentially in their calling arguments. Each function passes a string to the interpreter that then evaluates the string in a global context. These methods will return to the caller if the interpreter returns TCL_OK. On the other hand, if the interpreter returns TCL_ERROR, the methods will call tkerror{}. The user can overload this procedure to selectively disregard certain types of errors.[4]

1. **Passing Results to/from the Interpreter:** When the interpreter invokes a C++ method, it expects the result back in the private member variable, tcl-> result.
2. **Error Reporting and Exit:** This method provides a uniform way to report errors in the compiled code.

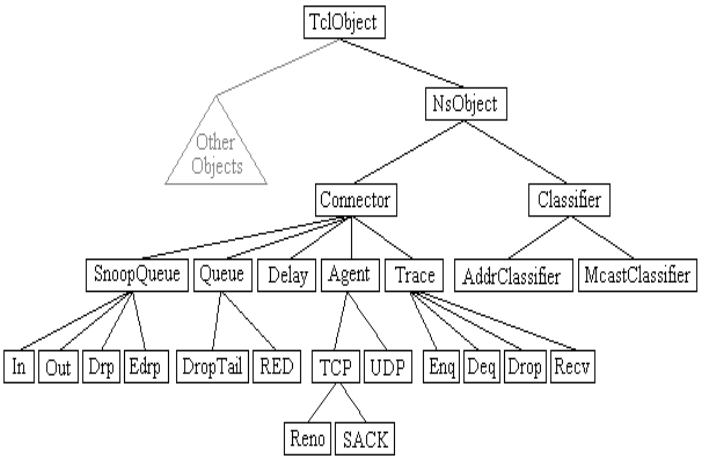


Fig 3. OTcl Class Hierarchy

VI. CONCLUSION

The main functionality of a surveillance wireless sensor net work is to track an unauthorized target in a field. The challenge is to determine how to perceive the target in a WSN efficiently. We proposed a unique idea to achieve a WSN system for detecting movements of a target using polygon (face) tracking that does not adopt any prediction method. Evaluation results demonstrated that the proposed tracking framework can estimate a target's positioning area, achieve tracking ability with high accuracy, and reduce the energy cost of WSNs.

REFERENCES

[1]. Detecting Movements of a Target Using Face Tracking in Wireless Sensor Networks , Guojun Wang, Member, IEEE, Md Zakirul Alam Bhuiyan, Member, IEEE, Jiannong Cao, Senior Member, IEEE , and Jie Wu, Fellow, Member IEEE.vol.25,no.4.

[2]. Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason. DOI 10.1109/TVT.2014.2313865

[3]. Evaluating Service Disciplines for On-Demand Mobile Data Collection in Sensor Networks Liang He, Member, IEEE , Zhe Yang, Student Member, IEEE , Jianping Pan, Senior Member, IEEE , Lin Cai, Senior Member, IEEE , Jingdong Xu, and Yu (Jason) Gu, Member, IEEE VOL. 13, NO. 4, APRIL 2014.

[4]. Sleep Scheduling for Geographic Routing in Duty-Cycled Mobile Sensor Networks. Chunsheng Zhu, Student Member, IEEE, Laurence T. Yang, Member, IEEE, Lei Shu, Member, IEEE, Victor C. M. Leung, Fellow, IEEE, Joel J. P. C. Rodrigues, Senior Member, IEEE, and Lei Wang, Member, IEEE. VOL. 61, NO. 11, NOVEMBER 2014

[5] Z. Wang, W. Lou, Z. Wang, J. Ma, and H. Chen, "A Novel Mobility Management Scheme for Target Tracking in Cluster-Based Sensor Networks," Proc. Sixth IEEE Int'l Conf. Distributed Computing in Sensor Systems (DCOSS), pp. 172-186, 2010.

[6] L.M. Kaplan, "Global Node Selection for Localization in a Distributed Sensor Network," IEEE Trans. Aerospace and Electronic Systems, vol. 42, no. 1, pp. 113-135, Jan. 2006.

 ISBN: 978-81-931039-3-7

DETECTION AND RECGONITION OF IRIS IMAGES

W. Persiba Sarojini Jeyaseeli[1], Dr.M.Pushparani[2]

[1]Guest Lecturer, [2]Professor and Head, Department of Computer Science,
Mother Teresa Women's University, (India)

ABSTRACT

In iris recognition, we proposed fusion between Hamming distance and FBD works better than the baseline of Hamming distance alone it performed a statistical test to determine whether this difference was statistically significant. The null hypothesis for this test is that there is no difference between the base line. Hamming distance method and the proposed fusion of Hamming distance and FBD. The alternative is that there is a significant difference. To test for statistical significance, it randomly divided the subjects into 10 different test sets. For each test set, the measured the performance of using Hamming distance alone and of using fusion of Hamming distance and FBD. Then, we used a paired t-test to see whether the proposed method obtained a statistically significant improvement. Thus provides the effective results.

Keywords: Hamming Distance, Fragile Bits, Score Fusion

I. INTRODUCTION

The most common iris biometric algorithm represents the texture of an iris using a binary iris code. Not all bits in an iris code are equally consistent. A bit is deemed fragile if its value changes across iris codes created from different images of the same iris. Previous research has shown that iris recognition performance can be improved by masking these fragile bits. Rather than ignoring fragile bits completely, it considers what beneficial information can be obtained from the fragile bits. We find that the locations of fragile bits tend to be consistent across different iris codes of the same eye. It present a metric, called the fragile bit distance, which quantitatively measures the coincidence of the fragile bit patterns in two iris codes. It find that score fusion of fragile bit distance and Hamming distance works better for recognition than Hamming distance alone. To our knowledge, this is the first and only work to use the coincidence of fragile bit locations to improve the accuracy of matches.

II. REVIEW OF LITERATURE

In this paper, we propose a novel possibilistic fuzzy matching strategy with invariant properties, which can provide a robust and effective matching scheme for two sets of iris feature points. In addition, the nonlinear normalization model is adopted to provide more accurate position before matching. Moreover, an effective iris segmentation method is proposed to refine the detected inner and outer boundaries to smooth curves. For feature extraction, the Gabor filters are adopted to detect the local feature points from the segmented iris image in the Cartesian coordinate system and to generate a rotation-invariant descriptor for each detected point. After that, the proposed matching algorithm is used to compute a similarity score for two sets of feature points from a pair of iris images. The experimental results show that the performance of our system is better than those of the systems based on the local features and is comparable to those of the typical systems. **[2].**

Wireless Local Area Networks (WLANs) are gaining gratitude as they are fast, cost effective, supple and easy to use. The networks face severe issues and challenges in establishing security to the user's of the network. With users accessing networks remotely, exchanging data by means of the Internet and carrying around laptops containing sensitive data, ensuring security is an increasingly multifarious challenge. Therefore it is essential to make sure the security of the network users. In order to offer network security many techniques and systems have been proposed earlier in literature. Most of these traditional methods uses password, smart cards and so on to provide security to the network users. Though these traditional methods are effectual in ensuring security they posses some limitations too. The different phases included in this proposed approach are user registration, Extraction of minutiae points and secret key, Iris localization and Normalization. Furthermore, biometric authentication systems can be more opportune for the users since it involves no password that might be feared to be forgotten by the network users or key to be lost and therefore a single biometric trait (e.g. Iris) can be used to access several accounts without the burden of remembering passwords. In this paper the Iris biometric is used to provide security. This proposed paper also explains some of the Iris localization and Normalization techniques to make the biometric template noise free. The new method uses entropy as the basis for measuring the uniformity of pixel characteristics (luminance is used in this paper) within a segmentation region. The evaluation method provides a relative quality score that can be used to compare different segmentations of the same image. This method can be used to compare both various parameterizations of one particular segmentation method as well as fundamentally different segmentation techniques. The results from this preliminary study indicate that the proposed evaluation method is superior to the prior quantitative segmentation evaluation techniques, and identify areas for future research in objective segmentation evaluation. **[1].**

The most common iris biometric algorithm represents the texture of an iris using a binary iris code. Not all bits in an iris code are equally consistent. A bit is deemed fragile if its value changes across iris codes created from different images of the same iris. Previous research has shown that iris recognition performance can be improved by masking these fragile bits. Rather than ignoring fragile bits completely, we consider what beneficial information can be obtained from the fragile bits. We find that the locations of fragile bits tend to be consistent across different iris codes of the same eye. We present a metric, called the fragile bit distance, which quantitatively measures the coincidence of the fragile bit patterns in two iris codes. We find that score fusion of fragile bit distance and Hamming distance works better for recognition than Hamming distance alone. To our knowledge, this is the first and only work to use the coincidence of fragile bit locations to improve the accuracy of matches. **[3].**

III. IRIS RECOGNITION SYSTEM

A typical iris recognition system consists of three major building blocks. Biometric technologies are the foundation of personal identification systems. It provides an identification based on a unique feature possessed by the individual. This paper provides a walkthrough for image acquisition, segmentation, normalization, feature extraction and matching based on the Human Iris imaging. A Canny Edge Detection scheme and a Circular Hough Transform, is used to detect the iris boundaries in the eye's digital image. The extracted IRIS region was normalized by using Image Registration technique. A phase correlation base method is used for this iris image registration purpose. The features of the iris region are encoded by convolving the normalized iris region with 2D Gabor filter. Hamming distance measurement is used to compare the quantized vectors and authenticate the users.

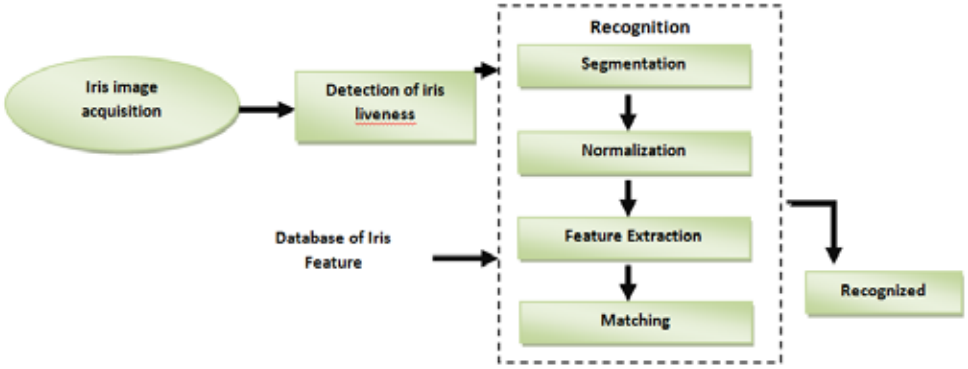


Fig.1 Flow Diagram of Iris Recognition System

3.1 Segmentation

Precise iris image segmentation plays an important role in an iris recognition system since success of the system in upcoming stages is directly dependent on the precision of this stage . The main purpose of segmentation stage is to localize the two iris boundaries namely, inner boundary of iris-pupil and outer one of iris-sclera and to localize eyelids. shows block diagram of segmentation stage. As it could be seen in this figure, segmentation stage includes three following steps:

1. Localization of iris inner boundary (the boundary between pupil and iris).
2. Localization of iris outer boundary (the limbic border between sclera and iris).
3. Localization of boundary between eyelids and iris.

3.1.1 Segmentation Process

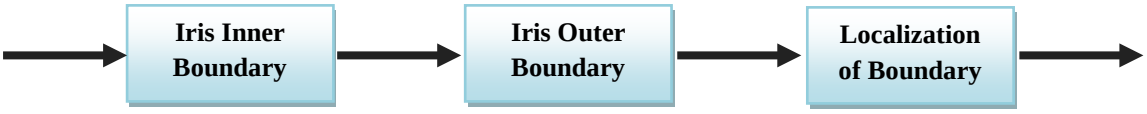


Fig.2 Segmentation Process

3.3 Normalization

The next focus of this work is on iris normalization. Most normalization techniques are based on transforming iris into polar coordinates, known as unwrapping process. Pupil boundary and limbus boundary are generally two non-concentric contours. The non-concentric condition leads to different choices of reference points for transforming an iris into polar coordinates.

Proper choice of reference point is very important where the radial and angular information would be defined with respect to this point.

• This is to deal with variation, between iris image pairs, of the number of bits actually compared to form the Hamming Distance.

• Stage 1: the raw Hamming Distance (HDraw) is given by the number of bits differing between the 2 IrisCodes divided by the number of bits compared (n, as determined from the probe and gallery mask bits).

• Stage 2: this modifies HDraw non-linearly, leading to HDnorm.

• By mistake, but fortuitously, our initial implementation of IrisCode pattern matching used only the Stage 1 Normalisation

3.2.1 Normalization of Extracted Iris

Once the iris region is successfully segmented from an eye image, the next stage is to normalize the iris region in rectangular block so that it has fixed dimensions in order to allow comparisons. The normalization process produces iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have characteristic features at same spatial location.

3.3 Feature Extraction

Hamming distance is measure two bit patterns or template. It will be provide the decision whether the two patterns are generated from the different irises or from the same one. The LBP score can join with Hamming distance using cascaded classifiers. Since their LBP method is slower than computing the Hamming distance, they suggest calculating the Hamming distance first. If the Hamming distance is below some low threshold, the comparison is classified as a match. If the Hamming distance is above some high threshold, the comparison is classified as a non-match. If the Hamming distance is between those two thresholds, use the LBP score to make the decision.

3.4 Matching

The feature encoding process will also need a corresponding matching metric, which gives a measure of similarity between two iris templates. This metric should give one range of values when comparing templates generated from the same eye, known as intra-class comparisons, and another range of values when comparing templates created from different irises, known as inter-class comparisons

3.5 Iris Image Acquistion

Image acquisition is considered as the most critical step for building the iris recognition system since all subsequent stages depend highly on the image quality. Another challenge of capturing the iris images is due to the smaller size of the iris and exhibition of more abundant texture features of iris under infrared lighting. A specifically designed sensor is used to capture the sequence of iris images. An iris image capturing device considers the following three key factors: The lighting of the system, The position of the system, and The physical capture system.

3.6 Detection of Iris Liveness

In order to avoid the forgery and the illegal usage of iris biometric features, the detection of iris liveness ensures that the captured input image sequence comes from a live subject instead of an iris picture, a video sequence, a glass eye, and other artifacts. No such major researches have been conducted for iris liveness detection. The utilization of the optical and physiological characteristics of the live eye is considered as the most important aspects for the assurance of the liveness of the input iris image sequence.

3.7 Recognition

The accuracy of the iris recognition system depends on this module. This module can be further subdivided into four main stages: Segmentation, Normalization or Unwrapping, Feature extraction, and Matching. In the first stage, the iris region is localized from the eye image, the segmented iris region is normalized in order to avoid the size inconsistencies in the second stage, then the most

discriminating features are extracted from the normalized image and finally, the extracted features are used for matching with the known pattern in the feature database.

3.8 Approaches of Iris Recognition

From the extensive literature review, we divide the iris recognition approaches roughly into four major categories based on feature extraction strategy: Phase-based approaches, Zero-crossing representation approaches, Texture-Analysis based approaches and intensity variation analysis approaches.

3.8.1 Phase-Based Approach

In this method, the iris structure is encoded by demodulating with Gabor wavelets. Each phase is quantized in the complex plane to the quadrant in which it lies for each local element of the iris structure and this operation is repeated all across the iris, at different scales of analysis.

3.8.2 Zero-Crossing Representation Approach

The zero-crossing representation of the 1D wavelet transform at different resolution levels of a concentric circle on an iris image is used to characterize the texture of the iris.

3.8.3 Texture-Analysis Based Approach

The iris pattern provides abundant texture information and it is desirable to explore the representation scheme to acquire the local information in an iris. According to the iris recognition approach based on texture analysis, the discriminating frequency information of the local spatial pattern in an iris is captured which reflect the significant local structure of the iris.

3.8.4 Intensity Variation Analysis Approach

In this scheme, the local sharp variation is used to represent the distinctive structure of the iris. The most discriminative variations of an iris image are characterized by constructing a set of 1-Dsignal by adopting wavelet transform to represent these signals.

IV. CONCLUSION

In this paper, “Detection and Recognition of Iris Image Acquisition” the input image is given then the iris liveness is detected by using some process and then finally the iris is recognized by segmenting, extracting the features. The feature is extracted from the database.

REFERENCES

[1] K. Saraswathi, B. Jayaram and Dr. R. Balasubramanian(2011) “Iris Biometrics Based Authentication and Key Exchange System”

[2] Karen P. Hollingsworth, Kevin W. Bowyer, Fellow, IEEE, and Patrick J. Flynn, Senior Member, IEEE(2011) Improved Iris Recognition through Fusion of Hamming Distance and Fragile Bit Distance

[3] Chung-Chih Tsai, Heng-Yi Lin, Jinshiuh Taur, and Chin-Wang Tao(2012) Iris Recognition Using Possibilistic Fuzzy Matching on Local Features

 ISBN: 978-81-931039-3-7

IMPLEMENTATION OF MULTIPLANAR RECONSTRUCTION IN CollabDDS USING JAVA TECHNIQUES

Gokul.R[1], J.Raamkumar[2], Mridu Pobon Rajkhowa[3]

[1]*PG Scholar, SKP Engineering College, Tiruvannamalai, Tamil Nadu (India)*

[2]*Lecturer, Govt. Polytecnic College, Tiruvannamalai, Tamil Nadu (India)*

[3]*Scientist-B, NIC, New Delhi (India)*

ABSTRACT

We propose to implement the conversion of slice views from DICOM images (CT Scan & MRI data) using java coding and slice orientation (direction cosine of the row and column with respect to the slice view of the image). Pixel size and Pixel Spacing are calculated with the help of row and column array from DICOM data for generating MPR view. For MPR different Affine Transformation like Scaling, Reflection, Rotation, Shear, Translation etc are to be applied on the image pixels.

Keywords: Affine Transformassion, Collab DDS, DICOM, MPR

I. INTRODUCTION

1.1 About CollabDDS

CollabDDS provides an integrated online environment to visualise medical and dental images for diagnosis and treatment planning. For visualization, different formats of data which can be loaded into CollabDDS like X-ray Images, JPEG/GIF/TIFF/WBMP/BMP /PNG, DICOM images (CT scan & MRI data), series. CollabDDS also provides excellent Image Manipulation features Remote Health Centres can be connected to expert radiologists and doctors in Centres of Excellence, by suitable tools and channel for data transmission and diagnosis. The repository of images with annotations by experts can also be used for education and research purposes. The high-bandwidth and low-latency capability of the National Knowledge Network (NKN) provides the ideal platform for real time collaboration using CollabDDS.

1.2 About MPR

In scientific visualization and computer graphics, Multiplanar Reformat technique is used in two-dimentional tomographic imaging (computed tomography). MPR allows images to be created from the original axial plane in coronal and sagittal plane and vice versa.

Multiplanar Reconstruction (MPR) allows images to be created from the original axial plane in either the coronal, sagittal, or oblique plane. Spiral/helical CT has greatly improved the quality of MPRs by eliminating the 'stair-step' artefacts that used to occur with conventional slice by slice CT. Multislice CT has further improved the quality of MPRs as it allows isotropic imaging in which the image quality of the reconstructed MPR is the same as the original axial image.

Multi-frame DICOM images contain a collection of slices of the body. For example, considering each axial slice represents an (X-Y) plane of the body, and then a collection of slices will represents Z axis.

In the simplest case, multi-planar reconstruction (MPR) involves generating perspectives at right angles to a stack of axial slices so that coronal and sagittal images can be generated. The described views can be graphically represented as the following:

- Axial view
- Sagittal view
- Coronal view

So if we have a multi-frame DICOM image that contains F frames of images with (W x H) dimension, then W would be the X axis, H would be the Y axis and F would be the Z axis.

The coronal view could be considered as the oblique view with 0 degree rotation angle about Z axis, while the sagittal view could be considered as the oblique view with 90 degree rotation angle about Z axis.

It is possible to perform MPR not only from multi-frame DICOM images, but also from a collection of single-frame DICOM images with the same width and height.

· **Axial**: The axial plane passes through the body from anterior to posterior and divides it into superior and inferior sections.

· **Coronal**: The coronal plane passes through the body from left to right and divides it into anterior to posterior sections.

· **Sagittal**: The sagittal plane passes through the body from anterior to posterior and divides it into left and right sections.

It is proposed to implement **Multiplanar Reformat** in **CollabDDS** as the reconstruction of the other two views would help the Radiology better visualize the images.

1.3 About DICOM

Digital Imaging and Communications in Medicine (DICOM) is a standard for handling, storing, printing, and transmitting information in medical imaging. It includes a file format definition and a network communications protocol. The communication protocol is an application protocol that uses TCP/IP to communicate between systems. DICOM files can be exchanged between two entities that are capable of receiving image and patient data in DICOM format. The National Electrical Manufacturers Association (NEMA) holds the copyright to this standard. It was developed by the DICOM Standards Committee, whose members are also partly members of NEMA.

DICOM enables the integration of scanners, servers, workstations, printers, and network hardware from multiple manufacturers into a picture archiving and communication system (PACS). The different devices come with DICOM conformance statements which clearly state which DICOM classes they support. DICOM has been widely adopted by hospitals and is making inroads in smaller applications like dentists' and doctors' offices.

1.3.1 Data format

DICOM differs from some, but not all, data formats in that it groups information into data sets. That means that a file of a chest x-ray image, for example, actually contains the patient ID within the file, so that the image can never be separated from this information by mistake. This is similar to the way that image formats such as JPEG can also have embedded tags to identify and otherwise describe the image.

A DICOM data object consists of a number of attributes, including items such as name, ID, etc., and also one special attribute containing the image pixel data (i.e. logically, the main object has no "header" as such: merely a list of attributes, including the pixel data). A single DICOM object can have only one attribute containing pixel data. For many modalities, this corresponds to a single image. But note that the attribute may contain multiple "frames", allowing storage of cine loops or other multi-frame data. Another example is NM data, where an NM image, by definition, is a multi-dimensional multi-frame image. In these cases, three- or four-dimensional data can be encapsulated in a single DICOM object. Pixel data can be compressed using a variety of standards, including JPEG, JPEG Lossless, JPEG 2000, and Run-Length encoding (RLE). LZW (zip) compression can be used for the whole data set (not just the pixel data), but this has rarely been implemented.

II. METHOD

2.1 DICOM image Parameters

Following the DICOM image Parameters are going to be used in MPR module.

2.1.1 Patient Orientation.

The Patient Orientation (0020, 0020) relative to the image plane shall be specified by two values that designate the anatomical direction of the positive row axis (left to right) and the positive column axis (top to bottom). The first entry is the direction of the rows, given by the direction of the last pixel in the first row from the first pixel in that row. The second entry is the direction of the columns, given by the direction of the last pixel in the first column from the first pixel in that column. Anatomical direction shall be designated by the capital letters: A (anterior), P (posterior), R (right), L (left), H (head), F (foot). Each value of the orientation attribute shall contain at least one of these characters. If refinements in the orientation descriptions are to be specified, then they shall be designated by one or two additional letters in each value. Within each value, the letters shall be ordered with the principal orientation designated in the first character."

2.1.2 Image Position

The Image Position (0020, 0032) specifies the x, y, and z coordinates of the upper left hand corner of the image; it is the center of the first voxel transmitted.

2.1.3 Image Orientation

Image Orientation (0020, 0037) specifies the direction cosines of the first row and the first column with respect to the patient.

2.2 MPR Module

Multi-planar reconstruction (MPR) module images are re-formats at arbitrary planes, defined by the operator, using the pixel data from a stack of planar images (base images).

The digital value for each pixel is assigned to a virtual voxel with the same thickness as the slice thickness of the base image. This yields a volume of data that represents the scanned object. The MPR module uses the virtual voxel data to create the pixel values for the reconstructed images. When the dimensions of the scanned voxels (as set by slice thickness and in-plane resolution) are equal, the data set is said to be isotropic. Where the dimensions of the scanned voxel are not equal in all three planes, the data set is said to be anisotropic. Isotropic data yields the best reconstructions.

The viewport is described by its origin, its row unit vector, column unit vector and a normal unit vector (derived from the row and column vectors by taking the cross product). Now if one moves the origin to 0,0,0 and rotates

this viewing plane such that the row vector is in the +X direction, the column vector the +Y direction, and the normal in the +Z direction, then one has a situation where the X coordinate now represents a column offset in mm from the localizer's top left hand corner, and the Y coordinate now represents a row offset in mm from the localizer's top left hand corner, and the Z coordinate can be ignored. One can then convert the X and Y mm offsets into pixel offsets using the pixel spacing of the localizer image.

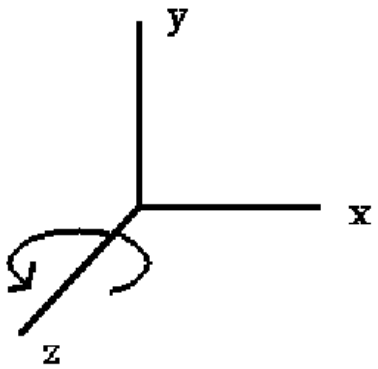
The actual rotations can be specified entirely using the direction cosines that are the row, column and normal unit vectors.

2.3 Module Calculations

2.3.1 3D Rotation

3D Rotation is more complicated than 2D rotation since we must specify an axis of rotation. In 2D the axis of rotation is always perpendicular to the xy plane, i.e., the Z axis, but in 3D the axis of rotation can have any spatial orientation. We will first look at rotation around the three principle axes (X, Y, Z) and then about an arbitrary axis. Note that for Inverse Rotation: replace q with -q and then R(R-1) = 1

2.4 Z-Axis Rotation



Z-axis rotation is identical to the 2D case:

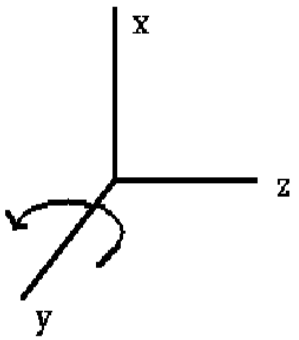
x' = x*cos q - y*sin q

y' = x*sin q + y*cos q

z' = z

$$Rz(q) = \begin{pmatrix} \cos q & \sin q & 0 & 0 \\ -\sin q & \cos q & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

2.4 Y-Axis Rotation



2.4.1 Y-axis rotation looks like Z-axis rotation if replace

X axis with Z axis

Y axis with X axis

Zaxis with Y axis

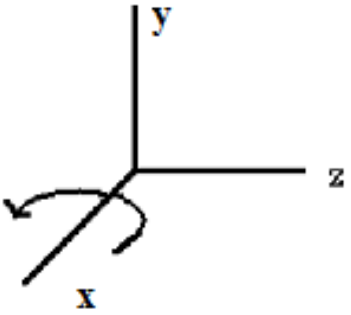
So we do the same replacement in equations :

z' = z*cos q - x*sin q

x' = z*sin q + x*cos q

y' = y

$$Ry(q) = \begin{pmatrix} \cos q & 0 & -\sin q & 0 \\ 0 & 1 & 0 & 0 \\ \sin q & 0 & \cos q & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



2.5 X-Axis Rotation

2.5.1 X-axis rotation looks like Z-axis rotation if replace

X axis with Y axis

Y axis with Z axis

Z axis with X axis

So we do the same replacement in the equations:

y' = y*cos q - z*sin q

z' = y*sin q + z*cos q

x' = x

$$Rx(q) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos q & \sin q & 0 \\ 0 & -\sin q & \cos q & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

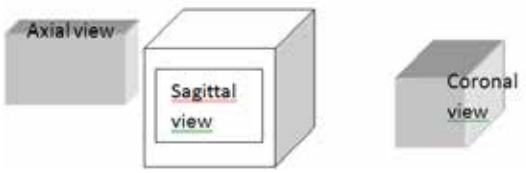
2.6 Rotation about an Arbitrary Axis

This is similar to 2D rotation about an arbitrary point. The general procedure is as follows:

1. Perform transformations which align rotation axis with one of coordinate axis (x, y, z)
2. Perform rotation about the axis
3. Do inverse of (1)

Special case: The rotation axis is parallel to a principle coordinate axis. This is directly analogous to the 2D case of rotation about a point. The steps are:

1. Translate rotation axis to coordinate axis
2. Perform rotation
3. Do inverse translation



In the general case, rotation about an arbitrary axis is more complicated. First we must define the axis of Rotation by 2 points - P1, P2 then do the following:

1. Translate so that rotation axis passes through origin.
2. Rotate so that the rotation axis is aligned with one of the principle coordinate axes.
3. Perform rotation of object about coordinate axis.
4. Perform inverse rotation of 2.
5. Perform inverse translation of 1.

We will arbitrarily choose the Z axis to map the rotation axis onto. The rotation axis is defined by 2 points: P1(x1,y1,z1) and P2(x2,y2,z2.). These 2 points define a vector:

V = (x2 - x1 , y2 - y1 , z2 - z1) = (dx, dy, dz)

Which has a unit vector

U = V |V| where |V| is the length of V = (VxV) = (dx^2 + dy^2 + dz^2)^1/2

Now **U** = (a,b,c) where

a = dx/|V|, b = dy/|V|, c = dz/|V| (these are called the direction cosines of x, y, and z)

(Note: the direction cosine of x = cos A where A = angle of **V** with respect to x axis)

Now we can perform the first translation (of the rotation axis to pass through the origin) by using the matrix **T** (-x1, -y1, -z 1), i.e., move the point P1 to the origin. Next we want to rotate to align **V** with Z axis. We do this in 2 steps:

1. Rotate **V** about X axis to put **V** in XZ plane.
2. Rotate **V** about Y to align with Z.

For rotation about X axis we need to find cos A, sin A where A = angle between projection of **U** (in YZ plane) and Z axis. Note: **U'** is no longer a unit vector, i.e. |U'| =/ 1

Uz = unit vector along z axis = (0,0,1)

now (U)' * (Uz) = |U'| * |Uz| cos A = d * cos A

|Uz | = (1)1/2 = 1

(U')(Uz) = 0 * 0 + b * 0 + c * 1 = c

therefore c = d * (cos A) => cos A = c/d

Now the cross product of 2 vectors (V1) X (V2) = W |V| * |V2|sin q where W is perpendicular to plane of V1, V2

so (U') X (Uz) = Ux|U' |* |Uz|sin A = Ux d * sin A

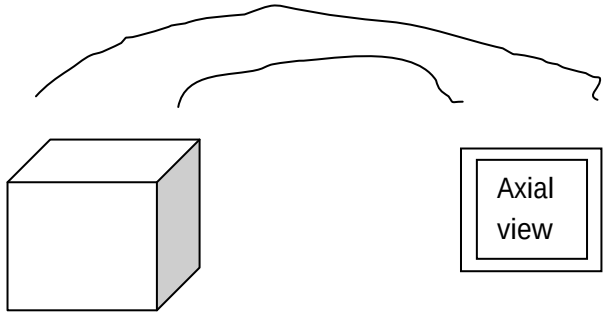
(0 0 0 0)

So Rx(a) = (0 c/d b/a 0)

(0 -b/a c/a 0)

(0 0 0 1)

Rx(a) --> Rotates **U** into XZ plane



Now compute Ry(B) for rotation to z-axis.

After rotation about x-axis the vector is as below:

Uy" = 0 since in XZ plane

Uz" = d = |U'| since just rotated U' into XZ plane

again from dot product:

cos B = U" *(Uz) / |U"||Uz| = 0 * a + 0 * 0 + 1 * d = d

Note: |U"|*|Uz| = 1 since both are unit vectors

from the cross product U" x Uz = Uz|U"||Uz|sin B

(from matrix) = Uy x (-a)

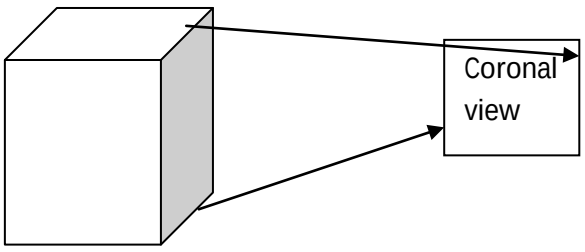
therefore sin B = - a

(d 0 a 0)

Ry(B) = (0 1 0 0)

(-a 0 d 0)

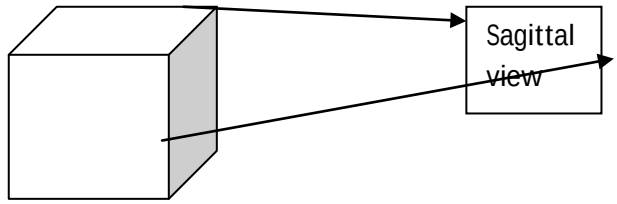
(0 0 0 1)



The result of this transformation is that V (= Rotation axis) is coincident with z axis.

Then apply

(cos q sin q 0 0)



Rz(q) = (-sin q cos q 0 0)
(0 0 1 0)
(0 0 0 1)

Then we must apply inverse transformations to get R.A. back to original position. Therefore, the complete composite transformation matrix is as follows:.

R(q) = T * Rx(A) * Ry(B) * Rz(q) * RY-1(B) * Rx-1(A) * T-1

n1 = a(x), n2 = b(y), n3 = c(z)

[R] =

Row1 n12 + (1 - n12)cosq	n1n2(1 - cosq) + n3sinq	n1n3(1 - cosq) - n2sinq	0
Row2n1n2(1 - cosq) - n3sinq	n22 + (1 - n22)cosq	n2n3(1 - cosq) + n1sinq	0
Row3n1n3(1 - cosq) + n2sinq	n2n3(1 - cosq) - n1sinq	n32 + (1 - n32)cosq	0
Row 4 0	0	0 s	1

III. RESULTS AND ANALYSIS

Generating three views from DICOM images using above methods

- view1 Axial
- view2 Coronal
- view3 Sagittal

still process is going on.

REFERENCE

Books

[1]. Digital Imaging and Communications in Medicine (DICOM) By Oleg S. Pianykh

[2]. Three-Dimensional Imaging for Orthodontics and Maxillofacial Surgery edited by Chung How Kau, Stephen Richmond

[3]. Rotation Transforms for Computer Graphics By John Vince

Websites

[1]. http://www.dcm4che.org/docs/dcm4che-2.0.20-apidocs/org/dcm4che2/data/Tag.html

[2]. http://nipy.org/nibabel/dicom/dicom_orientation.html

[3]. https://www.collabdds.gov.in/index.html

[4]. http://dicomiseasy.blogspot.in/2013/06/getting-oriented-using-image-plane.html

[5]. http://www.dcm4che.org/confluence/display/WEA/Home

 ISBN: 978-81-931039-3-7

CYBER TERRORISM

Bhawana

Asst.Prof. in Comp.Sci.,C.R.M. Jat College,Hisar, (India)

ABSTRACT

It is more than obvious that the way of conducting terrorism with the time is becoming more sophisticated. The cyber terrorism is real threat to fast technology developement. As internet usage is growing daily the world is coming closer. The world wide web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. Making the internet safer (and protecting internet users) has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. Implementing security involves assessing the possible threats to one's network, servers and information. This developing world of information technology has a negative side effect. It has opened the door to antisocial and criminal behavior. To understand cyber terrorism it is important to look at its background, to see how the terrorist organizations or individuals are using the advantage of new technology and what kind of measures governments and international organizations are taking to help the fight against cyber terrorism.

Keywords: Attack, Cyber , Dos, Systems, Terrorism

I. INTRODUCTION

The cyber terrorism as a concept has various definitions, mostly because every expert insecurity has its own definition. This term can be defined as the use of information technology by terrorist groups or individuals to achieve their goals. This may include the use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructure, and to exchange information and perform electronic threat. The threat of terrorism has posed an immense challenge in the pothreat can manifest itself in many ways, such as hacking computer systems, programming viruses and worms, Web pages attack, conducting denial of service (DoS) attacks, or conducting terrorist attacks through electronic communications. More common are claims that cyber terrorism does not exist and that actually it is a hacking and malicious attacks. Those who support these claims do not agree with the term "terrorism" because if we take into account the current technologies for prevention and care, the likelihood of creating fear, significant physical damage or death among population using electronic means would be very small. Considering the fact that the terrorists have limited funds, cyber attacks are increasingly attractive, because, their implementation requires a smaller number of people and certainly smaller funds. Another advantage of cyber attacks is that they allow terrorists to remain unknown, because they can be very far from the place where the act of terrorism is committed.

The articles envisages an understanding of the nature and effectiveness of cyber attacks and highlight what more could be done. The article is structured as given below:

- Definition of Cyber Terrorism
- Cyber Crime

- § Types of Cyber crime
- § Cyber Crime in Modern Society
- § How to Tackle Cyber Crime

¨ Cyber Security

¨ Recommendations

II. DEFINITION OF CYBER TERRORISM

Although there are a number of definitions which describe the term terrorism, one of the definitions that are frequently encountered is that terrorism is

"the unlawful use or threatening use of force or violence by a person or an organized group against people or property with the intention of intimidating or forcing societies or governments, often for ideological or political reasons."

Interactions between human motives and information technology for terrorist activities in cyberspace or in the virtual world can be addressed as cyber terrorism. Yet this is the definition of cyber terrorism that Sarah Gordon and Richard Ford from Symantec have used in their efforts to define "pure Cyber terrorism."

III. CYBER CRIME

As Internet usage is growing daily the world is coming closer. The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. However, it has also managed to create another problem for people who spend long hours browsing the Cyber World – which is cyber crimes. While law enforcement agencies are trying to tackle this problem, it is growing steadily and many people have become victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid being a victim of cyber crimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet. However, before you can understand more about this system, let us find out more about cyber crimes.

3.1. Types of Cyber Crimes

When any crime is committed over the Internet it is referred to as a cyber crime. There are many types of cyber crimes and the most common ones are explained below:

3.1.1 Hacking: This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

3.1.2 Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

3.1.3 Cyber Stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

3.1.4 Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.

3.1.5 Malicious Software: These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

3.1.6 Child soliciting and Abuse: This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

3.2. History of Cyber Crime

When computers and networks came into being in the 1990s, hacking was done basically to get more information about the systems. Hackers even competed against one another to win the tag of the best hacker. As a result, many networks were affected; right from the military to commercial organizations. Initially, these hacking attempts were brushed off as mere nuisance as they did not pose a long-term threat. However, with malicious software becoming ubiquitous during the same period, hacking started making networks and systems slow. As hackers became more skillful, they started using their knowledge and expertise to gain benefit by exploiting and victimizing others.

3.3 Cyber Crime in Modern Society

Today, criminals that indulge in cyber crimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day's work.

Cyber crimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cyber crimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes. The same systems that have made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals.

3.4 Categories of Cyber Crime

Cyber crimes are broadly categorized into three categories:-

3.4.1. Individual: This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming". Today, law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

3.4.2 .Property: Just like in the real world where a criminal can steal and rob, even in the cyber world criminals resort to stealing and robbing. In this case, they can steal a person's bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization. The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

3.4.3. Government: Although not as common as the other two categories, crimes against a government are referred to as cyber terrorism. If successful, this category can wreak havoc and cause panic amongst the civilian population. In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

3.5. How to Tackle Cyber Crime

It has been seen that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective. That is why commercial institutions and government organizations need to look at other methods of safeguarding themselves.

The best way to go about is using the solutions provided by Cross-Domain Solutions. When organizations use cross domain cyber security solutions, they can ensure that exchange of information adheres to security protocols. The solution allows organizations to use a unified system comprising of software and hardware that authenticates both manual and automatic transfer and access of information when it takes places between different security classification levels. This allows seamless sharing and access of information within a specific security classification, but cannot be intercepted by or advertently revealed to user who is not part of the security classification. This helps to keep the network and the systems using the network safe.

Cross Domain Solution offers a way to keep all information confidential by using safe and secure domains that cannot be tracked or accessed. This security solution can be used by commercial and governmental organization to ensure an impenetrable network while still making sure that users can get access to the required information easily.

IV. CYBER SECURITY

Cyber security comprehensively refers to the set of safeguarding measures intended to maintain integrity of information as it passes through heterogeneous networks and becomes vulnerable to malicious attacks from viruses and scripts. It strategically deals with checking user identity, associated risks and incident management. It is structurally composed of processes, technologies and practices devised to optimally mitigate the risks to computers, programs and networks.

Extremely sensitive data like defense information needs to be critically protected from unauthorized access to prevent harmful tampering, corruption and misrepresentation.

An individual user can implement checks to thwart unwanted manipulation of his data by continually updating the antivirus program, putting strong passwords and strictly guarding personal information over networks that are not trusted.

Cyber-security is intimidated by rapidly and regularly evolving nature of risks. The conventional wisdom of devoting the bulk of resources on the most critical system aspects to safeguard against formidable threats, while leaving minor components unprotected cannot be justified in the present scenario. The threat is accelerating at a pace that is beyond control and is significantly deviating from set norms. An adaptive and proactive system is being fostered to regularly monitor and assess real time the emerging threats.

Cyber-security is meant for proactive detection of loopholes in the security policies of the computer systems which can be exploited by people engaged in information warfare to seek entry in critical system to alter, destruct or hold government to ransom by threatening to damage sensitive information infrastructure. Critical information should not be leaked to unauthorized people. A truly secure network will maintain the integrity of data stored in it and also allow government to access and regularly supervise the entire array of information in it. Cyber-security or cyber assurance defines the mechanism to extend operational support for management and protection of networks, data and information. It also has provision for contingency support to facilitate safeguarding of cyber-dependent operations. The stress is on predicting potential cyber-attacks by simulating real time operating environment to understand the approach of intrusive elements and deter them. It calls for deployment of resources to backup critical information and survive any cyber-attack. The augmented operational capabilities will give a proactive response to any attempt of unauthorized access to information.

Cyber-security tactics recognize the fact that attacking a system is easier than defending it. The compromise of a system is contingent on the understanding gained by the hacker of a part of the system's technical architecture. The defenders however need to comprehensively analyze the entire infrastructural set-up and learn the specific needs of the managing organizations to better protect the system from internal and external attackers.

4.1. The Challenges Confronted by Cyber-Security Experts are

4.1.1. Multiple security models: A majority of large organizations need to manage numerous domains or data centers. Mostly, the management of such elements is entrusted to different enterprises and consequently there is no central cyber security governance mechanism. The situation can be simplified by implementing standardized processes as the management of heterogeneous architectures (application and infrastructure) makes things complicated.

4.1.2. Continuity of Operations: This has become complex owing to growing data center consolidation leaving little scope for redundant operations. The increasing architectural standardization has paved way for larger cross domain vulnerability. Besides, the shrinking numbers of regional 'continuity of operations' hubs has rendered it more fragile from network communications scenario.

4.1.3. Coordinated Help Desk: The demand for coordinated help desk operations deployed across organizations is on the rise after the scope of cyber security is getting clear. Coalition partners and related organizations have developed greater dependency on one another in respect to earlier times. However, the challenge of building a coordinated help desk has not been adequately addressed so far with the operations limited to particular domains and restricted to propagation of generalized threat/ incident reporting scenario only.

4.1.4. Social Engineering: It refers to activity category that concerns itself with combating non-traditional and non-security attacks and compromises. It can be deployed from internal or external perspective with the objective of exploiting inherent system weaknesses pertaining to security policies which paves the way for consequent technical exploitation.

4.1.5. Unstructured Data Security: Organizations have gradually moved from paper records to electronic versions. A majority of the data circulating within the organization is to an extent unstructured. Structure data sources can be covered with data security policies meant for formal record management. However unstructured data like emails, wikis etc. are less secure as unstructured data management policies have not fully evolved as yet.

V. RECOMMENDATIONS

Certain recommendations are given below:

(a) Need to sensitize the common citizens about the dangers of cyber terrorism. Cert-in should engage academic institutions and follow an aggressive strategy.

(b) Joint efforts by all Government agencies including defence forces to attract qualified skilled personnel for implementation of counter measures.

(c) Cyber security not to be given more lip service and the organisations dealing with the same should be given all support. No bureaucratic dominance should be permitted.

(d) Agreements relating to cyber security should be given the same importance as other conventional agreements.

(e) More investment in this field in terms of finance and manpower.

(f) Indian agencies working after cyber security should also keep a close vigil on the developments in the IT sector of our potential adversaries.

VI. CONCLUSIONS

There is a growing nexus between the hacker and the terrorist. The day is not far when terrorists themselves will be excellent hackers. That will change the entire landscape of terrorism. A common vision is required to ensure cyber security and prevent cyber crimes. The time has come to prioritize cyber security in India's counter terrorism strategy.

REFERENCES

[1]. S. Best, DeÞ ning Terrorism**:** http://www.drstevebest.org/Essays/DeÞ ning%20Terrorism.htm www.symantec.com/avcenter/reference/cyberterrorism.pdf

[2]. M. Cereijo Cuba the threat II: Cyberterrorism and Cyberwar, 16 Maj 2006: http://www.lanuevacuba. com/archivo/manuel-cereijo-110.htm

[3]. R. L. Dick, Director, National Infrastructure Protection Center, FBI Federal Bureau of Investigation, Before the House Energy and Commerce Committee, Oversight and Investigation Subcomittee Washington, DC, 05 April 2001, http://www.fbi.gov/news/testimony/issue-of-intrusions-intogovernment- computer-networks

[4]. www.terror.net: How Modern Terrorism Uses the Internet, 21 February 2007: http://www.asiantribune.com/index.php?q=node/4627

[5]. R. Lemos, Cyberterrorism: The real risk, 2002: http://www.crime-research.org/library/Robert1.htm D.Briere, P.Hurley, Wireless network hacks and mods for dummies, 2005, Wiley.

[6]. M. Bogdanoski, A. Risteski, & S. Pejoski, (2012, November). Steganalysis—A way forward against cyber terrorism.

 ISBN: 978-81-931039-3-7

DATA SECURITY USING COMPREHENSIVE RSA CRYPTOGRAPHIC ALGORITHM

G.Amala[1], A.Komathi[2]

[1]*Research Scholar, Department of Computer Science & Information Technology,*
Nadar Saraswathi College of Arts & Science, Theni, Tamil Nadu, (India)
[2]*Department of Computer Science & Information Technology,*
Nadar Saraswathi College of Arts & Science, Theni, Tamil Nadu, (India)

ABSTRACT

Data Security is the method of shielding information. More companies store business and individual information on computer than ever before. In the existing research, cryptographic block cipher concept with logical operation like XOR and shifting operation were used. In this the main drawback was that, generate key was based on Alphabets only. So any hackers had the chance to find out the secret random key using loop concept.

So In my Research, I proposed RSA cryptographic algorithm which uses Key Generation Algorithm with Hashing Function technique to encrypt and decrypt the given data. The Key will be generating by using Key Generation Algorithm and the Key will be based on higher sets of alphanumeric characters. So the Crypt analyzing process will be difficult compare to the previous one. Moreover, Here I used Hashing Technique for Cryptographic along with Qubit Key Generation Method. Experimental result will show the efficiency and security of my proposed algorithm.

Key Words: Information Security, Block Cipher Method, RSA Algorithm, Hashing Technique, Key Generation Method

I. INTRODUCTION

Information security has become a very critical aspect of modern computing system. With the global acceptance of the Internet, virtually every computer in the world today is connected to every other. While this has created incredible productivity and unprecedented opportunities in the world we live in, it has also created new risk for the user of these computers. The user, businesses and organisations worldwide have to live with a constant threat from hackers and attackers, who use a variety of methods and tools in order to break into computer system, steal information, change data.

Now a day, cryptography has many commercial applications. If we are shielding confidential data then cryptography is provide high level of privacy of individuals and groups. However, the main scope of the cryptography is used not only to provide confidentiality, but also to provide solution for other problems like: data integrity, non-repudiation, and authentication.

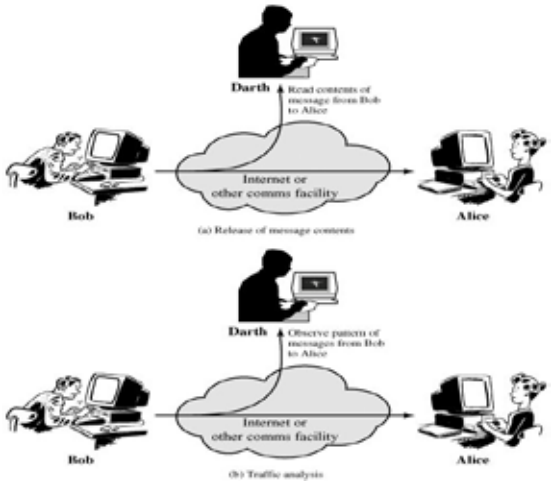


Fig 1 Passive Attacks

Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is very complicated to find out the specific algorithm, because we have previously known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity.

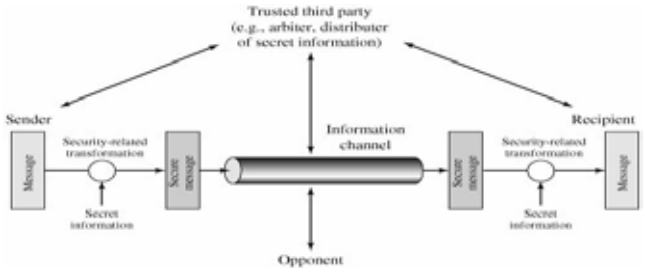


Fig 2 Model for Network Security

Security Services: If we are taking about security of information then following services come in mind.

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuses of resources)
- Availability (permanence, non-erasure)

II. LITERATURE REVIEW

2.1 Advance Cryptography Algorithm for Improving Data Security

In this technique they describe about a new cryptography algorithm which is based on block cipher concept. In the algorithm they have used logical operation like XOR and shifting operation. In this technique they used a random number for generating the initial key, where this key will use for encrypting the given source file using proposed encryption algorithm with the help of encryption number. Basically in this technique a block based substitution method will use. In this technique they will provide for encrypting message multiple times. Initially that technique is only possible for some files such as MS word file, excel file, text file.

2.2 Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (Cp-Abe) System for the Dtns

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

III. DESCRIPTION OF RSA ALGORITHM

Keeps security in sending secrets message using RSA Algorithm implemented through web service: The RSA algorithm can be used for both public key encryption. Its security is based on the difficulty of factoring large integers. RSA algorithm segregated into two parts:

Encryption of secret message: Rather represent the secret message as an integer directly, we generate a random session key and use that to encrypt the secret message with a conservative, much faster symmetrical algorithm like Triple DES. We then use the much slower public key encryption algorithm to encrypt just the session key.

Decryption encrypted secret message: The sender A then transmits a message to the recipient B in a cipher text format. The recipient B would extract the encrypted session key and use his private key (n,d) to decrypt it. He would then use this session key with a conventional symmetrical decryption algorithm to decrypt the original message. Typically the transmission would include in secret message details of the encryption algorithms used (CIPHER Text). The only secret necessary to be kept, as always, should be the keys.

Session Key: A session key is decryption and an encryption key that is randomly generated to ensure the security of a communications session between a user and another computer or between two computers.

Qubit Generation: To get the secret key and random string, then change it into hex-code and then convert it into binary, find the least bit of the two binary values and get the quantum bit of 0 and 1.

IV. PROPOSED WORK

In this paper I am proposed a block based symmetric cryptography algorithm. In this technique I have used a pseudo random prime number and exponential values of random number for generating the initial key using session key method, where this key uses for encrypting the given source file using RSA algorithm. Our proposed system using 512 bit key size with combination of alphanumeric method to encrypt a text message. It will be very difficult to find out two same messages using this parameter. To decrypt any file one has to know

exactly what the key block and to find the random blocks with the combination of alphanumeric numbers, theoretically one has to apply 2256 trail run and which is intractable. But initially that technique is not possible to find the combination of alphanumeric methods using 2256 trail run.

4.1. Session Key Generation Steps

- It is a shared secret key which is used for encryption and decryption.
- The size of session key is 512 bits with combination of alphanumeric characters.
- This session key is generated from pseudo random prime number and exponential values of random number.

4.2. Proposed Algorithm

- Get the secret key, then convert it into hex-code and then convert it into binary.
- Find the least bit of the two binary values and get the quantum bit of 0 and 1.
- Generate the quantum key using the qubit and session key this depends on the qubit.

Combinations,

1. If (Last two bit = 0) then $1/\sqrt{2}(p[0] + p[1])$.
2. If (Last two bit = 1 && 0) then $1/\sqrt{2}(p[0] - p[1])$.
3. If (Last two bit = 0 && 1) then p[0].
4. If (Last two bit = 1) then p[1].

- Encrypt the session key by using the master key and store all the values.
- Key distribution center distributes the original session key and qubit to the sender for Encrypting the message.
- Key distributor center also distributes the key and qubit to the corresponding receiver to Decrypt the received messages.

V. SAMPLE RESULT

Fig 3 : Login for User

 ISBN: 978-81-931039-3-7

Fig 4 Secret Key Request

Fig 5 Get Secret Key from Key Generator

Fig 6 Get Secret Key in File Format

Secret Key – Send to File

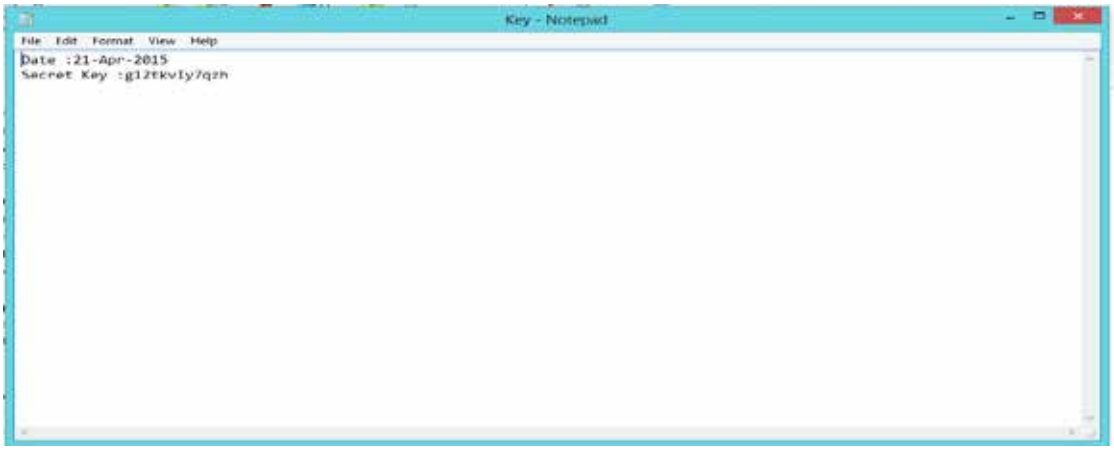


Fig 7 Get Secret Key in File Format with Combination of Alphanumeric Method

VI. CONCLUSION

In this proposed technique is especially for block cipher method and it will take less time of the file size is large. The important thing of our proposed method is impossible to break the encryption algorithm without knowing the exact key value. We ensure that this encryption method can be applied for data encryption and decryption in any type of public applications for sending confidential data.

REFERENCES

[1] DriptoChatterjee, JoyshreeNath, SubadeepDasgupta, AsokeNath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 987-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[2] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms "2009 International Conference on computational Intelligence and Security 978-0-7695-3931-7 / 09 $26.00 © 2009 IEEE DOI 10.1109 / CIS. 2009.81.

[3] Symmetric key cryptography using random key generator A.Nath, S.Ghosh, M.A.Malik, Proceedings of International conference on SAM-2010 held at Las Vegas (USA) 12-15 JULY, 2010, Voll-2,P-239-244.

[4] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010. [5] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag. [6] By Klaus Felten "An Algorithm for Symmetric Cryptography with a wide range of scalability" published by 2nd International Workshop on Embedded Systems, Internet Programming and Industial IT.

[7] Majdi Al-qdah& Lin Yi Hui "Simple Encryption/Decryption Application" published in International

[8] T Morkel, JHP Eloff" ENCRYPTION TECHNIQUES: A TIMELINE APPROACH" published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[9] Text book William Stallings, Data and Computer Communications, 6eWilliam 6e 2005.

[10] Md. Nazrul Islam, Md. MonirHossain Mia, Muhammad F. I. Chowdhury, M.A. Matin "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" Ninth ACIS International

Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 978-0-7695-3263-9/08 DOI 10.1109/SNPD.2008.101 IEEE 2008.

[11] [Rijn99]JoanDaemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999.

[12] SwatiKamble, "Advance Cryptography Algorithm for Improving Data Security" National Conference On Research Trends In Electronics, Computer Science & Information Technology And Doctoral Research Meet, Feb 21st & 22nd, 2014. NCDRM-2014.

[13] Dr.AnandaRao.G, Srinivas.Y, VijayaSekhar.J, Pavan Kumar.ch " Three Party aunthentication key distributed protocols using implicit and explicit Quantum Cryptography." Indian journal of Computer Science and Engineering(IJCSE), ISSN:0976-5166.

 ISBN: 978-81-931039-3-7

IDENTIFICATION OF FACTORS IN IMPLEMENTATION OF QUALITY CIRCLE

Ajay Kalirawna [1], Rajesh Attri[2], Nikhil Dev[3]

[1]*PG Scholar, YMCA University of Science & Technology, Faridabad, (India)*

[2,3]*Assistant Professor, Dept. of Mechanical, YMCA University of Science & Technology, Faridabad, (India)*

ABSTRACT

Quality circle (QC) is a management tool which is most widely utilized for enhancing the effectiveness of equipment's in an organization. QC provides a lot of benefits such as increase in product quality, improvement in organizational performance, motivation and team work among the employees etc. But, implementation of QC is not an easy task as it is full of lots of hurdles. The main objective of this paper is to identify the critical factors which help in the successful implementation of QC programs in manufacturing organization.

Keywords: Quality Circle, Factors, Identification, Implementation, Organization

I. INTRODUCTION

In olden times Indian industries were practicing on older concept of system, to manage the scientific techniques. The disadvantages of which were barrier of mistrust, Individualism & non-involvement of employees in management of organization. A quality circle is a volunteer group, composed of regular employees, who meet to discuss workplace improvement & make presentation to management with their ideas especially relating to quality of output. It improves the performance of the organization, motivates &enriches the work life of employees (Chaudhary and Yadav, 2012). In this some groups of employees are formed for performing some task and training is given to the groups in solving the problems and using the statistical tools. The employees are encouraged for team work and motivated to work in cooperative manner. These employees work in groups and for the effectiveness of the organization. These groups find out the solutions for the quality and services which can be implemented in the organization for obtaining better results. The members of the Circle are the employees who can have influence in problem solving or to those members affected by the problems. They often meet once a week, meetings that approximately last an hour. During the meetings, the members of the Circle analyze the problems in details. After the frequent meetings, the members of Quality Circles propose the solutions of the problems that are closely related to their daily activities. In order to come up with the best problem solutions, the members have to attend the induction trainings by using the newest methods and techniques (Syla et al., 2013).

II. BENEFITS OF QUALITY CIRCLE

There are many benefits from QC implementation; some of those benefits are as follow(Attri et al., 2014):

- ☐ Increase in company quality awareness;
- ☐ Increase in product quality awareness;

- ☐ Improvement in management;
- ☐ Improvement of customer relations;
- ☐ Improvements in the products and services offered;
- ☐ Improved relationships within the organization;
- ☐ Greater customer satisfaction; and
- ☐ Increased respect from competitors.

III. QC IMPLEMENTATION PROCESS

The steps involved in the implementation process of Quality Circle (Figure 1) are as follows:

1. Identification of problem: First of all the problem is identified by the Quality Circle members which is to be solved.
2. Analysis of the problem: The selected problem is then analyzed by basic problem solving techniques.
3. Generate alternative solution: On the basis of various causes, the alternative solutions are generated.
4. Selection of best solution: The best and the most suitable solutions are selected from the alternative solutions.
5. Prepare action plan: The members prepare plan for the area of implementation, date, time etc.
6. Presentation of solution to management: The solution is then presented before the management for the approval.
7. Implementation of solution: The management evaluates the solution and implement it for a small run to check its reliability.

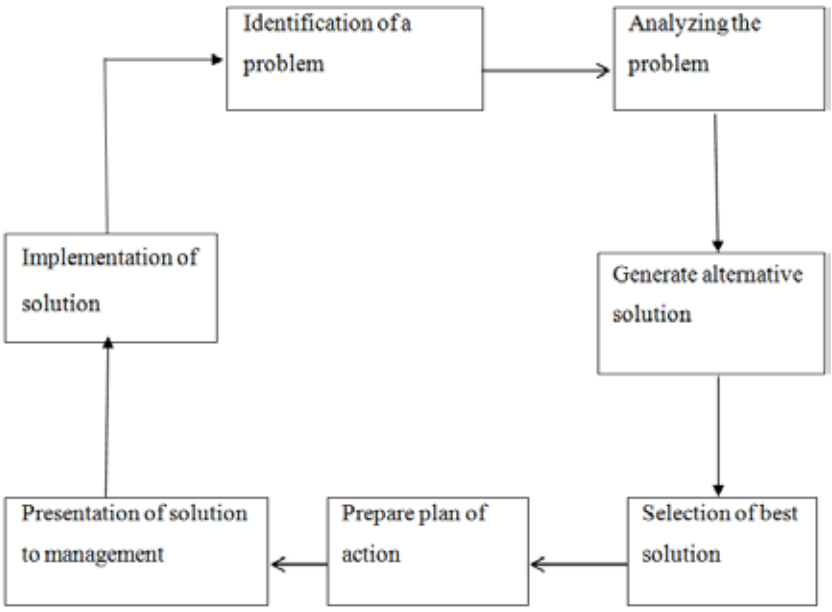


Figure 1: Working model of Quality Circle (Modified from Gaikwasd and Gaikwad 2002)

 ISBN: 978-81-931039-3-7

IV. FACTORS AFFECTING IMPLEMENTATION OF QC

- **Top management commitment and support:** The success of any management practices relies significantly on the maturity level of senior management leadership and commitment. Direct involvement of top management allows all decisions to be made quickly and facilitate QC journey (Patterson et al., 1995). Top management support is necessary to prove the availability of concrete actions.
- **Employee involvement:** Employee involvement is a process for empowering employees to participate in managerial decision-making and improvement activities appropriate to their levels in the organization (Brown et al., 2005). Innovation and technology incorporate the innovation into corporate culture, encouraging new ideas and processes and solutions by all the employees of the firm.
- **Providing Education and Training:** Increased involvement means more responsibility, which in turn requires a greater level of skill. This must be achieved through training. Quality training includes educating and training all employees, help employees to increase knowledge, provide information about the mission, vision, direction and organization structure to enable them to gain skills in an effort to improve the quality and thus solve the problem (Dale, 2009).
- **Flexibility:** Flexibility in operations and delivery may enable the user to give customized service to its customers, particularly in special or non-routine requests. Logistics flexibility, related to the different logistics strategies, which can be adopted either to release a product to a market (downstream or distribution flexibility) or to procure a component from a supplier (upstream or procurement flexibility (Adeleye and Yusuf, 2006).
- **Motivation:** Motivational factors can be divided into two factors i.e. external and internal factors. The first ones are related to improvements in terms of marketing and promotional aspects, increase in customer satisfaction and the improvement of market share, while internal benefits are related to organizational improvements, the reward system, team work, the measurement of performance and communication, continuous improvement (Kassicieh et al., 2008).
- **Strategic Planning:** Quality may be considered as a strategic competitive tool, and organizations cannot afford to ignore the strategic implications of quality for their competitive position. Strategic planning will result in a strategic training plan, and it can be used to predict the future training needs based on employee needs and demands of consumers (Patterson et al., 1995).
- **Proper Communication:** Communication inextricably linked in the quality process, yet some executives find it difficult to tell others about the plan in a way that will be understood (Brown et al., 2005). An additional difficulty is filtering. As top management's vision of quality filters down through the ranks, the vision and the plan can lose both clarity and momentum.
- **Continuous Improvement:** Very important is the continuous improvement stage of the post-certification period. The continuous improvement stage is actually the phase where the maintenance of the quality system is carried out. This phase is important if an organization wants to continuously improve and reap the long term benefits of having a quality management system in place (Dale, 2009).
- **Customer Satisfaction:** Quality Circle is a system focusing on customer satisfaction. The Quality Circle concept is one of the modern management concepts, which helped to increase the competitiveness between organizations. This has resulted from the level of customer awareness, which helps them to select a product

or service of high quality and at a reasonable price (Ali and Shastri,2010).

- **Proper Empowerment:** Employees have to take more responsibility with regard to their involvement in a team, in order to exert greater authority over their work environment. Employee involvement is a process for empowering members of an organization in decision making and to problem solving appropriate to their level in the organization (Casadesus and Gimenez, 2009).
- **Financial Resources:** There is a multitude of variables that could influence a company's business financial performance. From the financial perspective, Quality Circle certification would be beneficial to the promotion of activities, improvement of profitability and the productivity of facilities (Park, 2007)
- **Proper Leadership:** Top leadership is the key to any QC program and the driving force behind success and failure. Leadership associated with clear vision and directions can foster knowledge sharing and generate commitment (Ali and Shastri,2010).
- **Culture Change:** The principles of quality must be embedded into the culture of the organisation to foster the climate of open co-operation and teamwork among members of staff, suppliers and customers. Many researchers have showed from their work that culture of the organization should be such that it can accommodate the values of QMS system.
- **Process Approach**: A desired result is achieved more efficiently when activities and related resources are managed as a process. Process should be simple and easily understandable. Many researchers in their research have discussed that the approach should be simple so that the workers do not oppose the approach and work in a cooperative manner.

V. CONCLUSION

Quality Circle (QC) is a very effective tool which helps in solving many problems like decision making, consumption, effective management etc. For the effective implementation of QC, the top management of the organization must provide adequate training and education to their employees. This will in the improvement of attitude of the employees for their enthusiastically participation in the quality circle programs. So, this paper tries highlighting the main factors which helps in the implementation of QC in manufacturing organizations. These critical factors will enable the organization to develop proper strategies for effectively utilizing them in the successful implementation of QC programs.

REFERENCES

[1]. Adeleye, E.O. and Yusuf, Y.Y. (2006) 'Towards agile manufacturing: models of competition and performance outcomes', International JournalAgile Systems and Management, Vol. 1, pp.93–110.

[2]. Ali,M. and Shastri, R.K. (2010) Implementation of TQM in Higher Education, Journal of Business Management, Vol. 2, No. 1, pp. 9-16.

[3]. Attri R.,Dev N. and Kalirawna A.(2014) Identification of barriers in implementation of Quality Circle, Handbook of Management,Technology and Social Sciences, Vol. 2, pp. 110-112.

[4]. Brown, A. and Van der Wiele, T. (2005) Industry experience with ISO 9000, Asia Pacific Journal of Quality Management, Vol. 4, No. 2, pp. 8-17.

[5]. Casadesus, M. and Gimenez, G. (2009)The benefits of the implementation of the ISO 9000 standard: empirical research in 288 Spanish companies. The TQM Magazine, Vol. 12, No. 6, pp. 432-441.

[6]. Chaudhary R. and Yadav L. (2012) Impact of quality circle towards employees & organization: A case

study, IOSR Journal of Engineering, Vol. 2, No. 10, pp. 23-29.

[7]. Dale, B.G. (2009), Managing Quality, Third edition, Blackwell Publisher Inc., Oxford, UK.

[8]. Farris, D.R. and Sage, A.P. (1999) On the use of interpretive structural modeling for worth assessment, Computer & Electrical Engineering, Vol. 2, pp. 149-174.

[9]. Gaikwad,V.V. and Gaikwad, A.V. (2009)Quality Circle as an Effective Management Tool:A Case Study of Indira College of Engineering and Management Library, Available online at http://crl.du.ac.in/.

[10]. Kassicieh, S.K. and Yourstone, S.A. (2008) Training, performance evaluation, rewards, and TQM implementation success, Journal of Quality Management, Vol. 3 No. 1, pp. 25-38.

[11]. Kumar, M. and Antony, J. (2008) Comparing the quality management practices in UK SMEs, Industrial Management and Data Systems, Vol. 108, No. 9, pp. 1153-1166

[12]. Park, D.J. (2007) Business values of ISO 9000:2000 to Korean shipbuilding machinery manufacturing enterprises, International Journal of Quality & Reliability Management, Vol. 24, No. 1, pp.32-48.

[13]. Patterson J.W., Kennedy W.J. andFredendall L.D. (1995) Total productive maintenance is not for this company, Production and Inventory Management Journal, Vol. 36, No. 2, pp. 61-64.

[14]. Prasanna, N.K.K. and Desai, T.N. (2011) Quality Circle implementation for maintenance management in petrochemical industry, Journal of Engineering Research and Studies, Vol. 2, No. 1, pp. 155-162.

[15]. Shpresa, S. and Gadaf, R. (2013)Quality Circles: what do they mean and how to implement them?, International Journal of Academic Research in Business and Social Sciences, Vol. 3, No. 12, pp. 243-251

[16]. Singh, M.D., Shankar, R., Narain, R. and Agarwal, A. (2003) An interpretive structural modeling of knowledge management in engineering industries, Journal of Advances in Management Research, Vol. 1, No. 1, pp. 28-40.

[17]. Warfield, J.W. (1994) Developing interconnected matrices in structural modeling, IEEE Transcript on Systems, Men and Cybernetics, Vol. 4, No. 1, pp. 51-81

 ISBN: 978-81-931039-3-7

DESIGN AND CONTACT ANALYSIS OF RAIL TRACK USING SOLIDWORKS AND ANSYS

Gaurav Saini[1], Dr. Tilak Raj[2], Arnav Sharma[3]

[1,3]PG Scholar, YMCA University of Science & Technology, Faridabad, (India)

[2]Professor, Dept. of Mechanical, YMCA University of Science & Technology, Faridabad, (India)

ABSTRACT

Computer aided investigations are carried using ANSYS, to verify maximum stress and its location. To predict detailed stress 3D solid model has been chosen with the help of SOLIDWORK software.First 2D geometry is created using SOLIDWORKS than its revolved by revolve extrude command to make wheel. Additionally, after selecting the loading and boundary conditions and appropriate finite elements, the nonlinear axis symmetric 2D FE models were generated and simulated in non-uniform and non-homogeneous conditions. A solver mode in ANSYS software calculates the stresses, deflections, bending moments and their relations without manual interventions, reduces the time compared with the method of mathematical calculations by a human. ANSYS static analysis work is carried out by considered caststeel and their relative performances have been observed respectively.

***Keywords*: *ANSYS 11, SOLIDWORKS 2010, Stress Analysis, Wheel Rim*.**

I. INTRODUCTION

Railway transportation system, as one of the notable meansof commuting systems, has served for human societies andhas pursued its improvements as other promoted aspects oflife. In recent years, the capacity of carrying axial loads forworld railways as well as their velocities has been enhancedwhich results in increasing the amount of strains and stresseson lines and digression of rails. By this augmentation,interactions between railway components become more considerable.The rolling contact of awheel on a rail is the basis ofmany Rail-Wheel related problems including the rail corrugation,wear, plastic deformation, rotating interaction fatigue, thermo-elastic-plastic behavior in contact, fracture, creep,and vehicle dynamics vibration. Therefore, it has attracted alot of researchers to various railway networks.The stress distribution is an important factor at the Rail-Wheel contact interfaces, that is, two materials contacting atrolling interfaces which are extremely influenced by geometry of the contacting surfaces,material attributes, and loadingand boundary conditions. Convincing theories as well as computer software have been developed to evaluate all the influential parametersinvolving in the Rail-Wheel interaction. Recently, tendency towards finite element method (FEM) has increased because of its simplicity, accuracy, cost efficiency, and versatility. FE analysis results in a set of simultaneous algebraic equations[1].

1.1 Rails

Rails are longitudinal steel members that are placed on spaced sleepers to guide the rolling stock. Their strength and stiffness must be sufficient to maintain a steady shape and smooth track configuration and resist various forces exerted by travelling rolling stock. One of their primary functions is to accommodate and transfer the wheel/axle loads onto the supporting sleepers. Divided into three parts:

1.1.1 Rail head: the top surface that contacts the wheel tire

1.1.2 Rail web: the middle part that supports the rail head, like columns

1.1.3 Rail foot: the bottom part that distributes the load from the web to the underlying[2].

II.WHEEL ELEMENT AND MATERIAL

Permissible Load on wheel 98 ton is calculated from KARL GEORGE wheel catalogue.

Dead weight of vehicle	50 ton
Lining weight	5 ton
Carrying capacity	250 ton
Max drive wheel load	88 ton
Max permissible wheel load	98 ton
Permissible pressure per unit area	5.6 n/mm2(rail 590 N/mm2, wheel rim 590 N/mm2)
Wheel speed	30m/min
Number of wheel	4

CAST STEEL
G35CrNiMo6-6QT1, EN10293
MATERIAL NO. : 1.6579
Rm = 800 MPa (Min.)
Rp 0.2 = 650 MPa (Min.)
A = 12% Min.
KV = 30 J (Min.) ×
} FOR t = 150 TO 250 mm
×AVERAGE VALUE OF 3 SEPERATE SPECIMENS FOR IMPACT TEST CARRIED OUT AT ROOM TEMPERATURE. LOWEST INDIVIDUAL VALUE ≥ 21 J.

III. DESIGN OF WHEEL AND TRACK ASSEMBLY

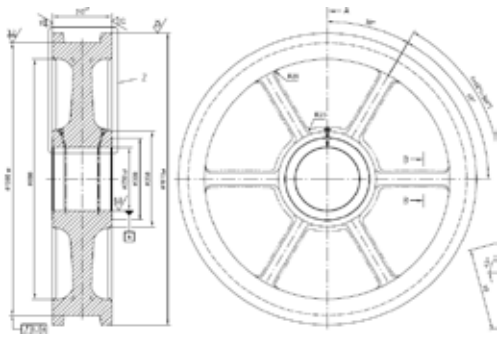


Figure 3.1 Drawing of wheel

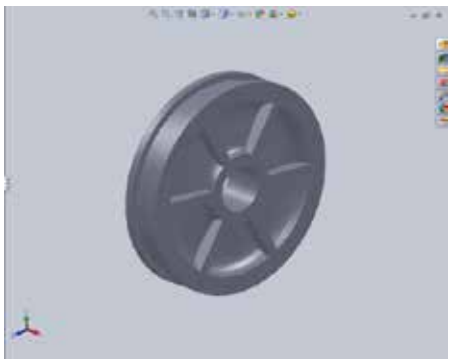


Figure 3.2 3D model of wheel on SOLIDWORK

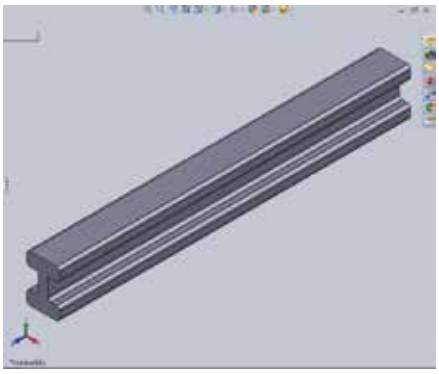


Figure 3.33D model of track

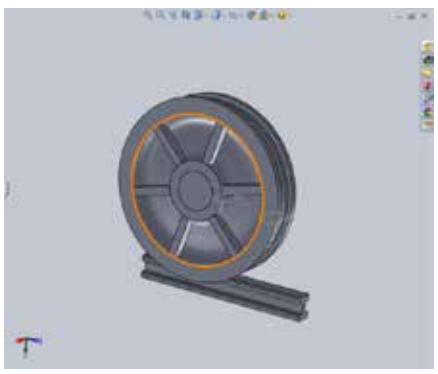
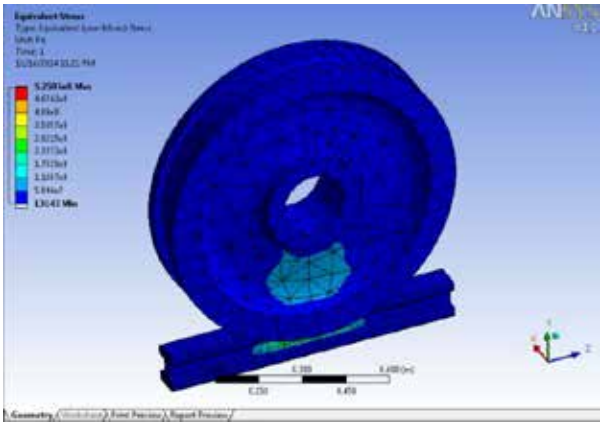


Figure3.43D model of wheel and track assembly

IV. ANSYS PROCEDURE FOR CONTACTANALYSIS



1. File of the wheel and track is saved in IGS format.
2. 3D model of wheel and track assembly is inserted in ANSYS.
3. Than simulation option is selected for analysisof wheel and track.
4. Connection is made between wheel and rail by connections in project tree.
5. Rough Contact between wheel and rail is selected by contact option.
6. Tetrahedral element is selected in Meshing method under mesh and mesh is generated.
7. Track is fixed in all 3 DOF by fixture option.
8. 98 ton of permissible load is applied on wheel. Stress result is obtained by showing the final result option

V. RESULT

		Maximum contact stress
1.	Yield strength	525 Mpa
2.	Factor of safety	1.23

VI. CONCLUSION

CAD model of the wheel track is generated in solidworks and this model is imported to ANSYS for processing work. An amount of force 98 ton is applied along the circumference of the wheel and track is fixed. Following are the conclusions from the results obtained:

- Maximum stress by ANSYS is lower than the yield stress of material.
- Von-mises stresses are less than ultimate strength.
- Since the von-mises stresses is less than the ultimate strength, talking deflections into account, cast steel is preferred as best material for designed wheel track.

VII. SCOPE FOR FUTURE WORK

In the above proposed work only force acting circumferentially on the wheel track is only considered, this can be Extended to other forces that act on the wheel rim and structural analysis is carried out, this can be extended to TransientAnalysis.

REFERANCE

[1] Mohammad Reza Aalami, Aras Anari,TorkanShafighfard and SiamakTalatahari "A Robust Finite Element Analysis of the Rail-Wheel Rolling Contact"Volume 2013, Article ID 272350, 9 pages.

[2] SakdiratKaewunruen and Alexander Remennikov "Dynamic properties of railway track and its components: a state-of-the-art review" volume 2008.