Bio-Hash Secured Hardware e-Health Record System

M. M. Sravani and S. Ananiah Durai

***Abstract*—Dual securing strategy for all-hardware e-Health Record System is designed and developed for improved security and reduced Hardware Execution Time (HET). A compact novel Hashed Minutiae Random Fusion (HMRF) logic enables to achieve high irreversibility and increased non-reconstruction capability of the bio-template based Bio-Hash key. AES encryption of the patient's health data during Write mode and decryption during View mode are seamlessly performed through the lively generated key, yielding low HET through optimized slack. On the other hand, biometric controlled key retrieval during Read only mode for a single user access is performed on the pre-scrambled Bio-Hash key, to enable bypassed decryption (direct) of the Patient's health data for self-review. The proposed pseudo cascaded SHA-3 (Secured Hash Algorithm) architecture being the first stage in HMRF, hashes the biometric minutiae of both Patient (P) and Medical Practitioner (MP) with low Latency. Thus, facilitating in further lowering of the HET by reducing the clock count by one. The subsequent Random Compression Logic (RCL) skims the hashed value from 512 to 128 bits along with the help of priority compression logic (PCL) to achieve reduced bits handling thereby lowering the Power budget. Four fusion modes are leveraged to achieve better randomization and non-recoverability. Implementation of this HMRF logic on Virtex-7 (V7) FPGA device has yielded low Area of 4191 slices. Lesser Area of 11.6% is observed for this HMRF module compared to the reported design, excluding level shifter and PCL. Further, low HETs of 8.2/8.3/8.0 ns during Write/View/Read only modes respectively are being noticed. The dynamic Power dissipated for the three modes of operations are found to be 1.418/1.420/0.676 watts respectively.**

***Index Terms*—AES, bio-hash, fusion, health record, SHA-3.**

I. Introduction

BIOMETRIC authentication technique uses single or multiple bio-features to access the digitally secured e–record (database). As the biometric pattern is unique, either duplication or embezzlement is found to be almost impossible; therefore, it is extensively employed in various access control applications. Extraction of biometric features for such applications can be categorized as Biological, Behavioral, and Morphological. Preferably in biological biometric technique, the biological features such as DNA sequence, blood samples, etc., serve as access control component [1]. In behavioral biometrics, features such as the voice, heartbeat, etc., are utilized to provide controlled access [2]. Design of any access control system using biological & behavioral biometrics is cumbersome though it features high security due to its induplication possibilities. On the other hand, morphological biometrics requires only a simple system level design, as it exploits the advantage of unique morphological features. Further, the security level is equally high as that of other techniques [3]. Various design options by leveraging multiple morphologic features such as Fingerprint, Face, Iris, Ear, and Palm might further enhance the security levels. Few earlier access control applications that utilize morphological biometrics are key generators, electronic voting, digital signature and personal data identification. Most of these techniques primarily involves secured access of the highly confidential data stored in the local database [4], [5], [6], [7], [8]; however, least importance is given to secure the data itself.

Among the morphological biometric trait, fingerprint is especially found enormous employment in secret key generation. In an attempt for secured access, a bio-intermediate key was generated utilizing the fingerprint authentication in [4], which also provided shielding from possible Side Channel Attacks (SCA) as an added advantage. However, vulnerability to fault injection for effective key retrieval as demonstrated in [9], proves that the database is poorly secured. In another e-voting application, similar traits were employed to authenticate/identify the voter for casting votes [5]. Unsecured biometric template stored in the database for voter identity purpose will be vulnerable for reconstruction of bio-templates, which might lead to fake voting and manipulation, ultimately leading to system failure. In few other applications, morphological biometrics were utilized to access personal data such as age & gender [6], which were stored in an access controlled database. Such biometric application is found viable to enable even forensic analysis to track down the criminals involved in any criminal activities. However; there were instances that the offender gained illegal access to the weakly shielded database by manipulating the traits and had diverted the entire investigations. Though the database itself can be secured with the biometrics traits of authorities [8], the intruder may still gain illegal access to modify the personal information, which might lead to organizational failure.

Further, another application that involves digital signature of documents, is found widely employed in database access control. e-Health records, revenue records and banking transactions are notable applications that have implemented this database access control technique, to facilitate seamless authenticated online transactions and document downloads that eliminate physical presence of the individual [7]. Deliberate morphing

Manuscript received 1 August 2022; revised 18 October 2022, 10 January 2023, and 3 March 2023; accepted 25 March 2023. Date of publication 4 April 2023; date of current version 12 July 2023. This work was supported by VIT Chennai through the Seed grant Scheme, 2022-2023, under the file number YSS/2015/001395. This paper was recommended by Associate Editor Y. Zheng. *(Corresponding author: Ananiah Durai. S.)*

The authors are with the Center for Nanoelectronics and VLSI Design, School of Electronics Engineering, VIT Chennai, Chennai 600127, India (e-mail: mm.sravani2017@vitstudent.ac.in; ananiahdurai@gmail.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TBCAS.2023.3263177.

Digital Object Identifier 10.1109/TBCAS.2023.3263177

of the signature image traits at the registration stage might weaken the security level of the database. Multi-tier shielding can be an appropriate option to enhance the security of any such database access control systems. Two independent biometric sources have been utilized in [2] and [10] by either fusing 'Face & Voice' or 'ECG (Electrocardiogram) & Fingerprint', to enhance shielding. Usually, decision is done based on the fusion score during authentication phase, while such multi-biometric traits are involved. Though the access control has been enhanced by fusion of multiple biometrics, the database is still found to be poorly secured, as breaches through illegal fusion score matching is possible.

It is evident from the above scenario that most reported access control techniques have weak bio-key generator logic. Securing sensitive information such as digital medical records with such weak keys might render a poorly protected key database itself. This is due to the fact that most reported techniques have employed systematic key generator logic, which the intruder might recreate the biometric template with a conventional hash inversion to gain illegal access [11]. A highly random key generator must be rather a better alternative to overcome such security failures [10]. To further secure these biometric templates, a cryptographic hash functions can be employed to thwart such illegal access. On the other hand, the confidential medical data that populate the database are often unprotected; hence securing the medical report itself must be ensured. One such measure has been demonstrated to secure the patient's e-health record in [12].

An electronically maintained medical record that includes blood investigation reports, scan images, diagnostic history, and prescription/treatment of a patient is vital for any emergency/intensive care and for regular/follow-up care visits of the patient as well. However, unprotected/poorly secured database might lead to breaches resulting in un-authorized access leading to data tampering, forgery, and data manipulation/stealing, while sharing the e-documents. Securing such resources by cryptographic schemes is crucial. This paper proposes a dual cryptographic securing scheme to overcome the security issues prevailing in the existing e-Health Record System.

Contributions of this work include;

1) A novel HMRF key generator logic to generate highly random Bio-Hash key, for the mainstream AES engine that encrypts the patient's medical data.
2) A pseudo cascaded SHA-3 architecture (Initial block in HMRF) that effectively lessens the rounds during permutation, to provide reduced resource utilization and hence the area.
3) Duplex authentication scheme that utilizes biometrics of both P and MP, for secure population of health data in Write mode.
4) A key retrieval module that enables seamless decryption of health data during Read only mode for self-review.

Area, HET, Latency and Power performances of this dual cryptosystem are also analyzed and presented.

Section II of this paper starts with the discussion on existing methodology that secures the patient medical record, followed by insight into the existing cryptographic architectures of SHA-3 and AES. Whereas, in Section III, the proposed system that involves three modes of HMRF key generator and the AES encryption/decryption are explained. Simulation & hardware implementation results of the HMRF & AES engine, with its evaluation and comparison are provided in Section IV. Finally, concluding remarks on the module and system level performances are provided with the future scope of this work.

II. Prevailing Health Record System

Over the decade, software Health Record System has been developed for personal and organizational controlled access. A detailed review on few such reported Health Record Systems that are both centralized and localized are provided in the sub-sections with their specific weakness. Design specific potential improvement for each reported work is also suggested. In addition, the review of the SHA-3 and AES architectures being the core modules of the proposed system, is provided at the end with the hardware structure and functional drawbacks.

A. Secure Access Schemes of Digital Health Record

There is always a high probability that the patient may misplace/lose the crucial medical data while visiting the health care centers, which may delay the treatment during emergencies. The impact is horrendous for critical treatments such as cardiovascular treatment, maternal & child health care etc. Situation may be sometimes fatal if the patients are wheeled into the hospital in an unconscious state. Further, expecting the patients to keep medical records handy while visiting multiple hospitals for treatment might be futile. Moreover, preparing and maintaining hard copies of the patients' medical records might be unsafe and error-prone [9]. To overcome such mishaps, a system of digital medical record (DMR) has been developed by several countries to take care of the citizens' health. Further, announcement/warning for any outbreak of epidemic/pandemic diseases such as COVID, SARS-Cov, Ebola, etc., can be done at the initial phase when e-Records of the citizens' health are maintained. To make this into a reality, developed/developing countries have designed a few digital health setups to store/access e-Health Records for effective patient care. Personal Health Record (PHR), Electronic Health Record (EHR), and Electronic Medical record (EMR) [12], [13] are few medical record systems popularly implemented.

PHR system was designed and developed by EU & USA for patient's personal use. It enables individual to track their medical record that is stored in the cloud. Further, to strengthen the data security different policy-based schemes such as attribute-based systems, attribute-based encryption, cipher text policy, interplanetary file systems, and blockchain technology [14], [15], [16], [17] have been introduced. Even though such schemes in PHR provide high security, its high cost renders as unaffordable for the common public especially for the low income group. Similar to PHR, an EHR system being an organizational medical database structure, was developed by experts for a confined environment within hospitals or chain of health cares. Viewing of medical record by patient through EHR enables them to manage their personal health check-ups and follow up with the assigned physician. Authorized access by both physician and patient through digital signature validation, served as an additional security feature of this system. The cloud upload of medical record is permitted only when the patient verifies and approves it. Simultaneously, the physician can also cross verify the uploaded record through a specific pin-protected access control [18]. This has ensured accurate health care database management facilitated through the blockchain. The primary weakness of the system is the storage of patient's both private and public keys in the same server, which the adversary can conveniently utilize it as loop hole for a potential attack. Security strength provided by the cybersecurity framework is the major concern for such electronically maintained health data. Manipulation and misuse of complete data were prominently observed for revenge motive by the adversaries of the patients.

EMR is another improvised standard for immediate medical care similar to EHR, which was developed and widely implemented by countries like the USA and the EU. The system helps in continuous assessment and monitoring of patient's response to treatment. Further, record maintained through EMR will tremendously help to track the patients' health in the event of a new disease outbreak [19]. Further, it also enables researchers, doctors, scientists, etc., to access those records for medical study, such as genome sequencing, in the event of new virus/bacteria outbreak. However, as the data are only password-protected, viewing and accessing are made available for any health department inside and outside of the country. Such poorly secured medical data may be vulnerable for manipulation by the neighboring countries triggering even a bio-war. For enhanced privacy in e-health record systems, smart contracts-based access control framework with ECC and EdDSA algorithms has been proposed later [13], [20]. In this, the actual ownership of the individual medical data is solely possessed by the individual itself. Therefore, it has been considered to be a more attractive method than the other reported health record system. However, leveraging patients' self-modification of their medical data might lead to self-manipulation at times for their personal benefit, such as false insurance claims, fake medical data manipulation for VISA purposes, and fake medical leave claims.

The earlier reported health record systems fail to provide integrity and confidentiality features to effectively secure the patients' health data. Though the cloud server is increasingly popular due to global access features, it's poor privacy and severe threats from the cryptanalysis make it unsuitable for sensitive data protection such as health data. An e-Health Record System powered by dual cryptographic engine that features highly secured storage and stringent access scheme is proposed in this work. In this approach a highly random Bio-Hash key enabled by the HMRF sub-system that yields a unique random key whenever invoked is designed. The medical data that are then encrypted by an AES engine through this generated Bio-Hash key can be limitedly shared within the organization's private network. Thus, the security is enhanced by eliminating the possibility of manipulation by the cryptanalyst. Further, this proposed system also facilitates viewing of the medical report by the individual at lower cost than in the organization portal. Thus, storage and viewing of reports take place within this trustworthy model. It is notable that this encryption method includes the non-repudiation and authorization features required by any secured e-Health Record System.

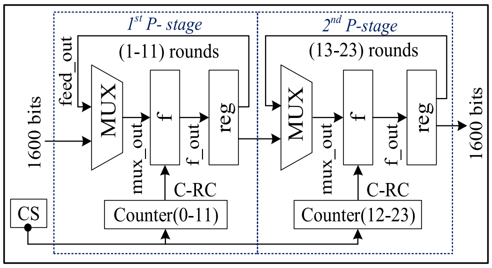

Fig. 1. The permutation module of cascade-P structure [21].

B. SHA-3 Architecture Review

The proposed HMRF logic that intends to generate the Bio-Hash key for the AES engine requires a SHA-3 architecture that features low Latency and low Area for an enhanced Efficiency (E_f). Reduced Area at this stage compensates for the additional data path and Area rendered by the subsequent Bio-Hash skimmer and Fusion logic. Earlier reported architecture in [21], has been designed such that the padder and permutation modules operate in 'split-transfer' mode through handshake protocol. First, the message input converted to a sequence of 32/64 bits by padding, is processed to yield 'r' bits through a high throughput load-shift-store (LSS) scheme. The permutation process is then initiated by the exchange of the handshake signals, viz. 'padd_ready' and 'f_{ack}', once the output buffer is full with 'r'. In the permutation model, the Cascade-P round function has been invoked to scramble the message bit through the dual functional structure that includes two cascade stages as shown in Fig. 1. The lead-lag counter logic initiates the first stage to perform the round operation for rounds (0-11) followed by the remaining round (12-23) by the second stage. For the subsequent rounds 'counter 1' leads and the 'counter 2' lags. Owing to the pseudo parallel operation, the Cascade-P design is mostly preferable for multi-block message schemes. In a single block message like e-Health Record System, this design would however provide the final scrambled output in usual 24 clock cycles. Though the design has an advantage of low operational clock counts, the Area performance is compromised due to additional logics that results in poor efficiency. Hence it is found that the performance of this design is inadequate for single block message. In an attempt to enhance speed of the architecture, a count generator has been designed in [22] that enables synchronized fetching of the RC constant from ROM (Read Only Memory); however additional memory elements have led to significant increase in slices, resulting in poor Area performance. On the other hand, a single block equation in [23], though appears to be an effective method to reduce LUT resources, the necessity of both 'With-RC' and 'Without-RC' logics in iota step renders poor Throughput (TP) resulting in low E_f. Further, the multi-architecture designs in [24] and [25], though appealed to enhance the Frequency (F); the logic stages utilized to implement such structures have directly increased the slice count and clock count, thus invariably affecting Area and Latency performances respectively. Therefore, a modified SHA-3 architecture to enhance Area without substantially lowering the clock count is essential.

C. AES Features

An AES engine that efficiently encrypts the medical data through the Bio-Hash key is chosen in this work as a primary encryption algorithm. This is due to its excellent feature of smaller key size. NIST declared that AES performs better in terms of security than the popular triple DES, while maintaining minimum key length varying from 128 to 256 bits. As the key size varies, so will be the number of rounds to perform AES encryption/decryption operations. The encryption process in AES starts with a key expansion block. During the round key operation, the 128 bits key is scrambled in each round to produce different keys, followed by the shift rows, sub bytes, and mix-column steps to finally generate the cipher value. During the last round operation, the mix-column step is ignored to properly rearrange the bits in a specific order. An inverse process is carried out in the decryption operation to retrieve back the original data [26].

In this work the utilization of both unidirectional SHA-3 for key generation purpose and compact key based AES for health data encryption, will render highly secured dual cryptographic scheme. The proposed system exploits the advantage of both high security & high-speed features of this dual crypto architecture, to efficiently implement an all-hardware e-Health Record System.

III. Proposed E-Health Record System

Methodology to securely Write/View of the patient's medical data starts with preprocessing stage that involves simultaneous Bio-Hash key generation and mapping of P & MP hashed biometric value. The MP chooses to either Write or View the medical record through the mode selector. Medical examination followed by diagnostic report generation is permitted if a Write mode is opted, else View mode is enabled for only reviewing the P's medical history. A Read only mode designed as a bypass loop, can be invoked directly by P for personal review purpose. Key retrieval logic validates P's biometric during this loop process, while comparing with all the keys stored in KD.

A compact hardware prototype has been designed to securely store/view the sensitive details of the patients' medical records. Pre-registration of the P's fingerprint biometric data to generate P specific hash bits of length 512, is first done before any medical consultation. HMRF logic then generates the Bio-Hash key from both P's & pre-generated MP's biometric hash value. All such generated keys from various Ps & MPs are mapped on to the concerned Ps for populating KD database. During the Write mode, MP will record the medical diagnostic report post the medical examination, with the authorization of P done through an enable line (E_n). A live key generator process begins simultaneously that involves skimming of both P's & MP's biometric hashed value to 128 bits, followed by fusion logic. The generated final Bio-Hash key after fusion, serves as the encryption key for AES. The Refer_bits, which are the 8 MSB bits of P's hash value, enables the key retrieval from KD, whenever a Read only mode is invoked by the concerned P. The proposed cryptosystem with all three functional modes is shown in Fig. 2.

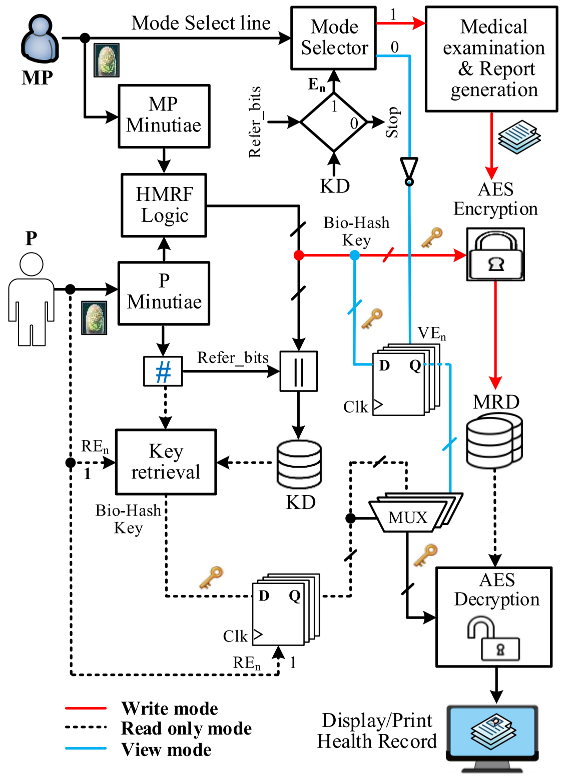

Fig. 2. Functional flow of e-Health record system.

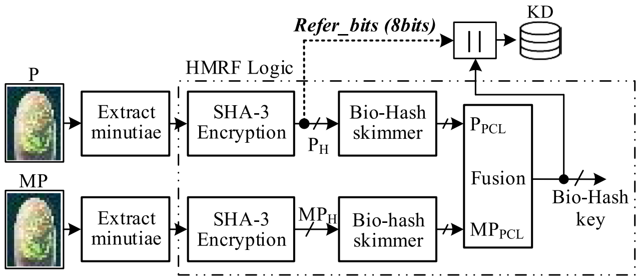

Fig. 3. Bio-Hash key generation with HMRF logic.

The solid arrows in red of Fig. 2 indicate the Write mode functional flow, whereas the blue line shows the View mode flow. Broken line shows the Read only mode process flow that will be specifically invoked by P as when required.

A. Bio-Hash Key Generation

A HMRF key generator is proposed to generate a highly secured Bio-Hash key as shown in Fig. 3. The pre-processing stage includes extraction of minutiae from biometrics followed by the conversion of the minutiae into hexadecimal. Hashing of this hexadecimal requires a highly secured SHA-3 structure,

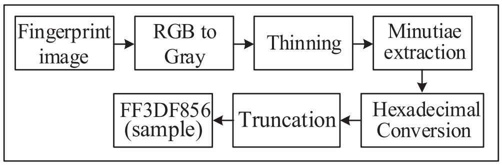

Fig. 4. Pre-processing of fingerprint image.

preferably with low Latency, low Area and high E_f. Therefore, earlier reported designs [21], [22], [23], [24], [25], which are poor in terms of Area, Latency and E_f, are modified to obtain a pseudo cascaded architecture to yield a comparatively low Latency, low Area and high E_f. This is achieved by decreasing the round function from 24 to 23. A skimming process that compresses the 512 bits output of the SHA-3 architecture to 128 bits, is employed using the Bio-Hash skimmer. The above process is carried out for both P and MP biometrics independently to obtain two individual block of 128 bits skimmed outputs. Skimming at this stage enables handling of reduced bits by the subsequent stages rendering reduction in Power budget and Area. Finally, quadruple fusion circuitry that randomly fuses both the skimmed 128 bits, yields highly secured irreversible Bio-Hash key of 128 bits.

1) Pre-Processing of the Biometric Traits: The fingerprint biometrics of the P & MP must be read in a locally centralized device, accessed through the GUI (Graphical User Interface) at any specific health center to ensure authenticity. The proposed system is compatible with any format of the biometric data available at the health center's e-Record facility. To extract the minutiae from the biometric images, RGB to gray scale conversion is done first followed by a thinning process. Segmentation algorithm is applied to remove the background noise, then the minutiae such as ridge bifurcation, ridge dot and ridge termination are identified and extracted [27]. These localized points obtained from multiple fingerprints are then converted to hexadecimal values for better handling of the complex large biometric data by subsequent stages. Finally, the hexadecimal value is truncated to get the 32 bits of biometric data, as depicted in Fig. 4. This process must be applied for feature extraction of both P and MP biometrics to get their respective 32-bit hexadecimal value; hence two separate logic circuits are implemented. These two hexadecimal values are then independently hashed by individual SHA-3 engine to obtain respective hashed biometric data.

2) Proposed SHA-3 Architecture: The existing Cascade-P SHA-3 architecture is mostly suitable for multi-block message, as the cascaded structure runs on reduced clock count for streaming the input messages. However, for a single-block biometric data, no significant improvement in clock count is noted, further the architecture fails to provide better Area performances [21] that is essential for a compact application such as the e-Health Record System.

The proposed pseudo cascaded architecture that includes a standalone 'round 0' operation provides better Area performance. As when the 'round 0' operation starts, the 'padd_ready' signal is pulled high to select the 'r' (padded biometric data) being the output bits of the padder. A concatenation is done with 'r' and capacity 'c' bits to obtain 1600 bits. A round function exterior to the round loop performs the zeroth round On-The-Go (OTG). During OTG operation, dedicated register provides the required zeroth RC (Round Constant) bits. A round loop function with a selection option between the OTG logic output and loop feedback output is designed to complete the remaining 23 rounds through the MUX, driven by 'loop_selector'. A high on the 'loop_selector' will allow the OTG output to be fed to the round function, else loop feedback output 'reg_out' will be selected for rest of the rounds, as shown on Fig. 5. The RC generator provides the RC value for 'round 1' through 'round 23' during every clock cycle. At the end of 'round 23', the hashed data are truncated to obtain 512 bits which, when byte inversion is applied, yield a final hashed biometric data. The proposed architecture completes the permutation process within 23 clock cycles compared to the existing Cascade-P structure, which reportedly consumes one additional clock cycles (i.e., 24 clock cycles) for a single-block biometric data. Two separate SHA-3 engines are utilized to hash both P and MP biometric data yielding P_H and MP_H hashed biometric data respectively.

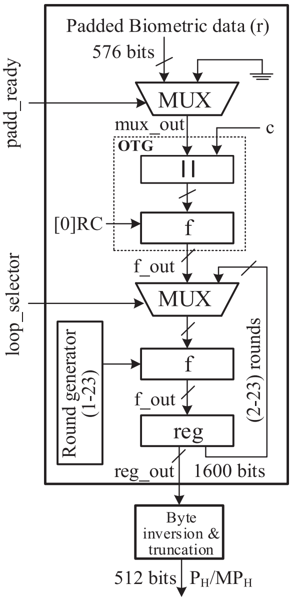

Fig. 5. Permutation module of pseudo cascaded architecture.

3) Bio-Hash Skimming Process: The two pseudo cascaded SHA-3 architectures provide two different digested outputs hashed from the minutiae of the P's and MP's biometrics. Bio-Hash skimmer that includes three stages of digital circuits, then effectively skims these hashed 512 bits (P_H/MP_H) to 128 bits (P_{PCL}/MP_{PCL}) for reduced bit handling. Initially, these hashed bits are skimmed by the first stage two level splitter logic that yields two block of 128 bits data. A Pre-computed Random Compression Logic (RCL) employed in the second stage, subsequently generates eight blocks of random bits from these two data blocks. Only one highly random block among these eight will be chosen by the final Priority Compressor Logic

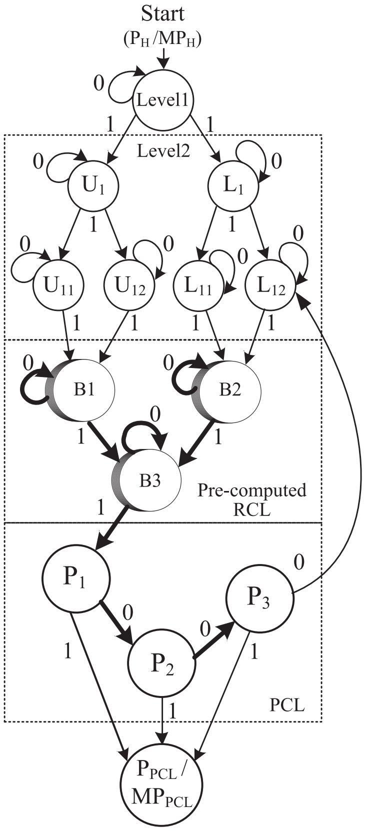

Fig. 6. Finite state machine of Bio-Hash skimmer.

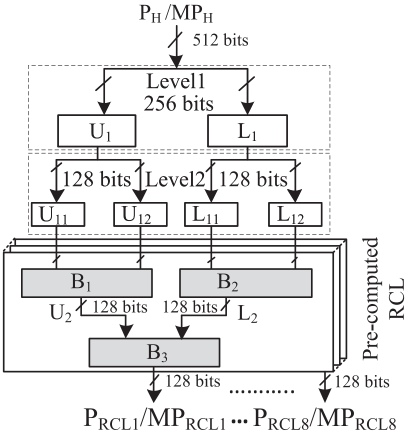

Fig. 7. Level splitters and pre-computed RCL.

TABLE I
RANDOM COMPRESSION LOGICS (RCL)

S. No.	B_1	B_2	B_3	Random compression logic
1	NAND	NAND	NAND	~(~(U_{11} & U_{12}) & ~(L_{11} & L_{12}))
2	NOR	NOR	NOR	~(~($U_{11} \vert U_{12}$) $\vert$ ~($L_{11} \vert L_{12}$))
3	XOR	XOR	XOR	((U_{11} ^ U_{12}) ^ (L_{11} ^ L_{12}))
4	NAND	XOR	XOR	(~(U_{11} & U_{12}) ^ (L_{11} ^ L_{12}))
5	XOR	NAND	XOR	((U_{11} ^ U_{12}) ^ ~(L_{11} & L_{12}))
6	NOR	XOR	XOR	(~($U_{11} \vert U_{12}$) ^ (L_{11} ^ L_{12}))
7	XOR	NOR	XOR	((U_{11} ^ U_{12}) ^ ~($L_{11} \vert L_{12}$))
8	NOR	NAND	XOR	(~($U_{11} \vert U_{12}$) ^ ~(L_{11} & L_{12}))

(PCL) circuit. The finite state machine that depicts the three stage skimming process is shown in Fig. 6.

In the initial stage of skimming, the 512 bits of hash digested bits (P_H/MP_H) are first divided equally by the 'Level1' splitter to yield U_1 and L_1 with an output block size of 256 bits each. Next, the 'Level2' splitter further subdivides the U_1 and L_1 into U_{11} & U_{12} and L_{11} & L_{12} respectively of each being 128 bits. Subsequently, the RCL that includes three hidden logic operations viz. B_1, B_2 and B_3 performs another two levels of compression for extreme skimming. In the first level of RCL, eight groups of B_1 and B_2 logic circuits yield eight different U_2 & L_2 datasets respectively, of each being 128 bits. B_3 logic circuit that performs the second level skimming, further compresses the data to obtain eight blocks of 128 bits. The above skimming process must be performed for both P_H and MP_H independently to yield eight blocks of 128 bits each, which are referred to as P_{RCL} and MP_{RCL} respectively, as shown in Fig. 7.

The hidden combination logic viz. B_1, B_2 and B_3 in RCL must be designed and implemented to achieve highly random hashed biometric data. The randomness at this stage can eventually yield an irreversible key at the final output of Bio-Hash skimmer. Implementations of these logics with simple universal gates such as NAND & NOR yielded only 8 combinational circuits. Among these 8 combinations, only few generated the required complex random value, while under test with sample datasets. However, inclusion of complex gate such as XOR, rendered increased combinations of up to 27. Moreover, comparatively more random values are generated. Implementation of all these 27 logics on any FPGA devices might render poor Area. Therefore, logic optimization must be performed by evaluating the randomness of all combinations using Machine Learning (ML). ML study with 500 data samples on these 27 combinational logics revealed that only eight of them that are shown in Table I, performed better and provided increased randomness. These 8 random logics have been found to generate high random output bits on the basis of maximum occurrence of 1 [28], which fall within the reference range of ($57 \leq$ '1' ≤ 71). This pre-computed compressor logic performed equally well with even 1000 different data samples (P_H/ MP_H).

The output from the 'Level2' splitter drives the pre-computed RCL to generate 8 combinations of 128 bits. Two Bio-Hash skimmer circuits designed in this work yield P specific and MP specific skimmed bits. The P_H specific RCL circuitry yields output combinations from P_{RCL1} till $P_{RCL8,}$ whereas the other that skims MP_H bits, yields outputs from MP_{RCL1} till MP_{RCL8}. Subsequently, two separate Priority Compressor Logic (PCL) circuits then investigate these P_{RCL} combinational outputs (P_{RCL1} till P_{RCL8}) and MP_{RCL} outputs (MP_{RCL1} till MP_{RCL8}), with three different priority ranges and select one highly random

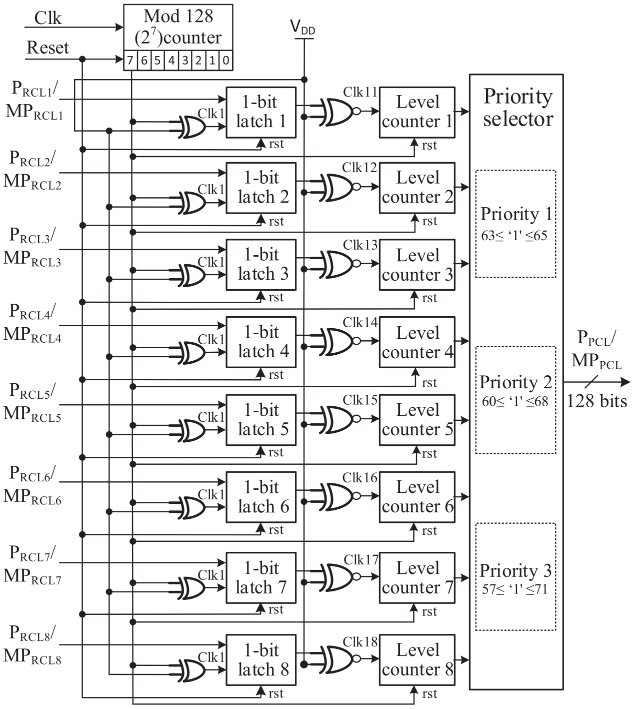

Fig. 8. Schematic of priority compressor logic (PCL).

TABLE II
HAMMING WEIGHT ESTIMATION

Hashed datasets	Hamming Weights of RCL outputs for the respective P and MP datasets							
	RCL_1	RCL_2	RCL_3	RCL_4	RCL_5	RCL_6	RCL_7	RCL_8
P_{H1}	*57*	*67*	**64**	*58*	*69*	*59*	*66*	*82*
P_{H2}	*50*	*66*	*68*	*66*	*68*	*63*	**65**	*85*
P_{H3}	*65*	*76*	*60*	*68*	*59*	*69*	**64**	*90*
$\mathrm{MP}_{\mathrm{H1}}$	*57*	*78*	*66*	**65**	*61*	*66*	*68*	*87*
$\mathrm{MP}_{\mathrm{H2}}$	*47*	*62*	*60*	*59*	**64**	*62*	*67*	*80*
$\mathrm{MP}_{\mathrm{H3}}$	*52*	*71*	*60*	*60*	*62*	*69*	**63**	*81*

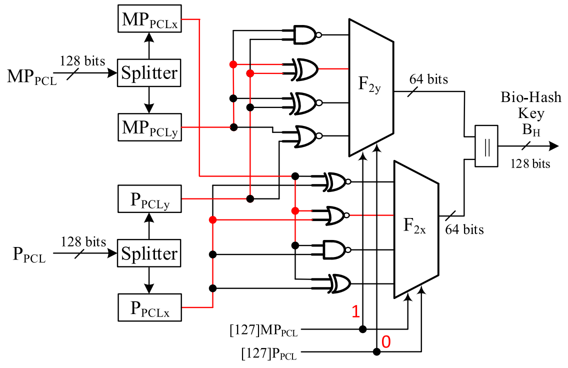

Fig. 9. Fusion logic circuit on F2 mode.

block of 128 bits from each. This is done by initially latching the $\mathrm{P}_{\mathrm{RCL}}/\mathrm{MP}_{\mathrm{RCL}}$ output bits ($\mathrm{P}_{\mathrm{RCL1}}/\mathrm{MP}_{\mathrm{RCL1}}$ to $\mathrm{P}_{\mathrm{RCL8}}/\mathrm{MP}_{\mathrm{RCL8}}$) on to the Level counter sequentially whenever the 'clk1' goes high. The 'clk1' logic is built using an XOR that goes high as when the Mod 128 counter starts counting from '0' till '127'. At the count of '128', the 7th bit that drives one of the input of XOR goes high, pulling the XOR output to '0'. This indicates that all the 128 bits of each $\mathrm{P}_{\mathrm{RCL}}$/ $\mathrm{MP}_{\mathrm{RCL}}$ has been successfully latched. The subsequent 'Level Counter' counts the number of 1s appearing in $\mathrm{P}_{\mathrm{RCL}}$/ $\mathrm{MP}_{\mathrm{RCL}}$ bits. A bit '1' of the latch output increments the 'Level counter' through the XNOR logic thereby the randomness of each bit sequence can be determined. Eight XNOR logic gates generate 8 independent clock to trigger the respective counter. This is done by driving one of XNOR input by the output of 8 respective latches, while the other is always held high. Once, the Mod 128 counter completes the count, the 7th bit resets all the latches and the level counters, as shown in Fig. 8. Now the PCL is ready to evaluate the next set of inputs.

A priority selector in the last stage of PCL identifies one of the best randomized output among the eight $\mathrm{P}_{\mathrm{RCL}}$/ $\mathrm{MP}_{\mathrm{RCL}}$ bit sequences, at the outputs of the 8 Level counters. Three priority range checkers that estimate the Hamming Weight (HW) will provide the most highly random skimmed outputs of both P and MP. The range logic 'Priority 1' (63≤'1'≤65), is set as the highest priority checker to determine the maximum non-zero bit sequence if any within this range. Failing which the next in line 'Priority 2' range logic (60≤'1'≤68) is invoked to determine the best random bit sequences. Failing of the above two checks will trigger the third range logic 'Priority 3' (57≤'1'≤71), to provide the final skimmed bits of both $\mathrm{P}_{\mathrm{PCL}}$ & $\mathrm{MP}_{\mathrm{PCL}}$. Hamming weights obtained for all the respective $\mathrm{P}_{\mathrm{RCL}}/\mathrm{MP}_{\mathrm{RCL}}$ for three datasets of $\mathrm{P}_{\mathrm{H}}/\mathrm{MP}_{\mathrm{H}}$ are shown in Table II. It is observed that for all considered input data, higher HW for at least one $\mathrm{P}_{\mathrm{RCL}}/\mathrm{MP}_{\mathrm{RCL}}$ is obtained validating that the Bio-Hash skimmer yields a highly unique and random 128 bits of outputs. Thus the key generated from such scrambled output will result in an irreversible complex key.

4) Fusion Process to Generate Bio-Hash Key: The P & MP skimmed values, viz., $\mathrm{P}_{\mathrm{PCL}}$ & $\mathrm{MP}_{\mathrm{PCL}}$ are randomly fused through a pre-designed fusion logic to obtain the final Bio-Hash key, as shown in Fig. 9. Fusion logic includes a first stage splitter and a random fusion circuitry. Initially, the 128 bits of both $\mathrm{P}_{\mathrm{PCL}}$ and $\mathrm{MP}_{\mathrm{PCL}}$ will be equally split as two set of each 64-bit blocks of data by the splitter. The MSB block of both $\mathrm{P}_{\mathrm{PCL}}$ [127:64] & $\mathrm{MP}_{\mathrm{PCL}}$ [127:64] are represented as $\mathrm{P}_{\mathrm{PCLx}}$ & $\mathrm{MP}_{\mathrm{PCLx}}$ respectively, whereas the LSB block $\mathrm{P}_{\mathrm{PCL}}$ [63:0] & $\mathrm{MP}_{\mathrm{PCL}}$ [63:0] are represented as $\mathrm{P}_{\mathrm{PCLy}}$ and $\mathrm{MP}_{\mathrm{PCLy}}$ respectively. These block of bits are then randomly fused by the subsequent random fusion circuitry that operates on four fusion modes, viz. F1, F2, F3 and F4. These four modes are selectively invoked based on the value of two bits selection line that are obtained by concatenating 128th bit of both $\mathrm{P}_{\mathrm{PCL}}$ & $\mathrm{MP}_{\mathrm{PCL}}$. The pre-designed fusion logic that exhibits four modes can be expressed as in (1) to (4). The structure of the fusion logic built with combinational circuits and two 4 × 1 MUXs, exhibiting the circuit function during F2 mode (i.e., highlighted when the 128th bit of $\mathrm{P}_{\mathrm{PCL}}$ & $\mathrm{MP}_{\mathrm{PCL}}$ is '0' & '1' respectively) is shown in Fig. 8. The outputs of these MUXs are then concatenated to yield a final 128 bits of Bio-Hash key. The patient medical details are then encrypted with this generated Bio-Hash key during the Write mode using AES encryption algorithm. For the purpose of key retrieval during registration and Read only mode, a KD database is populated with all such generated Bio-Hash keys. Secure storage of this key to shield KD against SCA, is facilitated by concatenation with secret bits. The Bio-Hash key MSBs are appended with the 8 MSB bits of hashed P biometric minutiae to form the P specific secret bits, referred here as 'Refer_bits'.

$$\begin{aligned}\mathrm{F1} = &\sim([127]\,P_{RCL}\,\&\,[127]\,MP_{RCL})\ \&\\ &\{(P_{RCLy}\ \sim\&\,MP_{RCLy})\,||\\ &\qquad(P_{RCLx}\ \sim\oplus\,MP_{RCLx})\}\end{aligned}\tag{1}$$

$$\begin{aligned}\mathrm{F2} = &\ (\sim[127]\,P_{RCL}\ \&\ [127]\,MP_{RCL})\ \&\\ &\{(P_{RCLy}\ \oplus\ MP_{RCLy})\,||\\ &\qquad(P_{RCLx}\ \sim|\,MP_{RCLx})\}\end{aligned}\tag{2}$$

$$\begin{aligned}\mathrm{F3} = &\ ([127]\,P_{RCL}\ \&\sim[127]\,MP_{RCL})\ \&\\ &\{(P_{RCLy}\ \sim\oplus\,\mathrm{MP}_{\mathrm{RCLy}})\,||\\ &\qquad(P_{RCLx}\ \sim\&\,MP_{RCLx})\}\end{aligned}\tag{3}$$

$$\begin{aligned}\mathrm{F4} = &\ ([127]\,P_{RCL}\ \&\ [127]\,MP_{RCL})\ \&\\ &\{(P_{RCLy}\ \sim|\,MP_{RCLy})\,||\\ &\qquad(P_{RCLx}\ \oplus\ MP_{RCLx})\}\end{aligned}\tag{4}$$

B. Write Mode and View Mode

The complete health record of the patient such as blood investigation reports, radiology images, diagnostics history, and prescription/treatment must be verified, updated, and approved by the MP. The MP is provided with an option of selecting Write/View mode through mode selector logic upon authorization by P through an enable signal (Shown in Fig. 2). In Write mode, the patient medical data in the form of either image or document is processed for encryption utilizing the generated Bio-Hash key for secure storage. In order to do so, the entire medical data are handled in sequence of 128 bits, to be encrypted with the Bio-Hash key (128 bits), through the AES hardware engine [26]. This encrypted data then can be stored securely in the medical record database (MRD) as depicted in Fig. 2. The filename of a specific medical record can be saved with patient and MP details for quick identification; alternatively, patient unique identification number also can be used to track down the details. View mode when opted by MP, invokes AES decryption engine directly through the Bio-Hash key. This enables the viewing of the past medical history of the patient under examination. A MUX logic is utilized to appropriately fetch the present Bio-Hash key directly from HMRF logic, rather than retrieving from the key database. D-flip-flops synchronizes both HMRF and the View mode logics with comparatively reduced Latency.

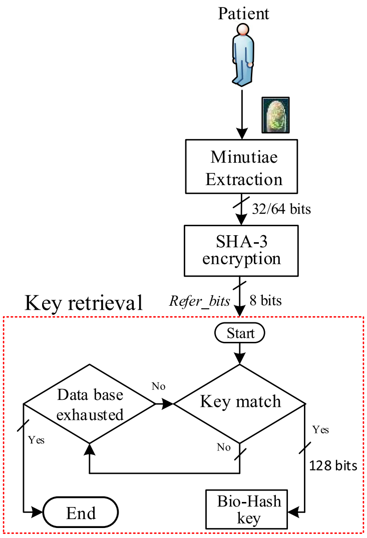

Fig. 10. Key retrieval process during read only mode.

C. Read Only Mode

Read only mode proposed in this work enables the secure view of medical report by the patient themselves. In this mode, the reverse process as applicable for any decryption process is performed to display the data as shown in Fig. 10. The patient is first required to enable this mode followed by extraction of the biometric minutiae. Representation of the minutiae is done in 32 bits hexadecimal to generate the Refer_bits through dedicated SHA-3 engine. Retrieval of the key from the key database starts with 'Key Match', in which the 8 MSB bits of all the stored keys is compared with the Refer_bits to determine the matching key. Once the key is determined the 8 MSB bits are truncated leaving with only 128 bits of the original Bio-Hash key. The retrieved key is utilized for decryption of the health data through the AES decryption engine. Upon successful decryption the patient can review their own medical details in Read only mode. Alterations of medical history/data is restricted to eliminate self-modification for ulterior motives in this mode.

IV. Hardware Implementation

The proposed hardware e-Health Record System involves dual cryptographic engine that secures both the key and the health data, functioning as a parallel architecture. Hierarchical module evaluation is preferred for fair comparison of the modules with the existing designs. The proposed pseudo cascaded SHA-3 architecture being the primary sub-module of HMRF Logic, determines the sub-system performance. Therefore, specific performance comparison of this sub-module is done with the existing designs [22], [23], [24], [25] and [29] to evaluate the Area, F, TP and E_f performances. The primary target devices for the system level implementation of AES+HMRF logic that

TABLE III
IMPLEMENTATION RESULTS OF SHA-3

Design		Device	Clock count	Area (Slices)	F (MHz)	TP (Gbps)	E_f (Mbps/ Slices)
Reported work	[22]	A7	24	4188	309	16.4	3.9
	[23]	V7	24	1432	326	7.8	5.5
	[24]	V5	24	1433	205	0.9	0.7
	[25]	V6	24	532 + 7 BRAM	200	4.8	4.6
	[29]	Virtex Ultrascale	24	352 + 130 DSP	526	23.8	-
This Work - Pseudo Cascaded SHA-3		V7	23	1745	415	10.4	6.0
		Zedboard	23	1606	438	10.9	6.8

includes the proposed SHA-3, are V7 and Zedboard boards. Individual functional mode performances are also discussed in the subsequent sub-sections.

A. Evaluation of Bio-Hash Key Generator

HMRF logic being a core module that generates the random Bio-Hash key from the P/MP biometric traits require stringent design specifications as it influences the overall system performances. A bottom-up evaluation approach is preferred as optimizing the system level performances depends solely on the bottom modules. The HMRF key generator being the core and crucial sub-system in the hierarchy, includes pseudo cascaded SHA-3, Bio-Hash skimmer (RCL and PCL logic) and Fusion logic. The sub-modules that contribute to the performances of HMRF logic are evaluated individually. Validation of the proposed pseudo cascaded SHA-3 architecture is carried out initially with target implementation being V7 & Zedboard. The primary target parameters of improvement are Area (in slices) and clock cycle count ($\mathrm{C_n}$). Latency can be then found from $\mathrm{C_n}$ as shown in (5) below;

$$\text{Latency} = C_n \times \text{CP} \tag{5}$$

Where, CP, the Clock period is 5 ns. The performance metrics of the proposed architecture over the state of the art reported designs [22], [23], [24], [25] and [29], are compared and tabulated in Table III. The pseudo cascaded architecture provides better performance in terms of Area as low as 1745 & 1606 slices on V7 & Zedboard respectively. Further, the number of clock cycles has been observed to be low, when compared to [22], [23], [24], [25] for a single block message, yielding a low Latency. Also, significantly high efficiencies of 6.0 Mbps/slices and 6.8 Mbps/slices have been noticed while implementing in V7 and zedboard devices respectively. Hamming distances (HD) between the proposed pseudo cascaded SHA-3 and the conventional design have been estimated to validate the computational effectiveness and hence the security strength of the hash digested outputs. Six different binarized fingerprint biometric datasets of P and MP, with each being 32 bits are hashed individually utilizing the pseudo cascaded SHA-3 architecture. The six set of hashed outputs obtained are $\mathrm{P_{H1}}$-$\mathrm{P_{H6}}$ & $\mathrm{MP_{H1}}$-$\mathrm{MP_{H6}}$ for P & MP respectively, with each output binary block being 512 bits. HD estimation done exclusively between $\mathrm{P_{H1}}$-$\mathrm{P_{H6}}$ and the conventional SHA-3 outputs of $\mathrm{x_1}$-$\mathrm{x_6}$ are plotted in Fig. 11(a), whereas HD between output data $\mathrm{MP_{H1}}$-$\mathrm{MP_{H6}}$ and the conventional SHA-3 outputs of $\mathrm{y_1}$-$\mathrm{y_6}$ are plotted in Fig. 11(b). It is noted that the HD for similar output data have significant variations from 296 to 359, validating that the proposed SHA-3 design has negligible correlation. Further, the range of HD varying from 307 to 359 for non-similar output data, proves that the pseudo cascaded architecture yields better security against pre-image collision attack [30]. Further the Hamming Weight for each biometric datasets irrespective of whether $\mathrm{P_H}$ or $\mathrm{MP_H}$, the proposed design has better non-zero outputs than the conventional design, as tabulated in Table IV. This indicates that the proposed design achieves better nonequivalence than the conventional architecture, rendering higher security.

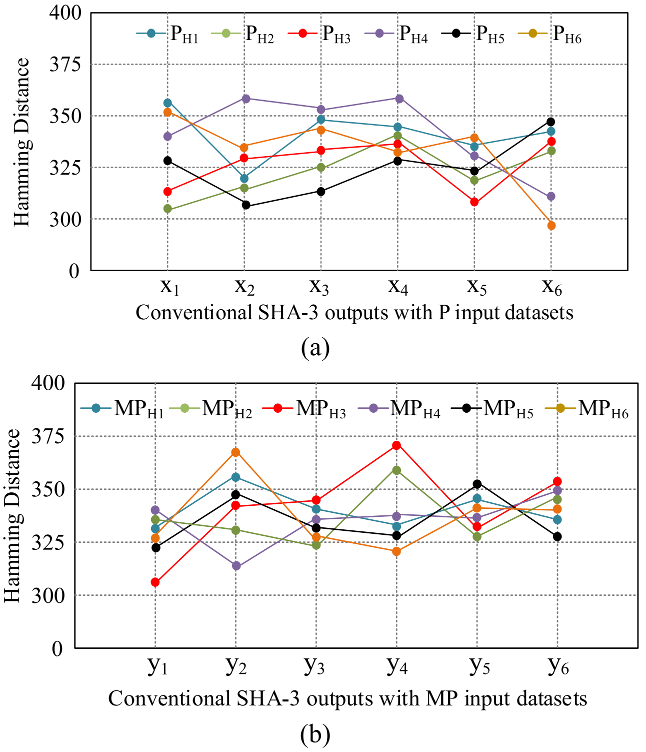

Fig. 11. HD estimation between outputs of the proposed SHA-3 design and the conventional design: (a) HD between $\mathrm{P_{H1}}$-$\mathrm{P_{H6}}$ and $\mathrm{x_1}$-$\mathrm{x_6}$ (b) HD between $\mathrm{MP_{H1}}$ - $\mathrm{MP_{H6}}$ and $\mathrm{y_1}$ - $\mathrm{y_6}$.

TABLE IV
AREA PERFORMANCE COMPARISON

S.No	SHA-3 (P & MP)		RNG (P & MP)		Fusion	
	Design in	Slices	Design in	Slices	Design in	Slices
1	[21]	5744	[31]	286	[36]	1203
2	[23]	2864	[32]	704	-	-
3	[24]	2866	[33]	684	-	-
4	This work	3490	This work	258	This work	99

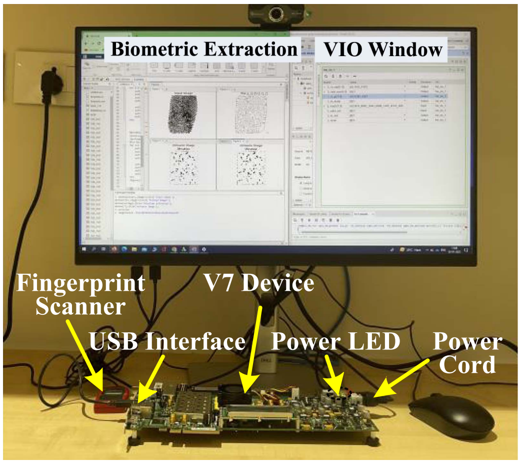

Fig. 12. Experimental setup of Bio-Hash key generator: Hardware interface of VC707 board with fingerprint scanner.

The experimental setup to generate the Bio-Hash key on V7 device of the VC707 FPGA board is shown in Fig. 12. The proposed Bio-Hash skimmer implemented on the V7 device has achieved an overall Area of 731 slices. RCL being the primary circuit in Bio-Hash skimmer, occupied significantly low Area of only 258 slices than the earlier designs [31], [32], [33]. Fusion logic, the last stage in HMRF has achieved 99 slices on V7 device. This is found to be extremely low when compared to the reported fusion methods designed in [3], [10], [34], [35] and fusion score approach in [36]. To compare the overall Area performance of HMRF sub-system (excluding level splitter and PCL) with the reported work, the best performed individual designs (such as SHA-3, Random Number Generator (RNG) and fusion techniques), reported in various research work have been collated. The combined Area performance of SHA-3 reported in [23], the RNG in [31] and Fusion design in [36], yields 4353 slices (2864 + 286 + 1203). This is 11.6% high when compared to the proposed HMRF logic with only 3847 slices, as evident in Table IV. Therefore, the proposed HMRF including level splitter and PCL is proved to have better Area performances of 4191, utilizing a Unitarian design approach.

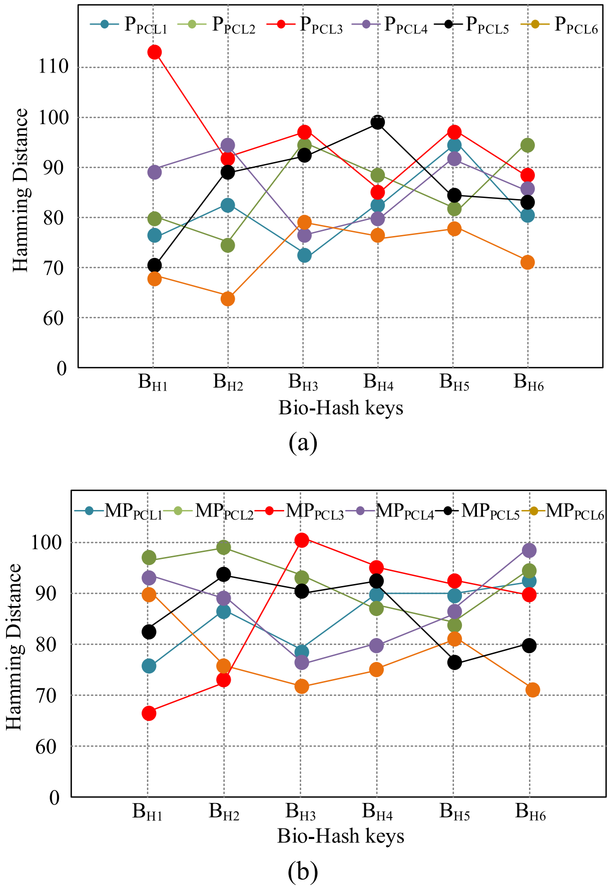

Fig. 13. HD estimation for six biometric input data (a) HD between Bio-Hash keys and P_{PCL} (b) HD between Bio-Hash keys and MP_{PCL}.

TABLE V
HAMMING WEIGHT ESTIMATION

Biometric datasets	SHA-3 (512)		Bio-Hash skimmer	BIO-HASH key
	Proposed	Existing		
P_1	260	249	63	69
MP_1	264	238	65	
P_2	244	229	64	70
MP_2	232	235	64	
P_3	240	271	64	72
MP_3	263	274	63	
P_4	252	260	64	74
MP_4	250	227	64	
P_5	238	222	65	61
MP_5	259	270	65	
P_6	251	252	63	59
MP_6	267	264	64	

The security analysis on the final Bio-Hash key is essential to validate its uniqueness and randomness [28]. Therefore, the output key generated by the proposed hardware from two independent biometric sources and as well as from a single source, were considered for the comparative analysis. Key generated from single source can be of either due to only P biometric (P_{PCL}) or only MP biometric (MP_{PCL}), of each being 128 bits. Hamming Distance has been estimated between the fused Bio-Hash key (B_H with length 128 bits) due to dual sources and, the key obtained from single source. The obtained Hamming Distance for six different biometric input datasets are shown in Fig. 13(a) and (b). The HD variation while considering the analysis between the six Bio-Hash keys (B_{H1} - B_{H6}) and, with all the other six keys of both P_{PCL} and MP_{PCL} is found to be in the range of 71 to 101, for similar input datasets. Though the datasets are similar, the generated Bio-Hash keys by the HMRF logic are unique with significantly larger hamming distances irrespective of the input sources. Further, the HD variation from 64 to 113 for non-similar datasets indicated that the Bio-Hash key is significantly unique for all types of input data. The non-zero bits present in the Bio-Hash keys for six different fusion input datasets range from 59 to 74, as shown in Table V. Thus the

TABLE VI
EVALUATION OF WRITE/VIEW/READ ONLY MODE

Operational modes	HET (in ns)	Dynamic Power (W)	Static Power (W)	Total Power (W)	Area (slices)
Write mode (HMRF + AES_E)	8.268	1.418	0.256	1.674	4339
View mode (HMRF + AES_D)	8.341	1.420	0.257	1.677	4306
Read only mode (AES_D + SHA-3 +key retrieval)	8.004	0.676	0.249	0.925	1878

randomness of the generated key is found to be significantly high for all different biometric data.

B. Hardware Evaluation of Write/View/Read Only Mode

The Bio-Hash key generated by the HMRF logic provides live key for AES encryption during Write mode and populate KD database securely. However, in View mode this live key feeds only AES decryption. On the other hand, a key retrieval logic retrieves the secured Bio-Hash key from KD to perform AES decryption during the Read only mode. A system level performance evaluation in terms of HET, Power and Latency is done for each functional modes with a standard 100 MHz clock. HET is proportional to both CP and Slack and can be directly determined from (6) as shown below;

$$\mathrm{HET} = \mathrm{CP} - \mathrm{Slack} \tag{6}$$

During Write mode, MP performs medical examination and generates report with authorization by P. This requires invoking of both HMRF logic and AES_ E (AES encryption) engine. On the other hand, the View mode enabled by both P & MP requires utilization of both HMRF logic and AES_D (Decryption) engine. HET is determined to be marginally high in View mode when compared to Write mode as shown in Table VI. The additional hardware requirement to synchronize key generator logic and mode selector logic has resulted in high HET during View mode. On the other hand, the Read only mode that invokes only SHA-3 engine and key retrieval module yields low HET of 8.004 ns and low Power of 0.676 Watt when implemented on V7. Two reported relevant works have been taken in to consideration for system level Latency comparison. The design in [37] has demonstrated key generation technique utilizing the conventional SHA-3 and SHA-2 architectures. Whereas, the other in [38] demonstrated improved security utilizing a dual encryption technique based masked key AES engine along with SHA-2. A bar chart comparative analysis with these above two reported works has (shown in Fig. 14), revealed that the proposed work in Write mode out performed in terms of Latency performance though the frequency is comparatively low.

C. Authentication Analysis of Key Retrieval

Matching analysis [34] to determine the accuracy level of fingerprint recognition during key retrieval at decision level is essential. To validate the robustness of the authentication system, large databases that include fingerprints captured under different situations and cases are required for a comprehensive assessment. The open databases, FVC 2004 & LivDet2015 that include real fingerprints captured with different scanners (such as Optical sensor and Thermal Sweeping sensor) at different scenarios (Fingers when dry and wet), and as well as synthetically generated fingerprints, have been considered in this work for experimental analysis. Randomly, 20 and 16 subjects from LiveDet2015 and FVC 2004 databases respectively are chosen for P's fingerprint samples. MP's fingerprints are also chosen from the respective database for the purpose of Bio-Hash Key generation, to populate the KD database. Authentication analysis performed utilizing the designed key retrieval module, yielded satisfactory performance with accuracies of 98.9% for LiveDet2015 database and 98.2% for FVC 2004 database. The True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) prediction parameters for a total of 640 real world biometric samples [39] of LivDet2015 and 352 samples of FVC 2004 database [40], are provided in Table VII. The False Acceptance Rate (FAR) and False Rejection Rate (FRR), are found to be as low as 2.3% & 0.78% respectively for LivDet2015, and 2.08% & 1.17% respectively for FVC 2004 database.

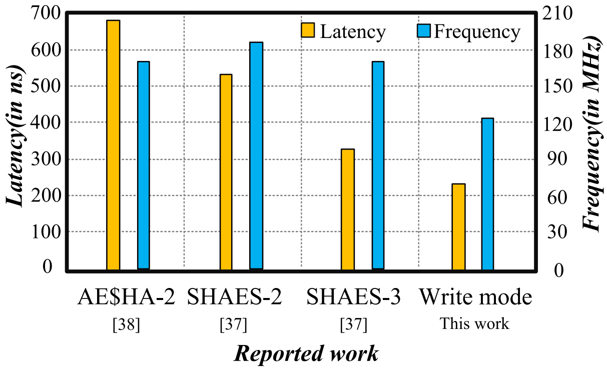

Fig. 14. Latency performance analysis.

TABLE VII
KEY MATCHING ANALYSIS AT DECISION LEVEL

	LivDet2015 database			FVC 2004 database		
	Subjects -20	Predicted		Subjects -16	Predicted	
	Total - 640	Positive	Negative	Total - 352	Positive	Negative
Actual	Positive 512	TP 508	TN 125	Positive 256	TP 253	TN 94
	Negative 128	FP 3	FN 4	Negative 96	FP 2	FN 3

V. CONCLUSION

The proposed Bio-Hash secured e-Health Record System is a novel all-hardware design when compared to the EHR, EMR, and PHR. The HMRF implemented on V7 is found to have a clock count of 46 with Latency being 230 ns while on Write mode during encryption. This is much better when compared to similar designs that were partially implemented on

Virtex 2 board, with reported Latency being in the range of few milliseconds [8]. The proposed HMRF logic (excluding level splitter and PCL) also performed better in terms of Area as low as 3847 slices, when compared with the total Area of the individual design reported in [23], [31] and [36]. Furthermore, evaluation of the individual Write/View/Read only modes resulted in satisfactory performances with HET being 8.268/8.341/8.004 ns respectively. The reuse of key generator logic circuit during three modes of operation has facilitated in Area reduction when implemented on V7 device. As both the MRD & KD are further secured with highly random Bio-Hash key, the medical record is effectively shielded against SCA. The Area and Power performances of the three functional modes and the system level implementation are shown in Table VI. Thus it is certain for conclusion that a highly secured electronic hardware health record system is designed, developed and evaluated in this work. As a future work ASIC based Medical data securing system with an off-chip memory for the database will be designed to enable portability for hand-held applications.

Acknowledgment

The overwhelming support extended by Dr. Amalin Prince. A, Associate Professor, BITS Pilani, K. K. Birla Goa Campus, in carrying out the experimental testing and verification is duly acknowledged. Further, the access provided to the reconfigurable computing laboratory facilities has immensely attributed to the successful completion of the real time testing of the e-Health Record System.

References

[1] J. Dong, X. Meng, M. Chen, and Z. Wang, "Template protection based on DNA coding for multimodal biometric recognition," in *Proc. IEEE 4th Int. Conf. Syst. Inform.*, 2017, pp. 1738–1742.

[2] X. Zhang, D. Cheng, P. Jia, Y. Dai, and X. Xu, "An efficient android-based multimodal biometric authentication system with face and voice," *IEEE Access*, vol. 8, pp. 102757–102772, 2020.

[3] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, "Deep hashing for secure multimodal biometrics," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1306–1321, 2021.

[4] R. Dwivedi et al., "A fingerprint based crypto-biometric system for secure communication," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 4, pp. 1495–1509, 2020.

[5] N. Ansari, P. Sakarindr, E. Haghani, C. Zhang, A. K. Jain, and Y. Q. Shi, "Evaluating electronic voting systems equipped with voter-verified paper records," *IEEE Secur. Privacy*, vol. 6, no. 3, pp. 30–39, May/Jun. 2008.

[6] J. Galbally, R. Haraksim, and L. Beslay, "A study of age and ageing in fingerprint biometrics," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 5, pp. 1351–1365, May 2019.

[7] F. J. Zareen and S. Jabin, "Authentic mobile-biometric signature verification system," *Inst. Eng. Technol. Biometrics*, vol. 5, no. 1, pp. 13–19, 2016.

[8] C.-L. Lei and Y.-H. Chuang, "Privacy protection for telecare medicine information systems with multiple servers using a biometric-based authenticated key agreement scheme," *IEEE Access*, vol. 7, pp. 186480–186490, 2019.

[9] M. M. Sravani and S. A. Durai, "Attacks on cryptosystems implemented via VLSI: A review," *J. Inf. Secur. Appl.*, vol. 60, 2021, Art. no. 102861.

[10] M. Hammad, Y. Liu, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," *IEEE Access*, vol. 7, pp. 26527–26542, 2019.

[11] B. Topcu, C. Karabat, M. Azadmanesh, and H. Erdogan, "Practical security and privacy attacks against biometric hashing using sparse recovery," *EURASIP J. Adv. Signal Process.*, vol. 2016, no. 1, pp. 1–20, 2016.

[12] World Health Organization, "Management of patient information," *Glob. Observatory E Health Ser.*, vol. 6, p. 80, pp. 1–80, 2012.

[13] J. Liu, H. Tang, R. Sun, X. Du, and M. Guizani, "Lightweight and privacy-preserving medical services access for healthcare cloud," *IEEE Access*, vol. 7, pp. 106951–106961, 2019.

[14] K. Edemacu, B. Jang, and J. W. Kim, "Efficient and expressive access control with revocation for privacy of PHR based on OBDD access structure," *IEEE Access*, vol. 8, pp. 18546–18557, 2020.

[15] X. Yang, T. Li, X. Pei, L. Wen, and C. Wang, "Medical data sharing scheme based on attribute cryptosystem and blockchain technology," *IEEE Access*, vol. 8, pp. 45468–45476, 2020.

[16] M. M. Madine et al., "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020.

[17] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[18] J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS," *IEEE Access*, vol. 8, pp. 59389–59401, 2020.

[19] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5914–5925, Apr. 2021.

[20] M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data," *IEEE Access*, vol. 8, pp. 52018–52027, 2020.

[21] M. M. Sravani and S. A. Durai, "On efficiency enhancement of SHA-3 for FPGA-based multimodal biometric authentication," *IEEE Trans. Very Large Scale Integration Syst.*, vol. 30, no. 4, pp. 488–501, Apr. 2022.

[22] R. Paul and S. Shukla, "Partitioned security processor architecture on FPGA platform," *Inst. Eng. Technol. Comput. Digit. Techn.*, vol. 12, no. 5, pp. 216–226, 2018.

[23] S. El Moumni, M. Fettach, and A. Tragha, "High throughput implementation of SHA3 hash algorithm on field programmable gate array (FPGA)," *Microelectronics J.*, vol. 93, Nov. 2019, Art. no. 104615.

[24] M. Knezevic et al., "Fair and consistent hardware evaluation of fourteen round two SHA-3 candidates," *IEEE Trans. Very Large Scale Integration Syst.*, vol. 20, no. 5, pp. 827–840, May 2012.

[25] A. Alzahrani and F. Gebali, "Multi-core dataflow design and implementation of secure hash algorithm-3," *IEEE Access*, vol. 6, pp. 6092–6102, 2018.

[26] H. Hidayarni, A. Nabihah, and R. S. Hawa, "The 128-bit AES design by using FPGA," *J. Phys.: Conf. Ser.*, vol. 1529, no. 2, 2020, Art. no. 022059.

[27] M. Fons, F. Fons, and E. Cantó, "Fingerprint image processing acceleration through run-time reconfigurable hardware," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 57, no. 12, pp. 991–995, Dec. 2010.

[28] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 5th ed., London, U. K.: Pearson Educ. Inc., 2011.

[29] D.-E.-S. Kundi and A. Aziz, "A low-power SHA-3 designs using embedded digital signal processing slice on FPGA," *Comput. Elect. Eng.*, vol. 55, pp. 138–152, Oct. 2016.

[30] S. Onopa and Z. Kotulski, "Improving security of lightweight SHA-3 against preimage attacks," *Int. J. Electron. Telecommun.*, vol. 64, no. 2, pp. 159–166, 2018.

[31] M. Garcia-Bosque, A. Pérez-Resa, C. Sánchez-Azqueta, C. Aldea, and S. Celma, "Chaos-based bitwise dynamical pseudorandom number generator on FPGA," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 1, pp. 291–293, Jan. 2019.

[32] S. Kalanadhabhatta, D. Kumar, K. K. Anumandla, S. A. Reddy, and A. Acharyya, "PUF-based secure chaotic random number generator design methodology," *IEEE Trans. Very Large Scale Integration Syst.*, vol. 28, no. 7, pp. 1740–1744, Jul. 2020.

[33] L. G. de la Fraga, E. Torres-Pérez, E. Tlelo-Cuautle, and C. Mancillas-López, "Hardware implementation of pseudo-random number generators based on chaotic maps," *Nonlinear Dyn.*, vol. 90, no. 3, pp. 1661–1670, Nov. 2017.

[34] C. Li, J. Hu, J. Pieprzyk, and W. Susilo, "A new biocrypto system oriented security analysis framework and implementation of multibiometric cryptosystems based on decision level fusion," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 6, pp. 1193–1206, Jun. 2015.

[35] N. Celik, N. Manivannan, and W. Balachandran, "Multimodal biometrics for robust fusion systems using logic gates," *J. Biometrics Biostatistics*, vol. 6, no. 1, pp. 218–223, 2015.

[36] P. C. Bhaskar and V. R. Munde, “FPGA implementation of non-subsampled Shearlet transform for image fusion,” in *Proc. IEEE Int. Conf. Comput., Commun., Control Automat.*, 2017, pp. 1–6.

[37] M. M. Sravani, S. A. Durai, and A. Nabhiah, “FPGA implementation of novel hybrid hash function SHAES for digital signatures,” in *Proc. 4th Int. Conf. Elect. Electron. Eng.*, 2021, pp. 62–70.

[38] M. M. Sravani, S. A. Durai, M. P. Reddy, G. Sowjanya, and A. Nabihah, “FPGA implementation of masked-AE$HA-2 for digital signature application,” in *Algorithms for Intelligent Systems*, Berlin, Germany: Springer, 2022, pp. 469–483.

[39] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay, and S. A. Schuckers, “LivDet 2015 fingerprint liveness detection competition,” in *Proc. IEEE 7th Int. Con. Biometrics Theory, Appl. Syst.*, 2015, pp. 1–6.

[40] “FVC2004—Third international fingerprint verification competition,” 2022. [Online]. Available: http://bias.csr.unibo.it/fvc2004/download.asp

M. M. Sravani received the bachelor’s and master’s degrees from JNTU Anantapur University, Anantapur, India. She is currently working toward the Ph.D. degree with the Vellore Institute of Technology, Chennai, India, under the supervision of Dr. S. Ananiah Durai. Her research interests include cryptographic hardware implementation, reconfigurable computing, and digital logic design.

S. Ananiah Durai received the Doctorate degree in integrated circuit design from Massey University, Auckland, New Zealand. He is currenlty a Professor with the Centre for Nanoelectronics and VLSI Design, School of Electronics Engineering, Vellore Institute of Technology, Chennai, India. He has authored more than 20 research papers published in various peer-reviewed journals. His research interests include analog CMOS IC design, microsensor system design and integration in CMOS-MEMS, hardware security, and on-chip signal conditioning circuit design.