International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

# Cyber Security for Remote Patient Monitoring System

**B. Manjulatha**

Assistant Professor in CSE Dept., VBIT, Telangana, India

**Abstract:** ***The Internet of Things is an emerging topic of technical, social, and economic significance. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytic capabilities that promise to transform the way we work, live, and play. Projections for the impact of IoT on the Internet and economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025. Internet of Things (IoT) devices is rapidly becoming ubiquitous while IoT services are becoming pervasive. Their success has not gone unnoticed and the number of threats and attacks against IoT devices and services are on the increase as well. Cyber-attacks are not new to IoT, but as IoT will be deeply interwoven in our lives and societies, it is becoming necessary to step up and take cyber defense seriously. Currently, most proposed IoT attacks are proof-of-concepts and have yet to generate any profit for attackers. This does not mean that attackers won't target IoT devices in future, even if it is just to misuse the technology or have a persistent anchor in a home network. The use of weak passwords is a security issue that has repeatedly been seen in IoT devices. These devices often do not have a keyboard, so configuration has to be done remotely. Unfortunately, not all vendors force the user to change the devices' default passwords and many have unnecessary restrictions which make the implementation of long, complex passwords impossible. The Open Web Application Security Project's (OWASP) Lists Top Ten Internet of Things Vulnerabilities. This thesis has three main contributions. (i) It enables secure communication in the IoT using lightweight compressed yet standard compliant IPsec, DTLS, and IEEE 802.15.4 link layer security; and it discusses the pros and cons of each of these solutions. The proposed security solutions are implemented and evaluated in an IoT setup on real hardware. (ii) This thesis also presents the design, implementation, and evaluation of novel IDS for the IoT. (iii) Last but not least, it also provides mechanisms to protect data inside constrained nodes. This paper mainly focuses on Remote Patient Monitoring Systems. However, deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. Moreover, the physiological data of an individual are highly sensitive. Therefore, security is a paramount requirement of healthcare applications, especially in the case of patient privacy, if the patient has an embarrassing disease. Security is provided for data which is being fetched from the patients through wearable devices and transferred to the concerned doctors by using a public key encryption technique namely ECC (Elliptic Curve Cryptography) is used.***

**Keywords:** Wireless Medical Sensor Networks (WMSN), ECC, DTLS, IEEE 802.15.4 or ZigBee, OWASP.

## 1. Introduction

### 1.1 Health Monitoring System

In recent years, waiting time in hospitals, emergency admissions are extremely costlier. It also increases the workload of doctors and medical professionals. Managing the cost, quality of treatment and caring for seniors are important issues in healthcare. These issues have a demand for in-home patient monitoring.

The human body parameters are fetched by different ways through biosensors, wearable medical devices, and smart textiles. Then the collected details are forwarded to the remote server through the internet. Current Wireless Medical Sensor Network (WMSN) healthcare research trends focus on patient reliable communication, patient mobility, and energy-efficient routing, as a few examples. However, deploying new technologies in healthcare applications without considering security makes patient privacy vulnerable. Moreover, the physiological data of an individual are highly sensitive. Therefore, security is a paramount requirement of healthcare applications, especially in the case of patient privacy, if the patient has an embarrassing disease. Improving the efficiency of healthcare infrastructures and biomedical systems is one of the most challenging goals of modern-day society. In fact, the need of delivering quality care to patients while reducing the healthcare costs and, at the same time, tackling the nursing staff shortage problem is a primary issue. Sensor networks are being used in a wide range of application areas. The major application domains [1,2] are, home and office, control and automation, transportation, environmental monitoring, healthcare, security and surveillance, tourism, education and training and entertainment. In recent years, a great research undergoes in Sensor devices that can be used to monitor human activities. The application areas can be divided into two major categories—medical use, non-medical use. The medical applications can be of two types: wearable and implanted. Wearable devices are those that can be used on body surface of a human or just at close proximity of the user. The implantable medical devices are those that are inserted inside human body. The non-medical devices and their applications can be real-time video streaming using mp4 video player and real-time audio streaming using mp3 player etc. Sensor networks [3] can be realized through real-time, continuous vital monitoring to give immediate alerts of changes in patient status. The main purpose of using these home monitoring applications are used to collect periodic or continuous data and be uploaded to a physician and can allow long-term care and trend analysis. It can also reduce length of hospital stay. Manual tracking of patient status is difficult. Collection of long-term databases of clinical data can be used in future diagnosis.


**Figure 1:** Devices used for Remote Patient Monitoring System

### 1.2 Working of Wearable Devices using Wireless Sensor Networks

Different wearable devices are attached to the human body. With the help of Bluetooth or ZigBee protocol the patient details such as heart rate, BP, temperature etc are being transferred to central database. There filtration of data is done to reduce unwanted or invalid data which is nowhere used. Finally the data is stored in web server. From there the doctor receives the information which is required for undergoing further process. While transferring the data to central database an SMS alert is given for both doctor as well as the patient's relatives.


**Figure 2:** Transferring of data from Patient to Doctor

### 1.3 Application of Wireless Sensor for Better Health Care

The healthcare domain presents opportunities for a significant number of applications of wireless sensor technology. The following sections focus on three broad health monitoring applications that include Chronic Disease Monitoring, Personal Wellness Monitoring, and Personal Fitness. Within each of these applications, we describe several specific uses of wireless sensor technology.

**1) Chronic Disease Monitoring**

Chronic diseases encompass a wide range of health problems including diabetes, asthma, heart diseases and sleep disorders. . Since not all chronic disease monitoring is the same, we further refine the category as follows:

- Episodic patient monitoring is often utilized in non-critical patients to track specific indicators and identify the progress of the disease or recovery
- Continuous patient monitoring is often associated with acute conditions that require constant or frequent measurement of health status.
- Patient alarm monitoring can also trigger alarms based on preset conditions that are specific to the patient and the disease.

**Episodic Patient Monitoring Scenario**

This use case deals with non-acute or episodic patient monitoring. In this scenario, the patient's vital signs (e.g. heart rate, temperature) and disease-specific indicators (e.g. blood pressure, blood glucose level, EKG) are monitored to determine anomalies and spot trends. The monitoring is done periodically. All the information collected by the medical sensors is time-stamped and securely forwarded to a gateway that functions as a patient monitoring system. Additionally, the gateway forwards the aggregated information in a secure way to a database server. The medical personnel and the family can access the information stored in the database server to monitor the progress of the disease.

**Figure 3:** Shows a few examples of monitoring devices that can take advantage of ZigBee wireless technology

**Continuous Patient Monitoring Scenario:**

In this situation, the vital signs (e.g. heart rate, temperature, pulse oximeter) are monitored on a constant basis to allow continuous measurement of patients' health status at rest or during mild exercise for purpose of treatment adjustment, recovery or diagnosis. The patient or the care provider remotely activates the on-body sensors via the off-body unit. The measurement data from the body sensors is securely transmitted continuously to the on-body unit, where it is temporarily stored. Subsequently, the recorded measurement data is securely sent to the off-body unit via batch transmission for persistent storage and further analysis by the health care provider.

**Patient Monitoring Alarm Scenario:**

In this scenario, the patient's vital signs (e.g. heart rate, temperature) and disease-specific indicators (e.g. blood pressure, EKG, EEG) are monitored on a continuous basis. The data collected by the medical sensors is time-stamped and securely forwarded to a gateway that acts as a patient monitoring system. Additionally, the gateway securely forwards the aggregated information to a database server. In this case, a certain minimum bit error rate and maximum end-to-end latency not to exceed a few seconds should be

guaranteed. At pre-determined settings, alarms are issued and responses/actions could be triggered automatically.

**2) Personal Wellness Monitoring:**
Personal Wellness Monitoring is an area that will first focus on individuals age 65 or older. As an initial focus, the monitoring concerns the person's activity and safety. As this market develops, adoption of this technology will find applications for the general population.

**3) Personal Fitness Monitoring:**
Personal fitness is also a market segment showing high potential for use of wireless sensor technology both in the home and in health fitness centers. A large variety of devices and services are envisioned to accommodate the growing fitness market.

**Monitoring and Tracking Fitness Level Scenario**
This use case focuses on tracking the fitness level or progress made by an individual. A number of parameters that the individual wishes to monitor are recorded as the individual perform his/her workout routine. Additionally, the gateway sends the information to a database server for record keeping. Note that the information need not be sent in real time, but may be collected and transmitted after the workout routine ends. After the workout, the individual can review a history of these parameters to track and analyze their fitness level. In this use case, the application polls each sensor type at a different rate.

**Personalized Fitness Schedule Scenario**
This scenario focuses on personalization of the fitness schedule of an individual. The schedule to be followed by the individual can be entered by a trainer or the individual.

**Social Alarm Devices**
Social Alarm devices allow individuals, in their own home or residential-care facility, to raise an alarm and communicate with a caretaker when an emergency situation occurs. The caretaker may be a monitoring center, a medical care team or a family member.

## 2. System Architecture

The architecture for remote healthcare monitoring system is categorized into three types.

1) Wireless Body Area Network (WBAN);
2) Personal Server (PS) using IPDA;
3) Medical Server for Healthcare Monitoring (MSHM).

### 2.1 First Tier

The core of this system is the user called the patient. Wearable sensors are attacked to the patient body forming wireless body area network (WBAN) to monitor changes in patient's vital signs closely and provide real time feedback to help maintain an optimal health status. The medical sensors typically consist of five main components:

1) Sensor: it is a sensing chip to sense physiological data from the patient's body.
2) Microcontroller: it is used to perform local data processing such as data compression and it also controls the functionality of other components in the sensor node.
3) Memory: it is used to store sensed data temporally.
4) Radio Transceiver: it is responsible for communication between nodes and to send/receive sensed physiological data wirelessly.
5) Power supply: the sensor nodes are powered by batteries with a lifetime of several months [4].

Sensor nodes can sense, sample, and process one or more physiological signals. For example, an electrocardiography (EKG) sensor can be used for monitoring heart activity; a blood pressure sensor can be used for monitoring blood pressure, a breathing sensor for monitoring respiration, an electromyogram (EMG) sensor for monitoring muscle activity etc.

In our design, a sophisticated sensor is integrated into the WBAN called Medical Super Sensor (MSS). This sensor has more memory, processing and communication capabilities than other sensor nodes as shown in **Figure 4** above. MSS uses a radio frequency to communicate with other body sensors and ZigBee[5] is used as a communication protocol to communicate with the Personal Server.

In this design, we considered Bluetooth and ZigBee technologies. In case of Bluetooth specification, it supports maximum of seven active slaves (i.e. sensors to be controlled by one master, personal server). But the number of sensor nodes we are considering in this system are more than seven therefore Bluetooth technology is not acceptable option.

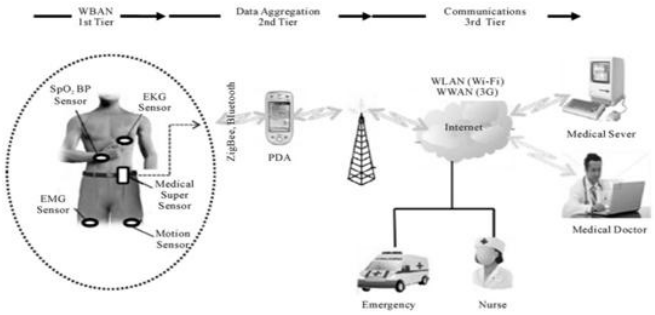



**Figure 4:** Architecture of wearable sensors for remote healthcare monitoring system

The second technology is ZigBee/IEEE 802.15.4 standard. It has a short range, low power consumption, low cost technology, capable of handling large sensor networks up to 65,000 nodes and reliable data transfer. Other reasons why it is used are stated below:

- Security: Patient information is vital; it must not be changed by unauthorized person. Data transfers from WBAN to the personal server and the medical server must be secured. ZigBee provides a low power hardware encryption solution using Elliptic Curve Cryptography (ECC) to encrypt data transmitted between MSS and personal server.
- Scalability: it is highly scalable for many devices.

- Interoperability between a variety of medical and non-medical devices with data management devices regardless of manufacturer.

However, Medical Super-Sensor (MSS) unobtrusively samples, collects multiple sensed vital signs by the body sensors, filtering out all redundant data thereby reducing large volume of data transmitted by BSNs, store them temporarily, process and transfer the relevant patient's data to a personal server through wireless personal implemented using ZigBee/IEEE 802.15.4. This improves overall bandwidth utilization as well as reducing power consumption.

### 2.2. Second Tier

**Personal Server**
The personal server interfaces the WBAN nodes through a communication protocol using ZigBee. It is implemented on an Intelligent Personal Digital Assistant (IPDA). It holds patient authentication information and is configured with the medical server IP address in order to interface the medical services. It collects physiological vital signals from WBAN, processes them, and prioritizes the transmission of critical data when there is sudden clinical change in the current patient condition and data content for example changes in cardiovascular signals, temperature, oxygen saturation, and forward it to the medical server.

Moreover, the IPDA has the capability to perform the task of analyzing the physiological data intelligently and do a local reasoning to determine user's health status based on data received from MSS and provide feedback through a user-friendly and interactive graphical user interface. 3G communications is used to connect personal server and third tier together but other long range communications protocols can also be used like GPRS, WWAN. IPDA is inactive mode when it has no data to receive from MSS or send to the medical server in order to save energy but wake up immediately from inactive to active mode to receive transmitted data and store it. It prioritizes all the received physiological data and send to the medical server based on the priority order so that the medical staff will be adequately prepared before the patient gets to them or send ambulance immediately to pick the patient so as to save his/her life.

**Table 1:** Physiological signal characteristics

| Physiological Signal | Parameter Range | Data Rate(Kbps) | Data Arrival Time (Sec) |
|---|---|---|---|
| Electrocardiograph (EKG) | 0.5 - 4 mv | 6.0 | 0.002 |
| Blood Flow | 1 - 300 ml/s | 0.48 | 0.025 |
| Respiratory Rate | 2 - 50 breaths/min | 0.24 | 0.05 |
| Oxygen Saturation ($SpO_2$) | 0.01 - 0.85/s | 2.3 | 0.16 |
| Blood Pressure | 10 - 400 mmHg | 1.2 | 0.01 |
| Blood PH | 6.8 - 7.8 PH units | 0.048 | 0.25 |
| Never Potentials | 0.01 - 3 mv | 240 | 5E-05 |
| Body Temperature | 32 - 40° | 0.0024 | 5 |

### 2.3 Third Tier

The third tier is called Medical Server for Healthcare Monitoring (MSHM). It receives data from the personal server, is the backbone of the entire architecture. It is situated at medical centers where medical services are provided. It is intelligent because it is capable of learning patient specific thresholds and learns from previous treatment records of a patient [6]. MSHM keeps electronic medical records (EMRs) of registered patients, which are accessible by different medical staff, including general practitioners, specialists and doctors from their offices in the hospital over the internet. The present state of the patient can be observed by the medical staff. MSHM is responsible for user authentication, accepting data from personal server, format and insert the received data into corresponding EMRs, analyze the data patterns.

The patient's physician can access the data and its patterns from his/her office via the intranet/internet and examine it to ensure the patient is within expected health metrics. If the received data is out of range (i.e. deviation from threshold) or recognize serious health anomalies condition, medical staff in the emergency unit can be notified to take necessary actions.

However, if the patient is in the remote area, the specialist doctor will observe the physiological data of the patient diagnose it, prescribe the necessary treatment and drugs for the patient. This information will sent back to the doctor in the remote hospital via the internet. The MSHM also provides feedback instructions to the patient, such as physician's prescribed exercises.

## 3. Methods

Internet of Things can be defined as: —A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data." Following are the various methods used to implement in health care monitoring systems.

### 3.1 OWASP

The OWASP[7] [8](Open Web Application Security Project) is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing Internet of Things technologies.

### 3.2 IEEE 802.15.4

IEEE 802.15.4 [9] is a standard created and maintained by consultants which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs). It is maintained by the IEEE 802.15 working group, which has defined it in 2003. It is the basis for the ZigBee, ISA100.11a, Wireless HART [10], MiWi etc .Alternatively, it can be used with 6LoWPAN [11] as Network Adaptation Layer and standard Internet protocols and/or IETF RFCs [12] defining the upper layers with proper granularity to build a wireless embedded Internet.

### 3.3 IPSec

Internet Protocol Security (IPSec) [13] is a protocol suite for secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).Internet Protocol security (IPSec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPSec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at the Application layer. Hence, only IPSec protects all application traffic over an IP network. Applications can be automatically secured by IPSec at the IP layer. Cryptographic algorithms defined for use with IPSec include:

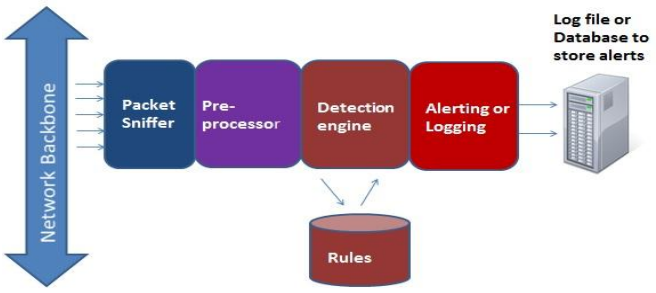
- HMAC-SHA1/SHA2/SHA3 for integrity protection and authenticity.
- for confidentiality ECC encryption algorithm

### 3.4 DTLS

It provides communications security for datagram protocols. DTLS allows datagram-based applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the stream-oriented Transport Layer Security (TLS) protocol and is intended to provide similar security guarantees. The DTLS [14] protocol datagram preserves the semantics of the underlying transport — the application does not suffer from the delays associated with stream protocols, but has to deal with packet reordering, loss of datagram and data larger than the size of a datagram network packet.

### 3.5 SNORT

Snort [15] is an open source network intrusion prevention and detection system. It uses a rule-based language combining signature, protocol and anomaly inspection methods. A network intrusion detection system (NIDS) tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic.




A Snort-based IDS consists of the following major components:

**1.** Packet Decoder **2**.Preprocessors 3.Detection Engine **4.**Logging and Alerting System **5.**Output Modules. Any data packet coming from the Internet enters the packet decoder. On its way towards the output modules, it is either dropped, logged or an alert is generated.

**Packet Decoder**: It takes packets from different types of network interfaces and prepares the packets to be preprocessed or to be sent to the detection engine.

**Preprocessors**: These are components or plug-ins that can be used with Snort to arrange or modify data packets before the detection engine does some operation to find out if the packet is being used by an intruder. Hackers use different techniques to fool an IDS in different ways.

**Detection Engine**: It is the most important part of Snort. Its responsibility is to detect if any intrusion activity exists in a packet. The detection engine employs Snort rules for this purpose. The rules are read into internal data structures or chains where they are matched against all packets. If a packet matches any rule, appropriate action is taken; otherwise the packet is dropped.

**Logging and Alerting System**: Depending upon what the detection engine finds inside a packet, the packet may be used to log the activity or generate an alert. Logs are kept in simple text files, tcpdump-style files or some other form

**Output Modules**: Output modules or plug-ins can do different operations depending on how you want to save output generated by the logging and alerting system of Snort. Basically these modules control the type of output generated by the logging and alerting system. Depending on the configuration, output modules can do things like the following:

1) Simply logging to /var/log/snort/alerts file or some other file 2) Sending SNMP traps 3)Sending messages to syslog facility 4) Logging to a database like MySQL or Oracle 5)Generating eXtensible Markup Language (XML) output 6)Modifying configuration on routers and firewalls.

### 3.6 ECC

Elliptical curve cryptography (ECC)[16] is a public key encryption technique based on *elliptic curve theory* that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the

properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA [17], and Diffie-Hellman [18]. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products. RSA has been developing its own version of ECC.

### 3.7 SHA-3

SHA-3[9] is a family of sponge functions characterized by two parameters, the bit rate r and capacity c. The sum, r + c determine the width of the SHA-3 function permutation used in the sponge construction and is restricted to a maximum value of 1600. Selection of r and c depends on the desired hash output value.

**Algorithm Steps:**

1) Initialization: Initialize state matrix as all zeroes.
2) Absorbing: Each r-bit wide block of the message is XORed with the current matrix state.
3) Squeezing: The state matrix is simply truncated to the desired length of hash output.

**Algorithm Implementation:**

*Theta (θ) Step: (0 ≤x,y≤ 4)*

C[x] = A[x,0]⊕A[x,1]⊕A[x,2]⊕A[x,3]⊕A[x,4]; (1)
D[x] = C[x–1]⊕ROT(C[x+1],1) ; (2)
A[x, y] = A[x, y]⊕D[x]; (3)

*Rho (ρ) and Pi (π) Step: (0 ≤x,y≤ 4)*

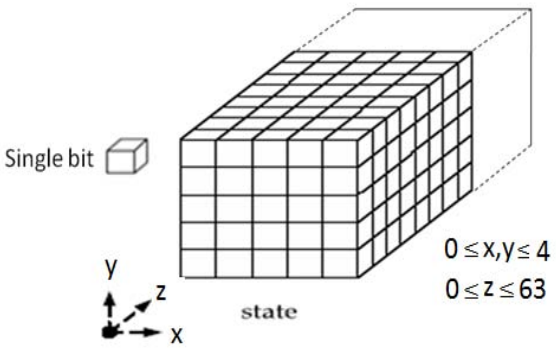
B [y, 2x+3y] =ROT (A[x,y], r[x, y]); (4)
Where r [x, y] is the Cyclic Shift Offset

*Chi (χ) Step:(0 ≤x, y≤ 4)*

A[x, y] =B[x,y]⊕((*NOTB[x+1,y])ANDB[x+2,y]); (5)*

*Iota (i):*

A[0, 0] =A[0, 0]⊕RC ; (6)
Where RC is the Round Constant




**State Matrix (A) of SHA-3**

## 4. ECC Implementation

An elliptic curve is given by an equation in the form of:

$$y^2 = x^3 + ax + b$$

Where $4a^3 + 27b^2 \neq 0$
Many interesting problems arise from the set of points on elliptic curves over a finite field under group operations. The finite fields that are commonly used are those over primes ($F_p$) and binary fields ($F_2^n$). The security of ECC is based on the elliptic curve discrete logarithm problem (ECDLP). This problem is defined as:

Given points X, Y on the elliptic curve, find $z$ such that:

$$X = zY$$

The discrete logarithm problem over this group in a finite field is a good one-way function because there are currently no known polynomial time attacks for solving the problem [18]. The methods for computing the solutions to the ECDPL are much less efficient than that of factoring, so ECC can provide the same security as RSA with smaller key lengths.

ECC was developed independently by Neal Koblitz and Victor Miller in 1985.

### 4.1 ECC Key Generation

To generate a public and private key pair for use in ECC communications, an entity would perform the following steps:

1) Find an elliptic curve $E(K)$, where $K$ is a finite field such as $F_p$ or $F_2^n$, and a find point $Q$ on $E(K)$. $n$ is the order of $Q$. Recommended domain parameters for $E(K)$ are suggested in [19].
2) Select a pseudo random number $x$ such that $1 \leq x \leq (n - 1)$.
3) Compute point $P = xQ$.
4) Your ECC key pair is $(P, x)$, where $P$ is your public key, and $x$ is your private key.

### 4.2 ECC Digital Signatures (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is defined in FIPS 186-2 [20] as a standard for government digital signatures, and described in ANSI X9.62. ECDSA was first proposed by Scott Vanstone [21] in 1992.

#### 4.2.1 ECDSA Signature Generation

To create a signature $S$ for a message $m$, using ECC key pair $(P, x)$ over $E(K)$, an entity performs the following steps [22]:

1. Generate a random number $k$ such that $1 \leq k \leq (n - 1)$.
2. Compute point $kQ = (x_1, y_1)$.
3. Compute $r = x_1 \pmod n$. If $r = 0$, go to step 1.
4. Compute $k^{-1} \pmod n$.
5. Compute SHA-3($m$), and convert this to an integer $e$.
6. Compute $s = k^{-1}(e + xr) \pmod n$. If $s = 0$, go to step 1.
7. The signature for message $m$ is $S = (r, s)$.

#### 4.2.2 ECDSA Signature Verification

To verify a signature $S = (r, s)$ for message $m$ over a curve $E(K)$ using the author's public key $P$, an entity performs following [22]:

1. Verify $r$ and $s$ are integers over the interval [1, $n$ - 1].
2. Compute SHA-3($m$) and convert this to an integer $e$.
3. Compute $w = s^{-1} \pmod{n}$.
4. Compute $u_1 = ew \pmod{n}$ and $u_2 = rw \pmod{n}$.
5. Compute $X = u_1Q + u_2P$
6. If $X = \dot{O}$, reject $S$. Otherwise, compute $v = x_1 \pmod{n}$.
7. Accept if and only if $v = r$.

## 5. Run Time Comparisions

Skill Estimation refers to the estimation of the skills of the students so that the learning environment can be adjusted to suit the student's skills. Skills were calculated based on the interaction of the student with the system or in the message boards or discussion forums. Here is a summary of assessment methods described in Brown's, ―Assessment: A Guide for Lecturers" (2001), a useful starting point to consider the variety of assessment possible:

| | |
|---|---|
| Cases and open problems | An intensive analysis of a specific example |
| Computer-based assessment | The use of computers to support assessments. |
| Essays | Written work in which students try out ideas and arguments supported by evidence. |
| Learning logs/ diaries | Wide variety of formats ranging from an unstructured account of each day to a structured form based on tasks. |
| Mini-practicals | A series off short practical examinations undertaken under timed conditions. Assessment of practical skills in an authentic setting. |
| Self-assessed questions based on open learning(distance learning materials and computer-based approaches) | Strictly speaking, a method of learning not of assessment. A process by which an assessment instrument is self-administered for the specific purpose of providing performance feedback, diagnosis and prescription recommendations rather than a pass/fail decision. |

## 6. Literature Survey

The paper examines various factors like technological, educational and political factors that drive learning analytics such as Big data, Online learning, political and economic concerns. Whereas educational data mining [9] focuses on how to extract useful data from a large learning dataset, learning analytics focuses on optimizing opportunities in online learning environment. Wolfgang Greller et. al. [10] propose a generic framework for Learning Analytics that considers six critical dimensions, namely, Objectives, Data, Instruments, Internal Limitations, External Constraints and Stakeholders. The paper also touches upon the ethical perspective of learning analytics to protect the learners. Erik Duval [11] discusses capturing of the attention data in learning environment in a number of ways such as posts, comments and messages. Data Infrastructure module makes use of Hadoop framework for distributed computation, distributed data storage and Data Broker service. Alyssa Friend Wise et. al. [12] investigates on how students contribute and reciprocate to International Journal of Computer Trends and Technology (IJCTT) – Volume 18 Number 6 – Dec 2014 ISSN: 2231-2803 http://www.ijcttjournal.org Page 261 messages in online discussions in learning environment. A valuable outcome of the findings was the invisible activity validation. Eg: ability to capture listening data such as people who were engaged intensely in discussions but did not post many comments and also the voracious speakers who had a need to improve on their listening efforts.

## 7. Conclusion

The proposed paper describes the usage of learning analytics[13] is very limited to Higher education institutions in India. In many cases, Higher education institutions in India are not aware of the courses needed by the students. Knowledge from the data mining should be brought out to higher education institutions so that courses could be structured based on the need. The literature review shows that the various research activities are concerned mainly on students after joining into a particular course. This proves to be detrimental if the student has not selected a course properly. Education is the basic need for the developing countries like India.

To increase the number of students continuing higher education, the future research work is towards the design of a system for students to choose courses in the Indian universities using Learning Analytics. An efficient course advisory system can enhance the student performance. Such course advisory system minimizes the drop outs in higher education due to improper course selection. Various Big Data techniques become more and more necessary in learning environments to increase the quality and performance of the students.

## References

[1] http://www.openolat.com
[2] WAGMOB ―Big Data and Hadoop ―, Kindle Edition.
[3] Karl Seguin ―The Little MongoDB Book"
[4] Tom White ―The Definitive Guide"
[5] Venables & Smith "A Beginner´s Guide to R by An introduction to R"
[6] Donald Miller and Adam Shook ―Map Reduce Design Patterns"
[7] Josh Diakun,Paul R Johnson" Splunk Operational Intelligence Cookbook",Kindle Edition
[8] https://en.wikipedia.org/wiki/IcCube
[9] Alejandro Peña-Ayala, ―Educational data mining: A survey and a data mining-based analysis of recent works", Expert systems with applications, Vol. 41, No. 4, pp. 1432-1462, 2014.
[10] Wolfgang Greller, Hendrik Drachsle., Translating Learning into Numbers: A Generic Framework for Learning Analytics, Educational Technology & Society, Volume 3, Issue 5, pp 42-57, ISSN: 1436-4522.
[11] Erik Duval, Attention please! Learning analytics for visualization and recommendation, 1st International

Conference on Learning Analytics and Knowledge, 2011, pp 9-17, DOI: 10.1145/2090116.2090118.

[12] Alyssa Friend Wise, Yuting Zhao, Simone Nicole Hausknecht, Learning analytics for online discussions: a pedagogical model for intervention with embedded and extracted analytics, Third International Conference on Learning Analytics and Knowledge, 2013, pp 48-56, DOI: 10.1145/2460296.2460308