IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 9, 2020, accepted January 1, 2021, date of publication January 6, 2021, date of current version January 14, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3049564

Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing

MARYAM SHABBIR[1], AYESHA SHABBIR[1], CELESTINE IWENDI[2], (Senior Member, IEEE), ABDUL REHMAN JAVED[3], MUHAMMAD RIZWAN[1], NORBERT HERENCSAR[4], (Senior Member, IEEE), AND JERRY CHUN-WEI LIN[5], (Senior Member, IEEE)

[1]Department of Computer Science, Kinnaird College for Women Lahore, Lahore 54000, Pakistan
[2]Department of Electronics BCC, Central South University of Forestry and Technology, Changsha 410004, China
[3]Department of Cyber Security, Air University, Islamabad 44000, Pakistan
[4]Department of Telecommunications, Brno University of Technology, 616 00 Brno, Czech Republic
[5]Department of Computer Science, Electrical Engineering, and Mathematical Sciences, Western Norway University of Applied Sciences, 5063 Bergen, Norway

Corresponding author: Jerry Chun-Wei Lin (jerrylin@ieee.org)

This work is partially supported by the Western Norway University of Applied Sciences, Bergen, Norway.

ABSTRACT Despite the numerous and noticeable inherited gains of Mobile Cloud Computing (MCC) in healthcare, its growth is being hindered by privacy and security challenges. Such issues require the utmost urgent attention to realize its full scale and efficient usage. There is a need to secure Health Information worldwide, regionally, and locally. To fully avail of the health services, it is crucial to put in place the demanded security practices for the prevention of security breaches and vulnerabilities. Hence, this research is deliberated on to provide requirement-oriented health information security using the Modular Encryption Standard (MES) based on the layered modeling of the security measures. The performance analysis shows that the proposed work excels, compared to other commonly used algorithms against the health information security at the MCC environment in terms of better performance and auxiliary qualitative security ensuring measures.

INDEX TERMS MES, health information security, mobile cloud computing, requirement-oriented approach, modular protection-based computing.

I. INTRODUCTION

As computing technologies have rapidly growth [1], [2], cloud computing has earned a lot of popularity in recent years through applications, services, storage, and computing over the Internet. It is commonly utilized in many domains like Medical Science, Agriculture, Business, Information Technology, and many others. Additionally, it encourages resource provisioning flexibility and cost-effective decoupling administrations. Smart devices like smartphones and tablets are progressively turning into a fundamental constituent of human life as a convenient and effective tool for communication that is not limited by place and time. Smart device users assemble rich experience of different administrations from mobile apps such as Google Applications and iPhone applications which run on the remote servers using wireless connectivity to the network. The integration of cloud computing with mobile phones is known as Mobile Cloud Computing (MCC) [3], [4].

As MCC can offer a few significant benefits, for example, expanded battery life and high-level storage capability, scalability, adaptability, and a few key demands keep on being a significant hindrance to MCC. An overview of MCC is depicted in FIGURE 1. One of the leading difficulties incorporates the security and privacy of confidential information. Nowadays, MCC is highly involved in cloud based-health monitoring, but due to lack of proper security, it is not getting as much attention as it should be. Such challenges need to be addressed to appeal to the mobile cloud user towards MCC [5]–[7].

The associate editor coordinating the review of this manuscript and approving it for publication was Gautam Srivastava.

TABLE 1. Medical records.

Records	Details
Primary Records	Age, Gender, Marital status, Education, Family situation, Family history of the disease, Economic situation
Lifestyle	Physical Activity, Diet, Smoking, Drinking, and Occupational visits.
Health Disorders	Eye, Foot, Diabetic, Nephropathy, Cerebrovascular, Cardiovascular, and other disorders.
Recall Records	Medications, Accessory evaluations, Signs, symptoms, and cause for referral to a doctor.
Daily review Records	Difficulties like Hypertension and Hypoglycemia.
Examinations	Cerebrovascular, Cardiovascular state, Blood lipids, Blood pressure, Blood glucose control or others.
Diagnosis regimens	Administering drugs, a Lifestyle guide

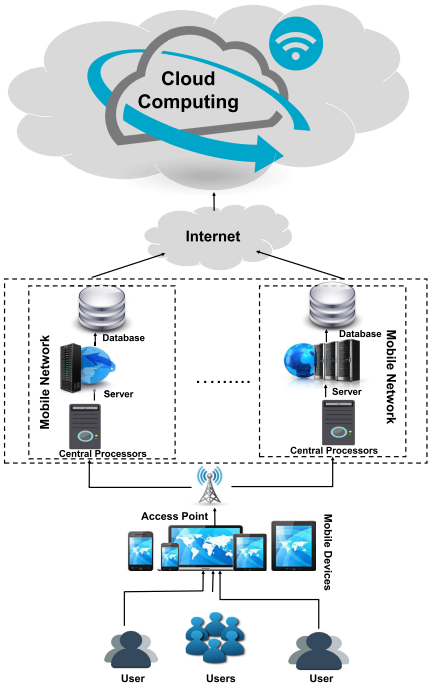


FIGURE 1. Mobile cloud computing.

Security of Health Information (HI) is an iterative procedure (with the technological improvements) along with the changes to the healthcare environs. By the adaptation of new schemes to upgrade the quality and effectiveness of HI in practice, it is additionally imperative to reconsider the security policies and practices of HI [8]–[12]. Recognizing the threats and securing the HI is challenging and demanding for small health-centers. This research is intended to enable the practice to get ready for those demands and challenges, for effective risk assessment, and provide suitable security approaches to ensure HI security. MCC is a potential approach for versatile electronic services. In like manner, MCC is probably going to be an incredible approach to monitor the healthcare space. MCC offers new sorts of administrations and offices for patients and guardians.

In the healthcare domain, MCC offers several favors [13] as:

1) Portability: The facilitation of remote access monitoring of health information in a ubiquitous and distributed manner.
2) Scalability: The facilitation of remote access to patient information.
3) Modernization: MCC lessens the barriers to the modernization of healthcare applications.
4) Performance: A quick access to computing, big data storage can be done by MCC. It provides easy information sharing and cost reduction as well.
5) Collaboration: It provides team-care facilitation and maintained collaboration.

The integration and federation requirements from distinct domains like health insurance, hospitals, and medical laboratories, have evolved the domain of Health Information Security (HIS). HIS can be regarded as the utilization of e-commerce policies and practices and the infrastructure of Information Technology (IT) for the manipulation, sharing, and processing of Health Information (HI). It is one of the rising fields of public health and medical informatics. HI requires organized and coordinated tactics, which comprises the collection of HI monitoring and securing approaches at cloud [14]. Among other solutions, MCC can be the leading HI monitoring approach. The integration of Cloud Computing, Healthcare Computing, and Mobile Computing are known as Healthcare Mobile Cloud Computing (HMCC) as shown in FIGURE 2. Table 1 presents the types of medical records. While the threats to different kinds of medical records and their impacts can be categorized as given in Tables 2 and 3.

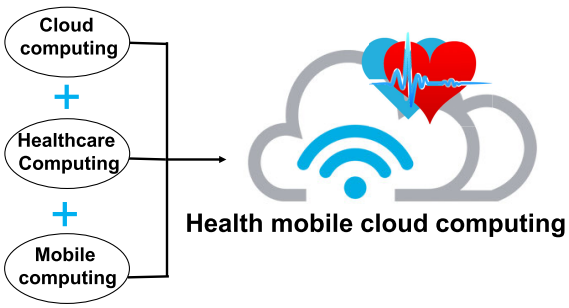


FIGURE 2. Health mobile cloud computing [15].

Although HI offers interesting security and protection challenges that require a crisp assessment of the standard facilities and approaches to deal with HI security [16]–[18]. The importance of security and protection in healthcare raises the issues of the information classification, which is the primary determinant in the adaptation and successful utilization of

TABLE 2. Categorization of HI threats.

Threat	Description
HI-Repudiation	Cannot get HI (outside the trust-limit) from a source. Consideration of auditing and logging to record the summary, time, and source. Devising the claims: cannot compose information got from an individual on the trust-boundary's opposite side.
HI-Tampering	Refer to consistent Cross-Site Scripting (CSS) risks and threats as it does not clean the inputs and output of the information storage device and to CSS risks. Altering or reading the information sent over a verified dataflow. Attacker tampering and prompting device corruption. Log-files based attacks.
HI-Spoofing	Attacker spoofing, prompting data revelation. Consider utilizing a standardized verification scheme to distinguish the procedure of destination. Attacker spoofing, prompting wrong information transmitted to the web-servers. Attacker spoofing, rather than the information is written to the device, prompting the target of the attacker.
DDoS-Attack	To a server, a DDoS attack that associates with a biosensor, the device of the user, is a potential danger that can make a service unfeasible. Resource utilization can be difficult to manage, and there are times that it works well to let the Operating System carry out the tasks.
Confidentiality Breach	A confidentiality breach happens when information or data given in certainty to the cloud service provider by the user is revealed to an outsider without the consent of the user.
HI-forgery /Eavesdropping	Attack to individual data and clinical records that move between the server and the biosensor, the server, and the medical-framework, or the server and the device of the user.

TABLE 3. Impacts of security loss.

Security-concerns	Impact
Confidentiality loss	Reputation loss; Legal claims; Trust loss; Embarrassment for patient
Availability Loss	Financial impacts; Low-level quality of service; Legal impacts; Inadequate treatment for the patient
Integrity Loss	Financial issues; Inadequate management; Poor treatment of the patient
Repudiation Issues	Reputation loss; Accountability loss; Financial issues
Non-auditability	Inadequate management; Inability to claim penalties and take legal action
Authenticity Loss	Poor treatment of the patient

HI. Current schemes in the domain of HI management highlight the requirement for extensive joining of confidentiality, privacy, and security safeguards inside the HI security approaches and practices. This raises significant challenges that require a comprehensive approach for security engineering to identify, classify, and secure the variety of HI [19]. The following questions represent the objectives behind this research:

- How can a layered security modeling approach be applied toward HI security and what are the significant consequences of this?
- What kind of threats can be prevented by the Layered Security modeling?
- How can we protect the HI against the MCC insider's (cloud service provider's) attacks?
- How can a modular protection-based computing scheme be utilized in an MCC environment, with some modules at the user side, and few at the cloud side?
- How can we have a requirement-centric and data nature-centric securing approach against HI confidentiality?

General cloud-based healthcare management is shown in FIGURE 3. Although various cryptographic and non-cryptographic schemes have been utilized for the assurance of privacy and security preservations of HI at MCC, however, this research is aimed at utilizing and analyzing a layered security-based data nature-centric cryptographic scheme i.e., MES, against the assurance of HI confidentiality in the MCC environment. Additionally, we provided the secure HI sharing mechanism among the intended parties

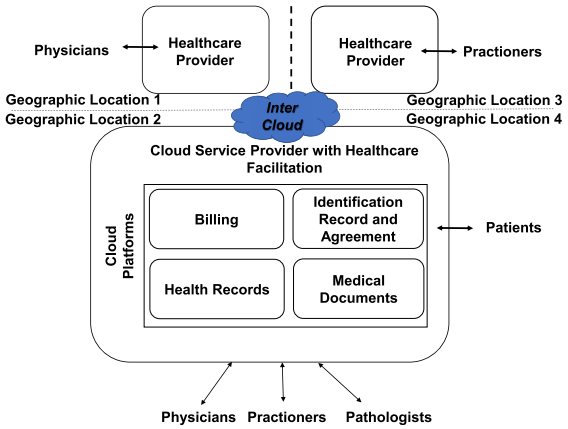


FIGURE 3. Medical data management at cloud [20].

(healthcare, patient, doctor, or referral by one doctor to some other specialist) based on the requirements. The upcoming paragraph provides a short description of the intended scheme discusses how MES ensures confidentiality.

MES is a modular symmetric cryptographic algorithm. Using this scheme, the first module with entropy-based Key generation is actualized on the MCC client-side and the second extender/contractor module is intended for the extension and compression of health records before transferring data to the cloud. Then the remainder of the modules are performed on the crypto-cloud and lastly, the multi-cloud-based storage is carried out. Consequently, such a modular scheme at different layers drives us towards the multi-layered modular security of health records at the cloud. In this way, even the

cloud service provider cannot approach the HI, because each cloud service provider approaches the enciphered version of the health record (i.e., the block of data, not the entire data). In this way, it would protect the HI, from insider access as well as from outside access too. The differentiating features of the intended scheme in the MCC environment are presented below:

- The proposed work provides secure HI storage against ensuring the confidentiality of the cloud service provider.
- It ensures the confidentiality of HI against any hacker or third party/malicious outsider.
- It provides a requirement centric approach against ensuring the confidentiality of HI (i.e., separate classification of security provision based on the sensitivity level of HI).
- Full control of the patient to their HI.
- Unwanted attempt to access the HI would be restricted.
- Only the patient has full access to his data. Also, based on a requirement can be shared with others i.e., specialists and experts.
- Layered modeling with modularity support against the intruder's attacks to HI.

The proposed work would tackle all the above-mentioned concerns. The remainder of the article is arranged as follows. Section II provides the literature of this research. Section III presents an overview of the methodology. Section IV elucidates the detailed mechanism of the proposed work. Section V explains the performance analysis of the proposed work, whereas Section VI concludes the study.

II. RELATED WORK

The section presents the literature survey of the HI security threats and approaches against ensuring its confidentiality in the cloud. Potent security and privacy risks and threats of MCC have appeared as considerable issues. MCC's users and enterprises are greatly dependent on their provided services. Numerous research attempts and solutions have been proposed to attend privacy and security challenges.

Tele-monitoring (not a novel innovation in Information-Technology) has been utilized to remotely screen the patient's health (that are present in far off places), like clinical centers and emergency clinics. These days, it is a potent E-health service. By the utilization of telecommunication technologies, the diagnosis, evaluation, and treatment of the patient are being carried out. While performing diagnosis and treatment, access to Electronic Health Information (EHI) is a prerequisite. Despite the emerging popularity of EHI cloud-based maintenance and monitoring, there are numerous security challenges. Among these challenges, attack for information theft is a key challenge. AlSheikSalem and Al-Ani [15] proposed a scheme for private healthcare information security utilizing fog computing i.e., tri-party one round authenticated key agreement protocol. Where among the participants, a session key can be generated, and consequently, a decoy technique based, secure healthcare information accession scheme was implemented.

One of the emerging technologies in healthcare monitoring is the Internet of Things (IoT). This technology refers to interact with everyday objects. Several studies [21]–[23] analyzed the scenarios of connectivity of wireless sensors (connected to the objects) and the interconnection of multiple objects. The key benefit of the utilization of such technologies is the betterment of the quality of E-health facilitation. In these systems, the information gathered by these sensors is susceptible. Accordingly, this sensitive information needs to be secured. Vijayalakshmi and Arockiam [24] presented a hybrid scheme to overcome this security challenge. This scheme is comprised of a cryptography approach for the prevention of unauthorized access. Hence, this scheme supports secure E-health information transmission.

Ciphertext Policy Attribute-Based Encryption (CP-ABE) for the realization of fine-grained access control against smart health security was performed by Zhang *et al*. [25]. The utilization of CP-ABE in smart-healthcare comprises different issues. To tackle these challenges, a privacy-aware smart health access control system is provided (i.e., PASH with the primary constituent is the partially hidden CP-ABE). In PASH, only the name attribute is disclosed and in encrypted smart health records, the access policy's attribute values are hidden. Moreover, the more susceptible data is carried by the attribute values. An effective decryption test of SHR is realized by PASH (it requires few bilinear-pairings).

Physicians perform the remote monitoring of patient's data using electronic healthcare systems. The E-health systems provide easy data management by using different technologies like cloud computing but on the other hand, it entails many security issues. Due to different security and privacy challenges, to preserve the patient's secrecy, an efficient and flexible scheme is required that ensures the disclosure of information to selectively authorized entities. Accordingly, Sánchez-Guerrero *et al*. [26] proposed a secrecy-aware profile management scheme that generates a strong distinctive credential for the user claims (which comprises the generation of adaptive Merkle trees through user profiles).

In the domain of Mobile Healthcare Social Network (MHSN), data privacy is one of the leading challenges. A secure profile matching and data-sharing scheme in cloud computing for MHSN are proposed by Huang *et al*. [27]. The Identity Based Broadcast Encryption (IBBE) is used for outsourcing the enciphered data to the cloud. Moreover, efficiently and securely the sharing of data to the doctor's group is performed. To propagate the doctor's referral to another doctor, an attribute-based conditional data re-encryption is used where the encrypted text is transformed into a new enciphered text (without leaking the sensitive information).

While sharing and performing the integration of E-health information, to tackle the security and privacy challenges, this manuscript focused on providing a solution to these challenges at the Internet applications. Bao *et al*. [28] proposed an application layer based signal scrambling scheme (to scramble the healthcare information, a tiny data is utilized). A random number generator or a piece of data is utilized for

the tiny data derivation (that increases the flexibility of the scheme).

For the physiological parameters of the patient in Sensor Cloud Infrastructure (SCI), Masood *et al*. [29] provided a six-step based framework. These steps are: (i) the preliminary selection, (ii) systems entity's selection, (iii) technique selection, (iv) patient's physiological parameter's assessment, (v) security analysis, and (vi) performance estimation. For healthcare data confidentiality, cloud computing is a very promising technology. It is required alongside the use of electronic communication with the amalgamation of other securing techniques. Among different schemes, Health Insurance Probability and Accountability Act (HIPAA) is the leading one provided by Mbonihankuye *et al*. [30]. For the adequate and well-preserved record-keeping of healthcare data, different analytical and conservational methods can be utilized.

Electronic healthcare-services utilize different schemes for patient-care, which can be utilized in different clinical-applications. Patient data is enciphered to ensure authoritative access to patient's sensitive information. In the framework provided by Padmashree *et al*. [31], the patient gives the key to the specialist. While in emergency-care, a patient offers an Attribute-Based-Key (ABK) with a lot of emergency-supporting representatives and allows access to the specialist for using the Emergency Key (EK). The Doctor decodes the clinical-records by utilizing ABK and EK, to protect the life of the Patient. Cyber-attacks in social insurance have extended by 125% since 2010 and are presently the main source of HI security threats, as pointed by Ködmön and Csajbók citekodmon2015informaciobiztonsag accordingly provided a mix of LSB and 3DES to enhance the security measures applied to medical-information. To build up the experimental simulation, the Java programming language was utilized. Common block ciphers against the HI security at cloud comprises AES, DES, 3DES, IDEA Blowfish, RC5, and RC6, etc.

Incremental and Iterative approaches are not normally considered in existing methodologies for Information Security (IS) frameworks, narrated by Shameli-Sendi *et al*. [33]. Accordingly, the author proposed a framework to execute high quality and successful IS. It was delegated to relegate the organizational tasks and assignments. Fuzzy logic was applied to evaluate the risk level. De Carvalho Junior *et al*. [34] intended to pinpoint the limitations, concerns, and implementation associated characteristics over the role-based access control. In light of the assessment and finding for role-based access control detection, it is the crucial consideration of HI monitoring requirements. A few schemes cater to the role-based access control adjustments to adapt to HI challenging security demands. Overall, current role-based access control schemes are not concerned with the HI industry. Several studies [35], [36] were presented for efficient and secure architecture against the searchable health-information.

A scheme that joins the watermarking scheme with encryption techniques for the exchanged medical image's security is the primary issue of this research. The framework depends on a hybrid approach to facilitate with medical image's diverse security highlights while exchanging the medicinal records. The specialists are presented by Al-Haj and Abdel-Nabi [37]. These days, cyber-attackers are focusing on healthcare and medicinal services as the most favored domain as highlighted by Alharam and El-Madany [38] presented a comparison of the various cybersecurity applications and concentrated on the Advanced Encryption Standard utilization for protecting medicinal services against cyber-assaults, and its applications in e-HI. Several works [39]–[42] presented the review of the security and privacy issues of E-health.

In Tele-monitoring, there exist several studies focusing on medical record sharing and efficient resource provisioning for the autonomous healthcare systems [43]–[50], but these frameworks deficit in providing a data nature-oriented security approach. Lastly, by having an overview of the previous related researches, we can analyze that the existing schemes lack in providing a multi-layered, requirement-centric, and data nature-oriented scheme that provides secure acquisition, storage, and sharing of HI at the cloud or MCC environment.

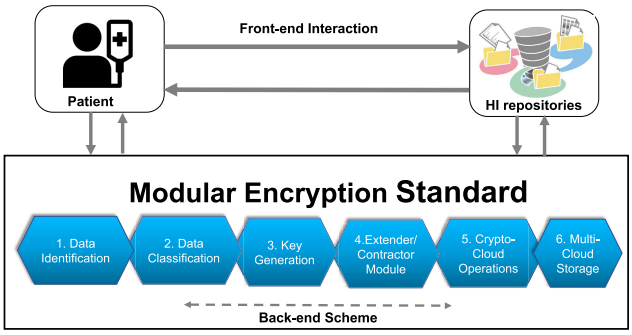


FIGURE 4. Overview of the steps against the assurance of HI confidentiality at MCC.

III. OVERVIEW OF THE PROPOSED WORK

This section presents an overview of the proposed work. The steps that need to be performed while using MES against ensuring the HI confidentiality at MCC are depicted by FIGURE 4, while FIGURE 5 presents the overall scenario for HI security using MES at MCC. Among these six steps, some of them are performed at the MCC user side; rest of the confidentiality ensuring measures at the intermediary cloud (i.e., Crypto-cloud) and finally, the data is stored using multi-cloud. These measures are crucial to protect HI against the different kinds of attacks at the cloud i.e., insider's and outsider's attacks. This research is intended to come up with the solution against the 5th category of the threat as given in Table 2.

This scheme begins with Health record identification and classification. This classification and identification are from the perspective of the level of confidentiality required. Most importantly at the MCC client-side (1st module), an entropy-based generated key would be allocated (arbitrarily created key). The HI owner chooses the key accordingly,

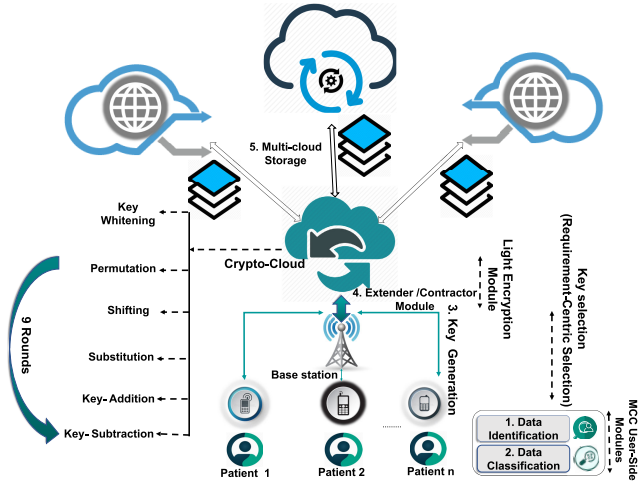


FIGURE 5. Healthcare monitoring using MES.

based on the type of information stored. The key selection is dependent on HI identification and classification. Now, the next module would encipher the health record (to some extent) utilizing the contractor/extender scheme. Here the acceptance of 56-bit based plaintext and extension to 64-bit (i.e., light encryption) would be done. After going through the contractor/extender scheme, it is passed to the mediator cloud i.e., crypto-cloud. In this way, information is not given over to the CSP as is (i.e., in genuine plaintext form however rather the extended version), in other words, the information transmitted to the crypto-cloud is not the real type of information but expanded form. Next, the crypto-cloud is meant for cryptography i.e., for performing the securing step (defined in Section IV) and here the HI would be divided among distinct blocks, and these blocks would be put away at multi-clouds (i.e., the enciphered version).

IV. PROPOSED METHODOLOGY

MES includes three significant measures. These measures are ''Identification (IDN)'', ''Classification (CLF)'', and ''Securing (SC)''. IDN and CLF are performed at the MCC user side. While the SC step is performed at the Crypto-cloud. Crypto-cloud is the intermediary cloud that is dedicated to performing cryptography measures.

A. IDENTIFICATION

The requirement for securing HI is directed by IDN and CLF characterization (as per the level of confidentiality of HI). Here, the identification (to distinguish the criticality and sensitivity of HI) would be performed. The IDN of Health records depends on the MCC client's highlighted prerequisites. It usually comprises two general classifications, with subsequent sub-classifications. Confidential HI (with high-level security), and open/public HI (which does not require security).

Algorithm 1: Algorithm-MES Encryption

Declaration;
PT ← Plaintext;
N ← Size of PT;
CT ← Ciphertext;
PPT ← Padded form of PT;
BPT ← Binary form of PT;
EPT ← Extended form of PT;
AGK ← Auto-generated Key;
K_i ← Key, $i = 0, 1, \ldots, 9$;
CT ← Ciphertext;
Execution- Encryption;
N ← Length(PT);
BPT ← BinaryFormatting(PT);
if $N < 64$ **then**
    PPT ← Padding(BPT);
EPT ← Extension(PPT);
KEY-Transformation(AGK);
Key-Whitening(K_0);
while $i < 9$ **do**
    Permutation(EPT);
    CT ← Shifting(EPT);
    CT ← Substitution(EPT);
    CT ← Key-Addition(K_i);
    CT ← Key-subtraction(K_i);
    i++;
end
KeyEncryption(AGK)

B. CLASSIFICATION

In HI, classification selects the degree of secrecy based on the nature of the record. It is useful in picking the HI that really ought to be secured, and it consequently decreases the security expenses. These two classifications are categorized into five distinctive sub-classifications (based on the degree of sensitivity). The 5 diverse sub-classifications are referenced beneath. The securing measure comprises five unique kinds of keys for the beneath referenced five sub-classifications.

1) NON-SENSITIVE DATA

- Public Data e.g., Doctor's/specialist's availability hours and clinics etc.

2) SENSITIVE DATA

- Less-Sensitive Data e.g., patient name, gender, etc.
- Moderately-Sensitive Data e.g., Doctors/specialists or the medical centers to which the patient is referring, patient-doctor appointment date, timings, etc.
- Highly-Sensitive Data e.g., Patient's diagnostic reports, etc.
- Extremely-High Sensitive Data e.g., Genetic Information, etc.

Algorithm 2: Algorithm-MES Decryption

Declaration;
PT ← Plaintext;
CT ← Ciphertext;
N ← Size of CT ;
PPT ← Padded form of PT;
UPCT ← Un-Padded form of CT;
SCT ← String form of CT;
CCT ← Contracted form of PT;
AGK ← Auto-generated Key;
K_i ← Key, $i = 0, 1, \ldots, 9$;
PT ← Plain Text;
Execution- Decryption;
Key-Decryption(AGK);
KEY-Transformation(AGK);
while $i < 9$ **do**
    PT ← Permutation(EPT);
    PT ← Shifting(EPT);
    PT ← Substitution(EPT);
    PT ← Key-Addition(K_i);
    PT ← Key-Substraction(K_i);
    PT ← i-Key-Whitening(K_0);
    i++;
end
SPT ← StringFormate(CT);
if $PPT! = NULL$ **then**
    UPCT ← Un-padding(SPT);
CCT ← Contraction(UPCT);
N ← Length(PT);

C. SECURING

The securing measure comprises the rest of the cryptographic steps. These steps would be performed at the crypto-cloud. This step comprises 9 rounds, with 10 keys (key-0 for key whitening and the rest of the 9 keys for the 9 rounds). FIGURES 6 and 7 shows the modular interaction for the entire mechanism of HI storage and permitting access of HI at the cloud. The algorithm for the MES encryption and decryption is presented in the next section.

D. MODULAR INTERACTION

Three modules at the user side provide the connection of the patient to the smart devices. Next at the second layer, the connection of smart devices to the crypto cloud is done by implementing the 'securing' measure, which comprises eight sub-measures. Lastly, the connection of crypto-cloud to multi-cloud is done (i.e., the encrypted ciphertext is transferred to multi-cloud) (see FIGURE 6). FIGURE 7 depicts the modular interaction for allowing access to confidential HI (by the patient to the doctor or specialist).

E. MATHEMATICAL MODEL

The used notations in the designed model is then shown in Table 4.

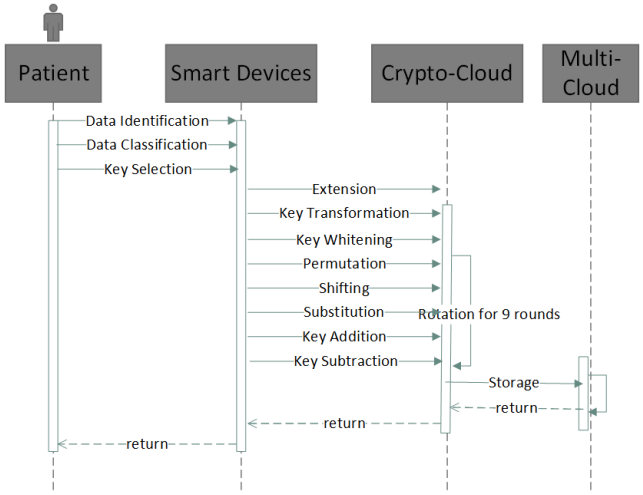


FIGURE 6. HI storage at cloud using MES.

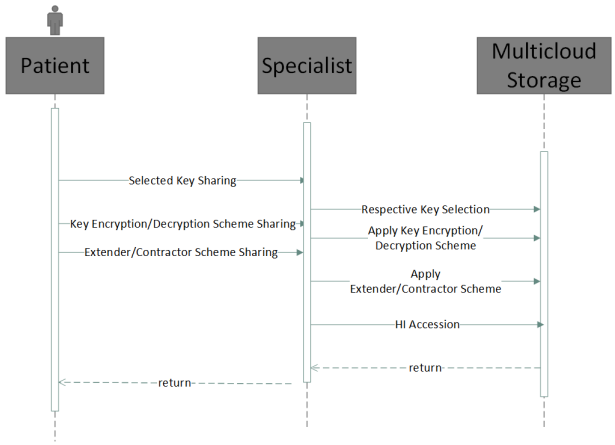


FIGURE 7. HI storage sharing using MES.

TABLE 4. The used notations.

PT	Plaintext
K	Key
Ext	Extension
Cn	Contraction
LEPT	Lightly Encrypted Plaintext
Exp	Expansion
DExp	Discard Expansion
Pr	Permutation for r^{th} $round$
Sr	Substitution for r^{th} $round$
K_L^r	Left half key for any r^{th} $round$
K_R^r	Right half key for any r^{th} $round$
fXfY	Fx

In the case of x-bit block and y-bit key, a Block Cipher (BC) is described in the Equation 1.

$$(PT, K) \rightarrow CT \tag{1}$$

$$CT = \varepsilon(PT, K) \tag{2}$$

Equations (1) and (2) show the encryption criteria on the plaintext using the private key. The detailed mathematical model is provided below:

1) ENCRYPTION AT THE PATIENT SIDE

Plaintext extension from 56 bit to 64 bit is described by the Equation (3). The resulting data is regarded as Lightly Encrypted Plaintext.

$$LEPT = Ext(PT) \tag{3}$$

To perform Key whitening, LEPT is temporarily extended from 64 bits to 128 bits and described in Equation (4). The key used for key whitening is K0. The K0 is the single key that transforms the LEPT one time. However, for the rest of the keys (i.e., K1 to K9), each key transforms the LEPT twice.

$$(LEPT)Exp \bar{\oplus} K_0 \tag{4}$$

To discard the temporary contraction, DExp is applied to reduce the LEPT to 64 bit, which is described in Equation (5).

$$DExp((LEPT)Exp) \bar{\oplus} K_0 \tag{5}$$

Next, the Permutation for any r^{th} round is performed as described in Equation (6).

$$(LEPT \bar{\oplus} K_0)P^r \tag{6}$$

After performing the substitution for any r^{th} round, the key addition (for any r^{th} round) by the left half key and key subtraction (for the same r^{th} round) by the right half key are then performed, which is described in Equation (7).

$$(((LEPT \bar{\oplus} K_0)P^r)S^r \bar{\oplus} K_L^r) \bar{\oplus} K_R^r \tag{7}$$

2) DECRYPTION AT THE PHYSICIAN/SPECIALIST SIDE

If the MCC user/patient/doctor tries to access the HI from the cloud, the decryption would be then performed. At the decryption side, the right half key of the r^{th} round would be subtracted to cancel out the effect of key subtraction, which is done at the encryption side, and described in Equation (8).

$$(((LEPT \bar{\oplus} K_0)P^r)S^r \bar{\oplus} K_L^r) \bar{\oplus} K_R^r \bar{\oplus} K_R^r \tag{8}$$

Next, using the left half key for any r^{th} round, key addition is performed to cancel the effect of key addition at the encryption side, which is described in Equation (9).

$$((LEPT \bar{\oplus} K_0)P^r)S^r \bar{\oplus} K_L^r \bar{\oplus} K_L^r \tag{9}$$

For any r^{th} round, the inverse substitution is performed to cancel the effect of substitution at the encryption side, which is described in Equation (10).

$$S_r'(((LEPT \bar{\oplus} K_0)P^r)S^r) \tag{10}$$

For any r^{th} round, inverse permutation is performed to cancel the effect of permutation at the encryption side as described in Equation (11).

$$P_r'((LEPT \bar{\oplus} K_0)P^r) \tag{11}$$

Key whitening at the decryption side would negate the key whitening effect at the encryption side, which is described in Equation (12).

$$LEPTK_0 \bar{\oplus} K_0 \tag{12}$$

After performing the contraction at the decryption side, LEPT is converted to normal PT, which is described in Equation (13).

$$PT = Cn(LEPT) \tag{13}$$

Consequently, the resulting plaintext is obtained at the decryption side as the elucidated above. A flowchart of this entire MES scheme is shown in FIGURE 8.

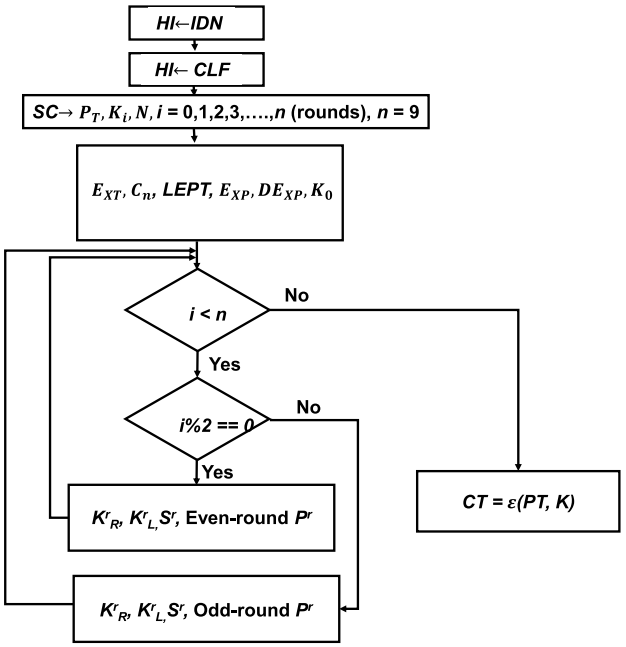


FIGURE 8. Flowchart for data enciphering.

3) HI SHARING AT MCC USING MES

The following steps are performed while sharing HI using MCC as shown in FIGURE 9.

1) HI capturing after a health inspection. The patient gets the Health Inspection Report (HIR) on mobile.
2) Transfer of HI from Mobile devices to the cloud and from healthcare to the cloud.
3) In case of treatment (from Patient to Specialist/Doctor), the sharing mechanism describes the access to HI.
4) The doctor accesses the HI from the cloud (by following the mechanism).
5) The doctor diagnoses and suggests any further referral (if required).

4) PATIENT EXAMINATION

The patient gets HIR from the HealthCare Center (HCC). Mutual authentication is performed by the HCC and cloud.

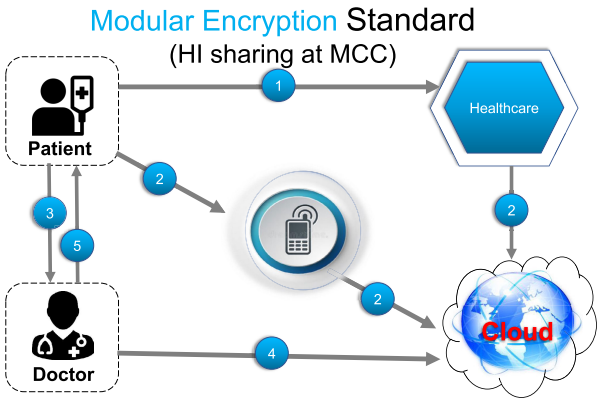


FIGURE 9. HI sharing at cloud using MES.

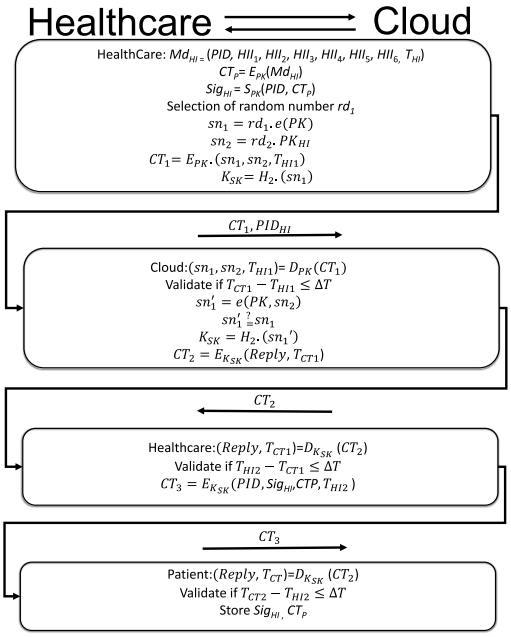


FIGURE 10. Patient examination.

TABLE 5. HI Items (HII).

HI-items	Description
PID	Identity of Patient
HII1	Common Inspection
HII2	Scopy-Exam
HII3	X-ray
HII4	Blood test
HII5	Electrocardiography
HII6	Disease preventive Series

The HCC uploads the HIR to the patient's cloud. An exemplary view of HI items is given in Table 5. The flowchart of the Patient examination stage is presented in FIGURE 10.

Step 1: The HCC utilizes the patient's key (i.e., PK) to encipher the HIR and uses the key to sign the HIR as follows: Md_{HI} is the medical HI. The inspected patient items are presented in Table 6.

TABLE 6. Patient's Inspected HI Items (PI_HII).

HI-items	Description
PID	Identity of Patient
PI_HII1	Blood Pressure
PI_HII2	Pulse Oximetry
PI_HII3	Electroencephalography
PI_HII4	Electrocardiography

Step 2: After getting the message, the key PK is used by the cloud for message decoding.

Step 3: After getting the message, the HCC uses the session-key KSK for deciphering the message.

Step 4: Upon getting the message, the session key KSK is used by the cloud to decipher the message.

A random-number chooses rd1 and utilizes the cloud's key PK to encipher the message for authentication as given below.

5) PATIENT'S DATA UPLOADING

The patient uses the cell phone to gather the HI acquired from healthcare. Before setting off to the hospital, the patient uses the cell phone to move the deliberate HI to the cloud. The flowchart for the transferring of HI to the patient can be seen in FIGURE 11.

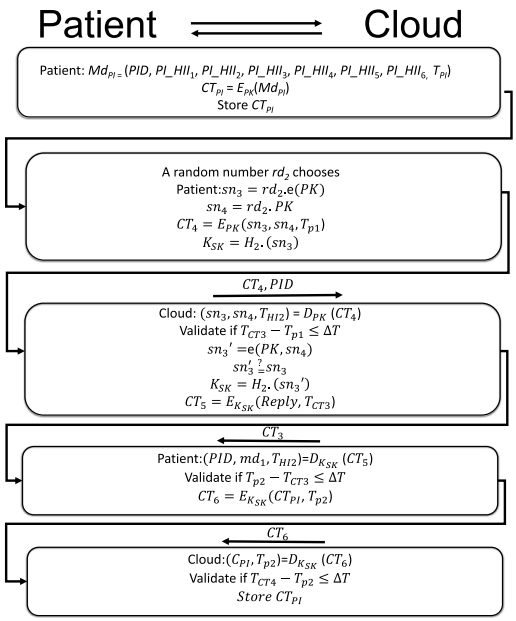


FIGURE 11. Patient's data uploading.

Step 1: The patient inspected medical HI mdPI is sent to the patient by a secure-channel. After the message is received, the patient uses the key PK for message enciphering.

Step 2: The patient picks an arbitrary number of rd2 and utilizes the key PK to encode the message.

Step 3: After getting the message, the cloud utilizes the key PK for message decoding.

TABLE 7. HI risk management at mobile cloud computing using MES.

Risks Management		Description
		Access Management
Malicious-Insiders	✓	Layered modeling with Multi-cloud utilization to protect HI from malicious insiders (Cloud Service Providers)
Malicious-Outsiders	✓	The only owner has full control over HI. No malicious outsider can get access to the HI without owner permission.
		Security Enhancing measures
Modularity	✓	Modularity helps in providing security measures at different layers.
Encryption key management	✓	Five different key varieties, with key encryption as well.
		Requirement Centric Approach
Identification and Classification Measure	✓	Identification and classification help in providing a requirement centric approach (based on the degree of severity and sensitivity of information).
Securing Measure	✓	The entire cryptography approach is comprised of the securing measure.

Step 4: After getting the message, the session key (i.e., KSK) is used by the patient for message decoding.

Step 5: After accepting the message, the cloud utilizes the session key (i.e., KSK) for message decoding.

6) PATIENT TREATMENT

FIGURE 12 shows the patient treatment stage. It comprises the following mentioned steps:

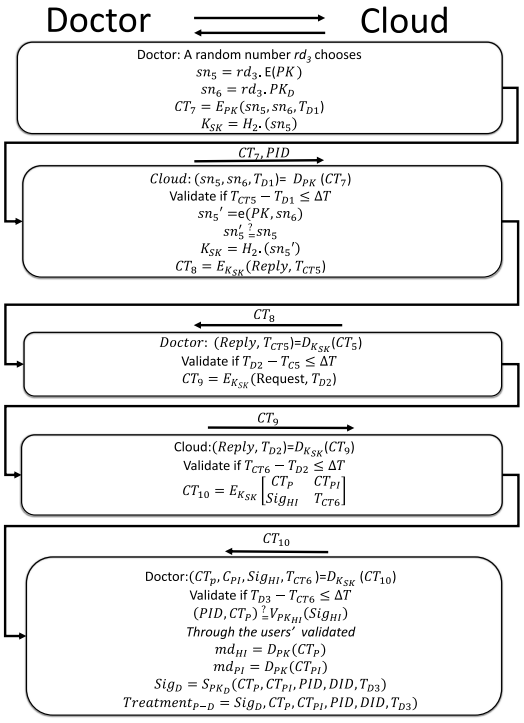


FIGURE 12. Patient's treatment.

Step 1: An arbitrary number rd3 is chosen by the doctor and he utilizes the key PK to encode the message.

Step 2: In the wake of accepting the message, the cloud utilizes the key PK to decipher the message.

Step 3: After accepting the message, the session KSK key is used by the specialist to decipher the message.

Step 4: After accepting the message, the session key KSK is utilized by the cloud to decode the message.

Step 5: After accepting the message, the session key is utilized by the doctor to decode the message.

Step 6: After accepting the message, the cloud utilizes the session key KSK for message decoding. The specialist signs the HIR, (after the treatment) and the gathered inspected patient data.

The qualitative risk management strategies/confidentiality ensuring measures of MES is presented in Table 7.

V. EXPERIMENTS AND RESULTS

This section presents the MES analysis from different perspectives in the MCC environment. MES at cloud was executed utilizing the following mentioned specifications. This section shows the outcomes we obtained from the performance analysis of our proposed work. We examined the performance analysis factors of MES solely and in a comparative view with other common enciphering block ciphers. Table 8 shows the environmental set up for the proposed scheme performance analysis.

TABLE 8. Setup for experiments.

Setup	Description
System	64-bit OS, X-64 based Processor
OS	Windows 10
Processor	Intel(R) Core(TM) i7-7500U CPU @ 2.70 GHz 2.90GHz
Platform	Visual C++ (Visual Studio Community 2017)

A. MODULARITY CHECK

The module-based processor utilization of MES with different sizes of inputs can be seen in Table 9. Furthermore, the module-based execution time of the MES is given as follows.

MES encryption's elapsed time estimation is done. Enciphering time is the time taken by the cryptographic scheme for the transformation of actual data to cipher-text. For any algorithm, the encryption time helps in figuring the throughput. It determines the speed of encryption. The higher the throughput, the lesser the power utilization would be. By using different sizes of inputs, different outcomes were acquired, as explained below. The following graphs showed the supremacy of the proposed work over other algorithms. The outcomes acquired were recorded in seconds.

TABLE 9. Rate of processor utilization.

	Modular-Analysis	Time (1KB sec)	Time (2KBs sec)	Time (3KBs sec)
1	**Key-Transformation**	0.0620079	0.00341145	0.00275324
2	**Key-Whitening**	0.000007030	0.000019749	0.000001057
3	**Rounds**	0.000371302	0.000035610	0.000025030
4	**Key-Encryption**	0.000394236	0.000004572	0.000003534

TABLE 10. Distinct processors based analysis.

Processor Categories	MES Elapsed Time
Intel(R) Core(TM) M-5Y10c CPU @ 0.80GHz 1.00 GHz	0.0542858(sec)
Intel(R) Core(TM) i3-4030U CPU @ 1.90GHz 1.90 GHz	0.515033(sec)
Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz 2.90 GHz	0.330330(sec)

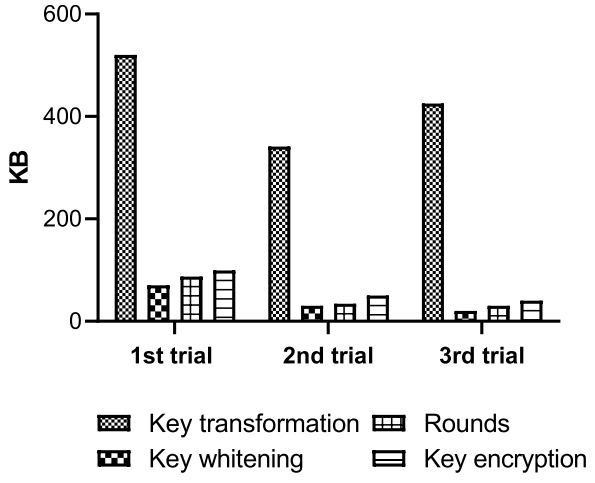


FIGURE 13. Modular analysis of MES.

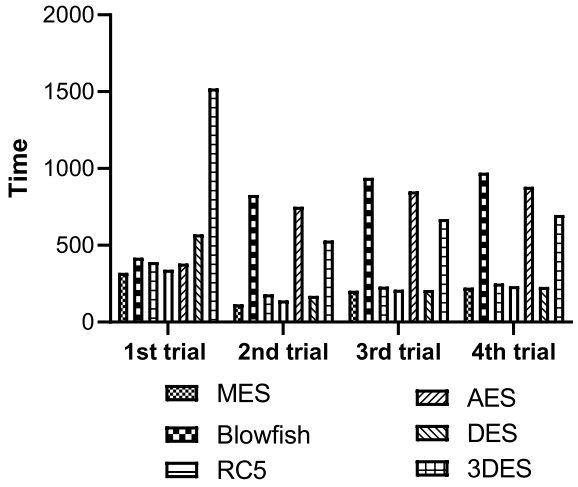


FIGURE 14. Processor utilization rate.

The processor time of each round [8] was analyzed by having different input sizes. Key transformation utilizes generally more CPU cycles than the other modules of MES. The applicability of MES can be seen from the acquired results. The modular analysis of MES is provided in FIGURE 13. FIGURE 14 elucidates the performance analysis of MES with other cryptographic algorithms dependent on processor utilization. This section presents the comparison of commonly used cryptographic block ciphers with MES against HI security at the MCC environment.

Table 10 depicts the outcomes of the execution time of MES on different types of processors. This analysis was done using different data sizes. Secondly, these results were obtained using various generations of Intel processors and the processor utilization time was obtained against each experiment. The processor usage is the analysis of the time that a CPU takes to a particular computation. It reflects the load of the processor. The more CPU used in the enciphering technique; the higher the processor load would be. These experiments are done to check the effectiveness and the effect of the different sizes of inputs and the impact of different platforms on the processor time estimation.

B. MEMORY UTILIZATION

For performance analysis, one of the most critical parameters is memory utilization. The below graphs explain the memory utilization of AES, Blowfish, RC5, RC6 DES, 3DES, and MES. FIGURE 15 depicts the memory utilization of these algorithms. This analysis was carried out with the assistance of the ''Visual studio analysis tab''. MES diagnostic session took 10.043 sec with memory utilization was in kilobytes. While for AES it was 15.265, for Blowfish it was 10.457, for RC5 it was 15.342, for RC6 it was 10.587, For DES it was 15.578, and for 3DES it was 20.025 sec with memory consumption in kilobytes.

C. KEY VARIANCES BASED ANALYSIS

The types of keys (according to user-specified requirements for attaining a specific level of security) or key variations of these different schemes can be seen in FIGURE 16. This is a qualitative comparative approach. DES, 3DES, RC5, RC6, Blowfish, and IDEA facilitates the single type of key (no requirement centric approach), AES gives 3 sorts of keys, and MES gives 5 different types of keys (High degree of requirement-centric approach). Hence, from the below graph, it can be observed that MES possesses the highest level of key variances.

D. KEY-DATA COLLIGATION-RATE FOR SINGLE ROUND

Generally, each key transforms the data twice for each round, except for the Key whitening (KW) step. Aside from KW,

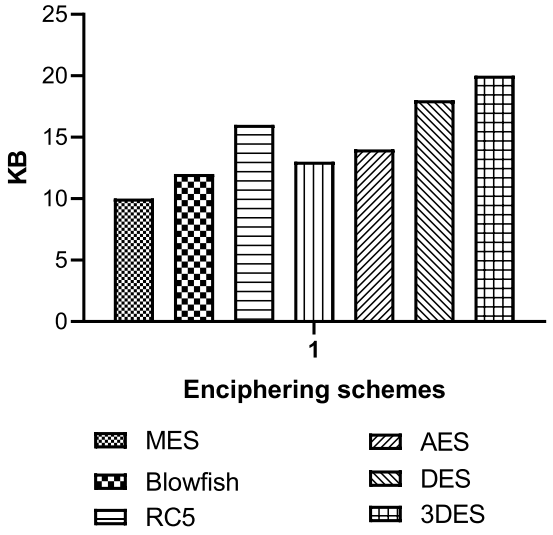


FIGURE 15. Memory utilization.

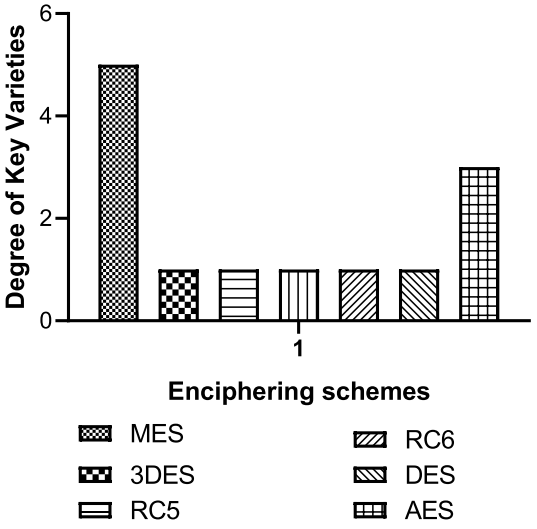


FIGURE 16. Degree of key-varieties.

it is eighteen times key subsuming with information rather than nine times (for 9 rounds), as the key subtraction and key addition are the keys subsuming measures. FIGURE 17 expounds the relative investigation of RC5, RC6, Blowfish, IDEA, AES, DES, 3DES, and MES from the single round key subsuming point of view, where MES performs the transformation twice in each round when contrasted with IDEA, DES, 3DES, RC5, RC6, Blowfish and AES (MES has the highest degree of Key-data colligation rate).

E. TIME/SPACE COMPLEXITIES AND RESULTS ANALYSIS

Like AES, DES, 3DES, etc., MES also works on the static block-sizes. It is independent of the input size and takes $O(1)$ time complexity. The space complexity of MES is $O(n)$. These results can be determined by the designed Algorithms 1 and 2. Moreover, from the above experiments, it can be visualized that MES has better performance than other commonly used algorithms in terms of low

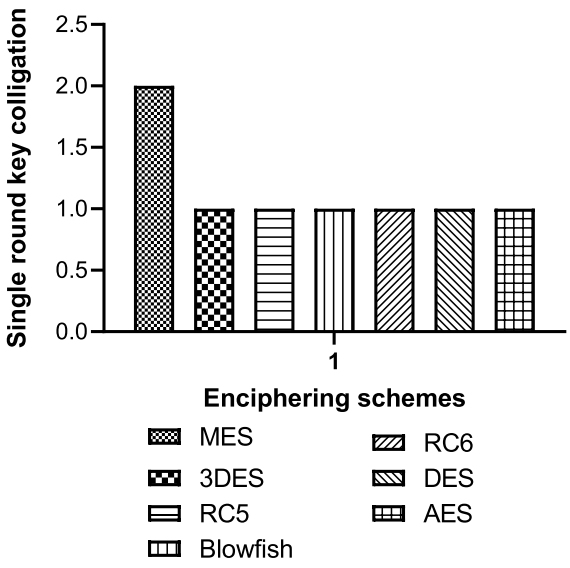


FIGURE 17. Key-data colligation rate.

processor utilization rate, less memory utilization, the highest degree of key variances, and highest data colligation rate and this low memory and processor utilization makes a more favorable choice for mobile devices (i.e., energy and resource-constrained devices). Due to the other distinct qualitative security ensuring measures shown in Table 6, the designed scheme can provide acceptable results in the MCC environment.

VI. CONCLUSION

Despite the prospective solutions offered by MCC in Health record monitoring, numerous impediments restrain the key potentials of MCC. Among these obstacles, security and privacy are the key hindrances in the utilization of MCC in healthcare. This is one of the considerable research gaps. Accordingly, this research utilizes a layered, modular, data nature-centric cryptography approach, for example, MES, that utilizes secure HI sharing, and storage mechanisms. The Comparative results show that this scheme outperforms other commonly used techniques (from different performance factors) in the MCC environment. Some limitations and future directions of the proposed work are given below.

Currently, this approach is intended for the enciphering and deciphering of textual data and there is no consideration of the image-oriented data-set yet. However, in future work, this issue would be considered. Secondly, layered modeling may sometimes result in lowering system efficiency. Accordingly, the efficiency of the proposed work can be further improved by the integration of quantum computing to make it more adaptable for mobile and smart devices. In the future, we may ensure patient privacy using the blockchain security model.

REFERENCES

[1] J. C.-W. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, and M. Aloqaily, "Privacy preserving multi-objective sanitization model in 6G IoT environments," *IEEE Internet Things J.*, early access, Oct. 21, 2020, doi: 10.1109/JIOT.2020.3032896.

[2] J. C.-W. Lin, Y. Shao, Y. Djenouri, and U. Yun, "ASRNN: A recurrent neural network with an attention model for sequence labeling," *Knowl.-Based Syst.*, vol. 212, Jan. 2021, Art. no. 106548.
[3] H. Qi and A. Gani, "Research on mobile cloud computing: Review, trend and perspectives," in *Proc. 2nd Int. Conf. Digit. Inf. Commun. Technol. Appl. (DICTAP)*, May 2012, pp. 195–202.
[4] W. Xu and D. Wu, "A data privacy protective mechanism for WBAN," in *Proc. Wireless Commun. Mobile Comput.*, 2015, pp. 421–430.
[5] A. Nirabi and S. A. Hameed, "Mobile cloud computing for emergency healthcare model: Framework," in *Proc. Int. Conf. Comput. Commun. Eng.*, 2018, pp. 375–379.
[6] L. Griebel, H.-U. Prokosch, F. Köpcke, D. Toddenroth, J. Christoph, I. Leb, I. Engel, and M. Sedlmayr, "A scoping review of cloud computing in healthcare," *BMC Med. Informat. Decis. Making*, vol. 15, no. 1, pp. 1–16, Dec. 2015.
[7] L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, "Mobile cloud computing model and big data analysis for healthcare applications," *IEEE Access*, vol. 4, pp. 6171–6180, 2016.
[8] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, "eHealth cloud security challenges: A survey," *J. Healthcare Eng.*, vol. 2019, Sep. 2019, Art. no. 7516035.
[9] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019.
[10] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4946–4967, Jun. 2019.
[11] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and privacy-preserving challenges of E-health solutions in cloud computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019.
[12] A. Algarni, "A survey and classification of security and privacy research in smart healthcare systems," *IEEE Access*, vol. 7, pp. 101879–101894, 2019.
[13] A. Bartuskova, O. Krejcar, and I. Soukal, "Framework of design requirements for E-learning applied on blackboard learning system," in *Proc. Comput. Collective Intell.*, 2015, pp. 471–480.
[14] X. Wang and Z. Jin, "An overview of mobile cloud computing for pervasive healthcare," *IEEE Access*, vol. 7, pp. 66774–66791, 2019.
[15] O. AlSheikSalem and M. S. Al-Ani, "Mobile cloud computing applied to healthcare approach," *Int. J. Inf. Technol. Converg. Services*, vol. 6, no. 5, pp. 1–8, 2016.
[16] H. Patel, D. S. Rajput, G. T. Reddy, C. Iwendi, A. K. Bashir, and O. Jo, "A review on classification of imbalanced data for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 4, 2020, Art. no. 1550147720916404.
[17] C. Iwendi, S. Ponnan, R. Munirathinam, K. Srinivasan, and C.-Y. Chang, "An efficient and unique TF/IDF algorithmic model-based data analysis for handling applications with big data streaming," *Electronics*, vol. 8, no. 11, p. 1331, Nov. 2019.
[18] S. Kutia, S. H. Chauhdary, C. Iwendi, L. Liu, W. Yong, and A. K. Bashir, "Socio-technological factors affecting User's adoption of eHealth functionalities: A case study of China and ukraine eHealth systems," *IEEE Access*, vol. 7, pp. 90777–90788, 2019.
[19] N. A. Azeez and C. V. der Vyver, "Security and privacy issues in E-health cloud-based system: A comprehensive content analysis," *Egyptian Informat. J.*, vol. 20, no. 2, pp. 97–108, Jul. 2019.
[20] V. Casola, A. Castiglione, K.-K.-R. Choo, and C. Esposito, "Healthcare-related data in the cloud: Challenges and opportunities," *IEEE Cloud Comput.*, vol. 3, no. 6, pp. 10–14, Nov. 2016.
[21] A. S. Black and T. Sahama, "EHealth-as-a-service (eHaaS): The industrialisation of health informatics, a practical approach," in *Proc. IEEE 16th Int. Conf. E-Health Netw., Appl. Services (Healthcom)*, Oct. 2014, pp. 555–559.
[22] A. Alabdulatif, I. Khalil, and V. Mai, "Protection of electronic health records (EHRs) in cloud," in *Proc. 35th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC)*, Jul. 2013, pp. 4191–4194.
[23] M. Bahrami and M. Singhal, "A dynamic cloud computing platform for eHealth systems," in *Proc. 17th Int. Conf. E-Health Netw., Appl. Services (HealthCom)*, Oct. 2015, pp. 435–438.
[24] A. V. Vijayalakshmi and L. Arockiam, "Hybrid security techniques to protect sensitive data in E-healthcare systems," in *Proc. Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Dec. 2018, pp. 39–43.
[25] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018.
[26] R. Sanchez-Guerrero, F. A. Mendoza, D. Diaz-Sanchez, P. A. Cabarcos, and A. M. Lopez, "Collaborative eHealth meets security: Privacy-enhancing patient profile management," *IEEE J. Biomed. Health Informat.*, vol. 21, no. 6, pp. 1741–1749, Nov. 2017.
[27] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," *IEEE Access*, vol. 6, pp. 36584–36594, 2018.
[28] S.-D. Bao, M. Chen, and G.-Z. Yang, "A method of signal scrambling to secure data storage for healthcare applications," *IEEE J. Biomed. Health Informat.*, vol. 21, no. 6, pp. 1487–1494, Nov. 2017.
[29] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure," *Wireless Commun. Mobile Comput.*, vol. 2018, Nov. 2018, Art. no. 2143897.
[30] S. Mbonihankuye, A. Nkunzimana, and A. Ndagijimana, "Healthcare data security technology: HIPAA compliance," *Wireless Commun. Mobile Comput.*, vol. 2019, Oct. 2019, Art. no. 1927495.
[31] M. G. Padmashree, S. Khanum, J. S. Arunalatha, and K. R. Venugopal, "SIRLC: Secure information retrieval using lightweight cryptography in HIoT," in *Proc. IEEE Region 10 Conf. (TENCON)*, Oct. 2019, pp. 269–273.
[32] J. Ködmön and Z. E. Csajbók, "Információbiztonság az egészségügyben," *Orvosi Hetilap*, vol. 156, no. 27, pp. 1075–1080, 2015.
[33] A. Shameli-Sendi, M. Jabbarifar, M. Dagenais, and M. Shajari, "System health monitoring using a novel method: Security unified process," *J. Comput. Netw. Commun.*, vol. 2012, pp. 1–20, 2012.
[34] M. A. de Carvalho Junior and P. Bandiera-Paiva, "Health information system role-based access control current security trends and challenges," *J. Healthcare Eng.*, vol. 2018, pp. 1–8, 2018.
[35] W. A. Yasnoff, "A secure and efficiently searchable health information architecture," *J. Biomed. Informat.*, vol. 61, pp. 237–246, Jun. 2016.
[36] S. Arumugham, S. Rajagopalan, J. B. B. Rayappan, and R. Amirtharajan, "Networked medical data sharing on secure medium—A Web publishing mode for DICOM viewer with three layer authentication," *J. Biomed. Informat.*, vol. 86, pp. 90–105, Oct. 2018.
[37] A. Al-Haj and H. Abdel-Nabi, "Digital image security based on data hiding and cryptography," in *Proc. 3rd Int. Conf. Inf. Manage. (ICIM)*, Apr. 2017, pp. 437–440.
[38] A. K. Alharam and W. El-Madany, "The effects of cyber-security on healthcare industry," in *Proc. 9th IEEE-GCC Conf. Exhib. (GCCCE)*, May 2017, pp. 1–9.
[39] X. Larrucea, I. Santamaria, and R. Colomo-Palacios, "Assessing source code vulnerabilities in a cloud-based system for health systems: OpenNCP," *IET Softw.*, vol. 13, no. 3, pp. 195–202, Jun. 2019.
[40] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Informat.*, vol. 46, no. 3, pp. 541–562, Jun. 2013.
[41] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S.-J. Lim, "Privacy ensured E-healthcare for fog-enhanced IoT based applications," *IEEE Access*, vol. 7, pp. 44536–44543, 2019.
[42] K. Edemacu, H. K. Park, B. Jang, and J. W. Kim, "Privacy provision in collaborative ehealth with attribute-based encryption: Survey, challenges and future directions," *IEEE Access*, vol. 7, pp. 89614–89636, 2019.
[43] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, "Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system," *IEEE Access*, vol. 7, pp. 88012–88025, 2019.
[44] M. U. Sarwar, A. R. Javed, F. Kulsoom, S. Khan, U. Tariq, and A. K. Bashir, "PARCIV: Recognizing physical activities having complex interclass variations using semantic data of smartphone," *Softw., Pract. Exper.*, pp. 1–18. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.2846, doi:10.1002/spe.2846.
[45] X. Li, X. Huang, C. Li, R. Yu, and L. Shu, "EdgeCare: Leveraging edge computing for collaborative data management in mobile healthcare systems," *IEEE Access*, vol. 7, pp. 22011–22025, 2019.
[46] C. Iwendi, P. K. R. Maddikunta, T. R. Gadekallu, K. Lakshmanna, A. K. Bashir, and M. J. Piran, "A Metaheuristic optimization approach for energy efficiency in the IoT networks," *Softw., Pract. Exper.*, vol. 7, pp. 1–14, Feb. 2020.

[47] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, P. B, T. Reddy Gadekallu, P. Kumar Reddy Maddikunta, F. Fang, and P. N. Pathirana, "A survey on blockchain for big data: Approaches, opportunities, and future directions," 2020, *arXiv:2009.00858*. [Online]. Available: http://arxiv.org/abs/2009.00858

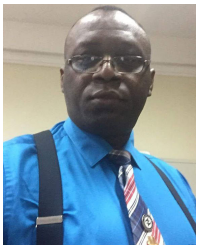
[48] A. R. Javed, M. U. Sarwar, S. Khan, C. Iwendi, M. Mittal, and N. Kumar, "Analyzing the effectiveness and contribution of each axis of tri-axial accelerometer sensor for accurate activity recognition," *Sensors*, vol. 20, no. 8, p. 2216, Apr. 2020.

[49] M. U. Sarwar and A. R. Javed, "Collaborative health care plan through crowdsource data using ambient application," in *Proc. 22nd Int. Multitopic Conf. (INMIC)*, Nov. 2019, pp. 1–6.

[50] A. R. Javed, M. U. Sarwar, M. O. Beg, M. Asim, T. Baker, and H. Tawfik, "A collaborative healthcare framework for shared healthcare plan with ambient intelligence," *Human-centric Comput. Inf. Sci.*, vol. 10, no. 1, pp. 1–21, Dec. 2020.

MARYAM SHABBIR is currently pursuing the M.S. degree with the Department of Computer Science, Kinnaird College for Woman, Lahore, Pakistan. Her research interests include machine learning, wireless sensor networks, mobile computing, and security issues in mobile cloud computing.

AYESHA SHABBIR is currently pursuing the M.S. degree with the Department of Computer Science, Kinnaird College for Woman, Lahore, Pakistan. Her research interests include machine learning, wireless sensor networks, mobile computing, and security issues in mobile cloud computing.



CELESTINE IWENDI (Senior Member, IEEE) received the second master's degree in communication hardware and microsystem engineering from Uppsala University, Sweden, in 2008, ranked under 100 in the world University ranking, and the Ph.D. degree in electronics from the University of Aberdeen, U.K., in 2013. He is currently listed as one of the Top African Scientists. He is also an ACM Distinguished Speaker, a Fellow of the Higher Education Academy, U.K., a Visiting Professor with Coal City University Enugu, Nigeria, and an Associate Professor with the BCC of Central South University of Forestry and Technology, China. He is a highly motivated researcher with a wireless sensor network security book and more than 100 publications. He has a strong teaching emphasis on communication, hands-on experience, willing-to-learn, and 19 years of technical expertise, and teaches Engineering team Project, Artificial Intelligence, Machine Learning, Data Networks, Electronics, Cybersecurity, Distributed Systems, and Control Systems. He has developed operational, maintenance, and testing procedures for electronic products, components, equipment, and systems, provided technical support and instruction to staff and customers. He is a wireless sensor network and an AI Chief Evangelist, a Researcher, a Community Developer, a Philanthropist, and an International Speaker in many top conferences and webinars. His research interests include wireless sensor networks, cybersecurity, security of things (SoT), machine learning, AI, communication controls, the Internet of Things (IoT), electromagnetic machines, 5G networks, and low power communication protocols. He has been a Board Member of the IEEE Sweden Section since 2017. He is an Editor of *International Journal of Engineering* and *Allied Disciplines* in 2015, a Newsletter Editor of IEEE Sweden Section from 2016 to 2018, the Editor-in-Chief of *Wireless Sensor Network Magazine*, in 2009, a Committee Member of International Advisory Panel, International Conference on Marine, Ocean, and Environmental Sciences and Technologies (MAROCENET) from 2014 to 2016, the Editor-in-Chief of *Journal of Wireless Sensor Networks*, in 2009, and an Advisory Board of *International Journal of Innovative Computer Science and Engineering* (IJICSE) in 2013. He is the Co-Chair of the Special Session on Wireless Sensor Networks: Hardware/Software Design aspects for Industry at the Prestigious International Conference of Industrial Technology ICIT.

ABDUL REHMAN JAVED received the master's degree in computer science from the National University of Computer and Emerging Sciences, Islamabad, Pakistan. He worked with the National Cybercrimes and Forensics Laboratory, Air University, Islamabad, Pakistan, where he is currently a Lecturer with the Department of Cyber Security. His current research interests include but are not limited to mobile and ubiquitous computing, data analysis, knowledge discovery, data mining, natural language processing, smart homes, their applications in human activity analysis, human motion analysis, and e-health. He aims to contribute to interdisciplinary research of computer science and human-related disciplines. He has authored more than 20 peer-reviewed articles on topics related to cybersecurity, mobile computing, and digital forensics.

MUHAMMAD RIZWAN received the M.Sc. degree from PUCIT, Lahore, Pakistan, in 2006, the M.S. degree from CIIT, Lahore, Pakistan, in 2012, and the Ph.D. degree from HUST, Wuhan, China, in 2017. In 2017, he joined the Department of Computer Science, Kinnaird College for Women, Lahore, as an Assistant Professor. He has authored or coauthored several peer-reviewed articles in professional journals and the proceedings of conferences. His research interests include the areas of machine learning algorithms, wireless sensor networks, mobile computing, self-organized networks, big data analytics, and the Internet of Things.

NORBERT HERENCSAR (Senior Member, IEEE) received the Ph.D. degree from the Brno University of Technology (BUT), Czech Republic, in 2010. In 2013 and 2014, he was a Visiting Researcher with Bogazici University, Turkey, and also with Dogus University, Turkey. In 2019, he was a Visiting Professor with the University of Calgary, Calgary, AB, Canada, for six months. Since 2006, he has also been collaborating on numerous research projects supported by the Czech Science Foundation. Since 2015, he has been an Associate Professor with the Department of Telecommunications, BUT. He is currently the Science Communications Manager and an MC Member of the COST Action CA15225 Fractional-Order Systems-Analysis, Synthesis and Their Importance for Future Design. He has authored about 90 articles published in SCI-E peer-reviewed journals and about 120 papers in conference proceedings. His research interests include analog electronics, fractional-order systems synthesis, and system designs for personalized medicine. He is a Senior Member of IACSIT and IRED and a member of the IAENG, ACEEE, and RS. Since 2013, he was an organizing or a TPC Member of the AFRICON, ELECO, I^2MTC, ICUMT, IWSSIP, SET-CAS, MWSCAS, and ICECS conferences. Since 2015, he has been serving for the IEEE Czechoslovakia Section Executive Committee as an SP/CAS/COM Joint Chapter Chair. Since 2017, he has been the General Co-Chair of the International Conference on Telecommunications and Signal Processing (TSP). Since 2011, he has also been contributing as a Guest Co-Editor to several special journal issues in *AEÜ - International Journal of Electronics and Communications*, *Applied Sciences*, *Radioengineering*, *Sensors*, and *Telecommunication Systems*. Since 2014, he has been serving as an Associate Editor for IEEE Access, *IEICE Electronics Express* (ELEX), *Journal of Circuits, Systems, and Computers* (JCSC), and an Editorial Board Member for the *Elektronika ir Elektrotechnika*, *Fractal and Fractional*, as well as *Radioengineering*.

JERRY CHUN-WEI LIN (Senior Member, IEEE) received the Ph.D. degree from the Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan, in 2010. He is currently a Full Professor with the Department of Computer Science, Electrical Engineering, and Mathematical Sciences, Western Norway University of Applied Sciences, Bergen, Norway. He has published more than 400 research articles in refereed journals (IEEE Transactions on Knowledge and Data Engineering (TKDE), IEEE Transactions on Cybernetics (TCYB), IEEE Transactions on Industrial Informatics (TII), IEEE Transactions on Intelligent Transportation Systems (TITS), IEEE Transactions on Emerging Topics in Computational Intelligence (TETCI), IEEE SysJ, IEEE SensJ, IEEE Internet of Things Journal (IOTJ), ACM TKDD, ACM TDS, ACM TMIS, ACM TOIT, and ACM TIST) and international conferences (IEEE International Conference on Data Engineering (ICDE), IEEE International Conference on Data Mining (ICDM), PKDD, PAKDD), 11 edited books, as well as 33 patents (held and filed, three U.S. patents). His research interests include data mining, soft computing, artificial intelligence, and machine learning, and privacy-preserving and security technologies. He is the Fellow of IET (FIET) and a Senior Member of ACM. He is the Editor-in-Chief of the *International Journal of Data Science* and *Pattern Recognition*, the Guest Editor/Associate Editor of several IEEE/ACM journals, such as IEEE Transactions on Fuzzy Systems (TFS), IEEE Transactions on Industrial Informatics (TII), ACM TMIS, ACM TOIT, and IEEE Access. He has been recognized as the most cited Chinese Researcher, respectively, in 2018 and 2019 by Scopus/Elsevier.