Nuclear Engineering and Technology 53 (2021) 3327–3334

Contents lists available at ScienceDirect

Nuclear Engineering and Technology

journal homepage: www.elsevier.com/locate/net

Original Article

Smart grid and nuclear power plant security by integrating cryptographic hardware chip

Niraj Kumar [a], Vishnu Mohan Mishra [b], Adesh Kumar [c, *]

[a] Department of Electronics & Communication Engineering, Uttarakhand Technical University, Dehradun, India
[b] Bipin Tripathi Kumaon Institute of Technology Dwarahat, Uttarakhand, India
[c] Department of Electrical & Electronics Engineering, School of Engineering, University of Petroleum and Energy Studies, Dehradun, India

ARTICLE INFO

Article history:
Received 16 February 2021
Received in revised form
16 April 2021
Accepted 5 May 2021
Available online 9 May 2021

Keywords:
Smart grid security
FPGA Synthesis
Cryptography
TACIT Algorithm
VHDL

ABSTRACT

Present electric grids are advanced to integrate smart grids, distributed resources, high-speed sensing and control, and other advanced metering technologies. Cybersecurity is one of the challenges of the smart grid and nuclear plant digital system. It affects the advanced metering infrastructure (AMI), for grid data communication and controls the information in real-time. The research article is emphasized solving the nuclear and smart grid hardware security issues with the integration of field programmable gate array (FPGA), and implementing the latest Time Authenticated Cryptographic Identity Transmission (TACIT) cryptographic algorithm in the chip. The cryptographic-based encryption and decryption approach can be used for a smart grid distribution system embedding with FPGA hardware. The chip design is carried in Xilinx ISE 14.7 and synthesized on Virtex-5 FPGA hardware. The state of the art of work is that the algorithm is implemented on FPGA hardware that provides the scalable design with different key sizes, and its integration enhances the grid hardware security and switching. It has been reported by similar state-of-the-art approaches, that the algorithm was limited in software, not implemented in a hardware chip. The main finding of the research work is that the design predicts the utilization of hardware parameters such as slices, LUTs, flip-flops, memory, input/output blocks, and timing information for Virtex-5 FPGA synthesis before the chip fabrication. The information is extracted for 8-bit to 128-bit key and grid data with initial parameters. TACIT security chip supports 400 MHz frequency for 128-bit key. The research work is an effort to provide the solution for the industries working towards embedded hardware security for the smart grid, power plants, and nuclear applications.

1. Introduction

An electrical grid is an interconnected network of generating stations, electrical substations, and high voltage transmission lines [1] to deliver electricity from producers to consumers. The delivery of electric power supply using electrical transmission grid and nuclear power plant (NPP) switchyard, has been considered one of the most reliable and secure electric power. It mitigates the accidents and safe in an emergency shutdown in plant operations [2]. Smart grid improves [3,4] and deploys the next-generation electric grid using automated controls, advanced monitoring, and maintaining demand-response load management, etc. into the electric power transmission and distribution system. The Energy Independence and Security Act (EISA) was regularized in the United States in 2007 to revolutionize the nation's electricity transmission and distribution. The smart grid is the new technology that focuses on areas of renewable energy resources, power electronics, and communication technology to establish a more eco-friendly, economic, reliable, secured, and sophisticated electric power system. The power industries are required to transform electricity to meet the requirements of the customers and cope with the latest supporting tools and establish a modern society enabled with digital technology. The architecture of a smart grid [5,6] consists of a network of different nodes, communication systems, and primary nodes such as substations, power generation stations, and energy appliances. A smart grid has different power electronics interface circuits, and many types of renewable resources are used to produce energy such as photovoltaic (PV), wind turbine, and battery storage system. An electrical distribution network consists of two

* Corresponding author.
E-mail addresses: adeshmanav@gmail.com, adeshkumar@ddn.upes.ac.in (A. Kumar).

https://doi.org/10.1016/j.net.2021.05.006

subsystems. These subsystems are the transmission subsystem and distribution subsystem. In the transmission system, the electricity is moved in bulk over AC and DC lines. The AC lines are ranging from 345 kV to 800 kV. The power is distributed to consumers at 132 kV and flows in one direction. However, a smart grid provides smart metering from both directions and tracks the amount of electricity consumed. In the conceptual model of NIST [7], seven logical domains are proposed for a smart grid: bulk power generation, transmission, distribution, customers, consumers, service provider, markets, and operations [8]. Bulk Generation, transmission, distribution, customers are for information flow and two-way power flow. Markets, service providers, and operations are for power management and information collection. The diagram shown in Fig. 1, supports millions of local area networks and backbone networks.

For interconnecting all the domains, the communication network [9,10] should follow the hierarchy and must be perfectly distributed, as conceptualized in Fig. 2. The use of a backbone network is to establish intercommunication. The backbone network consists of infrastructure nodes, which can be either high bandwidth routers to forward messages or gateways for local area networks, in different domains of the smart grid. Fiber optical technology [11,12] as conventional wireless communication can be used in the backbone architecture to achieve bulk data and high speed.

The power distribution system has SCADA as centralized control system [14,15]. It is used for controlling and monitoring of distribution system. It has four main blocks. Human Machine Interface (HMI) is used to process the data, a supervisory computer that is used to collect all the data and process it, Remote Terminal Unit (RTU) and Programmable Logic Controllers (PLC) [16,15]. With the help of certain dedicated lines, internet subsystem, SCADA systems are connected in a smart grid. NIST has initiated a group Cyber Security Coordination Task Group (CSCTG) [15], which addresses the policies for the smart grid. Cybersecurity can be protected using hardware with the help of smart switches used to perform traffic control, manage data flow, access control. The cyber threats and need for grid security are increasing day by day as the number of distribution units and consumers are increasing.

2. Related work

Nuclear power plant works on multi-operating conditions [17] with different power mode. The systems need more advanced technologies to realize condition monitoring to improve accuracy and efficiency. Nuclear power plants are an inherent part of the future smart grid [6]. Therefore, it is essentially required to consider the safety of smart grid communication infrastructure, to meet minimum failures and accidents. Smart grids are facing the challenges of vulnerable attacks as the IoT devices are integrated with the grid [15]. The IoT-based smart grid has millions of nodes communicating online, can face cyber-attacks. The cyber-attacks on a smart grid would have shattering effects on the reliability of the extensive infrastructure of the power grid since most of the appliances in our offices, hospitals, homes, and trains need the power to run. Smart grid attacks were categorized based on past attacks and incidents that happened on grid control systems [18] and big data analysis was carried on the data generated from the specific security device.

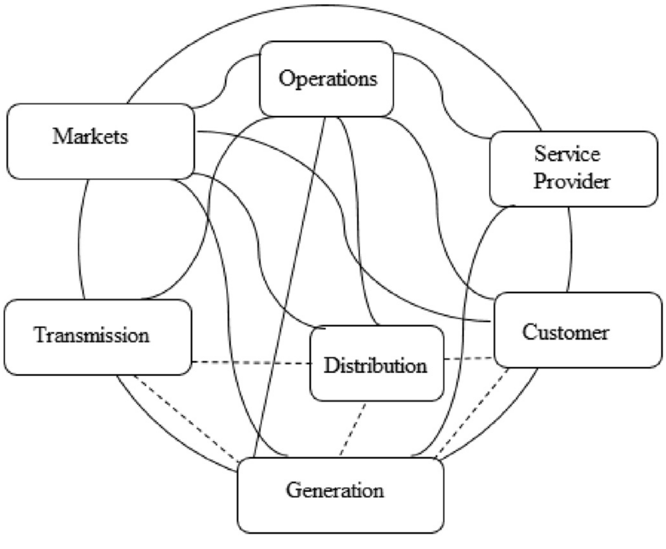

Fig. 1. Smart grid: a general model.

The adoption of FPGA technology for existing hardware replacement will enhance the system reliability for the safety and security issues in the nuclear plant. It is helpful to prevent instrumentation and control hardware failure and delays in communication within and between the systems [19]. PLC-based systems [20] can be replaced by FPGA in the nuclear power plant. FPGA is a hardware platform that configures a prototype version with a specific FPGA controller, then hazard analysis is required on FPGA software to check the feasibility of the system. FPGA chips [14] have been used extensively in nuclear power plants for instrumentation and control systems in the last 15–17 years. The nuclear power plant and grid security are addressed by embedding the FPGA-based hardware system in control networks to provide cybersecurity with high levels of reliability. The system was having a Detection on Attacking Control System (DACS), managing attacks with a central monitoring system (CMS) [21], to handle the real-time packets transfer to the destination using TCP protocols by embedding the FPGA. VHDL is a strong language used for the verification of FPGA-based Engineered Safety Features – Component Control System (ESF-CCS) for instrumentation and control in nuclear power plant [22].

The integration of software and FPGA hardware in nuclear plants ensures safety and security [23]. In the nuclear power plant, software verification is very vital and should be accomplished for safety and security at the system level. Software testing is one of the essential requirements for nuclear safety [24]. FPGA was used for wireless monitoring [2] in the power plant with the integration of GSM technology for hardware safety. The designed hardware chip was used to monitor the parameters of the boiler, generator turbine, and conveyer belt. VHDL programming was used for simulation and Virtex-5 FPGA for synthesis.

The smart grid has SCADA [25,26] as a core subsystem. SCADA performs power operation monitoring, transmission, and distribution. Many vendors offer SCADA solutions [8], in which power signals samples are delivered in transmission and distribution fields via a backbone network for centralized management. It follows high volumes of AC and DC facilities [27], for long-distance transmission. Moreover, underground cables can be used, in case of overhead lines are not possible. High-temperature superconducting cables can be used for electrical transmission because of their features such as low voltage drop, lightweight [10], fewer line losses, large current carrying capacity, and better performance. Advanced Flexible AC Transmission System (FACTS) and high voltage DC (HVDC) devices are used to provide flexible transmission, high power control, and communication that improve the grid in a faster and stable way and make the grid to be free from congestion. A smart grid uses wireline communication as well as wireless communication technologies [9] for sensing and monitoring the status of the sensors, and measuring line parameters

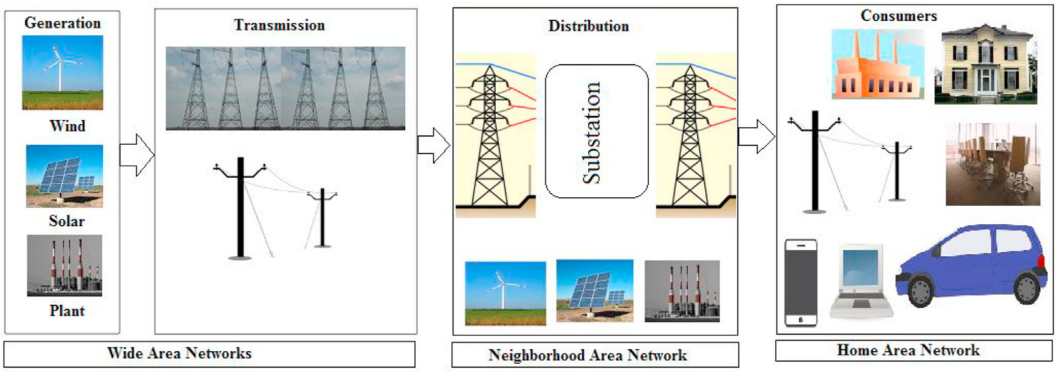

Fig. 2. Smart grid network architecture: with backbone and LANs [13].

[11]. The popular wireless technologies used in smart grids are wifi, Zigbee, etc. The sensors help to detect line failures, towers, identification of fault locations, and conductor temperature, etc. The integration of wireless technology in smart grids provides numerous advantages such as low-cost solutions, mobility, and untethered access to utility information.

Cybersecurity [16,21] is one of the biggest challenges for the smart grid. According to the guidelines [7] of NIST, smart grid objectives are depending on three security requirements. Availability, confidentiality, and integrity [28] are the main security objectives of the smart grid. Smart grid has an open network over a larger area. It is a big challenge in the smart grid to balance information security and communication efficiency. Smart grid networks have millions of electronics devices and users. User authentication and device identification are essential, and verification is a prerequisite for granting the service in the smart grid.

3. Problem and proposed solution

The nuclear power plant has issues in system safety, security, critical, and emergency preparedness that is inaccessible through the internet and IT networks [19,22]. This inaccessibility is usually possible using one-way communication hardware. Different procedural controls are used to avoid the illegal use of gateway and media equipment on the control network, which are typically separated based on management authority, function, or the number of traffic infrastructures during usual operation. The boundary control devices are imposed on several divisions of the network. These devices are intrusion detection systems, unidirectional gateways, firewalls, routers, and encrypted tunnels, in which the hardware security is controlled using control networks and applying security algorithms against insider threat by providing the training, behavioral observations, and security screening. The smart grid sever can communicate directly to intelligent electronic devices (IEDs) [20] which can be programmed based on the sensor data and readings without inputs received from the control server. The problem is that these IEDs do not have sufficient processing and computing capability to integrate common security challenges such as password protection, data encryption, and decryption. Microcontrollers, FPGAs [18,24], DSP processors are the latest hardware solutions that can be integrated to enhance the nuclear plant and smart grid hardware security [29].

The cryptographic-based approach [3,12] is a good solution for grid security in communication system hardware to protect information and secure communication. The design of the encryption and decryption algorithms in grid hardware is essential to provide data confidentiality in the smart grid. Encryption can be based on both symmetric and asymmetric key techniques. In the symmetric key technique, the same key is shared at both ends, encryption, and decryption [30]. Examples of such algorithms are AES [13], DES algorithms. In the asymmetric key approach, the private key is used to encrypt/decrypt the data at the transmitting and receiving end. There are a couple of research papers on network cryptographic encryption and decryption, but all the algorithms are limited to their text size and key size. F. Crope et al. (2011*)* suggested a new algorithm named TACIT [31] in which, it is possible to keep the block size and key size of 'N' bit. The algorithm provides good results in case of key size is kept greater than the block size. The hardware chip implementation of the algorithm is a big challenge especially in network security [21]. The grid and nuclear plant security can be enhanced with the implementation of the TACIT in hardware and integrated with FPGA [3]. The chip design for the TACIT algorithm and implementation on System-on-Programmable-Chip (SoPC) on FPGA will enhance the real-time security and data protection of the smart grid. The chip integration with hardware and related embedded devices in the grid will enhance the communication infrastructure. The research paper is not focusing on modification in a TACIT algorithm, but the hardware chip design is the new research work, and the chip synthesis on Virtex −5 FPGA guarantees the feasibility of the algorithm in smart grid hardware and nuclear plant security. The authors of the research paper [31] expressed that the algorithm is not integrated with hardware yet, only developed in C and C^{++} software programming languages. Based on this research gap and identification, it is formulated that the TACIT algorithm can be implemented in hardware chips using VHDL, and FPGA integration will be an added advantage for smart grid and nuclear plant monitoring and information security systems. The TACIT Encryption includes the following sequences.

Step 1 In the initial, read the text file and the technique of initial permutation to shuffle the location of each character in block text using key value.
Step 2 Each character is read from the text file against complete text and obtain the ASCII value of all the characters.
Step 3 XOR operation is applied for the 'n' bit key value and corresponding text value.
Step 4 Use TACIT Logic (n^k xor k^k) is employed and follow some specific operations. Here 'n' is the value computed from step 3.
Step 5 Convert the TACIT logic results into binary, obtained from step 4.
Step 6 Reverse the binary values of the data, from step 5.
Step 7 Get the decimal value against each binary data.

Step 8 The Unicode character is formed corresponding to their corresponding decimal value, which is represented as ciphertext.
Step 9 All the steps are followed for the next characters also until the entire file is completed.

In the same way, the TACIT decryption algorithm [31] steps are given below

Step 1 The ciphertext is encoded and obtained the decimal value of the text. Start the characters reading from the first character against ciphertext.
Step 2 Evaluate the corresponding binary value, further reverse it.
Step 3 Apply the TACIT logic here again but in a reverse way.
Step 4 XOR logical operation is applied with the n-bit key value.
Step 5 Determine the ASCII characters correspond to the binary values obtained from step 5.
Step 6 Now, reshuffling is required with the help of key value.
Step 7 All the steps are followed until full ciphertext is not completed.

4. Design methodology

The finite state machine (FSM) and behavior modeling are used to model the TACIT encryption algorithm. The encryption logic is designed in 8 states based on the one-hot encoding machine. In state-0 the key value of the encryption logic is converted into a binary value. In state-1, the input text value is logically XORed with the value of the key. The TACIT logic is n^k XOR k^k, not possible to implement directly. Therefore, there is a need for two states to implement the logic. In state-2, logic n^k is implemented, and logic k^k is implemented in state-3. In the state-4, actual logic is XORed to get the actual value of TACIT. In state-5, the value of the TACIT logic is changed by reversing the sequence from LSB to MSB and vice versa. In state-6, the decimal value of the corresponding digit is determined which nothing, but the ciphertext is. The actual binary ciphertext is read in state-7. There is the need to convert the logic into their equivalent ASCII values, which is done in state 8 using VHDL programming. The reverse FSM is applied to decrypt the grid data. The FSMs are depicted in Figs. 3 and 4 for encryption and decryption respectively.

5. Results & discussions

The simulation and synthesis results are extracted from Xilinx ISE 14.7 Software. The generated RTL view is depicted in Fig. 5. The explanation of all the pins is detailed in Table 1.

Figs. 6 and 7 show the simulation results of 64-bit block size encrypted/decrypted with 64-bit key value in hexadecimal, 128-bit block size encrypted/decrypted with 128-bit key value in ASCII, 128-bit block size encrypted/decrypted with 128-bit key value in hexadecimal, and 128-bit block size encrypted/decrypted with 128-bit key value in ASCII.

Test-1 (64-bit key): grid_data_in (64-bit) = 1′h4D65746572204F4E = “01001101 01100101 01110100 01100101 01110010 00100000 01001111 01001110” in binary or (Meter ON) in ASCII. The key (64-bit) = 1'h4164657368403132 (hexadecimal), = “01000001 01100100 01100101 01110011 01101000 01000000 00110001 00110010” in binary or Adesh@12 (in ASCII). Mode_selection = '1' and enable = ‘1’ in encryption and Mode_selection = '0' and enable = ‘0’ in decryption and clk of 50% duty cycle is applied. After the decryption the same grid_data_out (64-bit) is achieved. The simulation is performed with the grid parameters assumptions: Primary Voltage = 220 V, Secondary Voltage = 145 V, Frequency = 50 Hz, grid temperature = 55 °C, and Power = 5W.

Test-2 (128-bit key): grid_data_in (128-bit) = 1′h 47726964204F4E204D65746572204F4E = “01000111 01110010 01101001 01100100 00100000 01001111 01001110 00100000 01001101 01100101 01110100 01100101 01110010 00100000 01001111 01001110” in binary or (Grid ON Meter ON) in ASCII. The key (128-bit)= 1'h 55504553556E69766572736974794040 (hexadecimal) = “01010101 01010000 01000101 01010011 01010101 01101110 01101001 01110110 01100101 01110010 01110011 01101001 01110100 01111001 01000000 01000000” in binary or UPESUniversity@@(in ASCII). Mode_selection = '1' and enable = ‘1’ in encryption and Mode_selection = '0' and enable = ‘0’ in decryption and clk of 50% duty cycle is applied. After the decryption the same grid_data_out is achieved. The simulation is performed with the grid parameters assumptions: Primary Voltage = 220 V, Secondary Voltage = 145 V, Frequency = 50 Hz, grid temperature = 85 °C and Power = 5W.

The hardware utilization report contains the percentage utilization of hardware such as the number of slices, input LUTs, flip-flops, bounded IOBs, and global clock (GCLK) required in the design of the chip. The report also includes detailed information about the timing-related parameters such as the detail of maximum frequency, minimum period, minimum time required before clk, maximum time after clk, and combinational path delay. The memory required in the design is also reported by the hardware summary report. The targeted FPGA is Virtex-5 with xc5vlx20t-2-ff323 device and synthesis is carried for the same to keep hardware design parameters as optimal. The detail of the hardware and timing parameters is given in Tables 2 and 3.

Figs. 8 and 9 present the graph corresponding to the hardware resources utilization and timing-related parameters for different key sizes (8-bit, 16-bit, 32-bit, 64-bit, and 128-bit). The grid data is experimentally verified on LEDs of the Virtex-5 (xc5vlx20t-2-ff323) FPGA byte by byte. The hardware utilization is increasing as the grid data and key size are increasing. It is also noticed that the time-related parameters such as delay and frequency support to the device are increasing with key size. The hardware parameters reported in Tables 2 and 3 are directly extracted from the Xilinx ISE software. The device hardware utilization depends on the occupied number of logic gates, buffers, multiplexers, decoders, latches, flip-flops, etc., on targeted FPGA. The number of slices is 192, 208, 216, 225, and 248 for 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit key encryption/decryption respectively. The number of flip-flops are 172, 188, 192, 200 and 214 for 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit key encryption/decryption respectively. The number of LUTs are 48, 54, 58, 64, and 80 for 8-bit, 16-bit, 32-bit, 64-bit, and 128-bit key encryption/decryption respectively. The FSM computes more operations relating to XOR, shifting, bit reversing operations for encryption and decryption that enhances the utilization of the number of logic gates, slices, LUTs, and flip flops with the key size for the targeted FPGA. The larger key size enhances the number of transform cycles for the designed chip of encryption and decryption that enhances the combinational path delay, minimum and maximum timing of the clock. The performance of the chip is evaluated based on the maximum frequency support for the FPGA hardware. The frequency support of the designed chip is increasing from 235 MHz to 400 MHz with grid block data key of 8-bit to 128-bit encryption-decryption that signifies faster switching response of chip with larger key size and grid data.

6. Conclusions

SCADA system is the main important part of the smart grid, used

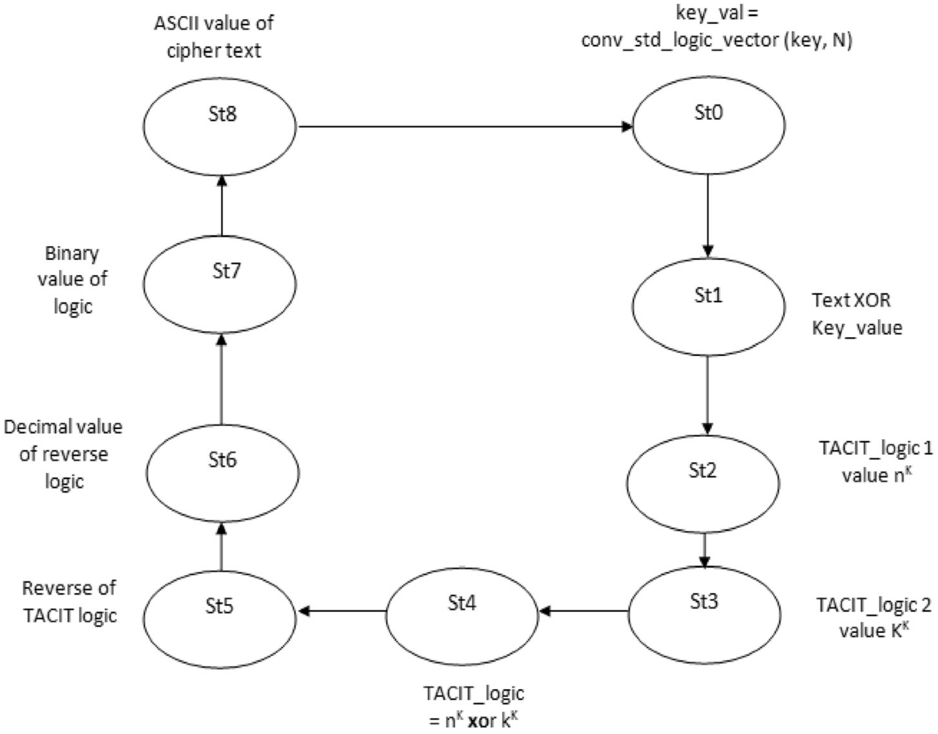

Fig. 3. FSM state diagram of the encryption.

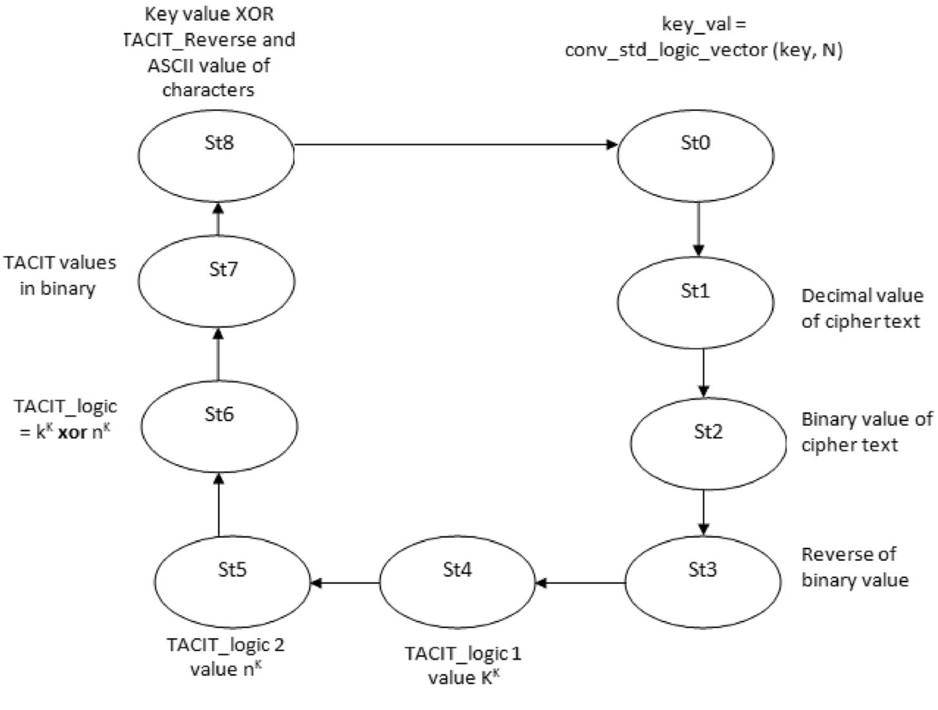
Key value XOR TACIT_Reverse and ASCII value of characters
key_val = conv_std_logic_vector (key, N)
St8
St0
TACIT values in binary
St7
St1
Decimal value of cipher text
TACIT_logic = k^K xor n^K
St6
St2
Binary value of cipher text
St5
St4
St3
Reverse of binary value
TACIT_logic 2 value n^K
TACIT_logic 1 value K^K

Fig. 4. FSM state diagram of the decryption.

to fulfill two main purposes one for the public control system and second is the public transport system. Different vendors are using self-products as the part of SCADA system similar to our computer systems. Therefore, there are chances of cyber-attacks and threats. The research paper addressed the smart grid and nuclear power plant security issues in hardware. The grid security can be improved with the integration of cryptographic encryption and a decryption-based chip. The proposed TACIT algorithm has shown good results and simulated data is tested for different test cases. The functional simulation is carried successfully in Xilinx ISE 14.7. The greatest advantage of the proposed algorithm is that it can have the key size of 'N' bit. Cybersecurity is an integral part of grid security concerns. It is essentially required that the smart grid must be free from security concerns for its modern infrastructure and

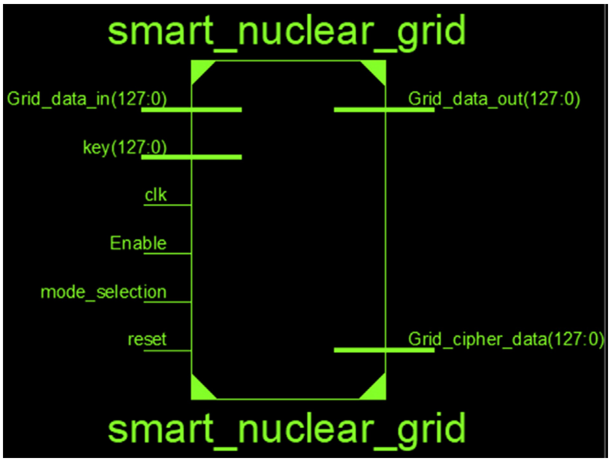

Fig. 5. RTL view of the designed chip.

Table 2
Hardware parameters summary as FPGA synthesis report.

Hardware Parameter/Key Size	8-bit	16-bit	32-bit	64-bit	128-bit
Slices	192	208	216	225	248
Slice Flip-flops	172	188	192	200	214
LUTs	48	54	58	64	80
Bounded IOBs	132	132	132	132	132
GCLK	1	1	1	1	1

popularity. The TACIT cryptographic encryption and decryption algorithm is successfully synthesized on Virtex-5(xc5vlx20t-2-ff323) FPGA, ranging from 8-bit to 128-bit key size and grid data. The simulation test cases also assure successful data communication with 64-bit and 128-bit key and grid data. The grid data can be integrated with embedded hardware and FPGA to provide grid data security from the distribution end to consumers or vice versa. In the future, grid security can be enhanced with a larger key size and grid block size with compression of data packets.

Table 1
Pins explanation in TACIT encryption/decryption chip.

Pins	Description
Grid_data_in (128-bit)	In the TACIT implementation, we have taken 128-bit plaintext input, which is encrypted with the help of different key sizes (8-bit, 16-bit, 32-bit, 64-bit, and 128-bit). It can vary up to 'n' bit.
Clock (1-bit)	It is the input pin attached to the FPGA pin to give the clock as a default input signal
Reset (1-bit)	It is an input pin to reset all the contents. If reset = '1', then all the contents will be zero.
Mode_selection (1-bit)	It decides the logic to work either in encryption mode or decryption mode. In encryption mode, mode_selection = '1' and in decryption mode, mode_selection = '0'.
Enable (1-bit)	It is the input logic used to enable or disable encryption and decryption logic. For encryption logic, enable = '1' otherwise decryption logic for enable = '0'
Grid_cipher_text (128-bit)	It is the value of the encrypted text generated by the TACIT encryption process. It is 128-bit in our tested design. It can vary up to 'n' bit
Grid_data_out (128-bit)	It is the output of the decryption module, generated after the completion of all steps execution of TACIT decryption. Based on plain text input, it also may be up to 'n' bit

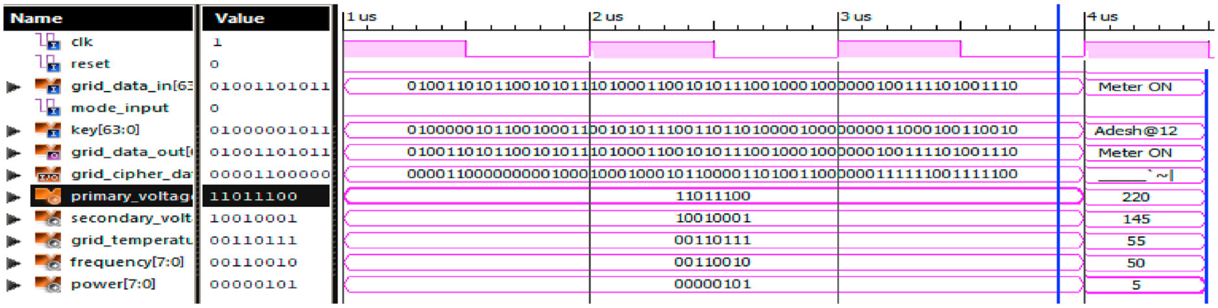
```
Name                 Value        1 us   2 us   3 us   4 us
clk                  1
reset                0
grid_data_in[63      01001101011  0100110101100101011101000110010101110010001000000100111101001110   Meter ON
mode_input           0
key[63:0]            01000001011  0100000101100100011001010111001101101000010000000011000100110010   Adesh@12
grid_data_out[(      01001101011  0100110101100101011101000110010101110010001000000100111101001110   Meter ON
grid_cipher_da       00001100000  00001100000000001000100010001011000011010011000000111111001111100  ______`~|
primary_voltag       11011100     11011100   220
secondary_volt       10010001     10010001   145
grid_temperatu       00110111     00110111   55
frequency[7:0]       00110010     00110010   50
power[7:0]           00000101     00000101   5
```

Fig. 6. Xilinx ISE 14.7 simulation for grid data and key size (64-bit).

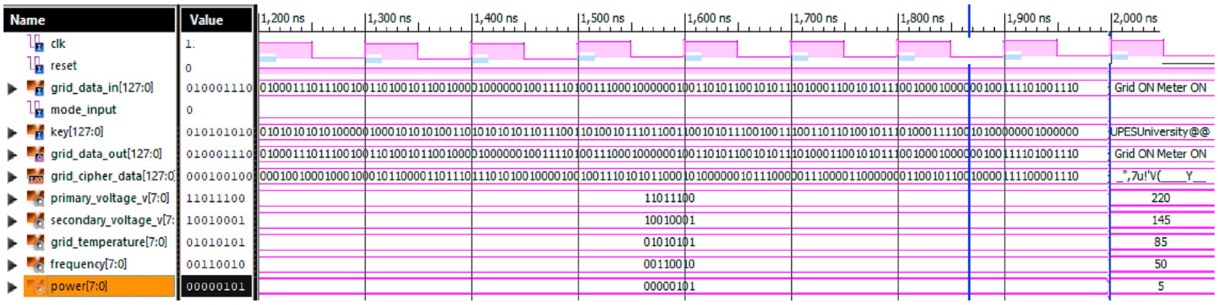
```
Name                     Value      1,200 ns  1,300 ns  1,400 ns  1,500 ns  1,600 ns  1,700 ns  1,800 ns  1,900 ns  2,000 ns
clk                      1
reset                    0
grid_data_in[127:0]      010001110  01000111011100100110100101100100001000000100111101001110001000000100110101100101011101000110010101110010001000000100111101001110  Grid ON Meter ON
mode_input               0
key[127:0]               010101010  01010101010100000100010101010011010101010110111001101001011101100110010101110010011100110110100101110100011110010100000001000000  UPESUniversity@@
grid_data_out[127:0]     010001110  01000111011100100110100101100100001000000100111101001110001000000100110101100101011101000110010101110010001000000100111101001110  Grid ON Meter ON
grid_cipher_data[127:0]  000100100  00010010001000100010110000110111101111010100100001001001110101011000010100000010111000001110000110000001100101100100001111 00001110  _",7u!'V(____Y__
primary_voltage_v[7:0]   11011100   11011100   220
secondary_voltage_v[7:   10010001   10010001   145
grid_temperature[7:0]    01010101   01010101   85
frequency[7:0]           00110010   00110010   50
power[7:0]               00000101   00000101   5
```

Fig. 7. Xilinx ISE14.7 simulation for grid data and key size (128-bit).

Table 3
Timing results of smart grid TACIT chip.

Timing Parameter/Key Size	8-bit	16-bit	32-bit	64-bit	128-bit
Frequency (MHz)	235.00	315.00	365.00	380.00	400.00
Minimum Period (ns)	1.1097	1.2641	1.3213	1.4010	1.5261
Minimum time before clk(ns)	3.1657	3.2911	3.4121	3.5626	3.9527
Maximum time after clock(ns)	4.0478	4.2910	4.3230	4.6131	5.1200
Combinational delay(ns)	8.912	9.0174	9.2626	9.7134	9.9512
Memory usage (kB)	241381	256728	324183	641952	893217
Speed grade	−5	−5	−5	−5	−5

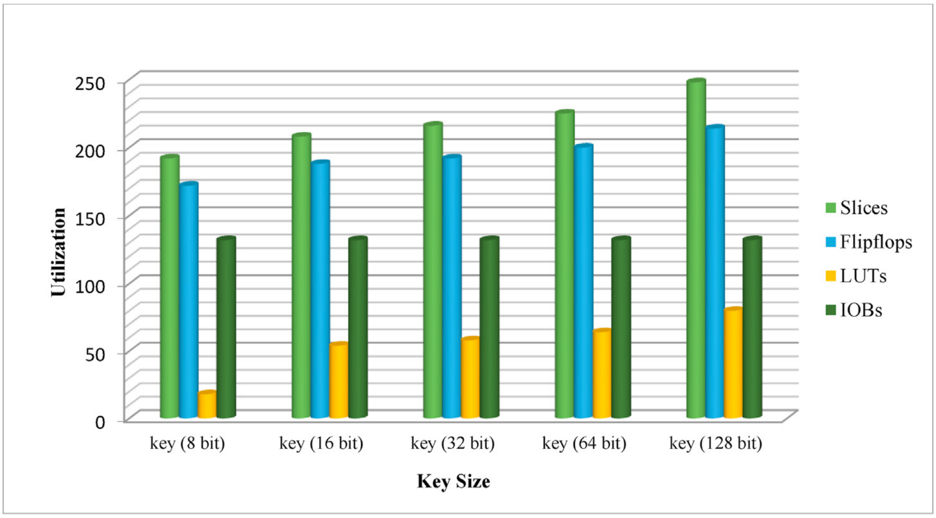

Fig. 8. Hardware summary as FPGA parameters.

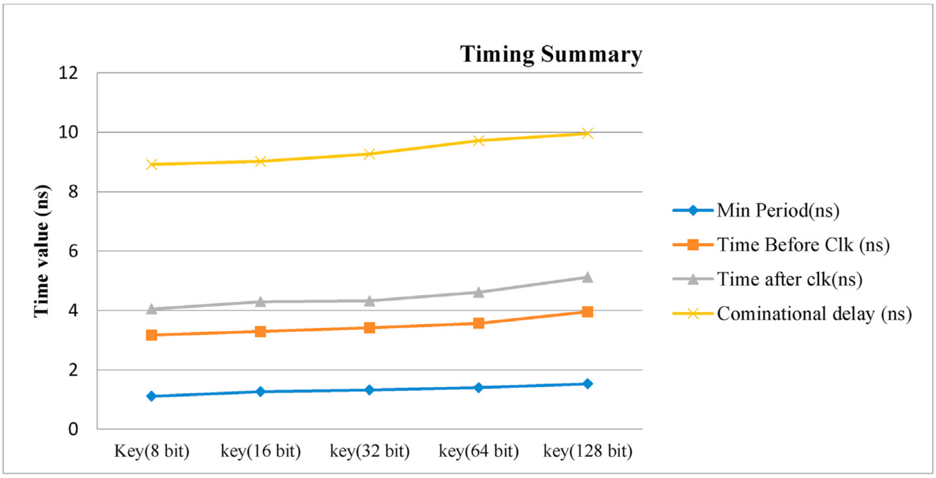

Fig. 9. Timing related parameters utilization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. Dubey, G. Karsai, P. Volgyesi, M. Metelko, I. Madari, H. Tu, S. Lukic, Device access abstractions for resilient information architecture platform for smart grid, IEEE Embed. Syst. Lett. 11 (2) (2018) 34–37, https://doi.org/10.1109/LES.2018.2845854.

[2] A. Kumar, K. Bansal, D. Kumar, A. Devrari, R. Kumar, P. Mani, FPGA application for wireless monitoring in power plant, Nucl. Eng. Technol. 53 (2020) 1167–1175, https://doi.org/10.1016/j.net.2020.09.003.

[3] A. Kumar, P. Kuchhal, S. & Singhal, Secured Network on Chip (NoC) architecture and routing with modified tacit cryptographic technique, Procedia Comput. Sci. 48 (2015) 158–165, https://doi.org/10.1016/j.procs.2015.04.165.

[4] A. Kumar, P. Vishnoi, S.L. Shimi, Smart grid security with cryptographic chip integration, EAI Endorsed Trans. Energy Web 6 (23) (2019) 1–12, https://doi.org/10.4108/eai.13-7-2018.157037.

[5] D. Mashima, Securing smart-grid infrastructure against emerging threats, in: Solving Urban Infrastructure Problems Using Smart City Technologies, 2021, pp. 359–382, https://doi.org/10.1016/B978-0-12-816816-5.00016-4.

[6] E. Brezhniev, O. Ivanchenko, NPP-smart grid mutual safety and cyber security assurance, in: Cyber Security and Safety of Nuclear Power Plant

Instrumentation and Control Systems, 2020, pp. 349–380, https://doi.org/10.4018/978-1-7998-3277-5.ch014.

[7] Report to NIST on smart grid interoperability standards roadmap EPRI, Jun. 17, http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf, 2009.

[8] A.R. Metke, R.L. Ekl, Security technology for smart grid networks, IEEE Trans. Smart Grid 1 (1) (2010) 99–107, https://doi.org/10.1109/TSG.2010.2046347.

[9] L. Chhaya, P. Sharma, G. Bhagwatikar, A. Kumar, Wireless sensor network based smart grid communications: cyber-attacks, intrusion detection system and topology control, Electronics 6 (1) (2017) 5, https://doi.org/10.3390/electronics6010005.

[10] L. Chhaya, P. Sharma, A. Kumar, G. Bhagwatikar, Communication theories and protocols for smart grid hierarchical network, J. Electr. Electron. Eng. 10 (1) (2017) 43.

[11] L. Chhaya, P. Sharma, G. Bhagwatikar, A. Kumar, Development of wireless data acquisition and control system for smart microgrid, in: Advances in Smart Grid and Renewable Energy, Springer, Singapore, 2018, pp. 667–673, https://doi.org/10.1007/978-981-10-4286-7_66.

[12] M.A. Ferrag, A. Ahmim, Security solutions and applied cryptography in smart grid communications, IGI Global (2016) 464, https://doi.org/10.4018/978-1-5225-1829-7.

[13] N. Kumar, V.M. Mishra, A. Kumar, Smart grid security with AES hardware chip, Int. J. Inf. Technol. 12 (1) (2020) 49–55, https://doi.org/10.1007/s41870-018-0123-2.

[14] A. Kovalenko, I. Babeshko, V. Tokarev, K. Leontiiev, FPGA technology and platforms for NPP I&C systems, in: Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems, 2020, pp. 419–457, https://doi.org/10.4018/978-1-7998-3277-5.ch016.

[15] K. Kimani, V. Oduol, K. Langat, Cyber security challenges for IoT-based smart grid networks, Int. J. Crit. Infrastruct. Protect. 25 (2019) 36–49, https://doi.org/10.1016/j.ijcip.2019.01.001.

[16] G. Dileep, A survey on smart grid technologies and applications, Renew. Energy 146 (2020) 2589–2625, https://doi.org/10.1016/j.renene.2019.08.092.

[17] B. Peng, H. Xia, X. Ma, S. Zhu, Z. Wang, J. Zhang, A mixed intelligent condition monitoring method for nuclear power plant, Ann. Nucl. Energy 140 (2020) 107307, https://doi.org/10.1016/j.anucene.2020.107307.

[18] S. Lee, J.H. Huh, An effective security measures for nuclear power plant using big data analysis approach, J. Supercomput. 75 (8) (2019) 4267–4294, https://doi.org/10.1007/s11227-018-2440-4.

[19] M.J. Burzynski, Case for the adoption of FPGA technology in the implementation and replacement of equipment and systems in nuclear power plants, ISOFIC (2017) 1–10, https://doi.org/10.1109/ACCESS.2019.2951938.

[20] S. Jung, J. Yoo, Y.J. Lee, A practical application of NUREG/CR-6430 software safety hazard analysis to FPGA software, Reliab. Eng. Syst. Saf. 202 (2020) 107029, https://doi.org/10.1016/j.ress.2020.107029.

[21] J.H. Roh, S.K. Lee, C.W. Son, C. Hwang, J. Kang, J. Park, Cyber security system with FPGA-based network intrusion detector for nuclear power plant, in: IECON 2020 the 46th Annual Conference of the IEEE Industrial Electronics Society, 2020, pp. 2121–2125, https://doi.org/10.1109/IECON43393.2020.9255158.

[22] R. Maerani, J.C. Jung, VHDL verification of FPGA based ESF-CCS for nuclear power plant I & C system, ISOFIC (2017) 1–6.

[23] W. Wang, Zhuo Lu, Cyber security in the smart grid: survey and challenges, Comput. Network. 57 (2013) 1344–1371, https://doi.org/10.1016/j.comnet.2012.12.017.

[24] W. Xiong, T. Bai, P.F. Gu, H.H. Liang, J.Z. Tang, Research on static testing technology of nuclear safety-critical software based on FPGA technology, in: International Symposium on Software Reliability, Industrial Safety, Cyber Security and Physical Protection for Nuclear Power Plan, 2019, pp. 516–523, https://doi.org/10.1007/978-981-15-1876-8_50.

[25] K. Sayed, H.A. Gabbar, SCADA and smart energy grid control automation, Smart Energy Grid Eng. (2017) 481–514, https://doi.org/10.1016/B978-0-12-805343-0.00018-8.

[26] M.A. Ferrag, M. Babaghayou, M.A. Yazici, Cyber security for fog-based smart grid SCADA systems: solutions and challenges, J. Inf. Secur. Appl. 52 (2020) 102500, https://doi.org/10.1016/j.jisa.2020.102500.

[27] J. Kim, E.S. Kim, J. Yoo, Y.J. Lee, J.G. Choi, An integrated software-testing framework for FPGA-based controllers in nuclear power plants", Nucl. Eng. Technol. 48 (2) (2016) 470–481, https://doi.org/10.1016/j.net.2015.12.008.

[28] S. Iyer, Cyber security for smart grid, cryptography and privacy, Int. J. Data Min. Bioinf. 372020 (2011) 1–8, https://doi.org/10.1155/2011/372020.

[29] EPRI 1019187, Technical Guideline for Cyber Security Requirements and Life Cycle Implementation Guidelines for Nuclear Plant Digital Systems, Electric Power Research Institute, Washington, D.C., 2010. October 29.

[30] M.M. Pour, A. Anzalchi, A. Sarwat, A Review on Cyber Security Issues and Mitigation Methods in Smart Grid Systems in Proceedings of the Southeast Con, Charlotte, 2017, https://doi.org/10.1109/SECON.2017.7925278, 2017.

[31] F. Crope, A. Sharma, A. Singh, N. Pahwa, An efficient cryptographic approach for secure policy based routing: (TACIT Encryption Technique), in: 2011 3rd International Conference on Electronics Computer Technology, vol. 5, 2011, pp. 359–363, https://doi.org/10.1109/ICECTECH.2011.5942020.