International Journal of

INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Study and VHDL Implementation of novel Automatic Smart Security System

Rahul Prakash, Vijay Kumar Ram, Vijay Singh, Parul Varshney, Shikha Agarwal, Rajneesh

Submitted: 05/10/2023 **Revised:** 21/11/2023 **Accepted:** 01/12/2023

Abstract—In this paper, we present the design of the smart security system. The design has been described using VHDL. Nowadays security system is very essential in day-to-day life to make the human life secure. There are many types of security system which are too expensive and difficult to use. For that reason, an effective security system, powerful and user-friendly way of 24 hours of real time monitoring at low cost is built. The overall project is divided into six parts or modules. The main objective of this paper is to provide a mature security solution to the authorized persons only.

Keywords— *Xilinx, VHDL, FPGA.*

I. Introduction

Every country is facing large number of security problems. Wired security systems are being used in market. Though we can easily find out the problems in a wired system than wireless system but we cannot forget that it is costly because it needs high power. Wired system does not inform the users about any threat if he is far away from the system. Nowadays the idea of energy saving is considered to be a convention and a large section of population started to understand its importance [1]. We are using FPGA as main controller of our system and different sensor and component connected to it. FPGA is programmed through VHDL language. In electronics a VHDL is specialize computer used to describe the structure design and operation of electronic circuit and most commonly digital logic circuit. We are using VHDL (Very High Speed Integrated Circuit Hardware and Descriptive Language). It is the most widely and well supported HDL's language. A FPGA is an integrated circuit design to be configured after manufacturing hence it is called field programmable [2]-[3]. These facts make it obvious that a smart security system will reduce the chances of intrusion and thus, can protect both life and property. Hence, it is necessary to develop and implement a very dependable smart security system that can protect the user and properties [4]. The smart security system project gives security and easiness into the daily life style., in our project I have worked over VHDL for the coding if the sensors and cadence for making layout of our described design of the smart security system. I have used PIR sensors, buzzers, motor relays etc [5,8-9]. he smart security system as developed here in, on the other hand, being very cost effective, also provides the user with a much greater security. The security is major concern to design this project. In the following section, we present an overview of the proposed system. We can use this security system at residential area, commercial properties and industrial area etc.

II.Over view of System and Tools

In this section we, briefly present the details of the system. we used six modules in our smart security system and every module connected to each other via logic gates and other components [10-11].

Department of EIE, SCRIET,CCS University, Meerut, Uttar Pradesh.
coolrahul2287@gmail.com
Department of ECE, SCRIET,CCS University, Meerut, Uttar Pradesh.
vijayk10ster@gmail.com
Department of EIE, SCRIET,CCS University, Meerut, Uttar Pradesh.
scrietvijay2010@gmail.com
Department of ECE, SCRIET,CCS University, Meerut, Uttar Pradesh.
parulspsvarshney@gmail.com
Department of AS, SCRIET,CCS University, Meerut, Uttar Pradesh.
sagarwal.scriet@rediffmail.com
Department of AS, SCRIET,CCS University, Meerut, Uttar Pradesh
rajneesh_ccs@rediffmail.com

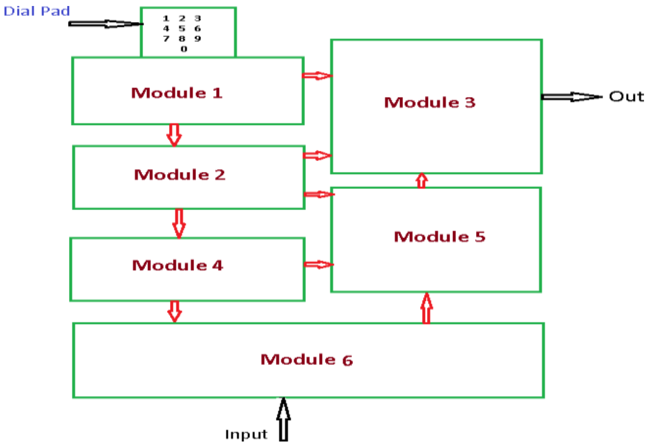


Fig. 1 Block diagram of smart security system.

III. Working of smart security system

- When anyone enters into the smart security system without entering the code then PIR sensor will detect then the alarm will be turn on and a light will glow that will be a red light.
- If anyone press the correct on keypad then PIR sensor will detect then it corresponding door will unlock and the person can enter through the smart security system.
- The alarm can be turn off by the button of keypad.
- These can count the person entering and exiting by the sensor at the smart security system.
- If a breach is detected, with the appropriate use of wired and wireless motion sensors, the alarm system will alert the user and security personnel.
- The system monitoring of the premises in real time.
- The smart security system is highly extensible and customizable [12].

IV. Discussion and Result

In this research paper, we propose a modular-based security system using VHDL as the primary design and implementation language. The system is designed to address the need for a flexible and scalable security solution that can be customized according to specific requirements.

A. Modularity in System Design:

The modular approach allows the security system to be divided into independent functional modules, each responsible for a specific aspect of security. These modules can be designed, verified, and tested independently, simplifying the overall system development process. Additionally, modularity enables flexibility in adding or removing modules as per the security needs of different environments.

B. Sensor Module:

The sensor module serves as the entry point of the security system, responsible for detecting various types of security breaches. It may include motion sensors, door/window sensors, temperature sensors, or any other relevant sensors depending on the specific application. The VHDL design for the sensor module involves the interface with the sensors, data processing, and event triggering.

C. Control Logic Module:

The control logic module acts as the brain of the security system. It receives inputs from the sensor module and makes intelligent decisions based on predefined rules or algorithms. The VHDL design for this module involves the implementation of decision-making algorithms, event correlation, and control signal generation for the response modules.

D. Response Modules:

The response modules are responsible for taking appropriate actions in response to security breaches. These actions may include sounding alarms, sending notifications, activating security cameras, or triggering emergency protocols. Each response module is designed as an independent VHDL module, allowing for easy customization and integration into the overall security system.

E. Communication Module:

The communication module enables the security system to interact with external entities, such as monitoring centers or mobile devices. It facilitates real-time notifications, remote control, and data exchange with the security system. The VHDL design for this module involves implementing communication protocols and interfaces to establish reliable and secure communication channels.

F. System Integration and Testing:

Once the individual modules are designed and verified, they are integrated into the complete security system. System-level testing is conducted to ensure the seamless interaction and coordination among the modules. VHDL simulation and verification techniques are employed to validate the overall system behavior and performance.

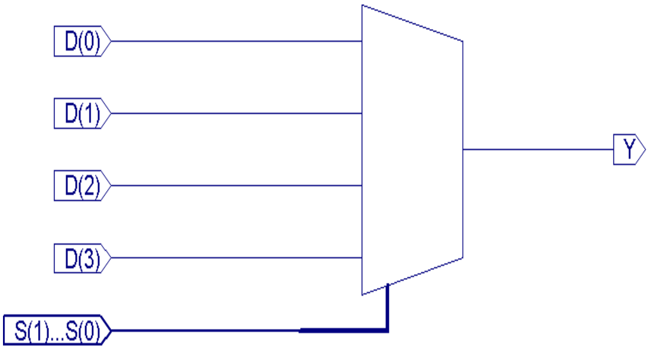
The modular-based security system design offers several advantages. Firstly, it allows for easy scalability and adaptability, enabling the addition or removal of modules based on specific security requirements. Secondly, it promotes reusability, as individual modules can be reused in different security system implementations. Lastly, the modular design facilitates efficient maintenance and troubleshooting by isolating and addressing issues at the module level. In this paper we use different types of components and logic gates.

E. MULTIPLEXER 4:1

We use MUX 4:1in memory and memory is used in Module 4 so here we discuss about MUX 4:1 and see the result of it. A 4:1 Multiplexer (MUX) is a digital logic component that selects one of the four input signals and forwards it to the output based on the select inputs. It is commonly used in digital circuits to route data from multiple sources to a single destination based on control signals [13].

The 4:1 MUX has four input lines (D0, D1, D2, D3), two select inputs (S1, S0), and one output line (Y). The select inputs determine which input line is connected to the output. The number following the colon in "4:1" represents the number of input lines, while the "1" represents the number of output lines.

The select inputs (S1, S0) are typically binary signals that can take on one of four possible combinations: 00, 01, 10, or 11. Each combination corresponds to a specific input line being selected and connected to the output.



For example, when the select inputs (S1, S0) are 00, the output line (Y) is connected to the first input line (D0). When the select inputs are 01, the output line is connected to the second input line (D1), and so on. The selected input signal is then propagated to the output, allowing data from the chosen input line to be passed through the MUX [14].

The MUX 4:1 provides a simple and versatile method for data selection and routing in digital systems. It is often used in applications such as data multiplexing, bus switching, data routing, and signal conditioning. By controlling the select inputs, different input signals can be selectively directed to the output, enabling efficient data manipulation and control in digital circuits.

Table 1 Truth table of multiplexer 4:1

S1	S0	D0	D1	D2	D3	Y
0	0	D0	D1	D2	D3	D0
0	1	D0	D1	D2	D3	D1
1	0	D0	D1	D2	D3	D2
1	1	D0	D1	D2	D3	D3

In the truth table, S1 and S0 represent the select inputs, and D0, D1, D2, and D3 represent the input data signals. The output Y represents the selected input based on the values of S1 and S0.

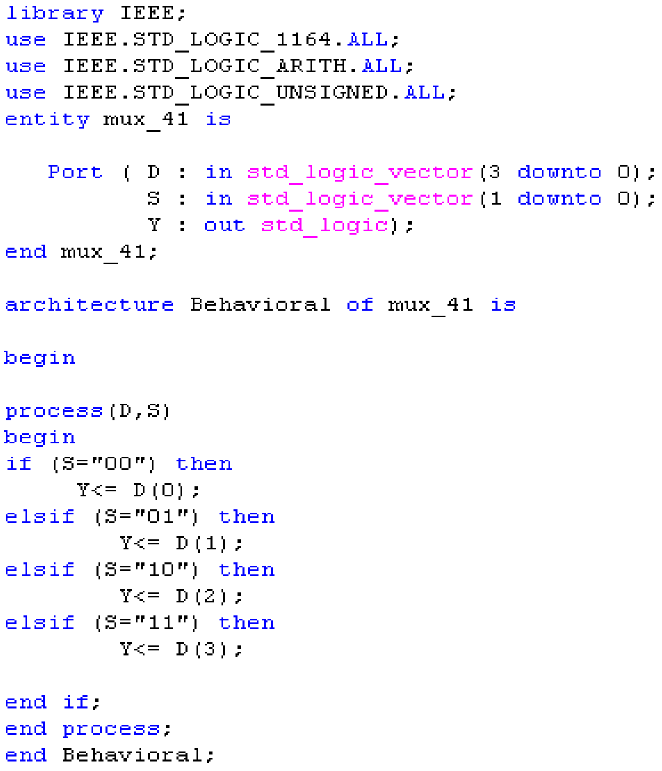
For example, when S1 = 0 and S0 = 1, the output Y will be equal to input D1. Similarly, when S1 = 1 and S0 = 0, the output Y will be equal to input D2.

The truth table shows how the MUX selects one of the four inputs (D0, D1, D2, D3) based on the binary values of the select inputs (S1, S0). The selected input is then forwarded to the output (Y), resulting in the desired data routing and selection functionality of the 4:1 MUX.

Boolean Expression:

The Boolean expression for a 4:1 Multiplexer (MUX) can be derived from its truth table. Considering the select inputs as S1 and S0, and the input data signals as D0, D1, D2, and D3, the boolean expression for the output Y can be written as

Y = S1' S0' D0 + S1' S0 D1 + S1 S0' D2 + S1 S0 D3



```
library IEEE;
use IEEE.STD_LOGIC_1164.ALL;
use IEEE.STD_LOGIC_ARITH.ALL;
use IEEE.STD_LOGIC_UNSIGNED.ALL;
entity mux_41 is

   Port ( D : in std_logic_vector(3 downto 0);
          S : in std_logic_vector(1 downto 0);
          Y : out std_logic);
end mux_41;

architecture Behavioral of mux_41 is

begin

process(D,S)
begin
if (S="00") then
     Y<= D(0);
elsif (S="01") then
        Y<= D(1);
elsif (S="10") then
        Y<= D(2);
elsif (S="11") then
        Y<= D(3);

end if;
end process;
end Behavioral;
```

Fig.2 RTL Schematic diagram of multiplexer 4:1

D) Register-Transfer Level Diagram:

The RTL (Register-Transfer Level) diagram for a 4:1 Multiplexer (MUX): In the diagram, the input data signals D0, D1, D2, and D3 are connected to the inputs of the 4:1 MUX. The select inputs S1 and S0 control the selection of the input data signals. The output Y represents the selected input that is forwarded to the output. The MUX block in the diagram represents the 4:1 Multiplexer component, which internally selects one of the input data signals based on the select inputs. The output Y is the result of the selection process. This RTL diagram visually illustrates the data flow and control signals of the 4:1 MUX, providing a high-level representation of how the inputs and outputs are connected within the multiplexer.

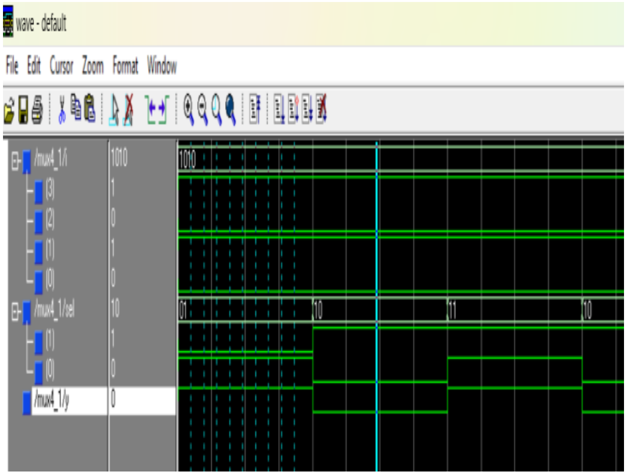


Fig. 3 Simulated results of multiplexer 4:1

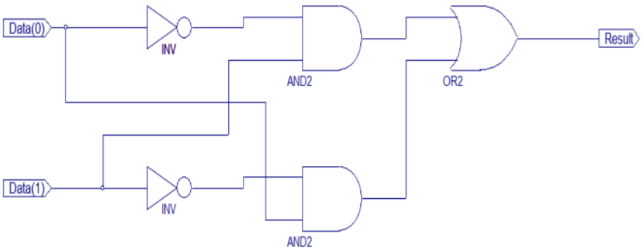


Fig. 4 RTL diagram of Full_Adder

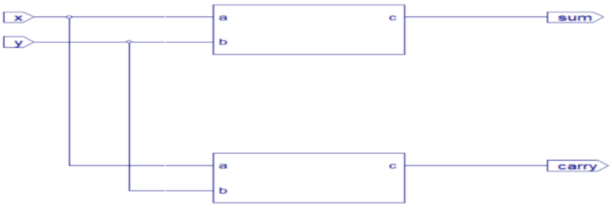


Fig.5 Register Transfer Logic of Half_Adder

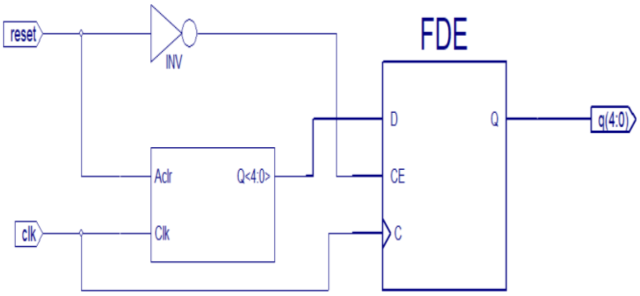


Fig. 6 Register Transfer Logic of Counter_4.

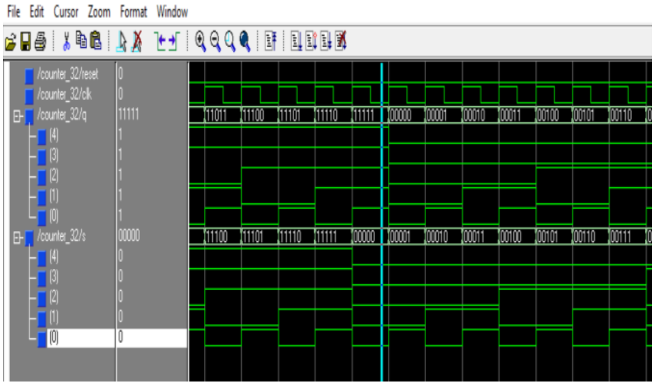


Fig. 7 Simulated result of counter_4.

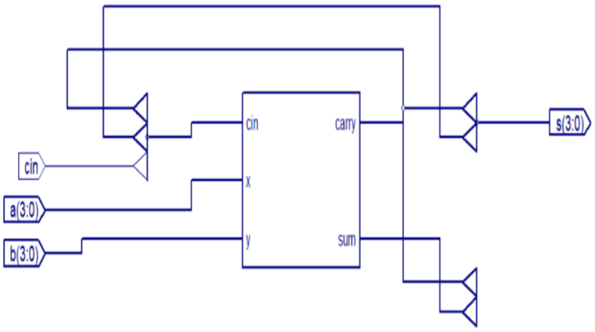


Fig. 8 RTL schematic of 4-bits parallel Adder.

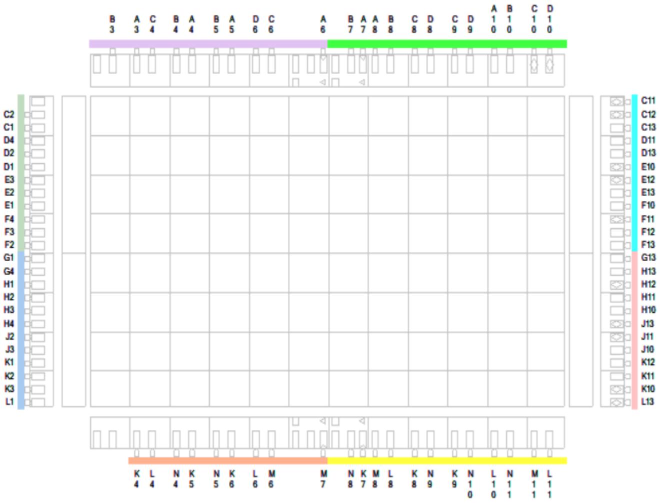
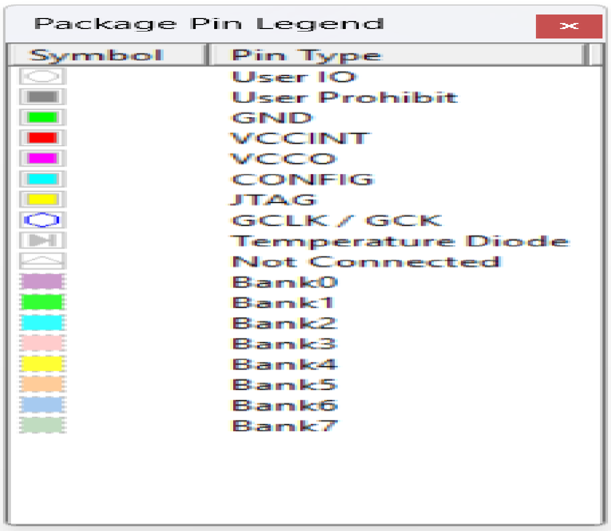

B3 A3 C4 B4 A4 B5 A5 D6 C6 A6 B7 A7 A8 B8 C8 D8 C9 D9 A10 B10 C10 D10
C2 C1 D4 D2 D1 E3 E2 E1 F4 F3 F2 G1 G4 H1 H2 H3 H4 J2 J3 K1 K2 K3 L1
C11 C12 C13 D11 D13 E10 E12 E13 F10 F11 F12 F13 G13 H13 H12 H11 H10 J13 J11 J10 K12 K11 K10 L13
K4 L4 N4 K5 N5 K6 L6 M6 M7 N8 K7 M8 L8 K8 N9 K9 N10 L10 N11 M11 L11

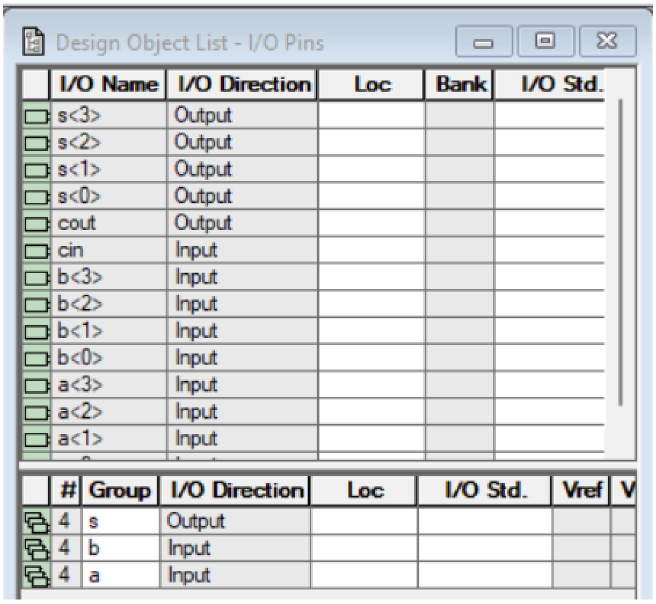
Fig. 9 PIN Description of 4-bit parallel Adder.



Package Pin Legend

Symbol	Pin Type
○	User IO
▬	User Prohibit
🟩	GND
🟥	VCCINT
🟪	VCCO
▬	CONFIG
🟨	JTAG
⬡	GCLK / GCK
▶	Temperature Diode
△	Not Connected
🟪	Bank0
🟩	Bank1
▬	Bank2
▬	Bank3
🟨	Bank4
🟧	Bank5
🟦	Bank6
▬	Bank7

Fig. 10 PIN Port description of 4-bits parallel Adder.



I/O Name	I/O Direction	Loc	Bank	I/O Std.
s<3>	Output			
s<2>	Output			
s<1>	Output			
s<0>	Output			
cout	Output			
cin	Input			
b<3>	Input			
b<2>	Input			
b<1>	Input			
b<0>	Input			
a<3>	Input			
a<2>	Input			
a<1>	Input			

#	Group	I/O Direction	Loc	I/O Std.	Vref	V
4	s	Output				
4	b	Input				
4	a	Input				

Fig. 11 I/O and O/P description of parallel Adder.

Conclusion

This study develops a safe encryption system that util ized FPGA technology in order to enable quick recov ery. The design performance was compared to various FPGA device families. Additional methods, like using one key as a public key and the other as a private key, can be employed in future work to enable greater complexity. Expanding keys will be useful as well. The Vertex 7 FPGA package ensures that the suggested secure parking system architecture is enhanced with Xilinx 14.7. Government equipment speeds up marketing time, lowers expenses, and increases output. Rapid reaction is provided by an FPGA-based parking system. Time savings and safe are the main advantages[8].

References

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, “Title of paper if known,” unpublished.2020

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.2020.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[8] K. Nagaraju1 , B. Alekhya2 , Namrata Vilas Sarode3 , and N. Manogna4, “Secure Car Parking System Using VHDL” ISSN: 2347-5552, Volume-10, Issue-6, November 2020.

[9] A. A. Tawfik, A. D. Elbayoumy, M. Hussein and A. H. Elghandour, "A New Security Mechanism for MIL-STD-1553 Using Authenticated Encryption Algorithms," 2020 6th International Conference on Computing and Informatics (ICCI), New Cairo - Cairo, Egypt, 2020, pp. 115-119, doi: 10.1109/ICCI61671.2024.10485025.

[10] T. P. Ramesh, S. Kumar, P. A. Ravi and A. K. Jouhari, "Simulation of Smart Sensors in Automobile using VHDL," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2019, pp. 299-302. keywords: {Smart Sensors;FSM;Modeling;WSN;VHDL},

[11] R. Amdouni, M. Gafsi, M. A. Hajjaji and A. Mtibaa, "FPGA implementation of a chaos-Towfish-based cryptosystem for medical image security," 2022 IEEE 21st international Ccnference on Sciences and Techniques of

Automatic Control and Computer Engineering (STA), Sousse, Tunisia, 2022, pp. 283-288, doi: 10.1109/STA56120.2022.10019069.

[12] M. Feldhofer, "An authentication protocol in a security layer for RFID smart tags," Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (IEEE Cat. No.04CH37521), Dubrovnik, Croatia, 2004, pp. 759-762 Vol.2, doi: 10.1109 /MEL CON .2004.1347041.

[13] D. Pradhan, B. K. Meher and P. K. Meher, "Digit-Size Selection for FPGA Implementation of Generic Digit-Serial Multiplication Over GF(2m)," 2020 1st International Conference on Circuits, Power and Intelligent Systems (CCPIS), Bhubaneswar, India, 2020, pp. 1-6, doi: 10.1109/CCPIS59145.2023.10291975.

[14] N. Alsaffar, W. Elmedany and H. Ali, "Application of RC5 for IoT devices in Smart Transportation System," 2019 8th International Conference on Modeling Simulation and Applied Optimization (ICMSAO), Manama, Bahrain, 2019, pp. 1-4, doi: 10.1109/ICMSAO.2019.8880351. keywords: {Encryption;Internet of Things;Hardware;Field programmable gate arrays;Registers;Smart transportation;IoT;ITS;RC5;VHDL;FPGA},