# Design of FPGA based Cyber Secured Encoder for IoT

**M. Sri Venkat Rami Reddy [1], Dr. D. Nageswara Rao [2], Venkata Krishna Bandi [3]**
[1] Assistant Professor and 2 Prfessor
1, 2 Department of Electronics and Communication Engineering
[1, 2] TKR College of Engineering and Technology, Hyderabad, India.
[3] Lecturer, Department of Computer Science, Debre Tabor University, Debre Tabor City, Ethiopia.

***Abstract:*** ***In today's scenario of cyber security, deciding secured design is a vital task. Standard design techniques used for securing embedded systems are not suitable for CPS due to the restricted computation and communication budget available. The sensitivity of sensed data and the presence of actuation components further increase the security requirements of CPS. To address these issues, it is necessary to provide new design method in which security is considered from the beginning of the whole design flow and addressed in a holistic way. We focus on the design of secure CPS as part of the complete CPS design process, and provide insights into new requirements on platform-aware design. With the planned implementation of IoT components with in an enterprise we can provide better cyber security. We are going to use a new design approach in IP based cyber secured design of FPGA based encoder with the help of a suite of protocols. The objective of this design is to improve the level of security to the system with the secured design of encoder.***

***Keywords: FPGA (Field Programmable Gate Array), Encoder, Cyber Security, Cyber Physical Systems (CPS), Internet of Things (IoT), IP (Internet Protocol).***

## 1. Introduction

The Internet of Things refers to network of physical objects. The internet of things is a cyber technology which comes third right after Internet and mobile communication network. To enable this new form of communications, we require transceivers compatible with IPv6 address. So, we can assign addresses to every thing on the surface of the earth. We can assign for every encoder and make it IoT enable Encoder as shown in Figure-1. Each object has a feature of internet compatibility. So, communication will be established between these objects and Internet-enabled devices. Figure-1 shows that IoT [1] is a combination of objects, network, data and services.

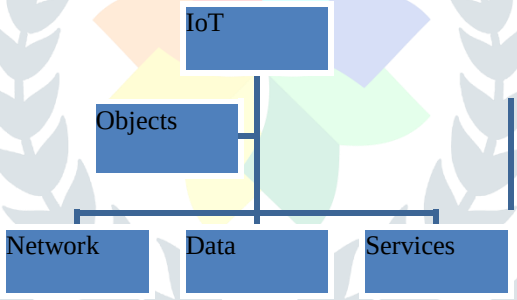


Figure-1: Simple description of Internet of Things enabled Encoder

## 2. Security Structure in the Framework

**2.1. Security Architecture in Perception Layer:** In perception layer of CPS, a closed system composed of sensor network, whose all communication with external networks must depends on the gateway node, the security issues of the sensor network itself is the unique factor to be considered in the design of security architecture.

**2.2. Security Architecture in Network Layer:** In network layer, both the sensory data and controlling commands are time sensitive, and a large number of heterogeneous networks with different performance and defense capability against cyber-attacks[3] make special security protocols aiming at network specificity an urgent demand. Security architecture can be divided into two sub-layers: point- to-point security sub-layer and end-to-end security sub-layer. The point-to-point security sub-layer could ensure the data security during the hop transmission [4]. Its corresponding security mechanisms include: mutual authentication between nodes, hop encryption and across-network certification. The end-to-end security sub-layer could ensure the end-to-end confidentiality and protect the network availability.

**2.3. Security Architecture in Application Layer:** The design of security architecture in application layer must follow the principle of differentiated services [3]. As there is a wide variety of applications of CPS, security requirements are different. Even for the same security service, there may be completely different definition for different users. Therefore, providing targeted security services according to the users' needs is the core idea of the design.

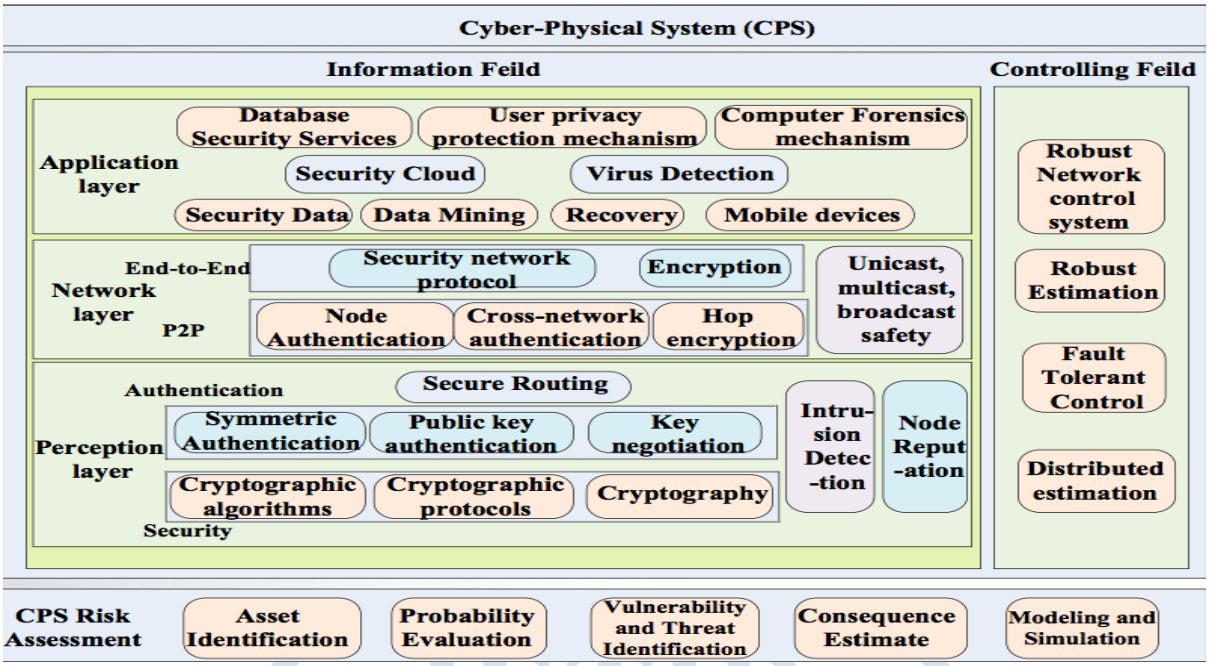


**Figure-2: Security Framework for Cyber Physical Systems**

## 3. Design of FPGA based Encoder for IoT

Security is fundamental for the successful roll-out of the Internet of Things. IP Sec is a set of security protocols which was developed by IETF (Internet Engineering Task Force) in November of 1998. It is an official standard for network security and was de signed for interoperability. The design of the encoder is compatible with both IPv4 and IPv6. IP Sec provides data integrity, basic authentication and encryption services to protect the data from modification and unauthorized usage using Authentication Header (AH), Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) protocols.

Edge nodes are currently the weakest-link in ensuring IoT security[1] and the protection of cryptographic keys locks down the edge nodes. The best way to achieve lock-down is by protected hardware. It is the only way to keep those keys and other secrets away from prying eyes. Encoder can be described as a key element of a device, circuit, system, that converts one form of energy, program, or an algorithm that transforms or translates information from one form to another. To design this encoder RC low-power bus encoding method is used[7].Encoders turn read able information into a cipher format. A decoder reverses the effects of this encoding to make the file readable. As the security is a major concern in internet of things (IoT), the secured transmission of data and images is mandatory to prevent any kind of unauthorized usage. We are making security conscious key management scheme using LV CMOS I/O standards of FPGA[5].

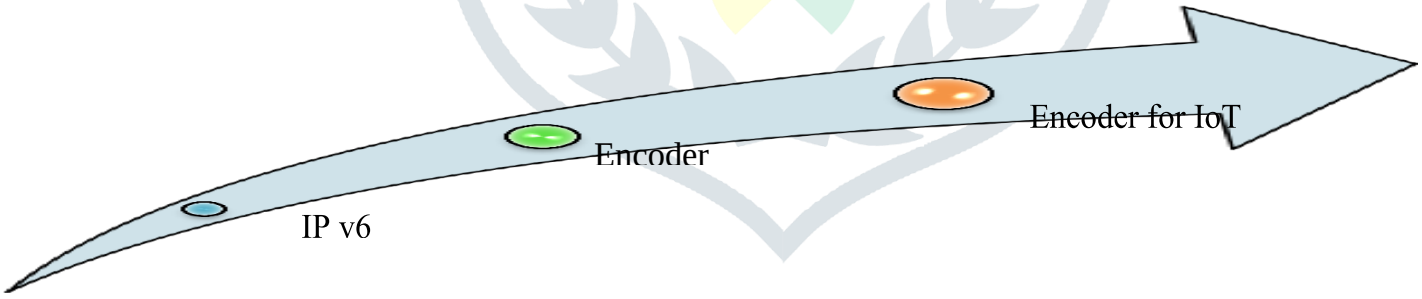


Figure-3: Cyber Secured Encoder for IoT Applications

We have used 16:4 bit encoder for the transmission of a private message to recipient. The message can be encoded by using various methods using algorithms like RSA, AES, DES etc. for strong encryption so that it be comes difficult for the hacker to crack [6].The message is encrypted as shown in theTable-1 below:

| ASCIICODE | PrivateMessage | Encoded Message |
|---|---|---|
| 5468 | Th | 1 |
| 654B | eK | 2 |
| 6579 | Ey | 3 |
| 746F | To | 4 |
| 756E | Un | 5 |
| 6C6F | Lo | 6 |
| 636B | Ck | 7 |

Table-1: Private Message to be Send to the Recipient

We have embedded an IP address (IPv6) in Encoder .This encoder is now network accessible. IP Sec, which provides Confidentiality, Authentication and Integrity, is integrated in IPv6. Because of the virus that is designed to damage the information on computer, IPv4 ICMP packets are frequently blocked by corporate firewalls. But the implementation of the Internet Control Message Protocol for IP v6, may be permitted because IP Sec. can be applied to the ICMP v6 packets. We test that encoder using I/O standard (LV CMOS). LV CMOS is a low voltage (LV) class of CMOS technology integrated circuits temperatures. CMOS is complementary type of MOS. We are operating this IOT compatible cyber secured encoder on various ranges of devices. And, we are analyzing that this is a secured encoder with respect to different LV CMOS I/O standards used in IoT applications as shown in Figure-4.

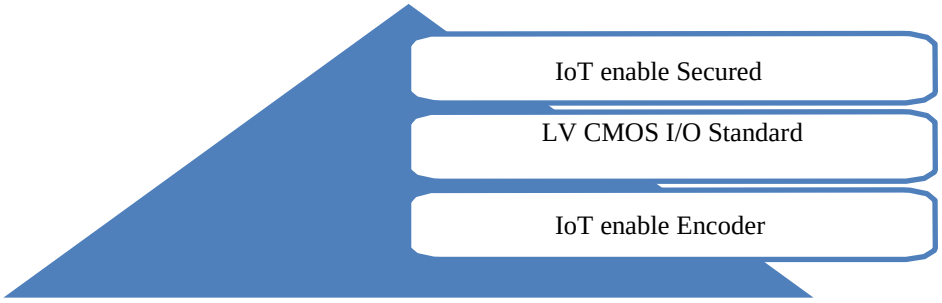


Figure-4: Components Cyber Secured Encoder for IoT

As shown in Figure-4, Encoder has 16-bit data input along with 1-bit enable and 128-bit IPv6 address. It encodes 16-bit input into 4-bit output. This encoder design is a part of real encryption system. When we provide output of this encoder to any decoder, output of decoder will be similar to input of encoder. This design is working based on security principles of authentication[8], integrity, confidentiality and availability. In other words, output of encoder is encrypted text (Encoded Message) where as input of encoder is plain text (Private Message) as per Table-1.

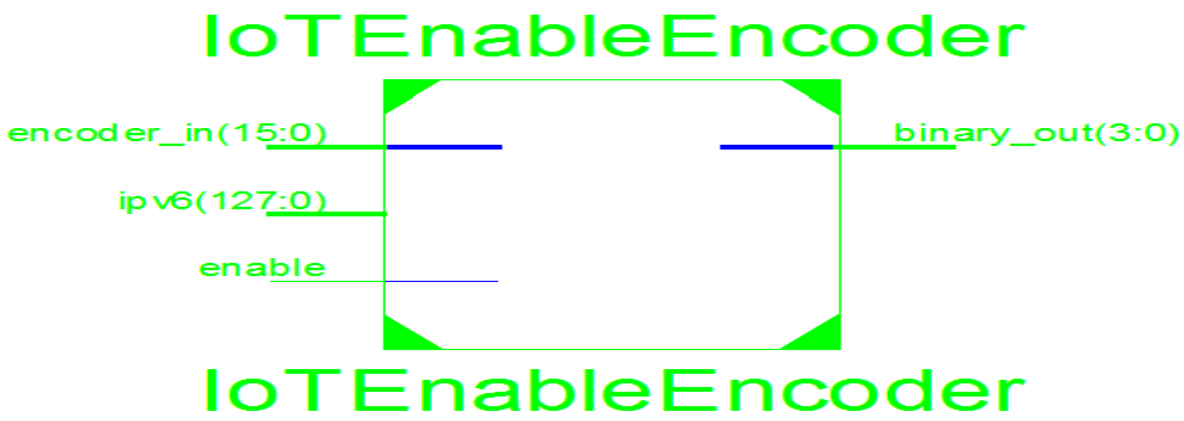


Figure-5: Result of IoT enable Secured Encoder

## 4. Conclusion

In this paper, we have focused on the cyber secured encoder design for securing Cyber-Physical Systems. We have used a simplified secured encoder design for ensuring security in CPS. We have presented a control-aware design to ensure attack-resiliency in CPS. We have addressed the security challenges related to the FPGA based encoder design for IoT.

**References:**

**[1]** Federal Trade Commission. (2015). Internet of Things: Privacy and Security in a Connected World. Retrieved from FTC website:https://www.ftc.gov/system/files/documents/reports/federal-tradecommission-staff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127iotrpt.pdf

**[2]** Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). IEEE Internet Initiative, Torino, Italy.

**[3]** X. Feng and T. Lu, "Security Analysis on Cyber-Physical System Using Attack Tree", The Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing,(2013).

**[4]** Y. Peng and T. Lu, "Cyber-Physical System Risk Assessment", The Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, (2013).

**[5]** K.Kaur,"Internet of Things Enabled Energy Efficient Green Communication on FPGA", IEEE 6th International Conference on Computational Intelligence and Communication Networks (CICN), Udaipur, (2014) November14-16.

**[6]** M.Palesi,"Data encoding schemes in networks on chip", IEEE Trans. Comput.-Aided Design Integration Circuits Syst.,vol.30.

**[7]** C.P.Fan and C.H.Fang, "Efficient RC low-power bus encoding methods for crosstalk reduction", Integration, VLSI J.,vol.44, no.1.

**[8]** X.Huang, "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems", IEEE Transactions on Parallel and Distributed Systems, vol.22, no.8.

**[9]** G.Kortuem,"SmartObjectsasbuildingblocksofInternetofthings",IEEEInternetComputing, IEEE Computer Society,(2010) January-February.

**[10]** J. Yang, C. Zhang, X. Li, Y. Huang, S. Fu, M.F. Acevedo. "Integration of wireless sensor networks in environmental monitoring cyber infrastructure", Wireless Networks, Springer/ACM, Volume 16, Issue 4, pp. 1091- 1108, May 2010

**[11]** Xiaohui Cheng; Fanfan Shen, "Design of the wireless sensor network communication terminal based on embedded Linux," Software Engineering and Service Science (ICSESS), 2011 IEEE 2nd International Conference on, vol., no., pp.598, 601, 15-17 July 2011

**About Authors:**

Mr.M.SriVenkatRamiReddy working as Assistant Professor of ECE in TKR College of Engineering & Technology, Hyderabad. He received the B.Tech. degree in Electronics & Communications Engineering from the J.N.T. University, Hyderabad, India, in the year 2004, and the M.Tech. degree in VLSI System Design from the J.N.T. University, Hyderabad ,India, in the year 2012.

His current research interests include VLSI based Systems Design, IoT (Internet of Things), Cyber Physical Systems(CPS), Network-On-Chip (NoC), System on Chip (SoC), Low Power VLSI. He is a Life Member of the Indian Society for Technical Education (ISTE), New Delhi, India.

Dr.D.Nageswara Rao working as Professor of ECE in TKR College of Engineering & Technology, Hyderabad. He received the B.Tech.degree in Electronics & Communications Engineering from the S.R.T.M.University,Nanded, India, in the year 1999, and the M.Tech.degree in VLSI System Design from theJ.N.T.University, Hyderabad, India, in the year 2004.He received Ph.D in VLSI domain from GITAM University in the year 2014.

His current research interests include VLSI, Image Processing, SOC, Low Power VLSI. He is a Life Member of the Indian Society for Technical Education (ISTE).

Venkata Krishna Bandi is working as Lecturer at Debre Tabor University, Debre Tabor City, Ethiopia. He has received B.Tech Degree in Computer Science from the J.N.T. University, Hyderabad, India, in the year 2005, and M.Tech Degree in Software Engineering. from the J.N.T. University, Hyderabad, India, in the year 2012.

His current research interests include Software Engineering, Cyber Security, Internet of Things (IoT), Cloud Computing and Data Mining.