International Journal of Current Engineering and Technology

Research Article

Internet of Things: A Comprehensive Analysis and Security Implementation through Elliptic Curve Cryptography

Hemant Kumar†* and Archana Singh†

†Department of Computer Science and Engineering, SHIATS Deemed University, Allahabad-211007, India

Accepted 15 March 2016, Available online 23 March 2016, **Vol.6, No.2 (April 2016)**

Abstract

In this paper many technical terms about internet of things (IoT) have been discussed. Basically this paper deals with the concept of interconnection among billions of electronic devices through internet. As we know that internet is a network among different computer through worldwide. But, we can't see IoT only in terms of communication of electronic devices but also a way by which we can improve the ideology of human being. This paper consists of four sections A, B, C and D respectively. Section A discusses about evolution of IoT, visionary approach of IoT, environmental considerations. While section B discusses about elements of IoT (WSN, RFID, and WLAN), IPv6 and some security concerns. Similarly Section C discusses about DIKW chain regarding IoT, implementation of IoT via WSN and some application of IoT. And Section D is fully dedicated to the security point of view of IoT. In this section we recommend the use of Elliptic Curve Cryptographic technique for security of communicating objects. Finally, this paper concludes with an opinion that how IoT will change the way of communication and how can we secure our IoT Infrastructure.

Keywords: *WSN, RFID, NFC, IPv6, IoT. ECC, ECDLP, Scalar Multiplication.*

1. Introduction

Whenever we hear about the term smart in modern IT system it seems to be very complex mean. Basically here the term smart refers to all those things which can be connected by any mean. The world is going to be connected day by day, all from natural to artificial object are getting connected and this connection between all these things produces a meaningful information or pattern for any specific task. Here, Internet of Thing (IoT) is also specific term, this term originating in 1999. IoT is a revolutionary concept in latest communication scenario. In the IoT there are so many devices connected either wired or wireless medium and communication between these devices or object takes place for enhanced & proper information.
With IoT, there are also some technical terms has been associated which are wireless sensor network, ubiquitous computing, mobile communication and cyber physical system. All these term has a specific role in deployment of the concept of Internet of Thing. In IoT scenario, there are lot of physical objects of our day to day life which can be well equipped with some electronic components like microchips, transceivers, digital communication and a proper communication protocol medium.

*Corresponding author **Hemant Kumar** is a M.Tech Scholar and **Archana Singh** is working as Assistant Professor

2. Section A

2.1 IoT Evolution

We can assume that the IoT evolution taken place from the idea of internet. Basically this internet facility is extremely responsible for the growth of the concept of IoT. whenever we think about IoT, there is a picture originates that so many physical objects are interconnected and produces some information after analyzing, actuating and sensing the things.

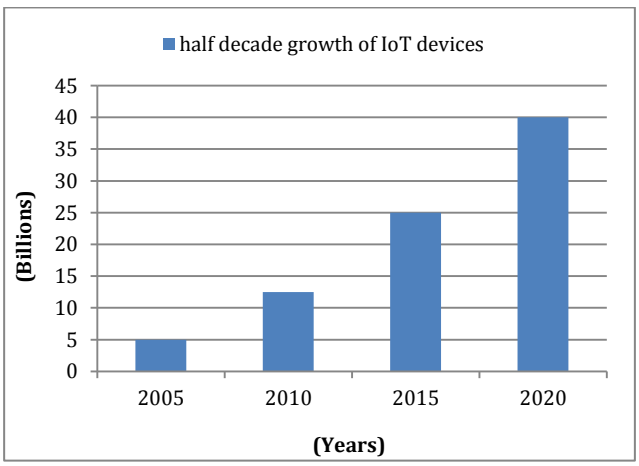

Fig.1 Typical growth of IoT

Currently IoT is expecting 40 to 50 billion devices will be connected with each other or with internet by the end of the 2020. In present the number of IoT devices has been more than the world population and this figures approximately 10 billion devices or electronic equipment which can be connected by any mean. The IoT makes an intelligent, optimistic and identifiable network canvas over the internet for reaching a point where thing are easily accessible.

We try to show the expected IoT devices that can be used worldwide and the increase of these devices is in the form of half decade basis. In the graph below the numbers are in billions of devices.

2.2 Visionary Approach of IoT

It is clear that IoT vision has a remarkable impact to the world. We can see vision of IoT in two references. In which first is network centric and second is object centric. Both of these has their own architecture system. While we think about object architecture, smart object are allocated to smart network infrastructure and when we talk about network then it is nothing but a huge amount of uniquickly identifiable address provided to the things or objects. In current scenario telecom industry is playing a vital role in order to full deployment of IoT. We can assume that telecommunication system is also a type of IoT. Now the question arises in what manner. So here is an answer, as we know that large number of telecom operator deployed the telecom antennas and towers having coordination with each other in order to provide proper communication network. So telecom towers may be a object and can be connected to different networks.

2.3 Environmental Impact of IoT

In order to evaluate pros and cons of IoT to the environment or ecological system, we have to notice about the rapid growth of production of electronic components or parts which are used in deploying IoT paradigm, It may be possible that these parts after sometimes will be debarred or waste then this waste will be dumped to landfills and causes soil health concerns and misbalanced of ecosystem of that particular area. And on the other side for making of such types of electronic parts some special type of rare earth material is needed for that earth mining takes place and reflects some cause of concerns .Now if we see positive impact of IoT to the environment then we can say that IoT plays an important role for weather forecasting, provide good mechanism to protect national coastal areas from flood and other threats by actuating, sensing the activity near about things. After deployment of IoT facility, we can protect our national parks, monitoring of air pollution level, monitoring of sea level. Therefore we can see lots of issues are there regarding IoT which needs to be solved out.

3. Section B

3.1 IoT Elements

IoT elements refer to all those technology which has been a integral part of IoT deployment. RFID, NFC and WLAN are the three basic technologies which has used in IoT infrastructure. In RFID (Radio Frequency Identification) is generally used to find things from a certain distance or a few meters, this technology used with a stationary object or device, firstly it will identify the object and then communicate with that object. Later on NFC has come into picture in early 2010,in this technology there is no limitation of few meters communication but two or more object can communicate with near field and this near field may be some long distance. In current scenario in order to full deployment of IOT network. Basically this technology creates a wireless local area network which posses some unique address to identify the intended object for defined communication.

3.2 Transition to IPv6

As we can see that IPv4 is only capable to fulfill the demand of internet of computers because here are limited number of computers holds IP address. But if we see the pattern of internet of thing then this is quite critical because large number of IP address required allocating every object and we can't do this with IPv4 because 32 bit address scheme is not suitable for IoT that is why IPv6 128 bit address scheme introduced for IoT. With this we can generate billions of IP address for fulfilling need of IoT object. While practically deployment of IPv6 is very costly and right now uses where complex computing taking place. With a large extent, we can imagine that without IPv6 there may not be future of IoT. IoT demands unique addressability for their resources. One reason for move to Ipv6 is that this scheme provides end to end encryption for communication, while IPv4 is not capable to provide such type of mechanism.

3.3 Security and Cost Concerns

In the near future lot of people can have variety of devices connected to IoT infrastructure and security of such devices is a great cause of concern because these devices uses small memory and relatively slow processor due to which chances of vulnerabilities is very high . But we can deploy some cryptographic technique specially designed for ECC (Elliptic Curve Cryptography) , with this a powerful mechanism can be used.

On the other hand cost of small IoT devices and infrastructure generally always high. Our focus is now to mitigate the cost of deploying IoT infrastructure. For that we have to optimized the IoT network, it means unused IoT object or devices will be off until there will not be a need to switch on. By doing this we can save

our energy and cost. Sometimes cost may increase because IoT infrastructure have to be established where there is too much geographical problems arises, this may be a cost effecting factor in order to IoT development.

4. Section C

4.1 IoT as a DIKW chain

We all are know that evolution of human being can possible because there was a communication with each other that's why we were able to process ideas and information. Same principle applies here in the IoT. This principle can be understood by monitoring how human processed data. If we see then we shall find that firstly data has been available for human and human processed this data and came to information. Basically this information is not fully processed then human added some raw facts into information and arrived to knowledge, furthermore this knowledge taken the form of wisdom and this is the condition where human could analyze their surroundings. This wisdom came from knowledge and some experience. Now we can say that if more data available then we will have more information. Similarly IoT unexpectedly increase the available data for us to process. This increase the capability of internet to available processed and systematic information for everyone.

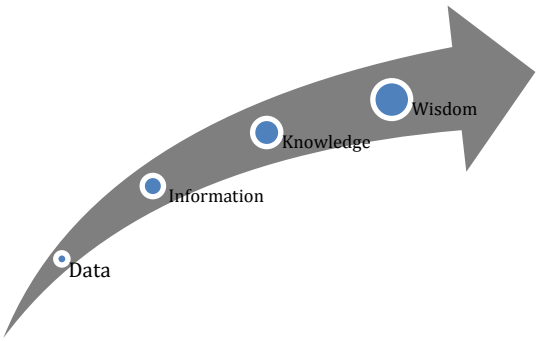

Fig.2 Implement DIKW chain in IoT

4.2 Architectural Constraint of IoT

IoT consists so many constraints for rapid establishment of IoT network. Some of them here we are discussing like –

4.2.1 *Actuator*

An actuator is a device for operating a process or system. It converts their obtained energy by air or electric current into physical movement.

4.2.2 Application Software

It provides services to the intended nodes in the IoT network, this software is specific in nature for what it is developed.

4.2.3 Controller

This may be a software or hardware system that can control the particular node or whole IoT network.

4.2.4 Gateway

A gateway in the IoT network provides a routing facility for propagation of information to the next node.

4.2.5 Interface

Predefined set of instructions that interact with the user and IoT object.

4.2.6 Internet

This is a globally managed interconnected computer network that implements communication among billion of computer users.

4.3 Application Areas of IoT

Today concept of IoT implementing in so many areas of human life like manufacturing, environmental monitoring, geographical condition checking, weather forecasting, soil testing, coastal areas monitoring etc. So these all are areas where IoT is using. But apart from these applications of IoT, in near future this is predicting that a web of IoT objects will be created around the world in which critical information will be propagated. Due to IoT we shall have available correct data by the correct time and we would take decision on time so that we can face any natural calamity. Thus we shall obtain comprehensive information for the better of human being.

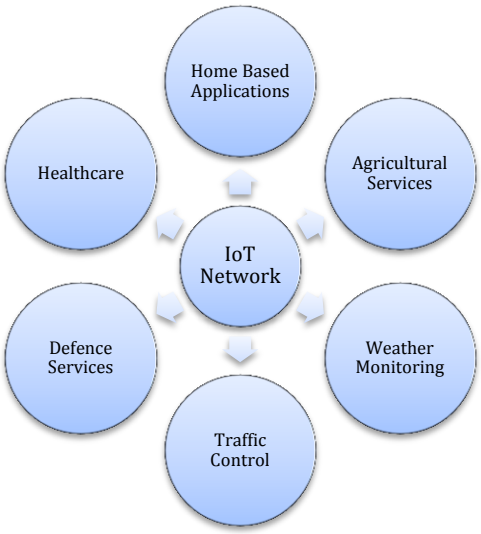

Fig.3 IoT Sectors

5. Section D

Security Implementation through Elliptic Curve Cryptography (ECC) in IoT

Elliptic curve cryptography were discovered by Neal Koblitz and Victor Miller in 1985. ECC is the most

efficient public key encryption method based on the concept of elliptic curve which is used for enhanced cryptographic key. Generally, ECC is used to compare with the public key encryption methods like RSA and diffie-hellman key exchange problem. ECC helps to provide greatest security with low power computing devices.

Some public key encryption methods like RSA, D-H key exchange and Digital Signature Algorithm (DSA) are very suitable for high power computation but when we go for IoT or cloud computing then there is a possibility that low power computing devices will not support such types of devices.

Table 1 Comparison Among different algorithm

Algorithm	Key Exchange	Encryption/Decryption	Digital signature
DSS	No	No	Yes
Diffie-Hellmen	yes	Yes	No
RSA	yes	Yes	Yes
ECC	yes	Yes	Yes

5.1 Fundamentals of ECC

ECC works on the concept of elliptic curve, an elliptic curve is a group of finite field and ECC uses this group for its working. The beauty of this technique is the use of elliptic curve and Elliptic Curve Discrete Logarithmic Problem (ECDLP) is one of the major algorithms of this technique that is when an elliptic curve E and points P & Q on E are given find k when Q=k.P

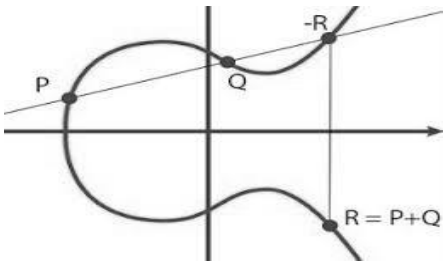

Fig.4 A Simple Elliptic Curve Example

As stated earlier that RSA uses large number size for its key, while ECC takes very small key size that is why here we focus on ECC. Now if we want greatest level of security then we have to use more efficient method which contains small key size. The newly added cryptographic system will ensure the equal or higher level of security.

An elliptic curve 'E' is a curve given by an equation for a cubic or quadratic polynomials f(x).

E: $y2 = f(x)$

For ensuring that the curve is non singular, f(x) has no double roots

Let E: y2=x3+ax+b

5.2 Point Doubling

Now if we have a point P_1 on any elliptic curve and we want to find P_2 such that ($P_2=2P_1$) then this called as point doubling.

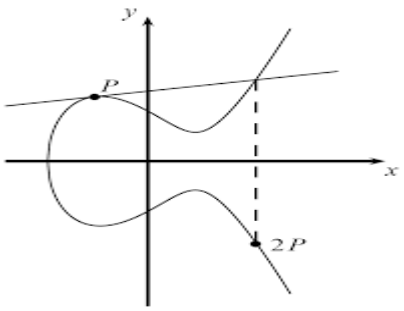

Fig.5 Point doubling in elliptic curve

5.3 Point Addition

Similarly, If we have two points P_1 and P_2 on any elliptic curve and we want to find P_3 on same curve in such a way that $P_3=P_1+P_2$ then this is called as point addition.

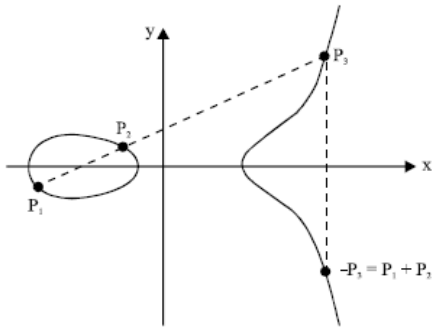

Fig.6 Point addition in elliptic curve

5.4 Elliptic Curve Discrete Logarithmic Problem

ECC contains elliptic curve defined over a finite field, these field of interest are prime field GF (P) and binary finite field GF ($2m$).

- A point P of higher order, present on elliptic curve (E)
- A scalar multiple of P, let it be k such that
  k.P =P+P+_ _ _ +P (k times)

So ECDLP involves scalar multiplication, now when we have k & P then we can easily compute k.P, while when we have to find k for given values of P & k.P then it is quite time consuming.

5.4.1 Scalar Multiplication

Now ECDLP also uses scalar multiplication so there is need to understand the concept of scalar multiplication in this scenario

In scalar multiplication there is a scalar multiple (k) which we multiply with the point P. Basically this

number is act as secret key for both sender and receiver of the message.

Now this is necessary to understand that ECC contain point addition and point doubling based on the value of k, this algorithm for scalar multiplication can be drawn as

Input: Point P element (x,y,z)
Output: k.P

1) Scan value of k from (MSB to LSB)
2) If MSB=0 then do point double on data points
3) Else if MSB=0 then do point addition+ point double on data points

5.5 Why we focused on ECC in IoT

5.5.1 Nature of Complexity

ECC uses scalar multiplication instead of multiplication or exponentiation in finite field. Solving Q=k.P is more difficult than solving factorization (used by RSA).Therefore ECC is much stronger and complex than any other cryptographic standard.

5.5.2 Use of Lower Key Size

Due to ECDLP, ECC needs very less number of bits for their public key encryption operation that is why level of security is same when 160 bit for ECC and 1024 bit for RSA is supplied.

5.5.3 Computing Efficiency

As we know that ECC uses scalar multiplication so it is much more computationally efficient than RSA and Diffie-Hellmen key exchange public key cryptography.

5.6 Findings

As we can see that the world of IoT is expanding day by day then it is quite obvious that the computing devices will also be increase. So there is a question arises of security of such types of devices from unauthenticated users or any intruders.

Right now, the world is relying on RSA public key cryptographic system in order to security point of view, but this will not go by the long time because of small computing objects will no longer efficient to handle large key size of public key algorithm like RSA.

Table 2 Comparable key sizes of ECC & RSA/DSA key exchange recommended by NIST.

ECC Key Size	RSA/DSA Key Exchange	Key Size Ratio (ECC/RSA)
106	512	1:5
132	768	1:6
163	1024	1:7
192	1536	1:8
210	2043	1:10
256	3024	1:12
384	7680	1:20

From the above table it is clear that the ECC method always uses lower key sizes for its functioning while algorithm like RSA or DSA uses large key sizes.

Therefore, we are recommending that in future we should have to adopt algorithm like ECC in small computing devices for IoT.

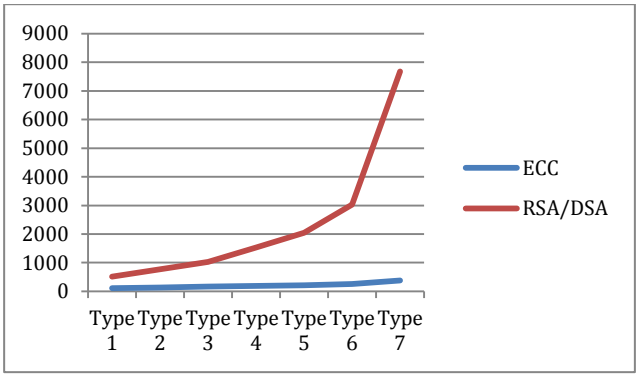

Fig.7 Growth of key sizes of ECC & RSA/DSA algorithm

Summary and Conclusion

The growth of the next era mobile communication will depend on the application capability for their end users. IoT is an intelligent growing technology that will work beyond its domain. As we can see that internet has changed the lifestyle of human being.

- Now we can say that IoT is a complex phenomenon which holds the interest of different entities for their specific domain. These entities may be any enterprise, company or any single end user of the system. Finally we can see that IoT has transformed the human from data to wisdom.
- As for as security of IoT is concern then we are recommending that Elliptic Curve Cryptography(ECC) encryption technique should be use in IoT network because of key advantages described in this paper.
- ECC offers the highest security on per key bit of any known public key method like RSA, Diffie-Hellmen. This offers the same level of security with small key size.
- Finally, its use in the IoT will makes a remarkable impact in order to security point of view.

References

K. Ashton, that "Internet of Things" thing, RFID Journal (2009).
H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realizing the Internet of Things, Cluster of European Research Projects on the Internet of Things —CERPIoT,2010.
J. Buckley (Ed.), the Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Auerbach Publications, New York, 2006.
M. Weiser, R. Gold, The origins of ubiquitous computing research at PARC in thelate1980s, IBM Systems Journal (1999).
Xue Sun, Mingping Xia "An improved proxy signature based on elliptic curve cryptography" DoI10.1109/ICCCS.2009.36.
F.Amin, A.H.Jahngir and H.rasifard "Analysis of Public-key cryptography for wireless sensor network security" World Academy of Science, Engineering and Technology41 2008.
Jamil, Danish.Zaki, Hassan. "Cloud Computing Security". In International Journal of Engineering Science and Technology.Vol.3 No.4April2011.
www.certicom.com.
William Stallings 'cryptography and network security principles and practices' fifth edition, Pearson, 2011.
N.Koblitz, Elliptic curve cryptosystem, mathematics of computation,vol. 48, pp.203-209,1987