Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.S1, 2018, pp.104-107
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2018.7.S1.1794

Automated Secured Data Delivery for Next Generation Optical Networks

J. N. V. R. Swarup Kumar[1] and D. Suresh[2]
[1]Research Scholar, [2]Assistant Professor
[1&2]Department of Information Technology, Annamalai University, Tamil Nadu, India
E-Mail: swarupjnvr@gecgudlavalleru.ac.in, deiveekasuresh@gmail.com

(Received 4 October 2018; Revised 18 October 2018; Accepted 1 November 2018; Available online 9 November 2018)

***Abstract* - The present cloud benefit measurements truly are stunning. By one year from now 80% of all new programming will be accessible as a cloud benefit, 58% of all Internet activity is guage to be video in only two years and before the decade's over, 20 billion brilliant gadgets will be associated with the system. There is no uncertainty this will make difficulties wherever in the system. However, with this test, there regularly comes chance to go into the new optical system; never again is it only an asset for transporting bits. What's more, it's more than expanding limit. What's new is the requirement for specialist organizations' optical systems to end up increasingly "coordinated" and "consumable" enabling them to understand the undiscovered capability of their system. It ought to be a basic element of the developing cloud framework associating clients to their substance and applications. Security is a basic necessity for the system in light of the fact that the touchy data can be gotten to remotely and this makes the whole framework helpless against pernicious assaults. This paper exhibits the AES-256 calculation with respect to FPGA and the Very High Speed Integrated Circuit Hardware Description language (VHDL) for a secured information transmission in the Agile Optical Networks (AON).**

***Keywords:* Data, Optical Networks, Communication Systems**

I. INTRODUCTION

PC correspondence began with copper wire as the medium for conveying electrical signals encoding the information to be imparted starting with one PC then onto the next. Copper as a medium of correspondence has various constraints and, over the most recent three decades, colossal advancement has been made in utilizing alternative media for correspondence. Optical filaments have largely replaced copper wire correspondences in center systems in the advanced world. An optical system interfaces PCs (or whatever other gadget which can produce or store information in electronic shape) utilizing optical fibers. To provide information correspondence, an optical system additionally incorporates other optical gadgets to create optical (electrical) signals from electrical (respectively optical) information, to reestablish optical flags after it spread through fibers, and to course optical flags through the system. Optical systems have discovered across the board utilize on the grounds that the transmission capacity of such systems utilizing current innovation is 50 tera-bits every second. Optical systems just supplanted copper wires with optical fibers. At present a larger part of PC and telecommunication frameworks requires information security when information is transmitted over system. Subsequently information encryption is performed to secure intrusion sensible information. Generally proper software algorithm is utilized for coding information at sender site and interpret at receiver one. Such an answer isn't sufficient and too moderate then fast handling is important because of high transmission medium data transfer capacity and constant prerequisites. In such circumstance increment of computational stage processor execution is essential, however utilization of quicker broadly useful processor is not productive. That is the reason equipment increasing speed of cryptographic algorithms is necessary. The simple great arrangement of decision for such dedicated hardware is reconfigurable devices. For whole number based information this innovation ensures better execution and lower power request. Furthermore due to the recognized distinguished features of hardware solution it also provides better information security against cracker's attack.

II. FIBER-OPTIC COMMUNICATIONS SYSTEM

The wellspring of fiber optics started from the optical semaphore broadcast to the advancement of the principal clad glass fiber imagined by Abraham Van Heel. Today more than 80 percent of the world's long-separate voice and data movement is proceeded over optical-fiber joins. Broadcast communications employments of fiber-optic connections are sweeping, reaching out from worldwide systems to PCs. There are diverse multi-mode and single-mode fiber composes starting at now used for preface, metro, airborne, submarine, and whole deal applications. Removable and reusable optical end as metal and plastic connectors assumes an essential job in an optical structure.

TABLE I OPTICAL FIBER LINK

	Wavelength	Attenuation	Maximum bandwidth for Communication	Repeater distance
First generation	850 nm	20 dB/km reduced to 5 dB/km	2-45 Mb/s	8-10 km
Second generation	1310 nm	0.5 dB/km	140 Mb/s	25 km
Third generation	1550 nm	0.25 dB/km	1-2.5 Gb/s	50-100 km
Fourth generation	1550 nm	0.15 dB/km	10 Gb/s to 1 Tb/s	100-500 km

III. AGILE OPTICAL NETWORK

With the end goal to understand this issue, communication systems need to give greater capacity that turned out to be more dynamic when initiating new services and should be more adaptable as far as design and configuration. The standard pattern of offering real-time applications dependent on a virtualized IT framework –, for example, server and storage – clearly affects the basic system infrastructure and its topology. Systems must be planned and manufactured distinctively with the end goal to give availability all the more progressively and to more readily use assets accessible in the system. Association ways must be streamlined and shortened to abstain from squandering of resources and lessen latency.

This is for what reason we're presenting Agile Optical Networking (AON) and it's changing the tenets of the game for service providers. AON is the term used to characterize the confluence of technologies that meet up to empower flexible, versatile, scalable, reliable and effective optical transport organizing at 100G for each wavelength and beyond. AON uniquely unites packet, electrical and photonic switching advancements across the board adaptable and efficient arrangement. It has the worked in flexibility and dynamism to wind up more promptly consumable and responsive in a genuine cloud environment. So service providers' optical transport systems can be a vital component of cloud systems.

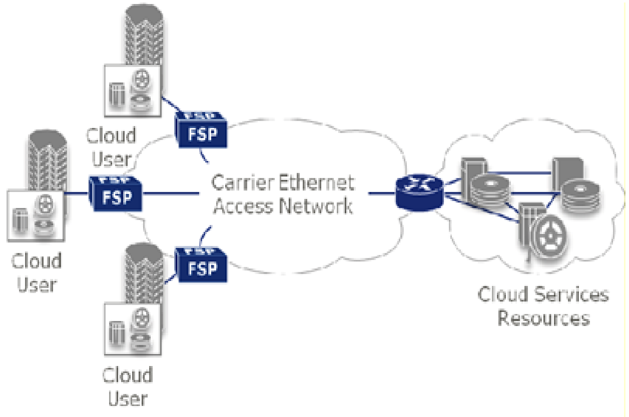

Fig. 1 Intelligent Ethernet demarcation for Cloud Computing access networks

IV. AES: SIGNIFICANCE OF HARDWARE IMPLEMENTATION

Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an affirmed cryptographic algorithm that can be utilized to secure electronic information. AES is compatible for any application that requires solid encryption technology. Typical applications may incorporate secure communications, program content protection for advanced media applications, storage area, systems, VPN, secure VoIP, remote LAN, electronic banking and so on.. AES is a 128-bit symmetric cryptographic algorithm. The NIST endorsed AES is a subset of these choices with a fixed block size of 128-bits, yet the key might be 128, 192 or 256-bits long. This implies, a fundamental AES engine is equipped for encoding plain content information in blocks of 128- bits utilizing any of the predefined key sizes. More elevated amounts of security can be accomplished by utilizing greater key sizes.

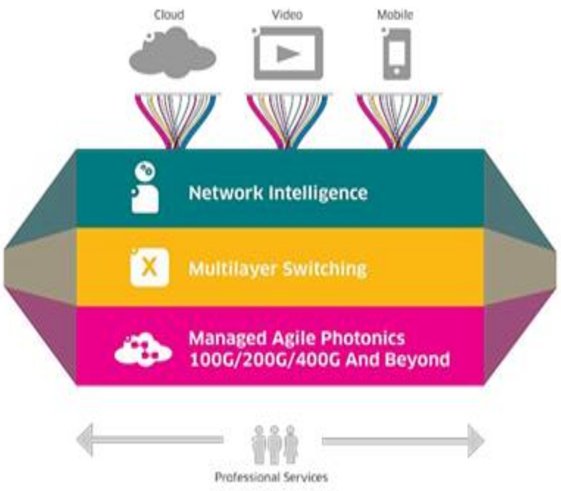

Fig. 2 Agile Optical Networking is made up of three key pillars that together serve as the foundation for a modern optical transport solution purpose-built for the cloud era

Field Programmable Gate Array (FPGA) is a coordinated circuit that can be obtained off the rack and reconfigured by makers themselves. With each reconfiguration, which takes only a little measure of a second, an incorporated circuit can play out an absolutely one of a kind capacity. FPGA includes a large number of comprehensive building squares, known as configurable logic blocks (CLBs), related using programmable interconnects. Reconfiguration can change a component of each CLB and associations among them, prompting a practically new advanced circuit.

The AES can be customized in programming or worked with unadulterated equipment. At any rate Field Programmable Gate Arrays (FPGAs) offer a snappier and more versatile arrangement. For completing cryptography in equipment, FPGAs gives just the fundamental critical choice rather than custom and semi-custom Application Specific Integrated Circuits (ASICs). Coordinated circuits that must be arranged the distance from the conduct depiction to the physical configuration are sent for an expensive and dreary creation.

The use of the AES calculation subject to FPGA devices has the purposes of enthusiasm over the execution reliant on ASIC is shorter structure cycle provoking totally working gadget models, Lower cost of the PC helped setup apparatuses, affirmation and testing, potential for snappy, minimal effort different reinventing and higher precision of correlation.

TABLE II AES VARIATIONS

	Block Size N $_b$ Words	Key Length N $_k$ Words	Number of Rounds Nr
AES-128bit key	4	4	10
AES-192bit key	4	6	12
AES-256bit key	4	8	14

Block size (Input) is 16 bytes or 4 words. Each word is 4bytes.

1. Number of columns (32-bit words) comprising the State. For this standard, N $_b$ = 4.
2. Number of 32-bit words comprising the Cipher Key. For this standard, N $_k$ = 4, 6, or 8.
3. Number of rounds, which is a function of N $_k$ and N $_b$ (which is fixed). For this standard, Nr = 10, 12, or 14.

V. AES STRUCTURE

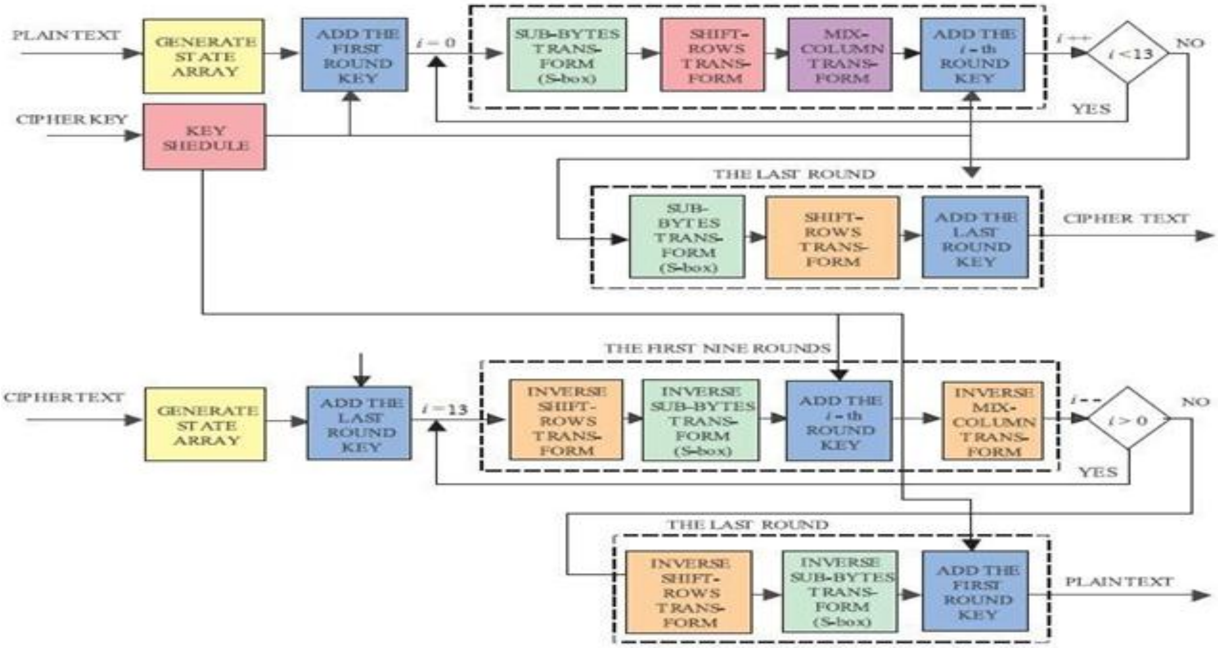

Fig. 3 AES - 256 complete Architecture

VI. PROPOSED SYSTEM: SECURITY IN AGILE OPTICAL NETWORKS

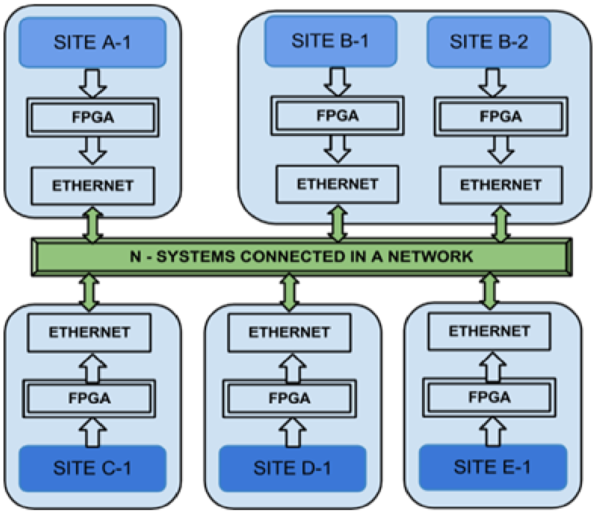

Fig. 4 Agile Optical Network

VII. RESULTS AND DISCUSSION

TABLE III RESOURCES USED

Logic Used	Used	Available	Utilization
Amount of Slice Flip Flops	2,621	9,312	28%
Amount of 4 input LUTs	2,871	9,312	30%
Amount of occupied Slices	2,495	4,656	53%
Amount of Slices containing only related logic	2,495	2,495	100%
Amount of Slices containing unrelated logic	0	2,495	0%

TABLE IV EFFICIENCY OF PROCESSING

Process	Clock frequency (MHz)	Time (ms)	Throughput (byte/sec)
Encryption	50	4.0274	3972.2
Decryption	50	4.1524	30825.1

TABLE V EXPERIMENTAL ANALYSIS

Design	Device	Frequency MHz	Slices	BRAMS
Elbirt *et al.,*	XCV1000-4	31.8	10992	0
M.McLoone *et al.,*	XCV812e-8	93.9	2000	244
K.U.Jarvinen *et al.,*	XCV1000e-8	129.2	11719	0
G.P.Saggese	XCV2000e-8	158	5810	0
F.Standaert	XCV3200e-8	154	15112	0
Proposed	Spartan 3eXc3s500e	50	*2,495*	320

VIII. CONCLUSION

The combination of a straightforward, versatile, flexible and productive AES cryptographic algorithm actualized in VHDL source code gives a brilliant stage to high security applications. A synthesizable VHDL code is produced for the execution of both encryption and decryption process. Optical Networks is a worldwide supplier of broadcast communications or telecommunications substructure solutions. With hardware-automated Optical + Ethernet transmission innovation, we can fabricate the establishment for fast and protected next- generation systems. The product supplies versatility, reliability, scalability, flexibility and security to clients' systems while evacuating unpredictability, complexity and cost.

REFERENCES

[1] Borkar, M. Atul, R.V. Kshirsagar and M. V. Vyawahare, “FPGA implementation of AES algorithm”, *2011 3rd International Conference on Electronics Computer Technology,* 2011.

[2] Marko Mali, Franc Novak and Anton Biasizzo “Hardware Implementation of AES Algorithm”, *Journal of Electrical Engineering,* Vol. 56, No. 9-10, pp. 265-269, 2005.

[3] FIPS 197, “*Advanced Encryption Standard* (AES)”, November 26, 2001.

[4] D. C. Kilper, K. Guan, K. Hinton, and R. Ayre, “Energy Challenges in Current and Future Optical Transmission Networks”, *Proc. IEEE,* Vol. 100, No. 5, pp. 1168-1187, 2012.

[5] Daniel C. Kilper, Michael S. Wang, Atiyah Ahsan and Keren Bergman, “Efficient and agile optical networks”, 2013 *17th International Conference on Optical Networking Design and Modeling (ONDM)* 16-19 April 2013.