Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

Enhanced Protection of Implants from Potential Threats of Data Theft and Misuse

Sagnik Dakshit,
Student, Cse, CIEM
Calcutta Institute of Engineering & Management
Kolkata, India

Md. Faraz Zakir,
Student, Cse, CIEM,
Calcutta Institute of Engineering & Management
Kolkata, India

Abhijit Mitra,
Asst. Professor, Cse, CIEM,
Calcutta Institute of Engineering & Management
Kolkata, India

***Abstract*— With modernization, the use of technology has become widespread. Today, our human bodies are also controlled by a number of Technical devices, some of which aid our survival medically like pacemaker and insulin or neuro controllers. This dependence on onboard storage computer devices has also increased the risk of malicious use of technology to hamper the well-being of a person. In consideration of recent implications of a Hacker having killed a man by pacemaker hacking accidentally we propose methods to prevent such accidents or malicious handling of sensitive data on which our lives depend. The procedure is complicated and involves multiple encryption and decryption but comes at a minimal cost in front of the value of our lives.**

Keywords—WBAN; WLAN; pacemakers; hacking; Fibonacci series; xor cipher; PN sequence; RSA algorithm; Hill cipher

I. INTRODUCTION

It is widely recognized that data security is playing a central role in the design of IT systems. With the wireless industry exploding, it faces a growing need for security. With advancement of embedded systems and wireless communications, these systems have become a part of not only human lifestyle but also within the Human body. It is widely recognized that data security is playing a central role in the design of IT systems. With the wireless industry exploding, it faces a growing need for security. Body Implant devices like the Pacemaker, Insulin Implants are in dire need of security as they are prone to attack like most other wireless embedded systems. Wireless telemetry is the remote monitoring of patient physiological parameters (e.g., cardiac signals, blood glucose, body temperature) over a distance via radiofrequency (RF) communications between a transmitter worn by the patient and a central monitoring station. Undoubtedly, this technology delivers mobility, comfort, and higher levels of patient care. In a recently published article Computer World [1] magazine a researcher has claimed to have killed a man by hacking his pacemaker. IT poses the question
of security of Medical Implants as they now hold the key to our longevity. Wireless sensor networks [10,11] are usually considered one of the technological foundations of ambient intelligence. Agile, low-cost, ultra-low power networks of sensors can collect a huge amount of important information from the surrounding environment. Using a biological analogy, sensor networks can be viewed as the sensory system of the intelligent environment of the human body. Sensor networks are irregular clusters of communicating sensor nodes, which collect and process information from onboard sensors, and they can share some of this information with neighboring or surrounding nodes or even with nearby data collection stations. In recent developments by NASA [3], they have developed a range of wearable and implantable biomedical devices will increase significantly in the next years, thanks to the improvements in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics, achieved in recent years. The technology will be used to treat the following as claimed by NASA. Cardiovascular (exclusive license already in place) spinal injuries and orthopedics (e.g., disc implants) Hydro-encephalitis Lactate acid level sensors Epilepsy. With increase in dependency on Wireless telemetry and embedded systems as implants in Medical healthcare, the threat of data misuse of unauthorized manipulation is faced. The risks to patients now are very low, but I worry that they could increase in the future, said Tadayoshi Kohno, a lead researcher on the project at the University of Washington, who has studied vulnerability to hacking of networked computers and voting machines.

II. DESCRIPTION

In this paper we try to analyze the possibility of attacks on one such Implant, the Pacemaker. The pacemaker nowadays uses a wireless radio transmitter which is used by authorized personnel to make changes in the settings of the pacemaker and to read the stored data on an onboard memory chip on the pacemaker. Erdem Topsakal [2] of Mississippi university in his paper Wireless Medical Telemetry: Current Status and Future Directions has given details of some configuration of antenna design of such devices. A small antenna operating at medical implant communications services (MICS) (402 MHz- 405 MHz) / MedRadio (401 MHz 406 MHz) and industrial, scientific and medical (ISM) 433 MHz and (2.4 GHz -2.48 GHz) bands is used as per our finding. [4] Researchers say that they have also been able to glean personal patient data by eavesdropping on signals from the tiny wireless radio that Medtronic, the devices maker, had embedded in the implant as a way to let doctors monitor and adjust it without surgery. [5] The possibility of inducing parasitic signals could raise critical security impacts. A potential hacker can use the frequency to alter the data

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

onboard the pacemaker or change its settings which can be fatal. Directed energy radio frequency weapons have been widely investigated for military applications aiming to either disturb or damage electronic devices. The main challenge, namely the generation of high amounts of energy, slowly evolved to the design of complex and efficient waveforms to decrease the required electromagnetic (EM) field intensity.

A. ICDs and Pacemakers

Internal Structure: Pacemakers and ICDs typically consist of a sealed, battery- powered, sensor-laden pulse generator; several steroid-tipped, wire electrodes (leads) that connect the generator to the myocardium (heart muscle); and a custom ultralow-power microprocessor, typically with about 128 Kbytes of RAM for telemetry storage. The devices primary function is to sense cardiac events, execute therapies, and store measurements such as electro-cardiograms. Healthcare professionals configure the settings on pacemakers and ICDs using an external device called a programmer. This Programmer uses wireless telemetry to make adjustments and read stored data from the memory. Pacemakers and ICDs often contain high-capacity lithium based batteries that last up to seven years. Rechargeable batteries are extremely rare, for practical, economic, and safety reasons. Device lifetime depends on the treatments required. Whereas pacing pulses consume only about 25 J, each ICD shock consumes 14 to 40 J. A single defibrillation can reduce the ICDs lifetime by weeks.

Working of ICDs and Pacemakers: Both heart pacemaker and ICDs the are size designed to treat arrhythmia. The device is connected to the heart or intestine via electrodes and continuously monitors the heart rhythm. Pacemakers automatically deliver low- energy signals to the heart to cause the heart to beat faster when the heart rate slows and vice-versa. ICDs include pacemaker functions but can also deliver high-voltage signals when low voltage fails. ICDs are superior in that they monitor the heart continuously. Pacemakers and ICDs save innumerable lives on a daily basis.

Wireless Telemetry: Previous generations of pacemakers and ICDs communicated at low frequencies (near 175 kHz) with a short read range (8 cm) and used low-bandwidth (50 Kbits per second) inductive coupling to relay telemetry and modify therapies. Medical Implant Communications Service, is used by some ICDs which operates in the 402- to 405-MHz band and allows for much higher bandwidth (250 Kbps) and longer read range (specified at two to five meters). As figure A illustrates, major pacemaker and ICD manufacturers now produce at-home monitors that wirelessly collect data from implanted devices and relay it to a central repository over a dialup connection. The repository is accessible to doctors via an SSL-protected Website.

Reliability: As pointed out in [10]; although pacemakers and ICDs often save lives, they have known to malfunction. Since 1990 the US Food and Drug Administration has issued dozens of product advisories affecting hundreds of thousands of pacemakers and ICDs. These statistics show that 41 percent of device recalls were due to malfunctions in firmware (216,533 out of 523,145 devices). Additional device programming glitches remain, as evidenced by a clock function abnormality that we recently observed in a clinical setting These problems existence underscores potential hazards that come with increasingly sophisticated implantable medical devices. Past abnormalities surfaced under accidental circumstances. The potential for intentionally malicious behavior calls for a deeper investigation into IMD safety from a security and privacy perspective. To address the issue of privacy and security in implants not restricted to Pacemakers we consider the types of attacks possible through wireless telemetry and propose solutions to make such devices more secure and private.

B. Attacks and Scenarios Possible

Firstly, let us study the types of Attacks possible. To understand the impact such an attack can have on a target, some attack scenarios have been studied considering public vulnerabilities and threats to medical security.

Spoofed/Altered Information: These type of attacks can create incorrect message and change the settings of the pacemaker.

Man in the Middle Attack: Its possible for hackers to trick communicating devices into sending their transmissions to the attacker's system. Here they can record the traffic to view later (like in packet sniffing) and even change the contents of files. Various types of malware can be inserted into these packets, e-mail content could be changed, or the traffic could be dropped so that communication is blocked.

Sinkhole Attacks: Sinkhole attack is a type of attack where compromised node tries to attract network traffic by advertise its fake routing update. The patch can be send as a message over a carrier radio frequency.

Sybil Attacks: The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks.

Wormholes message: This attack can get an opponent and a tunnel through various parts of the reply.

Jamming: There are a number of ways to jam a wireless network. One method is coding an AP with de-authentication frames. This effectively overwhelms the network and prevents legitimate transmissions from getting through.

Acknowledgement Spoofing: This attack has the goal of convincing the sender that a weak link is strong enough or that a dead node is still alive. That is how the adversary can remove information sending it to these weak links or to these dead nodes. This is possible due to the fact that the adversary can overhear packets addressed to other nodes and can have a general view of all the network knowing which links are weak or which nodes are dead.

C. Proposal to prevent such mishap

As seen in [8] has proposed a method of using a Singular Hash function SHA1 to establish a secure connection. Our two layered security is much safer. The first layer of Security is essentially establishing a secure channel for communication by Authenticating the Device attempting to communicate similar to a hash function by using a preset acknowledgement message using ECC algorithm which on

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

matching with the message on device will be allowed to communicate. On the second line of defense the sensitive data stored on board is encrypted using 5 different algorithms including RSA which was the proposal [8]. This Hybrid Encryption is the second layer of protection.

Acknowledgement/mutual authentication: Mutual authentication, can also be termed two-sided acknowledgment, using a private key for the pacemaker and a public key for its authorized stations Encryption using the ECC algorithm. It would prevent attacks like Acknowledgement spoofing and Sybill Attacks as only machines acknowledged by ECC algorithm can communicate. This is turn also prevents Jamming as Jamming is performed by unreliable sources and this method keeps out unacknowledged communicating devices. An efficient Certified Communication protocol can be used as described in [11] The protocol uses Deffie-Hellman Key exchange and an elliptical curve over finite field Z_p. An elliptic curve over the finite field Z_p is defined as the set of points (x, y), satisfying the elliptic curve equation $y^2 = x^3 + ax + b \; mod \; q$ where x, y, a, and b are the elements of the field. Note that the condition $4a^2 + 27b^2 = 0 \; mod \; q$ should be met.

(a) h( ): one-way hash function
(b) q: a large prime(q3)
(c) q: a large prime(q3)
(d) B: B ε E(Fq) with order q x(Q): x coordinate of point Q
(e) E_k(m): symmetric encryption of message m using k D k (c): symmetric decryption of cipher text c using k X_u: user us secret key
(f) Yu: us public key with Y_u, X_uB mod p
(g) A! B: A sends message to B
(h) R_u: a random number R_2 [2; n_2]

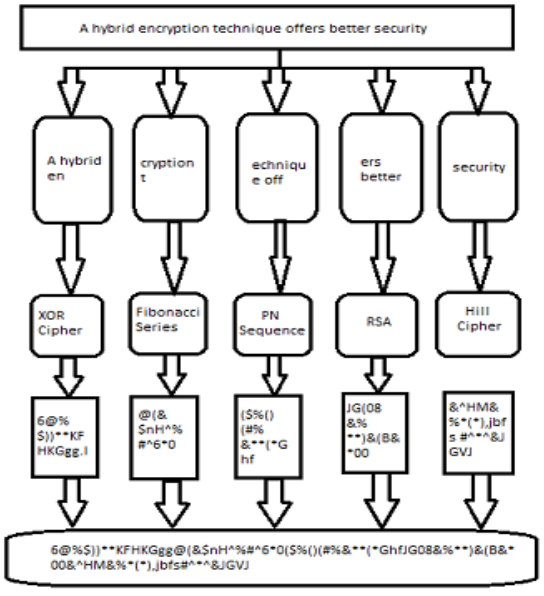
ECC Diffie-Hellman Protocol: The algorithm Diffie - Hellman key exchange protocol based on elliptic curve cryptography runs as follows:

(a) A selects a random number R_a and computes Y_a = R_a × B. Next, he sends Y_a to B.
(b) Similarly, B computes Y_b = R_b × B, where n_b is selected by B. He also sends Y_b to A.
(c) A generates the session key K = R_a × Y_b. B generates the session key K = R_b × Y_a.

Two keys computed in Step 3 are the same because
$R_a \times Y_b = R_a (R_b \times B) = R_b (R_a \times B) = R_b \times Y_a$. The key agreement protocol achieved mutual protocol key exchange, but does not provide mutual authentication, an adversary can easily forge a message required in the protocol. The protocol assumed that user A and B had
registered at certification authority (CA), and CA generated and issued user digital certificate, which is in the use of Elliptic Curve Digital Signature. The acknowledgement based authentication can be established as such:

Communicator	Implant
1) Choose R_1 where R_{12} (0,1)m 2) Calculate Y_1 where $Y_1 = R_1$ - p 3) Send Y_1 to Implant(I)	
	1) Choose R_2 where R_{22}(0,1)m 2) Calculate $Y_2 = R_2$ - p 3) Calculate $Y_1 = R_1$ - Y_1 and $Y_{12} = R_2 - Y_1$ 4) Compute h(Y_{12}; Y_1I ;CertI) 5) Send Y_1 , CertI, h(Y_{12}; Y_1I , CertI) to U
1) Authenticate CertI 2) Calculate $Y_{12} = R_1 - Y_2$ and Y_2I = R_1 - YI 3)Authenticate h(Y_{12}; Y_1b;CertB) 4) Calculate Y_2u = Ru -Y_2 5) Calculate E, Y_{12} (CertU; Y_2u) 6) Send E,Y_{12} (CertU; Y_2u) to I	
	1) Decrypt E, Y_{12}(CertI; Y_2u) 2) Authenticate CertU 3) Check Y_2u = R_2 - Y u =>(U and I share the session key Y_{12})

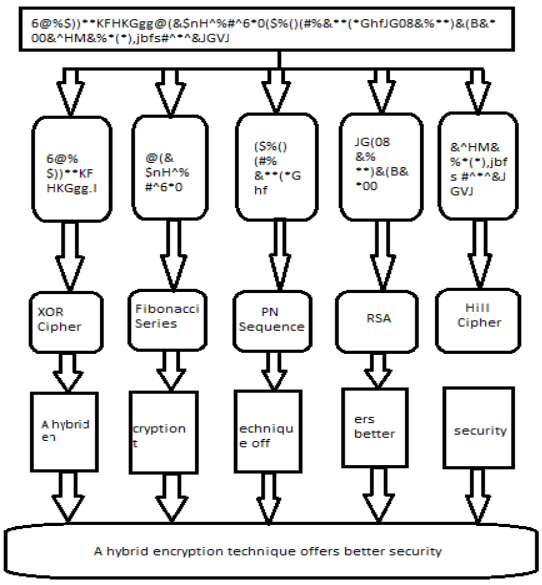
Hybrid Encryption: We propose to Store the sensitive data using a hybrid Encryption technique as proposed in [7] by Amardeep kaur and Satveer Singh. The entire data is organized as a single stream and then divided into 5 segments. Each of the segments are encrypted using 5 different algorithms using XOR, FIBONACCI, PN Sequence and RSA algorithm and Hill Cipher and Stored on board the Implant. For decrypting it we use the same algorithms in reverse order. In Hybrid technique this information is divided into five segments, the length of each segment depends on the sender. The text message encrypted using five different Crypto graphical algorithms. For example, let us say the stream has 51 characters, then the first 11 characters of the text message encoded using Fibonacci series, second 10 characters of text message encoded using XOR cipher, third 9 characters of text message encoded using PN sequence, fourth 11 characters of text message encoded using RSA algorithm and fifth 10 characters of text message encoded using Hill cipher.



Steps of Encryption

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

When the data is send to the user (Doctor or Pacemaker Mechanist) these text messages is divided into five different segments and after that decoded the text message to five different cryptography algorithms such as Fibonacci series, XOR cipher, PN sequence, RSA algorithm, Hill cipher which same as employed to encryption side and output obtain the original text message as shown in fig. 2



Steps of Decryption

The used Algorithm

1. Fibonacci Series
   a. Take the first segment of the text message
   b. Convert the character value into ASCII value.
   c. Generate the encrypted key(f) dependent on Fibonacci series.
   d. Generate the encrypted text message in sender side.

$$enc = b + f$$

   e. Generate the original text message in receiver side.

$$dec = msg4 - f$$

2. XOR Cipher
   a. Take the second segment of the text message.
   b. Convert the character value into ASCII value.
   c. Convert the encrypted key(kk) for size(kk)
      If key value==48
      Then kk=0;
      Else
      Kk= 1;
      End
   d. Generate the encrypted text message in sender side
      For size(b33)
      Xor(b33,kk)
      End
   e. Generate the original text message in receiver side
      For size(b44)
      Xor (b44,kk)
      End
3. PN sequence
   a. Take the third segment of the text message.
   b. Convert the character value into ASCII value.
   c. Generate the encrypted key(k key)
      for length(message)
      S + key = S
      k key = S;
      End
   d. Generate the encrypted text message in sender side

$$enc = b + k\ key$$

   e. Generate the original text message in receiver side

$$dec1 = enc1 - k\ key$$

4. RSA algorithm
   a. Take the fourth segment of the text message
   b. Select two prime numbers(p,q)
   c. Calculate the value of Pk = pxq
   d. Calculate the value of Φ = (p-1) x (q-1)
   e. Calculate the encryption key e using while loop
      x = 2; e = 1;
      while x < 1
      e = e + 1;
      x = gcd(Φ,e)
      end
   f. Calculate the decryption key d using e and Φ(d×e)
   g. Generate the encrypted text message in sender side
      for j = 1: length(msg)
      for i = 0:(Φ-1)
      cipher = crypt (msg, Pk, e)
      end
      end
   h. Generate the original text message in receiver side
      for j = 1:length(cipher)
      msg2 = crypt (cipher, Pk, d)
      end
5. Hill cipher
   a. Take the fifth segment of the text message
   b. Select the square 2 × 2 matrix.
   c. Group each pair of character into vector values.
   d. Generate the cipher text c operate the following method

$$C = PK\ mod\ M$$

   e. Generate the plaintext P operate the following method

$$P = CK^{-1}\ mod\ M$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

III. RELATED WORKS & THEIR DRAWBACKS

- K Han et al, proposed an efficient model for authenticated key agreement in dynamic WBAN and that this protocol enables reduced authentication process for mobile node and can be used in various application of WBAN.
- Vaidya et al, proposed a user authentication scheme in WBAN, which is a variation of strong password based solution proposed.
- Ying et al, proposed an efficient and scalable protocol to establish and update the authentication key between any pair of sensor nodes in dynamic WBAN. The proposed solution is suitable for both static and dynamic environments. The solution has less communication cost and high probability of sharing a key. Sonone et al., International Journal of Advanced Research in Computer Science and Software Engineering 4(11), November - 2014, pp. 110-114 2014, IJARC- SSE All Rights Reserved
- Chuchaisri: Proposed a 2 PKC-based broadcast schemes called the key pool scheme and key chain scheme using bloom filter to aid the node to decide/solve the dilemma when to forward the data first or authenticate first.
- Wong et al, proposed a dynamic user authentication scheme for WBAN. It allows the genuine users to query the sensor data from any of the sensor nodes by imposing very less computational load. This scheme claimed that it is secure against replay and forgery attacks in which it fails.
- Tseng et al, this paper shows that is vulnerable to replay and forgery attacks and proposed an authentication mechanism that retains the advantages of. The scheme possesses the advantage of resistance to the replay attacks and forgery attacks, with reduction in the risk of password leakage.
- Abhram and Ramanatha, proposed an authentication and initial shared key establishment model of hierarchical clustered networks.
- Perrig et al, proposed a suite of security protocols called Security Protocols for WBANs (SPINS) optimized for WBANs. SPINS includes two protocols: secure network encryption protocol (SNEP) and TESLA. SNEP provides unicast authentication, confidentiality, and replay protection through authentication with MAC and encryption. TESLA offers a solution for broadcast authentication.
- Zhu et al, in this proposed each node generates a one-way key chain and sends the commitment of it to their neighbors. If a node wants to send a message to its neighbors, it attaches the next authorization key from its key chain to the message. The receiving node can verify the validation of the key based on the commitment it has already received. This scheme does not provide a solution for attacks from inside where the adversary knows nodes cluster key.
- Fanatacci et al: proposed a distributed node authentication model that does not require a central authority to authenticate. This model has increased communication and computational overhead as every node shares partial information of others and all nodes involve in the authentication procedure as an authenticator.
- Huang et al, proposed a self-organizing algorithm using ECC which has 2 phases 1: Implicit Certificate Generation Process and Hybrid Key Establishment Process. Supports dynamic node re-authentication but the author did not state it. Proposed scheme has major problem where each sensor node must have direct contact with the CA which would be a bottleneck.
- Mahagoub: He proposed an efficient model that deployed a Partial key escrow table for sinks. Using this table, the sink can self- generate a shared key for the attached nodes. To support node mobility all the sinks, have to maintain this table, which is an overhead. In [19] Wang et al, proposed the dynamic window scheme using additive increase multiplicative decrease to regulate the window size. The scheme allows switching between the forward- first or authenticating first mode.
- Dong et al, overcomes the shortcoming of which is not effective against the malicious node attack, by establishing a group key with the nodes neighbors and filtering out misbehaving nodes. But this method despite improvements still allows the broadcast of forged messages.
- Ning et al, proposed a weak authentication scheme to filter bogus/false messages using one-way key chain. But this approach requires synchronization and periodic broadcasting between the access points and sensor nodes when it is used with signature based authentication.
- Wang et al, PK by using multiple short lived at the time of signature verification public keys in order to reduce the proposed small but requires that all sensor nodes stored in these keys when these keys lifetime expires then sink node periodically broadcasts and public keys redistributes.
- Ren et al, proposed a scheme of multi-user authentication using bloom filter to store multiple user IDs and Public keys. The disadvantage is that the Bloom filter can be forged and cannot prevent the DOS attack.
- T.H.Lee, proposed a password based authentication protocol similar to [11]. These algorithms and reduce computational load and have reliable time synchronization. They are weak against user-password security attacks and not mentioned about which MAC algorithm to use.
- T.Yao et al, proposed an authentication protocol for broadcasting messages using one way key chain and secure acknowledgements. But the drawback is there is no sync of time and whole broadcasting would be disrupted with single malicious node because of unknowing key chain.
- Kim et al, proposed the algorithm for detecting and dropping fabricated reports from representative nodes using message authentication nodes. However, this scheme brings to communication overload due to number of MACs which are computed by representative nodes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

- Y.K.Lee et al, The proposed scheme uses pre shared secret key which is obtained from ECDH key exchange algorithm and is based on modified SHA-1 hash function which helps to compute MAC for given messages. The algorithm provides both integrity and authenticity of the message with only one hash value.
- Ravi et al: proposed a PKC certificate based scheme for user authentication, certi_cate being generated by the Sink. This scheme is vulnerable to DOS attack.
- Omar et al: proposed a key distribution scheme for dynamic conferences. In this scheme a trusted server distributes private pieces of information to a set of users. Each member of any group of users of a given size can compute a secure group key.

REFERENCES

[1] http: // www. computerworld. com/ article/ 2981527/ cybercrime-hacking/researchers-hack-a-pacemaker-kill-a-man-nequin.html
[2] https: // technology. nasa. gov/ patent/TOP3-403
[3] 10.1109/USNC-URSI.2014.6955627
[4] http: // www. nytimes. com/ 2008/ 03/ 12/business/ 12heart-web. html? _r= 1& oref=slogin
[5] EMI Threats for Information Security: Re-mote Command Injection on Modern Smart-phones Chaouki Kasmi and Jose Lopes Esteves
[6] Volume 4, Issue 11, November 2014 ISSN: 2277 128X International Journal of Advanced Re-search in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com Study on Security Methods, threats in Wireless Body Area Networks Shub- hangi Sonone, Prof. VishalShrivastava Arya col-lege of Engg and Information Jaipur RajashthanTechnical University, Kota Rajashthan, India
[7] A hybrid technique of cryptography watermark-ing for data encryption and decryption.
[8] The Authentication and Key Agreement Proto-col Based on ECC for Wireless Communications by Zhang Juan and Deng Fangmin.
[9] Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H.Maise in their paper \Security and Privacy for Implantable Medical Devices"