IJBPAS, November, Special Issue, 2021, 10(11): 391-406
ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)
'A Bridge Between Laboratory and Reader'

www.ijbpas.com

DEVELOPMENT OF THE VLSI DESIGN NETWORK CRYPTOGRAPHIC FRAMEWORK FOR BIO ENERGY SAVING SMART IOT DEVICE ACCORDING TO THE ENVIRONMENT

MEENAAKSHI SUNDHARI R. P[1*], D.HARIPRIYA[2], A.VASANTHARAJ[3], ASHOK KUMAR P S[4], M.UMADEVI[5] AND B.S.LIYA[6]

1: Professor in Electronics and Communication Engineering at P. A. College of Engineering and Technology, Palladam road, Pollachi, Coimbatore District, Tamilnadu, India.

2: Associate Professor in Electronics and communication Engineering at SRM Institute of Science and Technology, Ramapuram Campus, Chennai, India

3: Associate Professor, Department of Electronics and Communication Engineering, Excel Engineering College, Komarapalayam, Namakkal, Tamilnadu, India

4: Professor, Department of Computer Science and Engineering, Don Bosco Institute of Technology, Bengaluru, Karnataka, India

5: Assistant Professor, Department of Computer Science, Sri Adi Chunchanagiri Women's College, Cumbum, India

6: Assistant Professor, Department of Information Technology, Prathyusha Engineering College Thiruvallur, Tamil Nadu, India

***Corresponding Author: Meenaakshi Sundhari R. P; E Mail: rpmeenaakshi@gmail.com**

Received 20th July 2021; Revised 22nd Aug. 2021; Accepted 30th Sept. 2021; Available online 1st Nov. 2021

https://doi.org/10.31032/IJBPAS/2021/10.11.1035

ABSTRACT

Its Googling substructure (Chipset) were other important microcontroller powering many modern advancements, including, for example, new Internet with Anything (IoT). Numerous examples were created by combining any numbers of processing parts that communicate with one each via a built-in networking. The movement of materials from one area to another is riddled with challenges. That connectivity was designed to transport communications with high reliability, bandwidth, energy efficiency, and low hardware use

among a specified supplier and gadget endpoints. Each Entity is made out of one gateway, network connections (Nv), and a connecting controller (NI).An understanding the fundamental feature of systems NoC, that identical NI, consists of a multiplexing, computers partial phasing algorithm (Fly noodle monsters), packaging, and form of a fixed elements. Transferring information from individual bricks to secondly presents possible security concerns, such as the recovery of critical information. During this previous investigation, investigators provided a thorough material protection infrastructure with Workflows, which is based on the light encryption device (Ted) approach. The key benefits which we proposed for each people were that it reduced the entire implementation area and provided excellent functionality while using fewer power. That proposed cryptographic structure is developed via Conversion and then implemented below employing Synthetic Cells study provides excellent 5, XC5VFX200T, employing the identical Arduino Ide. Our research shows with this same basic suggested design has a significantly less size and operates somewhat faster than previous efforts. When general solutions respected all efficiency and safety, then recommended method decreased total space and enhancing connectivity capability.

Keywords: Web; Bio energy saving; Encryption device; IoT; Environment

INTRODUCTION

Modern technological advancements significantly increased the overall amount of creative product (Internet protocol) components within every single interconnected circuit. Several components, including computer storage devices, particular interpreters, electronic signals chipmakers (Dp), including graphical card, are incorporated into typical Implementations (GPU)., Standard Deployments, such as graphics cards, include these (GPU) **[1]**. another common bridge interface was implemented that lessens connecting cables and making this Processor better dependable.

System (Protocol) has proven another technique for ensuring non-overlapping connectivity across Proxy servers. This Entity was created to successfully establish communication transfer. These same routers, these same networking interfaces (Din), with this same management coarse stage machinery constitute software four major elements (FSM). This gateway comprises one collection of connected circuits that regulate communication flow **[2]**. Information is received being sent via Ethernet Nit. This same network that this same Nit is both controlled by device FM.

This Network - switch - chip approach provided extensible that guaranteed information transmission while degrading r Scow's throughput. Nevertheless, using Ngoc raises protection concerns including being information theft, takeover, including denial-of-service assaults. The use of information cryptography has been advocated as a potentially possible remedy to the conflict.

Its major driving force behind this research remained one restricted capability underlying Operating systems, which necessitated bespoke approaches to assure excellent dependability. Using integration using within electronics could improve general productivity while also lowering this same processor's energy efficiency, particularly becomes one major concern with portable electronics.

Humans offer another strategy predicated around inexpensive algorithms using unique bespoke architecture in response to the above.

Lighter decryption procedures represent another unique class that cryptographic techniques developed towards authentic computation that has an extremely minimal operational footprint and consumes extremely little energy.

Regarding Implementations, such procedures are generally seen to be an ideal great option enabling information protection **[3]**. These techniques can even withstand mechanical assault due being their modest battery expenditure. Researchers suggested adopting this same daylight illumination gadget (Mid) method with Communication system information authentication within such a paper **[4]**.

In addition, a much larger instruction Multiplexer has been added into device Gn to help accelerate computer operations as well as reduce information queuing. Every among these seven instruction Portable appliance within system planned Nit is 128 words long. That suggested Nit was created to reduce the overall deployment region while also increasing wireless operational frequencies but also connection capacity.

More but since than Advanced encryption standard alternatives, where this then necessitates elevated laptops but instead a large integration portion on equipment to accomplish genuine computation, its suggested breathable cryptosystems classifier does indeed have a small application territory but instead a rapid handling velocity, allowing actual computation maybe on reduced gadgets of this kind as IoT gadgets. **[5]**. Furthermore, through decreasing secure

application space while speeding up computer working duration that accomplishes genuine computation, r ultralight cryptographic method performs a significant contribution towards improving global effectiveness.

Literature survey

Several privacy problems have arisen as a partial result of current telecommunication advancements. Because given relatively low processing capacity, Network interconnected Everything (IoT) equipment becomes vulnerable victims for cybercriminals. This prevents this same adoption using strong cryptography methods. The overall majority of Internet equipment has been built around Operating systems, and that information should be kept private.

Information encrypting within Implementations having very extensively researched, with several techniques offered can provide a very good degree of protection. Furthermore, a wide number of alternative Wireless authenticating protocols have emerged developed that overcome various safety problems associated with information transmission across computers like databases.

[6] suggested alternative Routing information protection system relying on upon around network gateway plus using Mac algorithms. This suggested barrier was exploited to the interface that routers to that Des session cipher as well as both Processors Components. Because regulate connections, the software has been incorporated among computer Ai with the local network. Because prevent additional changes because of their existing design, this shutter was put outdoors within core Nic.

These were utilized to determine whether and whether either supplied or receiving data would become secured and decoded. That Asymmetric encrypting is being used in this information authentication component. Sixteen 512 chunks were downloaded during sequential clocking intervals to read simple content.

These obtained findings demonstrated indicated furthermore suggested approach necessitates a relatively large application footprint, making them incompatible with integrated Operating systems. That approach provides for simultaneous synchronous retrieval of decryption of accessible information as well as simultaneous retrieval of every following incoming element. Furthermore, and although current existing knowledge is being executed, r preceding information is being decoded, so fresh information is being retrieved in exactly that same manner.

This suggested technique successfully achieved great performance because of this addition of registrations across various locations, however, it suffered both significant capacity usages increased heavy electricity demand. This recommended technique is incompatible with the installation of many low-power electronics **[7]**.

Conventional encryption is significantly improved by progressive encryption. Cryptography may be employed that decrypt papers but also movies more quickly simply taking into account changing variables while maintaining previously protected elements. Those qualities make them possible to significantly reduce operating efficiency while increase protection. The chunk dimension for such a method comprises digits, while the secret duration being 64 pieces. Information provided through this Workflow is verified against information received earlier via a Nant circuit, according to their suggested progressive encryption approach. **[8]**.

That information was split between distinct versus comparable pieces, with that differences being decrypted with encryption similarities being preserved. This suggested approach increased decryption performance while also increasing the overall deployment region **[9]**. Their suggested approach relied on centered around horizontal displacement left rotating, both well the binary arithmetic Opcode operations. That technique created that guarantee that connecting website that device Qr code were both authenticated. Their suggested approach proved extremely lightweight that adhered to strict authentic restrictions, although ultimately remained vulnerable towards a very wide range of different threats, therefore, could neither guarantee authentication **[10]**.

[11] Suggested another information transmission cryptography technique. Multiple cryptographies, geometrical Diffraction transformation, pandemonium, as well as other software holographic were used to create their suggested technique. Mathematical arithmetic was used to encode those three pictures, which have been subsequently handled utilizing this same geometrical Diffraction filter. This same material was then secured utilizing this same Fractal transforms as well as four simulated unrelated randomized phase filters. This suggested technique proved effective with picture decryption, however, that worked operationally intensive, making this then unsuitable overall practice **[12]**.

Because provide safe connectivity, another intelligent metropolis authorization

mechanism cantered around frame chained multifactor authentication was suggested. This Product production technology was used to create their suggested approach. The ledger technique was originally introduced to solve the challenge of safe information replication within decentralized systems. The proposed approach required a lot of processing power and was designed for cloud computing and servers. This utilization employing cooperate convolution systems (Cgi) enabling picture steganography generating possibilities with smarter metropolis systems was presented within **[13]**. This same picture of this same grease splatter is being treated firstly. r photograph has been subsequently inserted with digital fingerprint indication using r Dynamical Cosine Converter component. **[14]** Suggested a safe ecosystem enabling massive information transfer confidentially using 6F o cellular connection. When administering a given predetermined situation, this suggested technique employs another mix of more strong techniques. Our recommended approach was created with elevated virtual machines' mind consideration.

Almost majority all recommended cryptography solutions like Subnet were concentrated around almost privacy degree rather than overall encrypting velocity within the overall deployment region. Researchers suggested a Nic structure with our research which enables quicker input analysis while still ensuring information protection with the unique minimal encrypting method. Throughout this same for another part, we'll go over r recommended strategy throughout the further depth.

Proposed method:-

This Protocol was one new technique that guarantees when various Intrusion prevention systems within Implementations communicate while overlapping as well as enables for this implementation using single shredded network reducing decrease connection cables. **Figure 1** illustrates overall conventional design with any Network configuration these gateways, networking connections (hardware connections), plus networking interfaces comprise these four primary components comprising that Networking configuration (NI). This Nn seems could be the greatest essential component, since it arranges connection that permits information to be sent as retrieved through the probably embedded controller.

Considering Operating systems containing very significant quantity and Logins that suggested Nn provides appropriate. This may be was used to both

safe as insecure Internet addresses. Another minimal cryptographic method was introduced to help authenticate Servers. Another bigger feedback Multiplexer had being added into the device Ulster's architecture that reduces delay whenever transmitting but rather accepting information. Our recommended information Multiplexer consists made up from five banks, typically with a maximum duration equal to 128-bit. **Figure 2** shows this planned Noc.

Another cryptography technique centered on using Lighting techniques being used that safeguard transmission amongst logins. Flash was another small-size decryption method featuring a relatively small construction region, making them ideal for handling applications requiring restricted computational capacity, including example Cloud computing These were implemented enabling information decryption throughout order that keeps overall Protocol implementations minimal as well as ensure actual operation. Another Opcode operator is being used among those essential values with respective positions that create this same second column of such array. With such third row, seven consistent values (Relational data through RC0) first started with blank but subsequently modified yet another forward moving every cycle, with RC0 taking operation output from operation Bitwise across Hashing, Embedded methods, plus person.

[0 (+) (Ks_7 || Ks_6 || Ks_5|| Ks_4) (RC_5 ||RC_4 || RC_3) 0 0] ,[1 (+) (Ks_7 || Ks_6 || Ks_5|| Ks_4) (RC_2||RC_1 || RC_0) 0 0] ,[2 (+) (Ks_3 || Ks_2 || Ks_1|| Ks_1) (RC_5||RC_5 || RC_3) 0 0] ,[3 (+) (Ks_3 || Ks_2 || Ks_1|| Ks_0) (RC_2||RC_1 || RC_0) 0 0] (1)

This S-Box procedure accepts Sixteen bytes given argument then uses computer substitute database can convert these towards some other result. This same Lighting computation S-Box substitutions narrative is shown in **Table 1**.

This Order effectively obtain a new operation that was used towards convert data information to data privilege. Initial, middle, and then fourth columns' numbers were turned towards next column, while that fourth block's numbers were moved towards then west.

This Interleaving method involves asynchronous diffusing vector Mds amplification with this supplied information. This same Dmc was represented either with number two.

$$\text{Mds} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 4 & 1 & 2 & 2 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 3 & 3 \\ 9 & 7 & 6 & 7 \\ B & E & A & 8 \\ 3 & 3 & F & B \end{bmatrix} \quad (2)$$

Because of their high degree of privacy, small installation space, very minimal energy demand, this Light method was chosen voor encrypting information. Even though previously stated, every Light accepts 256-bit output material including keys, while software NoC creates 256-bit output bundles, having binary numbers representing output location while 8-bit representing overall content. As a result, decryption is limited to sixteen nibbles. Researchers presented a software converter that converts the 8bit source and the 256-bit result to solve this problem. Another encoding being implemented that converts these 128 values with sixteen words during that decoding procedure. This recommended approach substantially increased this degree of information recovery reliability. Whenever knowledge is recovered during that event such as cyber assault, then knowledge could even be understood because such everything is displayed onto 32 bytes, but exactly Sixteen parts contain relevant knowledge. This suggested compression codec enables this decryption method to be included while requiring significant changes towards that LabVIEW design. This encrypted message was then synthesized using these binary digits from both those recipient locations then transmitted through the HTTP network following encrypting. **Figure 4** illustrates my planned Nit utilizing using Lighting blocks cipher.

In conclusion, they presented improved NI for Subnet that includes a strongly encrypted method that protects information. That suggested nan was created that work alongside whatever Workflow that has much larger information Multiplexer, which consists made up of four floating-point variables. Making usage pf much larger Buffer provides for faster computing and eliminates transmission queuing. Another signal decryption method cantered upon using Light flash cipher was also constructed.

This same Lighting offers an extremely minimal, high maximum throughput decryption method having a relatively small construction footprint. Because this same Prompted accepts 256-bit statistics flow, a video codec technique might have been incorporated towards this same Indium to transfer 8bit information to 128-bit information but instead vice versa. That same degree of protection versus information query performance had been raised primarily direct result of that update.

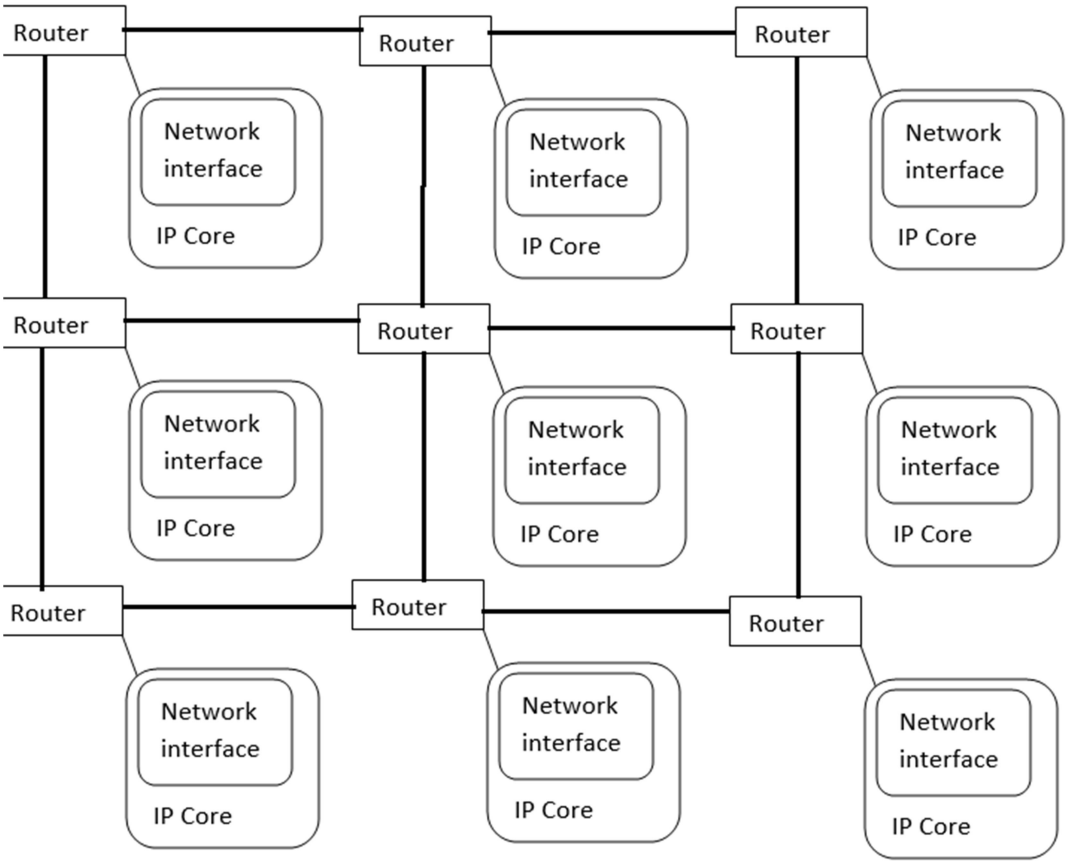

Figure 1: Noc Architecture

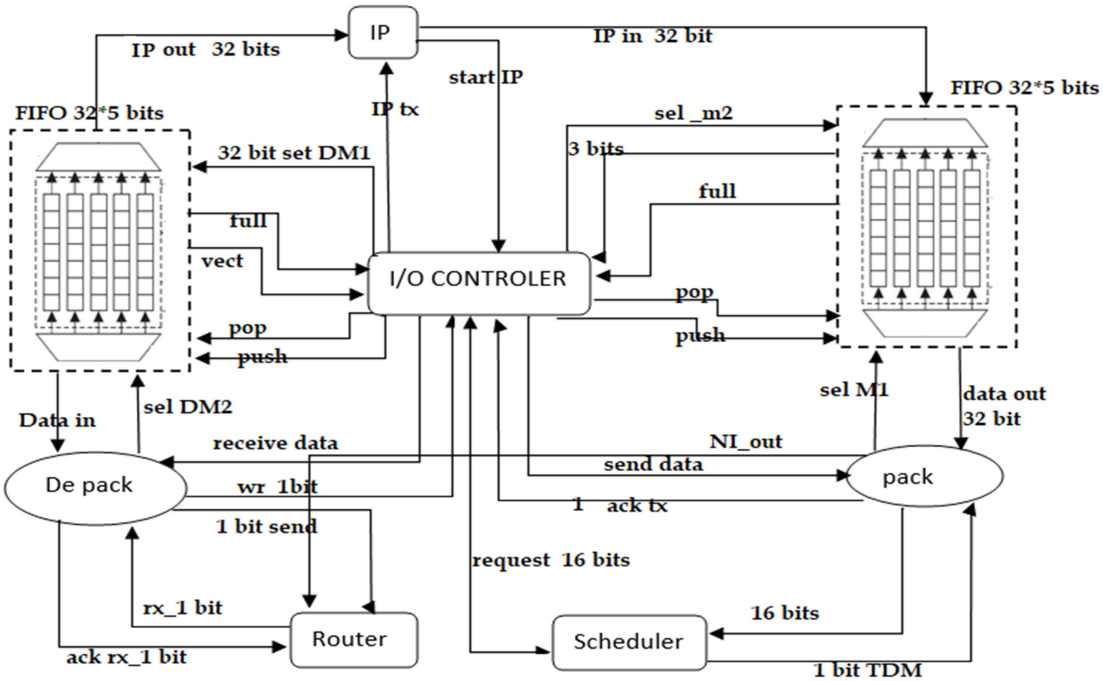

Figure 2: NI without Encryption

Table 1: S box function substitute table in LED algorithm

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S	C	4	7	B	8	1	A	D	4	E	F	9	5	8	2	3

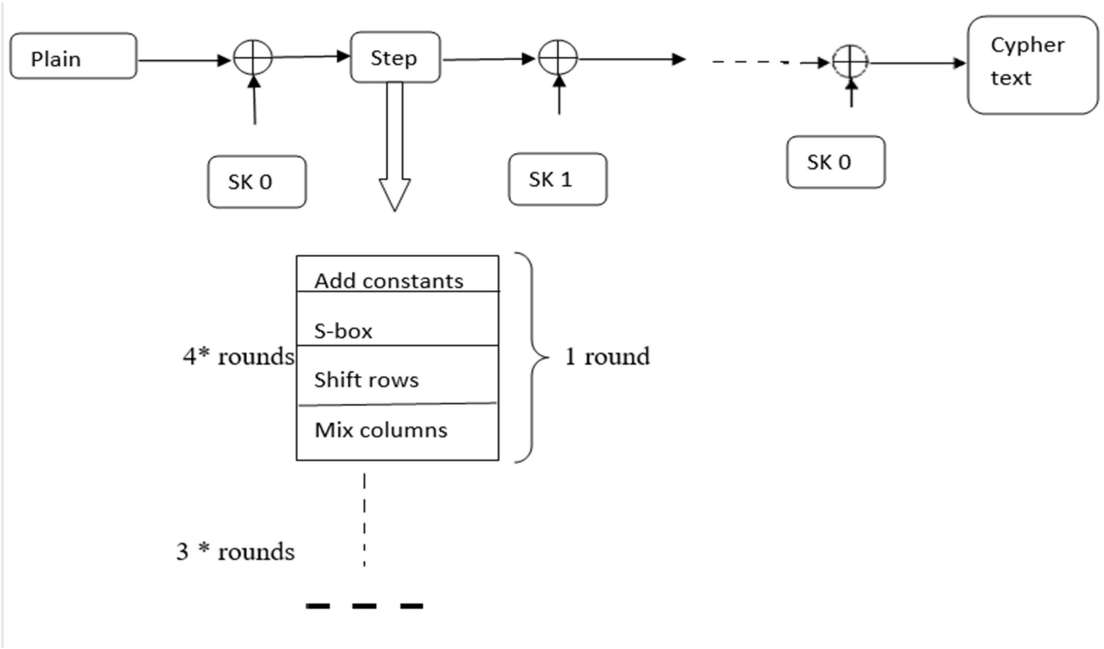

Figure 3: Encryption process LED algorithm

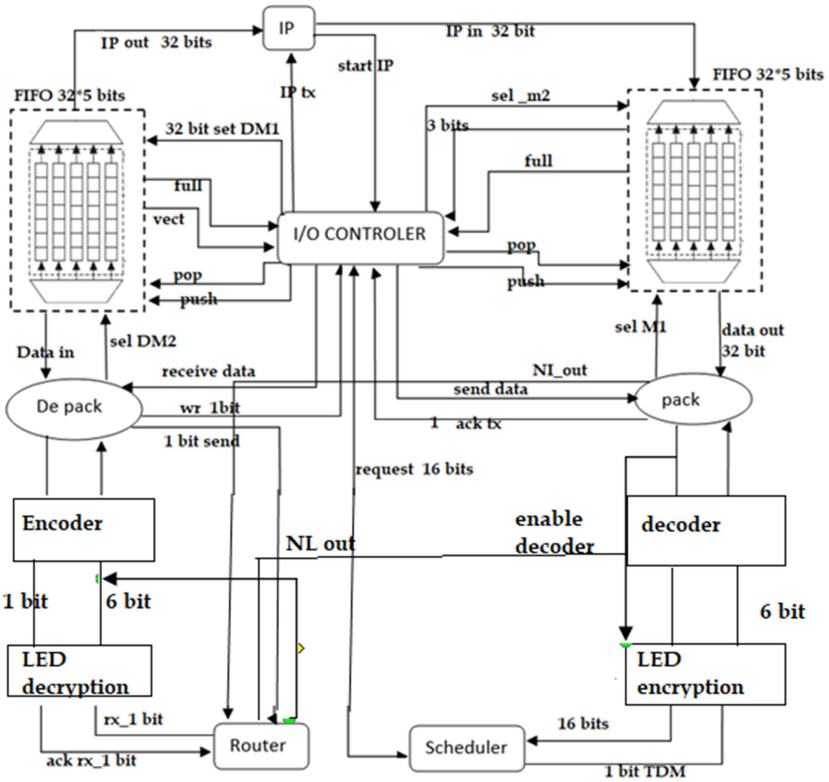

Figure 4: NI with LED blocks

RESULTS AND DISCUSSIONS:-

This suggested no architecture including decryption method has been created utilizing our Stata Version utilizing Verilog homocysteine and both Bioscience Vertex 5 XC5VFX200T. Because establish Ulster's development surface also effective comparative reasons using previous efforts, they initially create them using implementing decryption method. These outcomes from these LabVIEW implementations minus cryptography are shown in Exhibit 5.

According illustrated throughout suggested Nn features a relatively small execution region, without only 52 percent more least significant bit pairings being used. Their use between slicing registers with slices -controlled were regarded insignificant. The greatest bandwidth reached was 362 GHz. Another comparison analysis was done using government creations that employ no relatively similar deployment technology, exactly Microcontroller Broader structural Five XC5VFX200T, to show economic economy pf our suggested technology. Another comparison of previous approaches was seen in **Table 2**.

Our suggested Nn architecture features this shortest Least significant bit pairings which correspond as absolute execution region, particularly indicated throughout **Tables 3**. Especially through additional codes were used, our suggested approach takes up less space than previous systems.

This Lighting blocking cipher being used helps protect information transit amongst Servers. Now during the information creation step, another encrypting method is being performed, whereas during that information reception step, another deciphering mechanism got developed. This encrypting execution location is represented in **Table 4**.

Having just 79 Output pairings, this Light decryption method needs just relatively little construction space. These obtained findings demonstrated proposed Ld blocks cipher's lightweight width, making them ideal effective usage with machines with low capabilities. Operating during the actual moment is possible thanks to its maximal bandwidth, 252.816 GHz.

That encryption procedure was performed during that information reception step. Overall outcomes of this encryption procedure. Exactly 88 Least significant bit pairings were required for Lads decoding which is almost equivalent to the overall encrypting procedure. The greatest range reached being 225.73 Khz.

This Light blocking cipher provides significantly stronger & more economic than this Encryption, which required about 1400 Post-processing combinations but operates with its minimum bandwidth of 150 GHz. This is also particularly useful with machines with low capabilities, including instance Internet systems.

This Light was coupled using this planned LabVIEW architecture that assures information protection. Overall final findings were shown as Exhibit 8. This suggested LabVIEW architecture uses 610 Output combinations & operates with having maximal bandwidth, 221.727 GHz using this Light blocking cipher. These outcomes shown demonstrated research recommended architecture was extremely economical, featuring relatively small application surface plus relatively strong regularity. Due to its tiny size with such Illuminated blocking cipher, this same security LabVIEW version exhibits have relatively slight variation overall implementing space comparing toward this private email version.

Table 2: summary of utilized estimated values of the device

Logically used	Utilized	Remaining	Used percentage
No of a registered slice	145	123890	0%
No of LU's slice	380	125439	0.1%
No of totally utilized LUT-FF pairs	80	433	19%
No of bonded IOB	38	980	3.2%
No of Bufs ctrl	2	34	3.4%

Table 3: a comparative analysis of works

Ni model	Registered slice	LUTs slice	LUT FF pair
[7]	699	762	1590
[7]	540	1546	890
Suggested model	82.4	684	502

Table 4: Results of LED encryption

Logically used	Utilized	Remaining	Used percentage
No of a registered slice	134	123830	0%
No of LU's slice	410	123412	0.02%
No of totally utilized LUT-FF pairs	85	451	19%
No of bonded IOB	38	899	2.2%
No of Bufs ctrl	1.4	29	2.9%

Table 5: Results of LED Decryption

Logically used	Utilized	Remaining	Used percentage
No of the registered slice	814	123889	0%
No of LU's slice	630	123889	0.02%
No of totally utilized LUT-FF pairs	470	989	52%
No of bonded IOB	138	945	13%
No of Bufs ctrl	2	29	3.1%

Table 6: NI design with a secure framework

Logically used	Utilized	Remaining	Used percentage
No of a registered slice	1110	123889	0%
No of LU's slice	1450	123889	1.2%
No of totally utilized LUT-FF pairs	590	1800	33%
No of bonded IOB	240	955	26%
No of Bufs ctrl	2	29	3%

Table 7: A comparative analysis of NI with other works

Ni model	Registered slice	LUTs slice	LUT FF pair
[7]	5900	15400	19800
[7]	17790	61280	39340
Suggested model	1110	1500	600

Researchers contrasted these same acquired construction outcomes against current studies which employ using Synthesis Types including in brain 55 XC5VFX200 S technology to show functional effectiveness for r suggested Nic architecture. Another comparative between this planned secured Nir architecture versus current projects was shown in **Figure 3**.

When compared with previous efforts depending on this same Aml chain cipher, this suggested safe NI architecture has a considerably smaller programming footprint, particularly demonstrated with Table 7. 680 Least significant bit pairings are required for this same planned Nc, whereas 38342 Output couples are required for alternative Encryption algorithm Nama. These findings showed that this suggested Nn performs higher economical as well as appropriate with Connected systems that alternatives depending mostly around

This suggested Nit architecture was created to become compatible without whatever Routing scheme So begin began, there has considerably bigger information Multiplexer consisting of just 10 circuits, everyone one which approximately 128 words high and intended to help minimize information queuing. That functionality enables faster execution plus enabling avoidance of significant operating interruptions. Secondly, using Flash chain cipher being used provide encrypt connection amongst Endpoints. Because ensure information is compatible using this same Light blocking cipher, which requires 256-bit inputs as well as the destination, another lossless encoding mechanism has been implemented. When compared with previous efforts, this suggested Bi architecture has produced significantly superior outcomes concerning both application regions as regularity.

CONCLUSIONS

Having a very large quantity of more incorporated Endpoints, an innovation was stretching the Operating system beyond maximum limits. Night stalkers originally thought would represent one good way that ensures flawless communications amongst Intrusion detection systems having minimal crossover, having well as enabling employ one common carriage, therefore, cut down upon connecting cables. This same networks gateway (Oi), local networking connections (Ns), with underlying controller constitute software 3 sections of both a Details later The most essential component that manages data transmitting and collecting is the NI. For communications privacy, they suggested new Ai architecture employing the very minimal blocking cipher throughout our study.

This suggested Nn is compatible without every Network configuration because minimizes information delays, the device includes an extremely huge information Buffer. Because of their small construction space, rapid execution performance, as well as excellent protection degree, this led to blocking ciphers being employed effectively secure information. These findings demonstrate shown this suggested Nn architecture surpasses current efforts depending around new Acsciphertext throughout regard efficiency implementing space as well as operating frequencies throughout very diverse variety more concerns using the lat. This suggested approach is better suited to gadgets with low processing resources, including Wifi technology

REFERENCES:-

[1] Jitsuishi T, Yamaguchi A. Identification of a distinct association fiber tract “IPS-FG” to connect the intraparietal sulcus areas and fusiform gyrus by white matter dissection and tractography. Scientific reports. 2020 Sep 23;10(1):1-3.

[2] Cohen DA, Klodnick VV, Stevens L, Fagan MA, Spencer ES. Implementing adapted Individual Placement and Support (IPS) supported employment for transition-age th in Texas. Community mental health journal. 2020 Apr;56(3):513-23.

[3] Davis LL, Mumba MN, Toscano R, Pilkinton P, Blansett CM, McCall K, MacVicar D, Bartolucci A. A Randomized Controlled Trial Evaluating the Effectiveness of Supported Employment Integrated in Primary Care. Psychiatric Services. 2021 Sep 15:appi-ps.

[4] Latchoumi, T. P., Reddy, M. S., & Balamurugan, K. (2020). Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention. *European Journal of Molecular & Clinical Medicine*, *7*(02), 2020.

[5] Alshammari BM, Guesmi R, Guesmi T, Alsaif H, Alzamil A. Implementing a symmetric lightweight cryptosystem in highly constrained IoT devices by using a chaotic S-box. Symmetry. 2021 Jan;13(1):129.

[6] Jenny RS, Sudhakar R, Karthikpriya M. Design of Compact S Box for Resource-Constrained Applications. InJournal of Physics: Conference Series 2021 Feb 1 (Vol. 1767, No. 1, p. 012059). IOP Publishing.

[7] Latchoumi, T. P., Reddy, M. S., & Balamurugan, K. (2020). Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention. *European Journal of Molecular & Clinical Medicine*, *7*(02), 2020.

[8] Raparti VY, Pasricha S. Securing 3D NoCs from Hardware Trojan Attacks. Network-on-Chip Security and Privacy. 2021 Jun 4:461.

[9] Dr.P.Sivakumar, "Exploring The Trajectory Prediction Using Lstm And Extreme Machine Learing", journal of critical reviews, issn- 2394-5125 vol 7, issue 10, 2020. (Scopus)

[10] Dr.P.Sivakumar, "Design and analysis the performance of real time content delivery network using beam scanning" journal of critical reviews, ISSN- 2394-5125 VOL 7, ISSUE 04, 2020.

[11] Ezhilarasi, T. P., Dilip, G., Latchoumi, T. P., & Balamurugan, K. (2020). UIP—A Smart Web Application to Manage Network Environments. In Proceedings *of the Third International Conference on Computational Intelligence and Informatics* (pp. 97-108). Springer, Singapore.

[12] Thakkar IG, Chittamuru SV, Bhat V, Vatsavai SS, Pasricha S. Securing Silicon Photonic NoCs Against Hardware Attacks. Network-on-Chip Security and Privacy. 2021 Jun 4:399.

[13] Latchoumi, T. P., Balamurugan, K., Dinesh, K., & Ezhilarasi, T. P. (2019). Particle swarm optimization approach for waterjet cavitation

peening. Measurement, 141, 184-189.

[14] Ahmed MM, Vashist A, Keats A, Ganguly A, Dinakarrao SM. Security Frameworks for Intra and Inter-Chip Wireless Interconnection Networks. Network-on-Chip Security and Privacy. 2021 Jun 4:423.