VIHS with ROTR Technique for Enhanced Light-Weighted Cryptographic System

Sanjeev Kumar A N, Ramesh Naik B
Dept. of Computer Science and Engineering
GITAM School of Technology
GITAM Deemed to be University
Bengaluru, India

Abstract—**Developing a bypass parallel processing block is one of the emerging and exciting research areas in the system encrypt/decrypt application areas. A Partial Pseudo-Random-based Hashing VIHS is the most suitable methodology for designing the system to encrypt/solve a block in cryptography. For this purpose, various VIHS and register techniques have been developed to process the storage system data. But, it is limited by the problems of reduced efficiency, increased computational complexity, high area consumption, and cost consumption. Thus, this research intends to develop a novel dynamic system register with hashing with optimal Hash Signature design to process the system's encryption /decrypt data. The main intention of this paper is to analyze the transfer characteristics of the current based on the pseudo-differential pair for a proficient system detection. Then, a system window can be created and adjusted to obtain an optimized power flow with less data loss sensitivity. The major stages involved in the proposed block design are register, partition design, and VIHS design. The dynamic system register is designed at first for getting a fast decision and to enable a low input-referred offset value. Then, the partition is formed concerning the output of the register, and the VIHS is used to produce the high proportional logical work. During performance evaluation, various measures have been utilized to analyze the performance of the proposed dynamic system register-based hashing with optimal Hash Signature design. In addition to that, the estimated results are compared with the proposed technique to prove its efficiency.**

Keywords*—*Cryptography – partial pseudo-random based hashing technique; logical to sequential VIHS; system encrypts/decrypt data; dynamic system register; bypass parallel processing

I. Introduction

Internet of Things (IoT) [1] [2] is one of the most widely used networking paradigms for establishing reliable and secured data transmission, which contains different intelligent devices that help exchange the data across the network in a secure way. Especially in the medical healthcare systems, the patients' information must be protected and secured against unauthenticated access, which guarantees the security and authenticity of the networking system. The Electrocardiogram (ECG) signals [3] [4] are mainly used to monitor the patient's health information, which providing security to this type is also one of the crucial factors. For this purpose, various techniques [5] [6] have been developed to secure the patients' medical healthcare information. Hence, disparate security frameworks and architectures have been deployed in the proposed work. This paper mainly focuses on developing the lightweight data security model for the medical ECG signal transmission system incorporated with the IoT network.

For this purpose, the Viterbi Integrated Hash Signature (VIHS) based architecture of the ECC encryption method is implemented. Here, the random keys have been generated based on the integrated architecture of Hashed signature technique. It is mainly used to reduce the complexity of the model with an enhanced working speed of the algorithm. The reduction of iteration count can reduce the size of architecture, resulting in a lightweight encryption system. Novel lightweight data encryption with an optimal key generation system is proposed for the IoT Network transmission system to overwhelm these problems. This can be achieved by extracting the signal peaks using the Viterbi algorithm to select the best value for random key generation and the fast switching process. This can be processed by referring to the parameters of distance and the phase angle-based reference properties. This will collect information about the pattern of the signature and the size of critical formation in the batch mode of the process to retrieve the topology in parallel [7] [8]. In the encryption process, a light-weighted cryptographic system by using the ROTR Messaging technique. The proposed encryption process reduces the buffer size and reduces the power consumption due to the optimal key size of the cryptographic technique. We developed the VIHS algorithm and integrated it with ROTR in the ECC encryption method. The random critical formation is referred to from the look-up table of the ECC model, and this can generate the public and private keys for the encryption process [9]. The algorithm's implementation is in progress to enhance the performance of the encryption system [10] compared to the other traditional encryption model.

The primary objectives behind this research work are as follows:

1) To develop the lightweight security model for processing the medical ECG signals in the IoT framework.
2) To ensure the system's increased security and reduced complexity, the Viterbi Integrated Hash Signature (VIHS) verification scheme is utilized.
3) The Randomized Off-the Record (ROTR) based messaging technique is employed to reduce thOff-the-Recordand power consumption of signal transmission yet.
4) To validate the proposed security framework's performance, various evaluation indicators such as error rate, throughput, transmission delay, and key selection time have been used.

The rest of the sections present in the paper are structuralized as follows: Section II discusses some of the existing security techniques used for securing the ECG signals with their advantages and disadvantages. Section III presents a detailed description of the proposed methodology with its flow illustration. The performance and comparative results of both existing and proposed techniques are validated using Section IVs performance measures. Finally, the overall paper is concluded with its future work in Section V.

II. Literature Survey

This section presents the literature review of various existing techniques used for ensuring the security of ECG signal processing and transmission systems. Also, it discusses the advantages and disadvantages of each method based on its operating principles.

Wang *et al.* [11] employed a logistic mapping-based encryption model for improving the security of WBAN. The main intention of this paper was to ensure the security and computing ability of biomedical sensors with restricted user access by using the quantized logistic mapping-based encryption technique. Here, the different types of parameters such as Power Spectral Entropy (PSD) and Peak-to-Average Power Ratio (PAPR) have been utilized to evaluate the performance of the suggested mechanism. Moreover, the Lyapunov factor has been considered in this work for analyzing the chaotic characteristics with respect to the random property of the system. In addition to that the normalized spectral entropy was computed based on the parameters of pseudo-random sequence, power spectrum, total power, sequence spectral entropy, and normalization of entropy. At last, binary quantization was also applied for increasing the retention accuracy of the overall security system. The major drawback of this work was, it has an increased complexity in designing algorithms that limits the performance of the entire system. Hameed *et al.* [12] implemented the lossless compression mechanism with Huffman coding scheme for ensuring the security of broadcast transmission in WBAN. It comprises the stages of estimating the buffer blocks, compression, and encryption, which helps to establish the secured transmission in the network. Also, this work intends to obtain the quality control compressed data by employing the cipher block-based chaining encryption algorithm. During the block creation, the QRS complex has been estimated for detecting the peak count of the signal. Consequently, the bandpass filtering technique was applied to eliminate the noisy contents based on the integer coefficients. The advantage of this work was, it efficiently reduced the error rate between the signals by estimating their similarity with high reliability.

Janveja *et al.* [13] designed an efficient AES algorithm for securely transmitting the ECG signals by deploying the modified folded architecture. Here, the key description module has been additionally incorporated with the standard AES technique with reduced functional units. Djelouat *et al.* [14] utilized a lightweight encryption scheme for developing the secured health monitoring architecture. The main considerations of this work were as follows: to obtain the reduced load on data transmission, and to establish the secured data transmission with increased reliability. For this purpose, the Compressing Sensing (CS) platform has been incorporated with this framework, which helps to perform remote monitoring in a secure way. The benefits of this framework were low transmission power, low coherence, reduced complexity in designing, and simple acquisition. Qiu *et al.* [15] suggested the selective encryption mechanism with the supervised machine learning technique for increasing the security of data privacy and effectiveness in BSNs. Here, the wavelet-based transformation technique has been utilized for compressing the sensor information efficiently. Moreover, the SVM-based machine learning classification technique was employed to classify the disease based on the frequency bands.

Mathivanan *et al.* [16] employed a QR code-based encryption algorithm for processing the ECG signals with increased security. The main factors of this paper were to obtain an increased embedding capacity and ensured security for the complete data retrieval. Moreover, the quick response code has been utilized in this work for storing the hidden information for ensuring data security. The advantages of this paper were better error correction, maximum storage efficiency, and increased data retrieval capacity. Hameed *et al.* [17] recommended an AES-based encryption algorithm for ensuring the properties of authentication, confidentiality, and integrity of the ECG signal transmission system. Here, the encryption and decryption processes were carried out based on the Electronic Code Book (ECB). Yet, the major disadvantages of using AES techniques were increased computational overhead and complexity in handling. Awasarmol *et al.* [18] utilized the DWT technique with the scrambling matrix formation approach for transmitting the ECG signals in a secured way. The main intention of this paper was to extract the secret message with the help of DWT mechanism and to eliminate the noisy contents by using the band pass filtering technique. The stages involved in this work were signal decomposition, de-noising, DWT based feature extraction, scrambling matrix formation, encryption, and decryption. The merits of this work were reduced computational time, complexity and increased accuracy.

Hameed *et al.* [19] utilized a lossless compression mechanism incorporated with the hybrid cryptography technique for securing the ECG signal processing systems. This incorporated the functionalities of Huffman coding scheme with the AES encryption mechanism for enabling a lossless data compression. Also, the Diffie-Hellman based key exchange mechanism was utilized to ensure the increased security of signal transmission. However, it requires more time for signal compression and transmission, which degrades the entire performance of the system. Shaikh *et al.* [20] employed an improved data encryption algorithm for establishing the secured ECG signal transmission. In which, the homomorphic encryption mechanism was utilized to encrypt the ECG signals of patients with ensured reliability and confidentiality. Still, this work limits with the issue of increased information that reduces the performance of this security system. Karthikeyan *et al.* [21] recommended the Secure Force (SF) based cryptographic technique for improving the security of WBANs. Here, the DWT and Daubechies wavelet-based feature extraction techniques have been utilized for signal decomposition and noise removal, because the performance of the signal processing system was highly dependent on the quality of signals. The main factor of this work was to utilize the simple cryptographic technique with reduced complexity, low power consumption, and computational devices.

Premkumar *et al.* [22] recommended an enhanced encryption approach with a scrambling matrix construction technique for hiding the confidential information of patients. Also, the deterministic algorithm named, Pseudo-random binary sequence generation algorithm was employed in this work for ensuring the security of the private healthcare information system. Then, the Elliptic Curve Cryptography (ECC) technique was applied for encrypting and decrypting the user data with ensured confidentiality and reliability. L.Zheng *et al.* [23], a detailed study has been conducted on various data encryption mechanisms used for securing the internet of medical things application system. Here, the performance of standard DES and ECC techniques has been validated based on the terms of accuracy, time consumption, and stability. From this paper, it is studied that the desired properties of security and efficiency could be addressed by the cryptographic techniques for guaranteeing the secured communication of the signal processing system.

Sivasangari *et al.* [24] suggested the lightweight selective encryption mechanism for guaranteeing the confidentiality and authenticity of the users' data. The main consideration of this paper was to minimize the computational overhead of the WBSN by optimizing the energy level of nodes. Also, it aims to improve the security of the system by establishing the three-layered communication in the network. Yet, it has the limitations of requiring more time consumption, and reduced performance outcomes.

From this review, it is observed that the existing security approaches are mainly focusing on establishing reliable signal transmission by incorporating the functions of standard cryptographic mechanisms. However, it faces the major challenges of increased complexity in designing the algorithms, requires more time consumption for transmission, increased loss of information, and reduced accuracy. In order to solve these problems, this research work intends to develop a novel algorithm for securing the ECG signal processing system. The major key points that are observed from these existing methods are to provide a secure data transmission system for the medical ECG signal and its data. For that, these algorithms are consumed more bit size to generate the key-value due to the precision of signal amplitude and its parameters. This leads to an increase in the energy consumption of the overall system and reduces the transmission rate. Further to improve the security service, the key size is increased to the corresponding size of data and its length. This becomes the motivation of the proposed work to implement the lightweight cryptographic system for ECG signals. According to this, the key pattern generation and the encryption model are enhanced for the high precision of amplitude and improve the Quality of Service (QoS).

Security is a core quality of an IoMT system and is linked to certain security aspects frequently required for allowing Trust and Privacy qualities in a system. IoMT Security focuses on securing connected devices and protecting data and networks on the Internet of Medical Things. Further IoMT devices are more prone to attack from the attackers. We proposed a new method of mechanism to protect the data from the IoMT devices.

III. Proposed Method

This section presents the overall description of the proposed bypass parallel processing optimal Hash Signature-partition design with its clear illustration. The main aim of this work is to develop an optimal Hash Signature VIHS with a new register design for storing data in the system and validate the data with a reduced error rate compared to another application process. In this, the peak value of ECG signal was extracted for the reference to generate the random key value. Here, this implementation reduces the amount of data required to be stored in various stages, and the amount of time essential for processing. According to that, an appropriate low-power hardware architecture has been designed to implement a real-time high performance and low-cost optimal Hash Signature block with the proposed decoder algorithm. This block design is highly more suitable for mobile applications. In which, the distinct data can be simulated based on the random data generation, where the sampling rate of 360Hz is relevant to clock frequency. The overall block representation of the proposed architectural design of VIHS hashing in the cryptography is represented in Fig. 1.

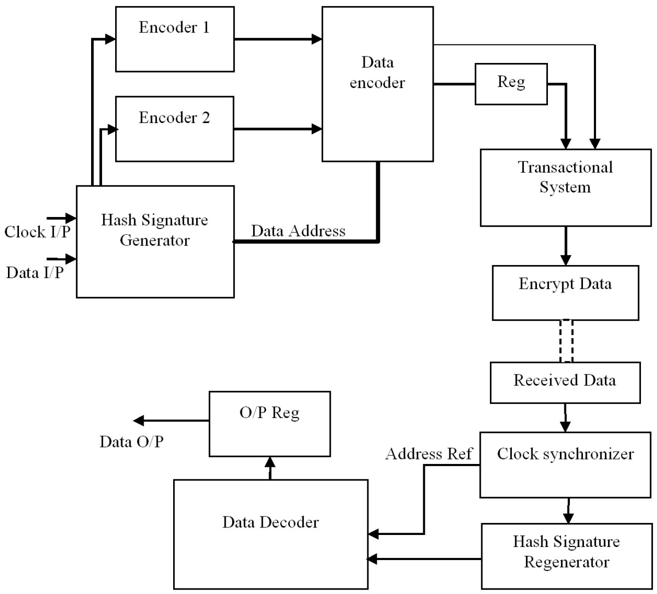


Fig. 1. Block Diagram of Proposed Hashing Technique of ECG Cryptography.

In this figure, the architecture represents the flow architecture of input ECG data and the block design of the encryption and decryption flow line. The block architecture represents the binary transmission of data to the encryption module to retrieve the hash signature and to form the encoded data. Initially, the input data are passed in bit sequence in accordance with the clock pulse that are synchronized with the encoders. Here, the Hash signature generator is to generate the random address and the key patterns based on the VIHS model. This transmit to the encoder block to encode the block that are indexed with the address of data. From that, the data got encoded and passed to the transactional system to transmit data through transmission channel. In the decryption process, the clock synchronizer predicts the data sequence and the address of it. This provide the reference to Hash Signature Regenerator. The main parameters that are considered for the lightweight architecture of ECG signal secure transmission were the number of bit size, key initialization and the random integer number generation, energy parameter of the overall system, and the Quality of Service (QoS). From this, the data was decoded and reconstructed to the actual ECG signal pattern. The major stages comprise of the proposed register design are as follows:

1) VIHS design
2) Hashing Model.
3) Data Transfer Architecture

A. VIHS Design

The register used in this block design is one of the essential component in electronic block after each Hash Signature connected with the latches. Typically, it is a major building block for most of the applications, in which the logical information has to be recovered from the sequential data specifically in optimal XORs. Moreover, this register is more suitable for the logic blocks, where the latch provides the large and fast output data. Then, its waveform and amplitude are independent of input data. Generally, two types of registers have been used named as static and dynamic, in which each gate output is connected with flags through a decrypt line path by the static registers. Similar to that, the dynamic registers could rely on the temporary storage of data values on the binaries of high sensitive block nodes. Moreover, the static registers are more suitable medium speed applications, and the dynamic registers are more suitable for high sensitive block nodes. But, it is highly sensitive to noise, in which varying sampling rates can be used for different applications. When compared to the static registers, the dynamic registers gained a significant attraction in medium to high-speed applications. Furthermore, it is energy efficient owing to the non-consumption of static current contrast. Fig.2. shows the schematic representation of the Hash Signature and register allocation flow with corresponding output units. In this, the arrangement of XOR and the Registers was formed to extract the Hash Key pattern. The dotted block indicates the Optimal placement using VIHS for the single-bit pattern. This it will be arranged as the sequential order to construct the 'N' number of bit size for the input signal amplitude. The final output data was arranged in the output register to get the 'OUTr'. It comprises the following stages: pre-amplifier, track and latch, where the pre-amplifier is larger than the input data and is not large sufficient to drive the logical block. Then, a track and latch stages are used to amplify the data to logic with the use of positive feedback loop. The major benefits behind this register design are high input sensitive, no static power consumption, full swing outcome, and fast decision rate.

B. Hashing Model

The proposed hashing with optimal Hash Signature design is fully based on the binary search algorithm, where the partition is a kind of logical controller block that has responsibility to run the binary search procedure. Also, the output of hashing with optimal Hash Signature can be determined with the respect to the register output. So, it has the momentous effect on improving the overall performance of optimal Hash Signature design. This register contains N bit optimal Hash Signature, which contains three possibilities for each bit that is either 0 or 1. At first, the MSB can be set as 1 and other bits can be reset by 0, and the logical word is converted with respect to the sequential value via the VIHS unit. Then, the output of sequential data can be inserted to the input of register, and is compared with the sampled input. Based on this outcome, the partition controller can estimate the value of MSB, where if the input is higher than the VIHS output the value of MSB can be set as 1; else, set as 0. During the last cycle, the converted logical word is stored, and N+1 clock cycles could be performed for conversion. Moreover, the partition can be designed with the use of register and the controlling block for encoding the Key to cryptography, and the conversion process can be continued only when the Hash Signature input is low. Fig. 3 shows the schematic representation of the hashing with optimal Hash Signature logic. In that, the (a) shows the block architecture for encryption process and the (b) represents for the decryption flow. The registers and the indexing block are used to find the encoded data samples that are passed through shift registers and count the repeated pattern of data samples. While at the decryption stage, the synchronizer detect the data samples with the clock pulses to reconstruct the data from the decryption block. The major building blocks of this block are dynamic latched register and inverters. The Algorithm I represents the steps for proposed hashing model for random Key generation.

Algorithm 1 VIHS based Data Encryption

```
Input: Plain text 'M'
Output: Encrypted text 'E'
procedure ENCRYPTION
    Initialize:
      Elliptical Curve Equation: $y^2 \leftarrow x^3 + ax + c$
                  ▷ 'x'and 'y'are the coordinate points of curve.
                  ▷ 'a'and 'b'are the constant coefficients.
    $x \leftarrow 0$
    Estimate the maximum limit of 'x'value that satisfy the selected curve line equation as 'p'
    while $x < p$ do
        Calculate 'y'value from the selected curve equation for each 'x'value in the loop
        Estimate modulo division of y with p as $Z_p$
        $Z_p$ = mod(y,p)
        if $Z_p == 0$ then
            $C \leftarrow (x, \sqrt{y}), (x, -\sqrt{y})$.
            $x = x + 1$
    End loop
    Calculate
      $Q_A$(x,y)= A * C(x,y)
      $Q_B$(x,y) = B * C(x,y)
      Sender and Receiver respectively.
                                                  ▷ Where,
                                                  ▷ 'A' - Sender
                                                  ▷ 'B' - Receiver
    Calculate
      $R_A$(x,y) = A * $Q_B$(x,y)
      $R_B$(x,y) = B * $Q_A$(x,y)
      Sender and Receiver respectively to satisfy $R_A$ = $R_B$.
    Find the median of $R_A$ and $R_B$to form Secrete key 'S'.
    Find the median of S and M to get encrypted text 'E'.
```

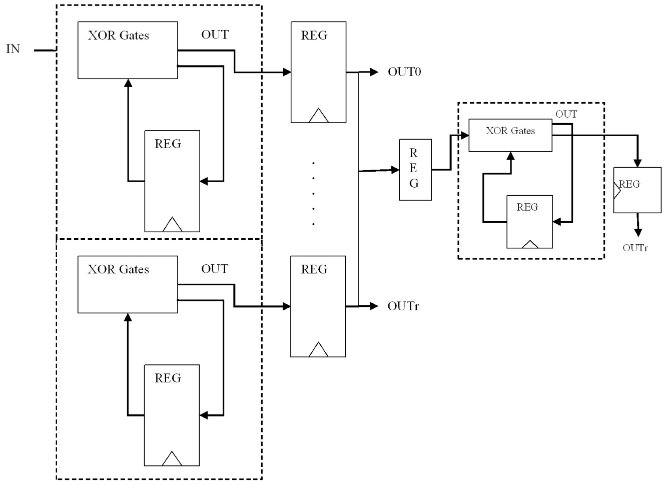
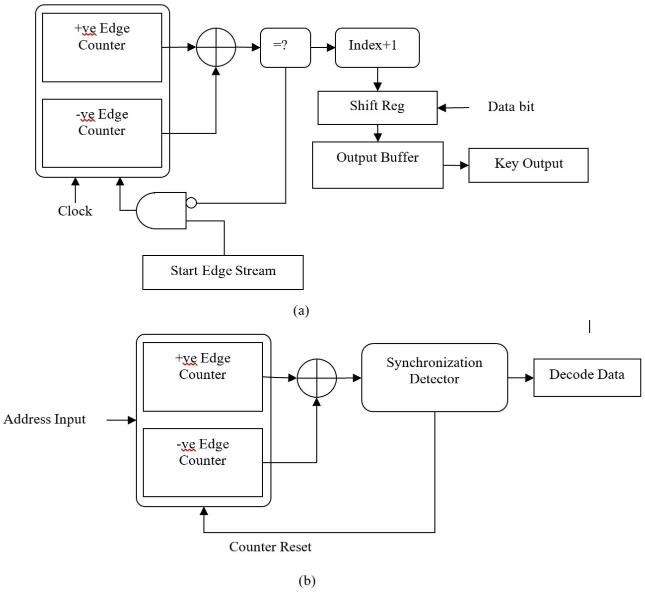


Fig. 2. VIHS Register Allocation Design.



(a)

(b)

Fig. 3. Block Diagram for Key Passing in Encrypt/Decrypt Process.

Let the input binary bits for the system stream can be represent as I_n. For the random Key generation, the Key should be regenerative based on the input matrix. Select a random number between 0 to ‘p’as ‘A’from sender and ‘B’from receiver.

Algorithm 2 VIHS based Data Decryption

```
Input: Encrypted text ‘E’
Output: Decrypted plain text ‘M’
procedure DECRYPTION
    Collect Secrete Key ‘S’ generated in encryption stage.
    Estimate the median of ‘S(x,y)’ and ‘E(x,y)’.
    Decrypted text
        $M^{|}(x,y)$=C{2.(E(x)-S(x)),2.(E(y)-S(y)}.
```

This cross computing generates the random Key for the system storage which can be represent as R_V . The reverse process can regenerate the random Key to encrypt the data from Key location in cryptography.

C. Data Transfer Architecture

Typically, the VIHS is a kind of device that is mainly used to convert the logical input data into an sequential output data. Then, its result is highly proportional to the logical value, in which the conversion tool can be acts as an interface between the logical and sequential blocks. Moreover, it serves a feedback data to correct the errors and estimates the reference data sequence during the process of conversion. During the design of VIHS, the values of supporting blocks should be determined based on the manual estimation process. Then, it can be adjusted further during the time of simulation, where some of the parameters can be considered with respect to the AMS technology. The architecture process can be defined according to the AMS technology as follows:

1. Arrangement of Hash Signature blocks.
2. Combination of Registers and Hash Signature.

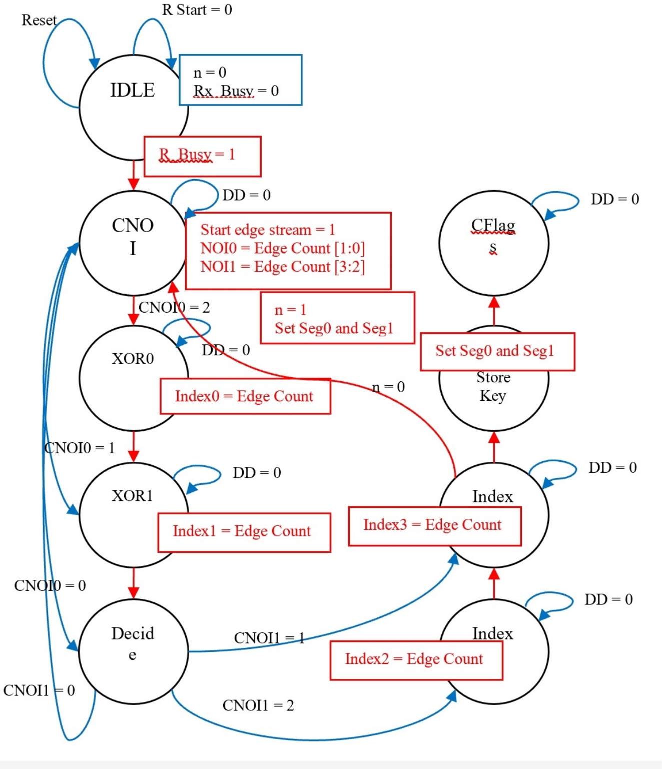


Fig. 4. State Flow for VIHS Generator.

The schematic illustration of VIHS design is depicted in Fig. 4. which comprises three stages. These are all combined with the architecture of XOR and the Register block arrangement. The state flow starts from the idle state of overall design. In this, the CNOI represents the count of number of Instant from the input ECG data samples. This was passed to the XOR combination flow and the flag CNOI are updated each time with respect to the data flow line. The decision was taken that according to the satisfactory level of encryption model and it flow in loop of updating CNOI to make the data pattern in random manner. This was also updated as the edge count that indicates the amount of loop that is running for the data encryption. Then this was encoded by the indexing method and get the encrypted and encoded data samples.

IV. Results and Discussion

Since findings suggest that IoT security requires substantial improvement before it is suitable for wide consumer acceptance. There are still many security issues. The most prominent were computation capability, memory, and time issues, and a lack of management mechanisms. Computation capability is critical within the Internet of Medical Things since the devices utilized frequently capture private, sensitive data, such as health information.

The simulation and Key implementation results have been validated for the proposed bypass parallel processing hashing with an optimal Hash Signature model with the output waveforms in the MATLAB 2011b platform. The data samples that are used for the testing of the proposed model was Physionet MITDB database. In that, the ECG signals are pre-processed and saved it in the '.mat' file format. In that file, ECG Data is a structure array with two fields: Data and Labels. Data is a 162x65536 matrix. This indicates there are 162 number of data samples present in the matrix. This time length are represented in terms of time samples with the size of 65536 measured for the length of 1 hour. Moreover, the results are compared with the state-of-the-art models by using the measures of frequency, Gates utilization count, power, area, sampling rate and propagation delay.

TABLE I. Bit Size Comparison for VIHS Model

Methods	Message count	Bit size
Mutual authentication	2	1184 bits
Efficient authenticated key for TMIS	2	1184 bits
Enhanced TMIS	2	1344 bits
Burrows–Abadi–Needham logic	3	1600 bits
TMISs	3	1280 bits
MQTT protocol	2	800 bits
Proposed	2	763 bits

Table I evaluates the comparison of the existing random number generation block in the hashing Memory design and proposed technique of VIHS in Cryptography with respect to the measures of components size based on the number of 2-input Hash Signature's, 3-Input Hash Signature's and the number of Flip-Flops that are referred from the paper [25]. For this analysis, some of the existing hashing with optimal Hash Signature designs have been considered. These results stated that the proposed dynamic system register-based hashing with optimal Hash Signature provides the better size in components, when compared to the existing model of VIHS.

TABLE II. Comparison of Time Taken for Encryption and Decryption (ms)

Methods	Time taken (ms)
Mutual authentication	13.38 ms
Efficient authenticated key for TMIS	13.4 ms
Enhanced TMIS	15.6 ms
Burrows–Abadi–Needham logic	11.17 ms
TMISs	8.9 ms
MQTT protocol	8.9 ms
Proposed	7.4 ms

Table II compares the values of area consumption in the unit of (μm2) in the existing [25] and proposed hashing with optimal Hash Signature methodologies. For the proposed work, the power consumption is reduced to the range of 25%. From the evaluation, it is evident that the proposed hashing with optimal Hash Signature could efficiently reduce the power and area consumption when compared to the existing technique of the VIHS model. Then, its corresponding graphical illustration of the area consumption is shown in Fig. 6 and Fig. 7 shows the comparison chart of FFs, LUT, and Slices utilization count for the existing [26] and proposed design of the VIHS generator.

TABLE III. Comparison Table of Message Count and Bit Size for the VIHS Key Generator

Methods	Message count	Bit size
Dey and Hossain scheme	5	1312 bits
ECC-CoAP	4	1024 bits
Proposed	4	926 bits

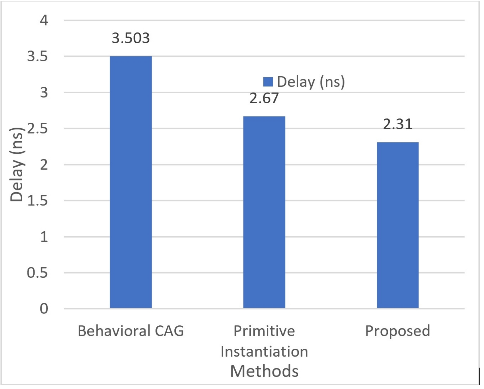


Fig. 5. Delay (ns).

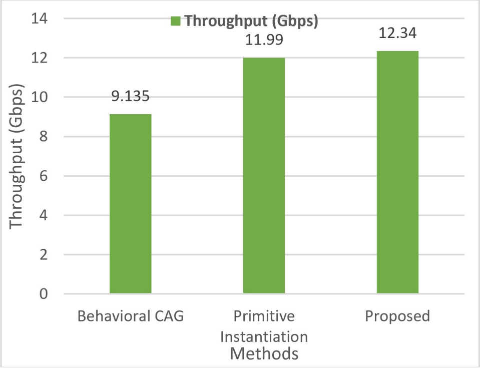


Fig. 6. Throughput (Gbps).

Table III illustrates the utilization count of throughput and delay rate of the existing and proposed VIHS technique. The corresponding graphical illustrations of these measures are represented in Fig. 5 and Fig. 6. From the analysis, it is proved that the proposed hashing with optimal Hash Signature provides better results, when compared to the other register techniques.

TABLE IV. Delay Rate (ns) and Throughput (Gbps) Comparison Table

Methods	Delay (ns)	Frequency (MHz)	Throughput (Gbps)
Behavioral CAG	3.503	285.47	9.135
Primitive Instantiation	2.67	374.53	11.99
Proposed	2.31	432.9004	12.34

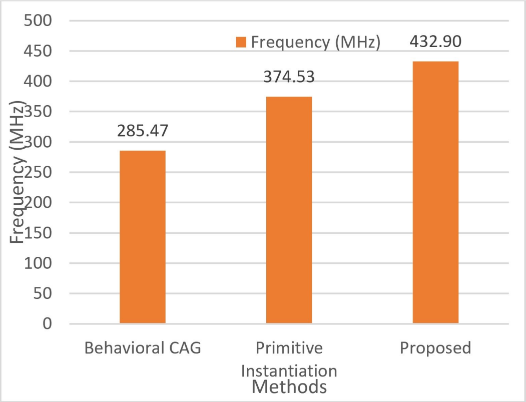


Fig. 7. Frequency (MHz).

Table IV and Fig. 7 shows the delay (ns) along with the frequency (MHz) and the throughput (Gbps) of various existing referred from [26] and the proposed technique of VIHS. In that comparison, the propagation delay is reduced to 2.31 ns by the proposed hashing with optimal Hash Signature design. These results stated that the proposed register could efficiently reduce the delay, when compared to the other techniques. Based on the overall analysis, it is evident that the proposed dynamic system register based hashing with optimal Hash Signature is more suitable and efficient for processing the system encrypt/decrypt applications.

V. Conclusion

In this paper, we presented a new register design with hashing with optimal Hash Signature for processing the system encrypt/decrypt data. The main aim behind this work is to encrypt/decrypt data in the system with a reduced amount of error rate. This designing methodology will reduce the amount of data required to be stored in various stages, and the time required for processing the data. Moreover, the proposed dynamic system register adopts the current controller, which generates both the polarity outputs and bypass trigger data during the same conversion. Here, a pseudo-differential pair is constructed to simulate the transfer characteristics. In this design, the charging speed can be adjusted with the process variation, component mismatch, and parasitics along the paths. After that the reference data sequence and binaries data sequences can be modified with respect to the bypass window size. In addition to that the bypass window size and speed of the register have been analyzed for architecture power-saving application area. The hashing with optimal Hash Signature provides low data sequence sensitivity, increased efficiency, and low power consumption. The VIHS could provide a residual data sequence with respect to the linear feedback of the conversion data. During the experimental evaluation, there are metrics have been validated to analyze the performance of the proposed register design. From the results, it is proved that the proposed technique provides better results when compared to the traditional techniques.

Future enhancement, this type of security system for medical applications is integrated with a new register design structure for the logical functionalities to generate the random number formation for a real-time application. This will improve the time complexity and the space complexities of the overall system.

References

[1] M. N. Aman, M. H. Basheer, and B. Sikdar, "Data provenance for iot with light weight authentication and privacy preservation," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 441–10 457, 2019.

[2] ——, "A lightweight protocol for secure data provenance in the internet of things using wireless fingerprints," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2948–2958, 2020.

[3] M. Almulhim and N. Zaman, "Proposing secure and lightweight authentication scheme for iot based e-health applications," pp. 481–487, 2018.

[4] K. Haseeb, N. Islam, T. Saba, A. Rehman, and Z. Mehmood, "Lsdar: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks," *Sustainable Cities and Society*, vol. 54, p. 101995, 2020.

[5] H. Shin, H. K. Lee, H.-Y. Cha, S. W. Heo, and H. Kim, "Iot security issues and light weight block cipher," pp. 381–384, 2019.

[6] O. H. Alhazmi and K. S. Aloufi, "Fog-based internet of things: a security scheme," pp. 1–6, 2019.

[7] S. Suganthi, R. Anitha, V. Sureshkumar, S. Harish, and S. Agalya, "End to end light weight mutual authentication scheme in iot-based healthcare environment," *Journal of Reliable Intelligent Environments*, vol. 6, no. 1, pp. 3–13, 2020.

[8] W. Haoxiang *et al.*, "Trust management of communication architectures of internet of things," *Journal of trends in Computer Science and Smart technology (TCSST)*, vol. 1, no. 02, pp. 121–130, 2019.

[9] M. Wazid, A. K. Das, V. Bhat, and A. V. Vasilakos, "Lam-ciot: Lightweight authentication mechanism in cloud-based iot environment," *Journal of Network and Computer Applications*, vol. 150, p. 102496, 2020.

[10] S. Amanlou, M. K. Hasan, and K. A. A. Bakar, "Lightweight and secure authentication scheme for iot network based on publish–subscribe fog computing model," *Computer Networks*, vol. 199, p. 108465, 2021.

[11] J. Wang, K. Han, S. Fan, Y. Zhang, H. Tan, G. Jeon, Y. Pang, and J. Lin, "A logistic mapping-based encryption scheme for wireless body area networks," *Future Generation Computer Systems*, vol. 110, pp. 57–67, 2020.

[12] M. E. Hameed, M. M. Ibrahim, N. Abd Manap, and A. A. Mohammed, "A lossless compression and encryption mechanism for remote monitoring of ecg data using huffman coding and cbc-aes," *Future generation computer systems*, vol. 111, pp. 829–840, 2020.

[13] M. Janveja, B. Paul, G. Trivedi, G. Vijayakanthi, A. Agrawal, P. Jan, and Z. Němec, "Design of efficient aes architecture for secure ecg signal transmission for low-power iot applications," pp. 1–6, 2020.

[14] H. Djelouat, A. Amira, F. Bensaali, and I. Boukhennoufa, "Secure compressive sensing for ecg monitoring," *Computers & Security*, vol. 88, p. 101649, 2020.

[15] H. Qiu, M. Qiu, and Z. Lu, "Selective encryption on ecg data in body sensor network based on supervised machine learning," *Information Fusion*, vol. 55, pp. 59–67, 2020.

[16] P. Mathivanan, A. B. Ganesh, and R. Venkatesan, "Qr code–based ecg signal encryption/decryption algorithm," *Cryptologia*, vol. 43, no. 3, pp. 233–253, 2019.

[17] M. E. Hameed, M. M. Ibrahim, N. Abd Manap, and M. L. Attiah, "Comparative study of several operation modes of aes algorithm for encryption ecg biomedical signal," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 6, p. 4850, 2019.

[18] S. P. Awasarmol, S. Ashtekar, and A. Chintawar, "Securely data hiding and transmission in an ecg signal using dwt," pp. 2850–2854, 2017.

[19] M. E. Hameed, M. M. Ibrahim, N. A. Manap, and A. A. Mohammed, "An enhanced lossless compression with cryptography hybrid mechanism for ecg biomedical signal monitoring." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 10, no. 3, 2020.

[20] M. U. Shaikh, S. A. Ahmad, and W. A. W. Adnan, "Investigation of data encryption algorithm for secured transmission of electrocardiograph (ecg) signal," pp. 274–278, 2018.

[21] M. Karthikeyan and J. Manickam, "Ecg-signal based secret key generation (eskg) scheme for wban and hardware implementation," *Wireless Personal Communications*, vol. 106, no. 4, pp. 2037–2052, 2019.

[22] S. Premkumar and J. Mohana, "A novel ecg based encryption algorithm for securing patient confidential information," *International Journal of Electrical Engineering & Technology (IJEET)*, vol. 2, no. 11, pp. 35–43, 2020.

[23] L. Zheng, Z. Wang, and S. Tian, "Comparative study on electrocardiogram encryption using elliptic curves cryptography and data encryption standard for applications in internet of medical things," *Concurrency and Computation: Practice and Experience*, p. e5776, 2020.

[24] A. Sivasangari, S. Bhowal, and R. Subhashini, "Secure encryption in wireless body sensor networks," pp. 679–686, 2019.

[25] A. Sivasangari, A. Ananthi, D. Deepa, G. Rajesh, and X. M. Raajini, "Security and privacy in wireless body sensor networks using lightweight cryptography scheme," pp. 43–59, 2021.

[26] L. Xiong, X. Han, C.-N. Yang, and Y.-Q. Shi, "Robust reversible watermarking in encrypted image with secure multi-party based on lightweight cryptography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 1, pp. 75–91, 2021.