IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received November 1, 2020, accepted November 25, 2020, date of publication November 30, 2020,
date of current version December 18, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3041327

A Hybrid MCDM Approach of Selecting Lightweight Cryptographic Cipher Based on ISO and NIST Lightweight Cryptography Security Requirements for Internet of Health Things

LI NING[1], YASIR ALI[2], HU KE[3], SHAH NAZIR[2], AND ZHAO HUANLI[4]

[1]Department of Information Engineering, Pingdingshan University, Pingdingshan 467000, China
[2]Department of Computer Science, University of Swabi, Swabi 23430, Pakistan
[3]Department of Electrical and Mechanical Engineering, Pingdingshan University, Pingdingshan 467000, China
[4]Henan Pinggao Electric Company, Ltd., Pingdingshan 467000, China

Corresponding authors: Li Ning (2645@pdsu.edu.cn) and Yasir Ali (yasiuop007@gmail.com)

ABSTRACT The most serious challenges currently faced by healthcare environment is the decision making related to the installation of the most suitable and appropriate lightweight authentication cipher that could provide solutions towards the authentication issues prevailing in IoHT devices. This decision making becomes more troublesome and tricky due to the number of factors that are taken into account such as availability of many existing ciphers, complex and multiple numbers of requirements involved and frequent changing of these requirements from one platform to another. This decision making is also hampered by the nature of IoT devices operating in healthcare environment as they come up with limited functionality, processing, bandwidth and memory. In this regard, we present an evaluation framework focuses upon the selection of best light weight cryptographic ciphers by considering the most important parameters or requirements of criteria. The proposed framework considers the requirements like performance, physical and security as suggested by widely accepted standards such as National Institute of Standards and Technology (NIST) and International Standard Organization standard such as ISO/IEC 29192 for building evaluation criteria. This framework evaluates and selects the best lightweight cryptographic among the 10 ciphers i.e. PRESENT-80, Scalable Encryption Algorithm (SEA), HIGHT, Lightweight Encryption Algorithm (LEA) Advanced Encryption Standard (AES-128), mCrypton, NOEKEON, Klein, Camellia and Tiny Encryption Algorithm (TEA) for the purpose of evaluation in IoHT environment. This framework uses two decision making methods such as Criteria Importance Through Inter criteria (CRITIC) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). CRITIC assigns weights to alternatives and TOPSIS is used for evaluating alternatives (ciphers) against the defined criteria of evaluation. The proposed work is novel due to number of reasons such as the newly defined criteria adopted in this framework is the first attempt to use the security requirements of International Standard Organization (ISO) and National Institute of Standards and Technology (NIST). Secondly, this is first time that CRITIC and TOPSIS methods have been applied for assessment and decision making in healthcare environment. Similarly, the selected lightweight authentication cryptographic ciphers are used for the first time for assessment in IoHT environment. This approach addresses both hardware and software characteristics for selecting the best security option for lightweight cryptographic security.

INDEX TERMS IoHT, CRITIC, TOPSIS, lightweight cryptography, authentication, ISO.

I. INTRODUCTION

Internet of Health Things (IoHT) is emerging as a new concept due to the integration of duo concepts such as IoT and healthcare system. It is also known as Internet of Medical things (IoMT). IoHT or IoMT is the connectivity of healthcare devices connected to the cloud for sending and receiving data related to the chronical diseases of patients [1]. The security of IoHT devices has always remained a challenging task due to vulnerabilities addressed by these

The associate editor coordinating the review of this manuscript and approving it for publication was Luis Javier Garcia Villalba.

devices in the operating environment but still IoT devices are rapidly increasing due to their multi applications features. The number of IoT devices is predicated to reach 75.44 billion by the end of 2025 [2]. This significant rise has led to security and privacy concerns because these devices are unable to defend themselves due to low processing and resource constrained nature [3]. IoT devices are vulnerable to many cyber-attacks such as Man In Middle, eavesdropping, replay attacks, phishing, Denial of Service (DoS), spoofing, phishing, privacy breach and many others [4], [5]. Similarly, these devices are operating in wireless network where, sensitive data is transmitted and collected by terminal node [6]. In order to protect sensitive data from falsification and eavesdropping, it is necessary to select that algorithm or protocol which fulfills the needs of lightweight security or cryptography in healthcare environment. Lightweight cryptography is opposed to conventional cryptography, where desktop, tablets or smart phones are involved but it is all about embedded systems, RFID and sensor networks [7]. Light weight cryptography is more suitable for constrained devices and lightweight algorithms can be implemented in RFID, FPGA and WSN [8]. Any lightweight protocol or primitive related to authentication is ought to be properly assessed against a certain criteria or set of requirements in IoHT environment. For this purpose, a hybrid multi criteria decision making approach has been proposed to select the best cryptographic protocol or primitive for lightweight security in Internet of healthcare things system. In this research work, any lightweight cryptographic protocol is opted for installation in IoHT devices after its checking against the some lightweight cryptography requirements or criteria. This criteria plays anchor role in selection of best lightweight authentication cipher. Therefore, cryptographic requirements for lightweight security are identified from International Standard Organization (ISO) standard such as ISO/IEC 29192 [9] and National Institute of Standards and Technology (NIST).

- **Contribution of proposed work**

Following are the major contributions presented by this proposed research work.

- In this proposed research work an evaluation framework is presented to address the issues related to decision making and selection of most appropriate and suitable lightweight cryptographic authentication cipher for healthcare environment. This first attempt of its kind that such type of evaluation framework in IoHT environment has been presented.
- NIST and ISO standards are used for the first time as benchmark for opting the best choice among the list of selected light weight authentication cryptographic ciphers. The literature has been thoroughly searched for validating the selected lightweight requirements or criteria. The parameters defined for criteria have never been used before as evaluation benchmark to the best of our knowledge.
- Earlier attempted works used only hardware or software based characteristics but this proposed work combines both hardware and software based characteristics such as performance, physical and security characteristics to address the lightweight authentication issues in IoHT environment.
- The selected list of lightweight authentication cryptographic ciphers has never been used before evaluation and decision making in IoHT based system.
- This is first time that hybrid multi criteria decision making methods like CRITIC and TOPSIS have been used for selection of lightweight cryptographic authentication cipher in medical care environment.
- The proposed framework provides features based or lightweight security requirements based cryptographic authentication for healthcare data by covering all the aspects for authentication such as memory requirements, size of code, power usage, latency, throughput, ROM size, key size and chip area.

The remaining section of this article is composed of seven (7) sections: section 2 describes motivation of this research, section 3 describes research gap and problem statement, in section 4 literature is discussed. In section 5, the need of MCDM approach for light weight cipher selection in IoHT is discussed. In section 6 research method to address the light weight security has been elaborated, section 7 discusses limitations and challenges faced by this research work and section 8 ends in conclusion.

II. MOTIVATION

Light weight security of IoHT is challenging task due to various number of criteria involved. Selection of light weight cryptographic primitive is always desirable to meet the authentication issues. This research work is motivated to achieve the following objectives.

- The major motivation of this work is to select the most appropriate lightweight cryptographic authentication ciphers against the security requirements or evaluation criteria defined based upon ISO standard and NIST security characteristics or requirements.
- Lightweight authentication of IoHT devices is a major issue as the landscape of these devices is moving rapidly, therefore, it is required to use a tailor- made lightweight authentication cipher which provides optimum security and performance for resource constrained devices such as RFID and sensor based devices.
- It is indispensable to use appropriate light weight authentication cipher for security of internet of health thing environment due to the structure of healthcare devices. IoT devices operating in medical care system come up with less memory, processing speed and bandwidth. A lightweight authentication cipher that addresses all the physical and performance characteristics of cipher is required.

- Hardware and software based performance of light weight cryptographic authentication algorithms are the key considerations but it is hard to select an cipher that holds both factors at the same time.
- Criteria for selection of most appropriate lightweight authentication algorithm has not been properly defined to due to involvement of many number of performance, physical and security properties related to lightweight cryptography.

III. PROBLEM STATEMENT

The research gaps related to light weight authentication of IoT in healthcare environment in current literature are identified and these are addressed in the proposed work. The main focus this work is to provide solution towards light weight security in healthcare environment by using hybrid MCDM approach. Hybrid MCDM approach as selective choice is used for the first time to address the light weight security of IoT system, although it has been used in health care for making decision for other different purposes such as mobile health care system, dementia care, IoT based enterprises and selection of contract and tender processes [10]–[13]. This research work is novel in nature due the existence of the following research gaps. The problem statement is composed of the following points.

- It is in dire need to select the most appropriate lightweight cipher due to the nature of data transmitted by IoHT devices. In healthcare environment, sensitive data related to the patients is transmitted from IoHT devices like smartphone, tablets, oximeter, glucometer, insulin pins, apple watch, smart contact lens etc. Light weight cryptography or security allows them to keep data secure and confidential. This can only be achieved by a proper lightweight cryptographic cipher that provides proper encryption, confidentiality, authentication and non-repudiation of data.
- From literature study, it has been observed that MCDM approach has never been used as decision making option for light weight security solution in IoT for healthcare system. In this research work, a hybrid MCDM approach is used to cope with selection problems of lightweight security in healthcare environment.
- There is significant rise in the light weight cryptography for IoT devices. A huge number of lightweight ciphers are available for IoT applications in healthcare environment. Selection of most appropriate and suitable cipher among the list of available ciphers becomes tricky due to many number of parameters involved. In healthcare environment, majority of the devices such as oximeter, glucometer and apple watch have limited capacities of power, memory and bandwidth.
- Similarly, the security properties or criteria for light weight security assessment are extracted from well-defined ISO security standard such as ISO/IEC 29192 [9] and NIST security requirements. This is first attempt of its kind to bring these security requirements for lightweight cryptographic security in IoHT system.
- Many existing works and approaches have identified security evaluation criteria or requirements from literature, which is not considered as standard, well-recognized and reliable. Due to this reason some security attributes related to hardware, software or security implementation might have been skipped. Ultimately, this leads to the situation, where, the most suitable and appropriate light weight primitive providing a full pledged light weight security remains as ‘‘unidentified’’ in this area.
- Majority of previous works are focused upon hardware based implementations of lightweight ciphers, but this proposed work combines both the software and hardware based approaches for selection of most appropriate lightweight authenticaion cipher among the list of ciphers.

IV. RELATED WORK

Most of the IoT devices operating in healthcare environment are vulnerable to various cyber threats and attacks. As, data related to patients are stored in cloud server of hospital center and it is mandatory to keep the data secured [14]. The security has been the most challenging task in IoHT environment and selection of algorithm that answers all problems related to lightweight security is hard to identify. MCDM approach has been used for IoT in various fields such as crime prevention, road safety, resource management, supply chain, energy system and cluster head selection. The role of multi criteria decision making analysis in healthcare has been briefly discussed by Frazão, *et al.* [15]. Different MCDM methods have applied for the purpose of selection in IoHT, like Dimitriologou *et al.* [10] presented a multi criteria decision model for dementia care. Similarly, multi criteria decision making analysis can be used for decision making regarding contracts and tender process in healthcare environment [11] Liu, *et al.* [12] presented a hybrid MCDM model for mobile healthcare system. Nabeeh, *et al.* [13] used neutrosophic approach with the support of Analytical Hierarchy Processes (AHP) MCDM method for IoT-based enterprises. Detail of different approaches or technologies for security evaluation of lightweight ciphers is shown in Table 1.

V. NEED OF MCDM APPROACH FOR SELECTING LIGHTWEIGHT CIPHER IN IoHT

Decision making is a complex and tricky job in healthcare environment due to the nature of real-world problems and conflicting objectives. The development of such a models or approaches is prerequisite to provide solutions towards selection and decision making problems when multiple criteria are taken into account. There are variety applications of MCDM approaches in healthcare for different purposes like performance management [34], service quality evaluation [35], supplier selection problems [36] and healthcare waste treatment [37] and security evaluation [38] and web services

TABLE 1. Approaches/techniques for lightweight ciphers.

Ref#	Technique/method	Author	Metric/Parameters of evaluation	Ciphers/Algorithms	Year
[16]	Hardware based approach	Stephanie et al	▪ Area ▪ Power ▪ Energy ▪ Throughput	▪ AES ▪ NOEKEON ▪ HIGHT ▪ ICEBERG ▪ KATAN ▪ PRESENT	2012
[2]	Arduino Platform	S. POLAT	▪ Code size ▪ SRAM usage ▪ Execution time ▪ Throughput	▪ AES ▪ Simon ▪ Speck ▪ Roadrunner ▪ Present ▪ Rectangle ▪ Pride ▪ SparX ▪ RC5 ▪ LED ▪ LBlock	2019
				▪ Fantomas ▪ Skinny	
[17]	Software based approach	Chao Pei et al	▪ Code size ▪ RAM size ▪ Cycles/byte ▪ Throughput ▪ Combine metric	▪ KLEIN ▪ LBlock ▪ PRESENT ▪ HIGHT ▪ Piccolo ▪ SIMON ▪ SPECK ▪ AES	2018
[18]	Java Cypto package	P. Patil et al	▪ Encryption time ▪ Decryption time ▪ Memory ▪ Avalanche effect ▪ Entropy ▪ Encoding bits	▪ DES ▪ 3DES ▪ AES ▪ RSA ▪ Blowfish	2016
[19]	Literature based comparison	P.Girija et al	▪ Throughput ▪ Latency ▪ Power ▪ Energy	▪ PRESENT ▪ HIGHT ▪ mCryption ▪ Camellia ▪ AES ▪ DES ▪ IDEA ▪ TEA etc…	2019
[20]	Software based approach	Eisenbarth et al	▪ Key bits ▪ Block bits ▪ Cycles per block ▪ Throughput @100 Kbps ▪ Logic processes ▪ Area	▪ PRESENT ▪ AES ▪ HIGHT ▪ Clefia ▪ mCryption ▪ DES ▪ DESXL ▪ Trivium ▪ Grain	2007
[21]	Hardware and software based approach	Goyal et al	▪ Technology ▪ Area ▪ Max-Frequency ▪ Max-Throughput ▪ Area efficiency ▪ Power	▪ PRESENT-80 ▪ PRESENT-128 ▪ AES-128 ▪ ECDH-10	2019
[22]	LPWAN and IoT infrastructures network	S. Rajesh et al	▪ File size ▪ Encryption time ▪ Decryption time	▪ NTSA ▪ TEA ▪ XTEA ▪ XXTEA	2019
[23]	Software platform	Figueroa et al	▪ Execution Time ▪ Memory use ▪ Charge Use ▪ File size ▪ Encryption ▪ Decryption	▪ AES ▪ PRESENT ▪ MSEA ▪ LEA ▪ ECB	2019

TABLE 1. ***(Continued.)*** **Approaches/techniques for lightweight ciphers.**

[24]	FELICS framework	Fernandes	▪ Code size ▪ Execution time ▪ Energy consumption	▪ AES ▪ CLEFIA ▪ NOEKEON ▪ PRESENT ▪ RECTANGLE ▪ RoadRunneR ▪ SPARX ▪ SPECK	N/A
[25]	Survey	Chaitra et al	▪ Key size ▪ FPGA Device ▪ Throughput ▪ Slices ▪ Efficiency	▪ AES, ▪ PRESENT-80,128 ▪ TEA ▪ HUMMINGBIRD	2017
[26]	Hardware base approach (AVR Technology)	S. Rana et al	▪ Block size ▪ Key size ▪ Code size ▪ RAM ▪ Encryption ▪ Decryption ▪ Key generation	▪ AES ▪ HIGHT ▪ LEA ▪ PRESENT ▪ RC5 ▪ SIMON ▪ SPECK ▪ SIT	2018
[27]	Literature analysis	Dhanda et al	▪ Security ▪ Area ▪ Latency ▪ Throughput ▪ Power ▪ Energy ▪ Hardware & Software Efficiency ▪ Figure of Merit	▪ Block ciphers ▪ Stream ciphers ▪ Hash functions ▪ Elliptic Curve Cryptography	2020
[28]	Hardware and software platforms	P. Singh et al	▪ Execution time ▪ Key size ▪ Block size ▪ File size ▪ Memory ▪ Power	▪ Rives Cipher 4 ▪ ChaCha20 ▪ AES ▪ 3DES ▪ DES ▪ Blowfish ▪ Twofish ▪ Rivest Cipher (RC2)	2018
[29]	AVR microcontroller	F. Mollaie et al	▪ Memory ▪ Energy ▪ Number of CPU clock	▪ HIGHT ▪ TEA ▪ KLEIN ▪ KATAN	2013
[30]	Simulation	Awotunde et al	▪ Encryption speed ▪ Memory usage ▪ CPU usage ▪ Key length	▪ Blowfish ▪ AES ▪ 3DES ▪ DES	2016
[31]	Microcontroller	F.Ullah et al	▪ Key size ▪ Block size ▪ S-box ▪ Round function ▪ Number of rounds ▪ Structure ▪ Key scheduling ▪ Code size ▪ RAM size ▪ Execution time	▪ Speck ▪ Simon ▪ AES ▪ RC5 ▪ Fantomas ▪ Robin ▪ L Block ▪ HIGHT ▪ PRESENT ▪ Piccolo ▪ TWIN ▪ PRINCE ▪ LED	2017
[32]	ASIC and FPGA platforms	Sadhukhan et al	▪ Space complexity ▪ Time complexity ▪ Data complexity ▪ Attack types	▪ PRESENT ▪ SIMON ▪ SPECK ▪ KHUDRA ▪ AES	2018
[33]	Literature based analysis	Hosseinzadeh et al	▪ RAM ▪ Gate equivalent ▪ Code size ▪ Latency ▪ Throughput ▪ Cycles per block	▪ HIGHT ▪ PRESENT ▪ LED ▪ PUFFIN ▪ TWINE etc..	
Proposed work	Microcontroller and hybrid MCDM method using ISO and NIST lightweight cryptographic security requirements	Yasir et al	▪ Chip Area ▪ Throughput ▪ Power consumption ▪ Memory size ▪ Latency ▪ Program code size ▪ RAM size ▪ Security strength	▪ PRESENT-80 ▪ SEA ▪ HIGHT ▪ DES ▪ AES-128 ▪ mCrypton ▪ NOEKEON ▪ Klein ▪ Camellia ▪ TEA	2020

evaluation [39]. This proposed work also made an attempt to provide solution towards the selection of lightweight ciphers for security in IoHT. Authentication and encryption/decryption in IoHT have become an issue due to the number of IoMT applications involved. But, the major issues are concerned with authentication and data integrity [40]. Therefore, it is indispensable to have a proper and best-fit authentication or encryption/decryption block cipher for IoMT applications which could secure the sensitive data related to patients. In this regard, the number of lightweight block ciphers for authentication and encryption/decryption in healthcare have been evolved in recent years, significantly. These lightweight block ciphers offer a variety of unique combination of features. This is the reason that network administrators, network policy makers or other stakeholders find it hard to select the most appropriate cipher for lightweight security that could provide solution towards all the security issues in IoHT. Our approach selects lightweight ciphers for IoMT applications by considering the number of criteria such as chip area, throughput, power consumption, energy, latency, program code size, RAM size and security strength. Without MDCM approach, this selection is not easy to get the best cipher among the plethora of lightweight block ciphers.

For example, some ciphers selected for implementation in IoHT must be energy efficient but on other hand they can be easily breached and they will suffer from software or hardware implementations issues. For instance, SEA cipher is easy to use, easily upgradable, simple, flexible and low-latency but on other hand it is slow in software implementation, limited in privacy and slow for real time applications. Similarly, TEA is cipher is easy to implement and requires less code size but its power consumption is high and has high energy per bit. Implementing a cipher based on considering one dimension or two dimensions is not a rational approach but a lightweight block cipher that is to be implemented must be evaluated against the number of performance evaluation criteria. This work has defined a distinct and multifaceted criteria for selection of lightweight block cipher which is to be implemented for IoMT applications in healthcare environment. The need of hybrid MCDM approach is to select a cipher that is more viable in terms of energy, power, code size, RAM, latency, throughput, security and gate area. The scenario of applying MCDM approach in IoHT for selection of lightweight block cipher is given Fig 1.

VI. RESEARCH METHOD

Lightweight security of nodes or any IoT device is of paramount importance from security perspective especially in Internet of healthcare things (IoHT). This security can only be achieved by having a proper and well-featured security scheme or algorithm that answers all the questions related to lightweight cryptographic security. The main focus in this research is to select the best algorithm/protocol or any other mechanism employed for lightweight cryptographic security as alternative. For this purpose, lightweight cryptographic requirements/properties of lightweight security are identified from ISO standard known as ISO/IEC 29192. It is a multi-part International Standard that defines lightweight to address key exchange, data confidentiality, authentication, identification, non-repudiation. This standard provides a standardized mechanisms for lightweight cryptographic applications such as radiofrequency identification (RFID) tags, smart cards, secure batteries, health-care systems and networking composed of sensors. These features/properties are used as metric for selection best algorithm or device that embeds the algorithm. These features are the most adopted and well-recognized to measure the strength of any lightweight cryptographic cipher or algorithm. ISO security requirements for lightweight cryptography such as (ISO/IEC 29192) [9] and NIST characteristics are used for building security evaluation criteria. Following are the major steps of research method.

A. CASE STUDY

In order to complete the data collection, two case studies were performed.

Case 1: In this case study, we highlighted the general issues related to lightweight authentication in broader sense such as the main problem related to authentication issue and root cause of the problem were brought into consideration. The cause effect of problems were discussed. A comprehensive and detailed observation was carried out to collect the required data related to problem. For this purpose open ended questions were asked to get deep knowledge about the problem domain and then the collected data was analysed for finding the criteria and alternatives. The proposed solutions of problem were chalked out and proper report was prepared related to the authentication problems in IoHT. From this case study it was concluded that the main issue is the selection and ranking of lightweight authentication cipher which can provide solution towards the lightweight authentication issues. In this step a proposed solution to the problem was suggested and step-wise procedure of this case study is given in Fig 2.

Case 2: In the second case of our study, the problem was discussed in more detailed and comprehensive manner to get deep knowledge about the problem of authentication in medical care environment.A proper and systematic procedure has been followed in pursuing this research. A survey was done to collect the requirements from medical IT personnel to know about their changing needs like power consumption, memory requirements, fast transmission, strength of security etc. This case study is conducted to get more and in-depth detail about the impacts of lightweight authentication cipher in healthcare environment. The main focus is to know about impacts of cipher in healthcare environment in terms of different parameters such as memory, throughput, latency, power, energy, chip area, program code size and key size. This group discussion is aimed to know from the IT experts in healthcare field about every detail of these security requirements. For this purpose, a questionnaire is presented to IT personnel in healthcare environment, which is comprised of 36 questions. After collecting comprehensive detail about security

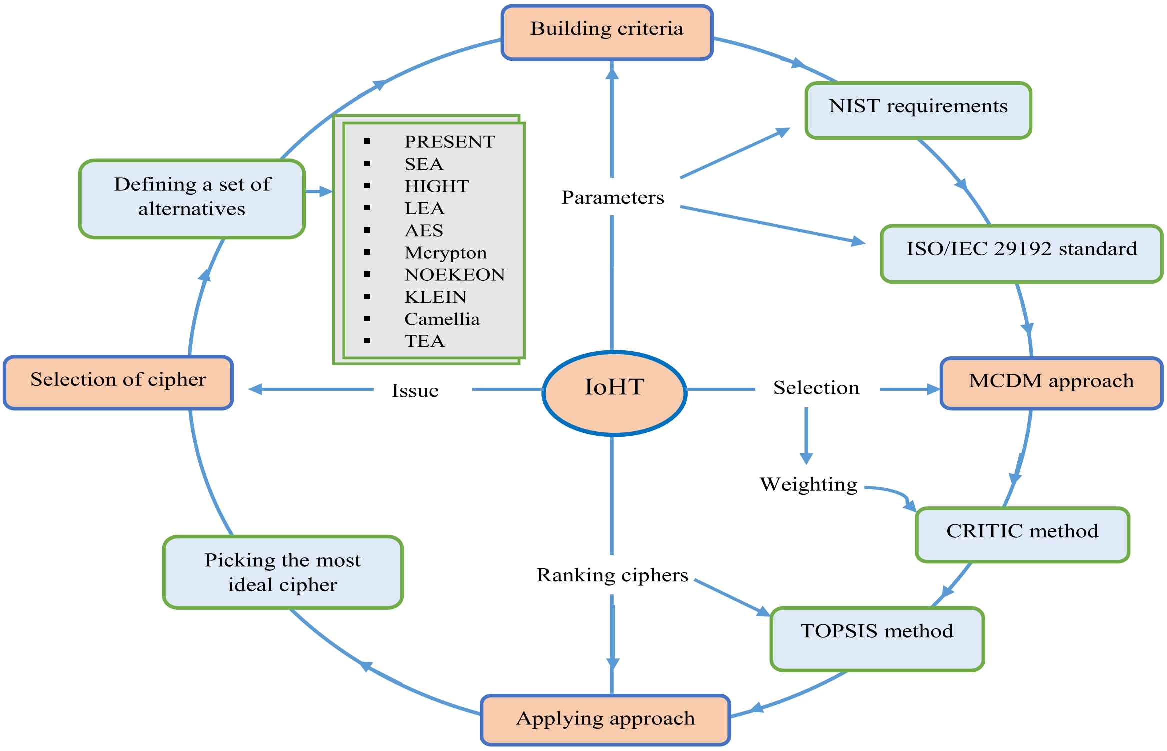

FIGURE 1. **Working of MCDM approaches in IoHT.**

requirements related to light weight block cipher, the required ciphers are selected against the requirements for evaluation purposes to get the best cipher. The detail of questionnaire for collection of data is given in Table 2. In order to build evaluation framework the security criteria and alternatives are selected. Then, selected security features or criteria is built based upon their needs. The selected ciphers for evaluation are totally based on the suitability to IoHT. The interaction and relation of security requirements in IoMT based system is shown in Fig 3.

In this figure IoMT gadgets before deployment in network are checked against the predefined criteria. This criteria is used as assessment for decision making regarding selection of most suitable lightweight cipher in healthcare environment. The selected cipher is most ideal as it covers all the dimensions of lightweight cryptographic security. Thus, it allows the secure and reliable communication from IoMT devices to gateway and data centers.

B. BUILDING SECURITY EVALUATION CRITERIA

For building criteria for lightweight cryptography, the security requirements are collected from three different sources such as literature, ISO light weight cryptography standard and NIST security requirements. In first step, a deep search of literature is performed to know about the most common security requirements. In this step, 85 light weight security requirement are identified. In second step, we removed those requirements, which were commonly used by different authors. In third step, we compared the security requirements obtained from literature with ISO and NIST security requirements. From ISO lightweight cryptography security standard, we derived 11 requirements and 10 requirements were identified from NIST. In fourth step, we have collected 48 security requirements. After complete analysis, we finally selected those requirements, which are most important for building the security criteria and adopted by many sources. The detailed procedure of building security requirements or criteria is depicted in Fig 4.

The number of citations of security requirements or criteria is depicted in Fig 5. In this figure, throughput and power are the most cited security requirements and used by different authors for light weight security evaluation.

Security criteria used by each author along with sources are given in Table 3.

Each requirement contributed towards building the security evaluation criteria are discussed below as.

1) CHIP AREA

Area occupied by semiconductor [9]. It can be also obtained by dividing layout area of application in μm^2 and corresponding area of NAND 2 gate. CMOS technology plays important role in chip area and hardware implementation of cipher and also have impacts on gate equivalence and energy usage. Chip area is an important factor and its smaller value is desirable [27], [41]. It can be represented by using the following equation.

$$C = \frac{L}{A_n}$$

where, C is chip area, L is layout area of application and A_n is corresponding area of NAND2 gate.

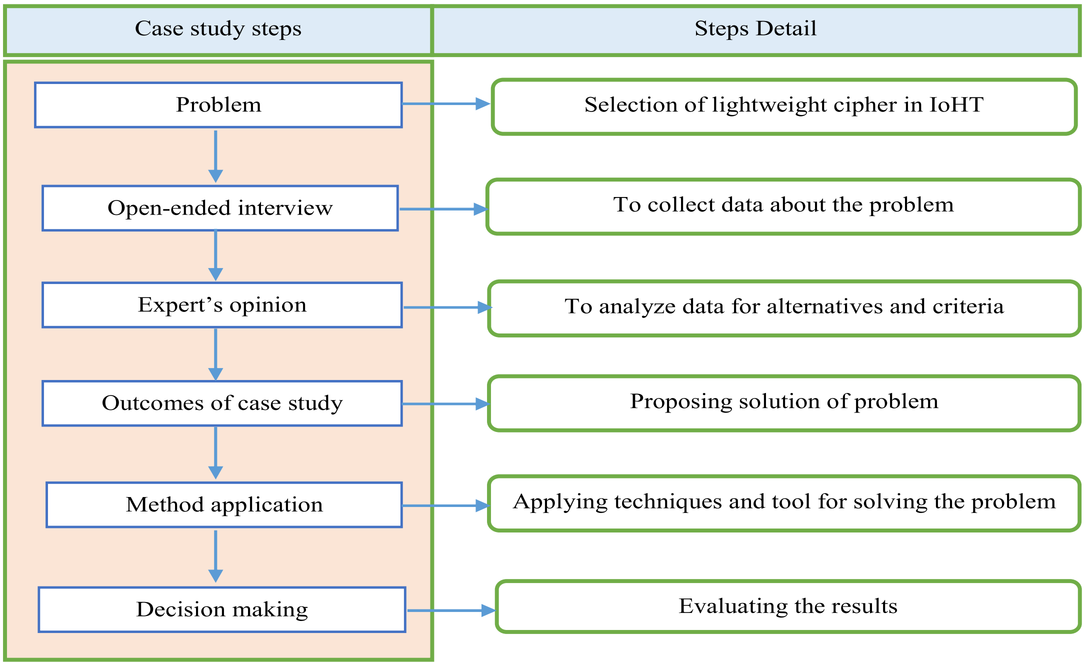
Case study steps
Steps Detail
Problem
Open-ended interview
Expert's opinion
Outcomes of case study
Method application
Decision making
Selection of lightweight cipher in IoHT
To collect data about the problem
To analyze data for alternatives and criteria
Proposing solution of problem
Applying techniques and tool for solving the problem
Evaluating the results

FIGURE 2. Case study steps.

2) THROUGHPUT

Throughput is the ratio of block size and time to encrypt one block. Throughput=Block size/Encryption Time of a block [42]. Throughput is number of bits generated per second at a specific frequency during the procedure of cipher encryption and decryption [27]. This frequency is identified in either 100 kHz and for of hardware based implementation 4 MHz is used [27]. Higher value of throughput is desired [41]. Mathematically it is written as.

$$T = \frac{B \times F}{N}$$

where, T is throughput, B is block size, F is frequency and N is number of cycles per block.

3) ENERGY CONSUMPTION

Energy consumption can be computed by power consumption over certain period of time [9]. Energy consumption also depends upon the block size and latency. The encryption and key scheduling also have impacts on energy consumption [29]. Energy consumption also depends upon the number of iterations [43]. The smaller value of energy consumption is desirable for IoT devices. According to [20] a fast executing algorithm can diminish the energy usage and increase the battery lifetime. In equation form energy can be written as.

$$E_b = \frac{L \times P}{B}$$

where, E_b is energy per bit in μJ, L is latency, P is power consumed by hardware or software in micro watt and B is block.

TABLE 3. Security requirements used by literature.

S.No	Requirements/Properties	Literature frequency citation
1	Chip area	[16] [20] [21] [27] [33]
2	Throughput	[16] [17] [19] [20] [21] [25] [27] [2] [33]
3	Power consumption	[16] [19] [21] [23] [24] [27]
4	Energy	[16] [19] [24] [27] [29]
5	Latency	[19] [27] [33]
6	Program code size	[17] [24] [26] [2] [31] [33]
7	RAM size	[17] [26] [2] [31] [33]
8	Security strength	[25] [26] [28]

4) POWER CONSUMPTION

It is amount of power needed to use the circuit [41]. Power can be found by GE and corresponding CMOS technology. The lower value of power is desired so cipher consumes less power will be preferred. Power consumption is dependent on opted technology and simulation method [27]. Lower value of power is desired. Power in equation form is represented as.

$$P = \frac{B \times E_b}{L}$$

where, P is power consumed, B is block size, L is latency and E_b is energy.

5) LATENCY

Latency is delay encountered by cryptographic scheme in real time communication system or it is time elapsed during the computation of cipher text or plain text. The lower value for latency is desired [27], [41]. Latency in mathematical form is

TABLE 2. Questionnaire form for collection information.

Attribute: Memory
Q1: How memory is important for gadgets in healthcare?
Q2: What are memory requirements of different ciphers implemented in healthcare?
Q3: Do the existing light weight ciphers suffer from memory constraint?
Q4: How the memory affect the performance of ciphers?
Q5: How much memory is sufficient to address the needs of IoHT?
Q6: Do they need more RAM size to store more data?
Q7: How much memory these IoHT devices are supporting?
Q8: Do IoMT devices enforce memory protection?
Q9: Is data storage in medical devices protected cryptographically?
Q10: Is any default data protection available for stored data?
Attribute: Throughput
Q11: Is throughput essential for IoHT system?
Q12: What are the expectations in terms of throughput from cipher?
Q13: What are the existing throughput of employed ciphers in IoHT?
Q14: Do they need more throughput or existing algorithms are providing enough speed?
Q15: The existing IoHT devices are compatible with receiving more bits of data?
Q16: What are the maximum and minimum limits of throughput in IoT?
Attribute: Latency
Q17: How much IoHT devices suffer from latency?
Q18: What are the latencies of existing ciphers?
Q19: What are the factors of creating latency in healthcare environment?
Q20: How much latency is permissible?
Attribute: Power
Q21: How long IoHT devices are providing power back up?
Q22: What are the power values for the existing ciphers?
Q23: What are the alternative sources of back up?
Q24: How power is important parameter IoHT applications?
Q25: What are the main reasons of high power consumption in IoHT devices?

written as.

$$L = k \times t_{cycle}$$

L is latency, k is number of clock cycles to compute a block of cipher text and t_{cycle} is Time for one cycle.

6) PROGRAM CODE SIZE

Size of cryptographic algorithm/mechanism code in bytes [9]. It is fixed amount of data, which evaluates function independently from input [41].

7) RAM SIZE

Size of temporary storage space a cryptographic mechanism requires in random access memory including the registers in the processor [9].Memory is often the most expensive part of the implementation of a lightweight primitive [41].

8) KEY SIZE

It is measured by number, which describes the amount of work or the number of operations required to break a cryptographic cipher or system [9]. Key size describes the strength of security.

C. BUILDING CIPHER PROFILES

Our method for selection of lightweight cipher is inspired by using NIST profiles that are built for variety of applications. These profiles describe different characteristics of cryptographic primitive. Profile consists different categories of characteristics such as physical characteristics, performance characteristics and security characteristics. Physical characteristics describes area in GE, memory (RAM\ROM) and implementation type [44]. Lightweight primitives can also be implemented in software, typically using microcontrollers. In this case, the relevant metrics are RAM consumption, size of code and throughput [41]. Performance characteristics show latency, throughput and power. Security characteristics

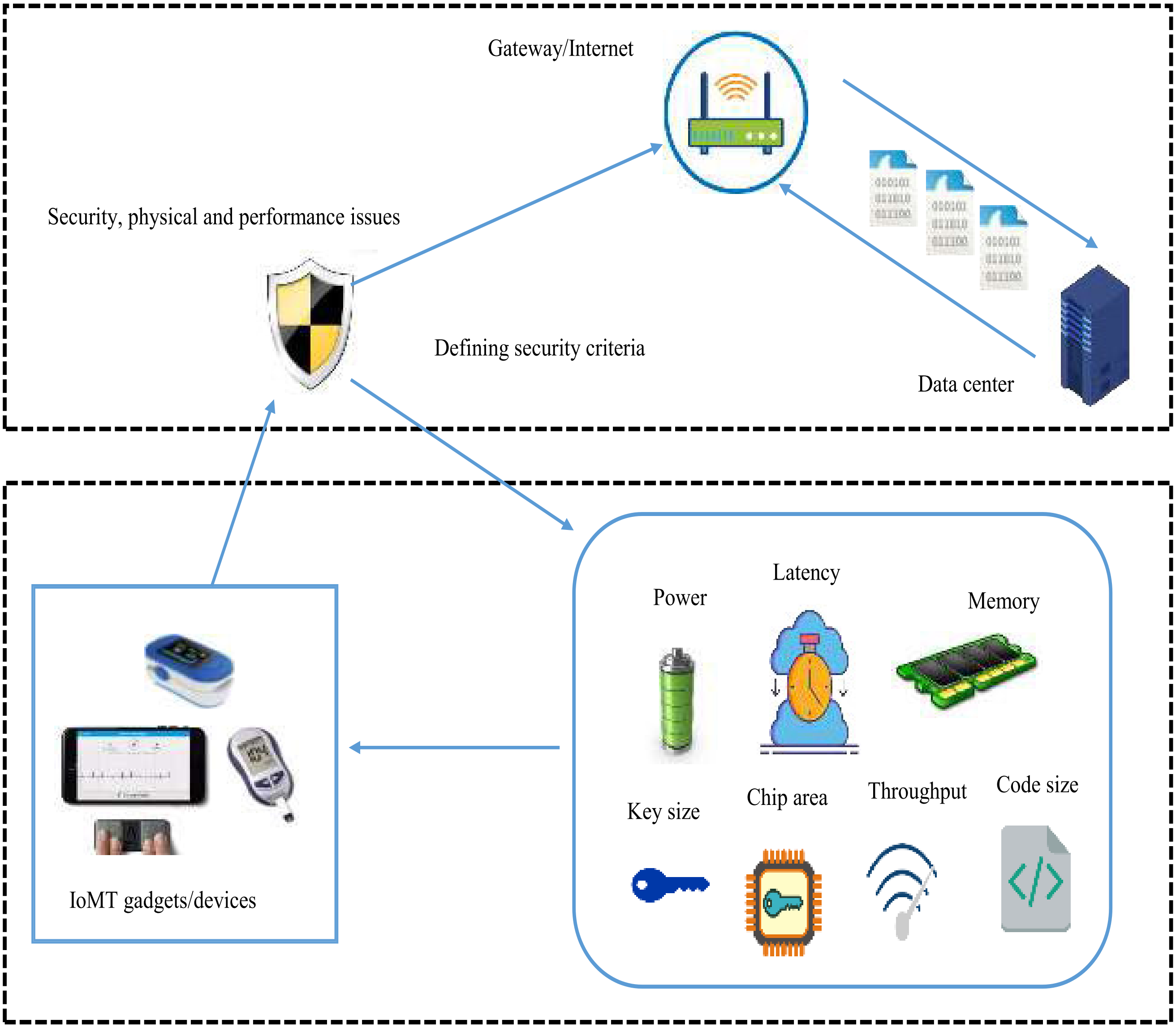

FIGURE 3. Security requirements based IoMT system.

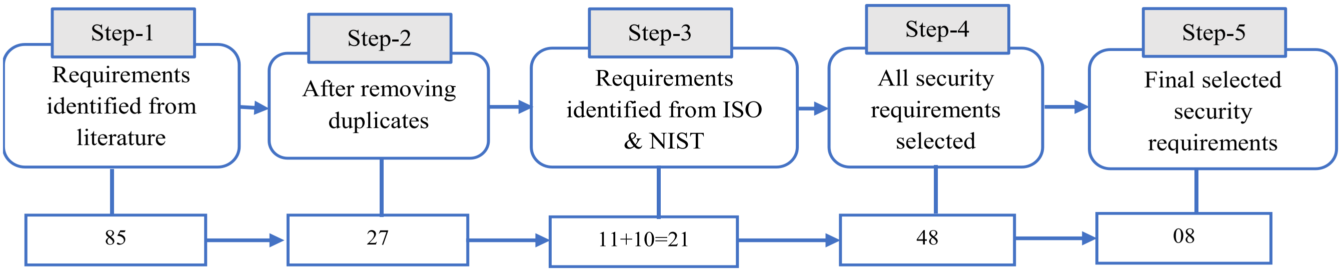
Step-1
Requirements identified from literature
Step-2
After removing duplicates
Step-3
Requirements identified from ISO & NIST
Step-4
All security requirements selected
Step-5
Final selected security requirements
85
27
11+10=21
48
08

FIGURE 4. Procedure of building evaluation criteria.

are minim security strength, attack models and side channel resistance environment. The profiles are built for 10 light weight cryptographic algorithms. For evaluation, 10 algorithms are selected and profile for each cipher is obtained by using the same hardware technology such as microcontroller. The hierarchical structure of profiles are given in Fig 6.

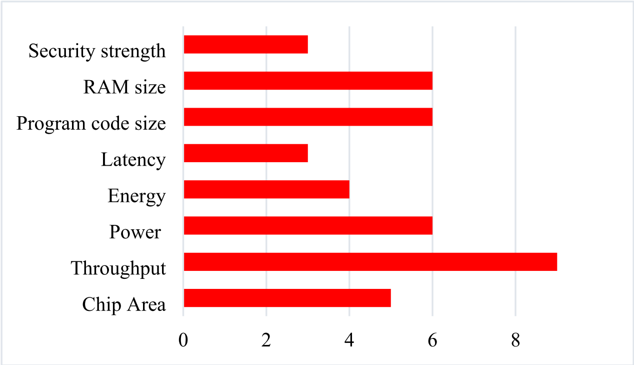

FIGURE 5. Number of citation of security criteria.

Each profile is composed of three parts such as performance characteristics, physical characteristics and security characteristics, which are discussed below as.

1) PERFORMANCE CHARACTERISTICS

The performance metrics can be described by throughput, power and latency. Both Power and energy metrics are related with constrained devices. Example of power consumption is RFID chip, which uses electromagnetic field to run its internal circuit. Latency is related with real time applications, where fast response time is required. Unlike conventional algorithms, for light weight application high throughput is not a design goal but still moderate level of throughput is required for applications [44].

2) PHYSICAL CHARACTERISTICS

Physical metrics describe gate area, memory such as (RAM/ROM), implementation type i.e. software or hardware and energy consumption [44]. Gate area is also known as chip area and ROM shows the code size.

3) SECURITY CHARACTERISTICS

Security characteristics of profile describe the security strength also known as key size, side channel resistance and attack models. In this work, building a profile for cipher, we have considered only security strength as a metric. NIST has termed the key size as security strength in their profiles, this is the main reason for calling the key size as security strength. The minimum key size for light weight cipher should be 112 to provide maximum security for longer period of time [45]. Similarly, the detail of all selected lightweight cryptographic ciphers for security evaluation purpose are given below as.

a: PRESENT-80

It is one of the first ciphers used for encryption of ultra-constrained devices. It is also as standardized in ISO/IEC 29192 standard [46]. Key size of PRESENT is 80/128-bit and it takes 31 rounds to converts 64-bit data blocks [19]. This algorithm is more ideal for devices with limited power abilities and restricted battery life due to small key size [42]. PRESENT algorithm is hardware efficient but its software implementation reduces the size of the code [46]. As far as the code size is concerned then PRESENT is a reasonable choice [20].

b: SEA

SEA is Scalable Encryption Algorithm, designed for processors with limited instruction set. The main goal of this design is to meet the low memory, small code and limited instruction sets [46]. This algorithm was initially designed to provide encryption at low cost on very low processers with limited instructions, memory and code size [47]. Both hardware and software implementation of SEA cipher are working well [48].

c: HIGHT

HIGHT is a block cipher which is presented by Hong *et al.* HIGHT has 64 bits block size and 128 size of key [41]. It completes its operation in 32 rounds [19]. It provides high security and employs Feistel structure [42]. This algorithm is targeted for systems with limited or low resources [49].

d: LEA

LEA is abbreviated for Lightweight Encryption Algorithm. This algorithm is stream cipher and was designed by Electronics and Telecommunication Research Institute of Korea. It has small code size and requires less power [46]. LEA completes in 24, 28 and 32 rounds. This algorithm is designed to apply to lightweight environments [50].

e: AES

Advance Encryption Standard or (AES) was developed by Singh and Deshpande [28]. It is available in key sizes of 128, 192 and 256 bits. The key size determines the strength of the cipher, higher the size of key more encryption the algorithm will provide [28]. It can be implemented in both hardware and software [46]. The block size of AES is 128 bits [24].

f: mCrypton

Mcrypton was developed in 2005 by Hosseinzadeh and Bafghi *et al.* [51]. It is miniature version of crypton and uses 64 bits block size by providing three key options such 64, 96 and 128 sizes [52]. It is more suitable for resource constrained computing scenarios such as sensor network and RFID tags [53]. It completes in 13 rounds [46].

g: NOEKEON

This algorithm is presented by Abdul-Latip *et al.* [54] for submission to the NESSIE project in 2000. Noekeon key size is 128 bits and it takes 16 rounds and each round is composed of three transformations [55]. It can be implemented both in hardware and software. The key scheduling of Noekeon allows to resist against the related key attacks [55]. This algorithm is vulnerable to related key cryptanalysis [46]. It uses bit-slicing techniques, which leads to lesser code size, better performance and less energy consumption [24].

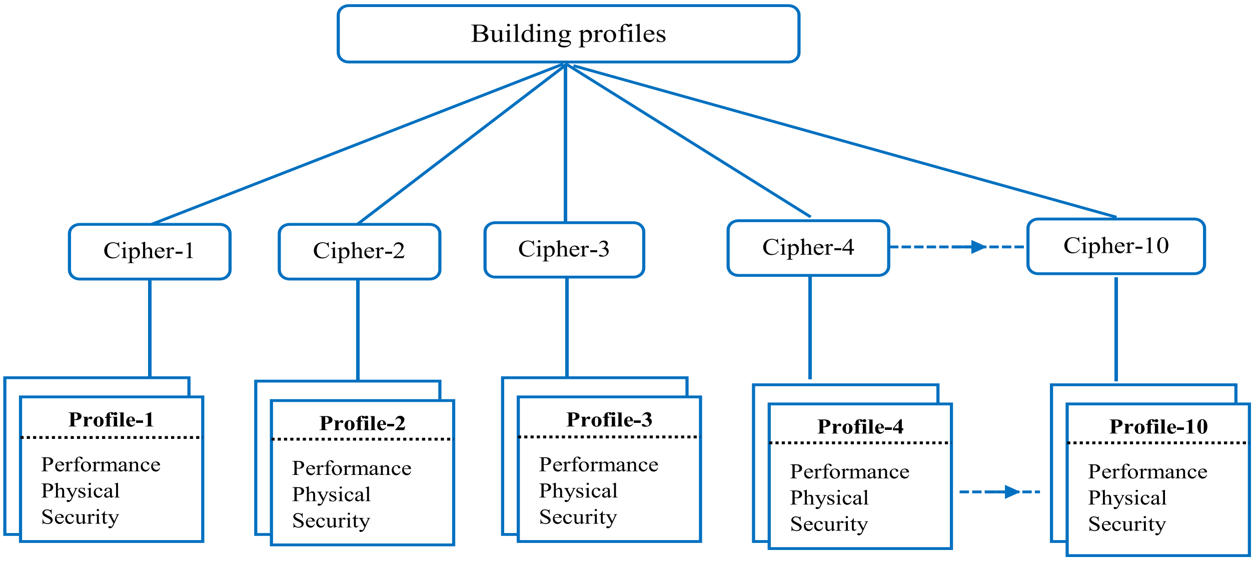

FIGURE 6. Hierarchical structure of profiles.

h: KLEIN

KLEIN cipher was designed by Zheng Gong *et al.* in 2011 [33]. It is lightweight block cipher with block size of 64 bits and key size of 64, 80 and 128 bits [56]. The Feistel structure of key scheduling of KLEIN cipher allows it to avoid key related attacks [56]. KLEIN has good software performance on legacy systems and at the same time its hardware implementation can also be compact [57]. KLEIN is based on Substitution-Permutation Network (SPN), which is used in AES and PRESENT ciphers [58], [59].

i: CAMELLIA

This cipher was presented by Nippon Telegraph and Telephone Corporation (NTTC) and Mitsubishi Electric Corporation of Japan [60]. It has good efficiency at both hardware and software and provides high level of security [60]. It is block cipher, which supports 128, 192 and 256 key sizes [61]. The new functions such as F L/F L^{-1} with the support of whitening layers of Camellia allows more security against attacks [62].

j: TEA

It is Tiny Encryption Algorithm with block size of 64 bits and key size of 128 bits [46]. It was developed by David Wheeler and Roger Needham at the Computer Laboratory of Cambridge University in 1994 [63]. It shows strong resistance to differential cryptanalysis. Its version are extended TEA and block TEA, which overcome the drawbacks of TEA cipher [46]. TEA hardware architecture provides simplicity, flexibility, less number of computations with the simple key scheduling [64]. XTEA is very fast algorithm as it does not use S-boxes and initialization time. The structure of XTEA algorithm is Feistal and it is used for real time applications [64]. The complete detail of all light weight ciphers selected for security evaluation is given in Table 4.

The detail of input data for profile entry is given in [46]. The selected ciphers will be evaluated based upon these profiles.

Profiles of individual ciphers are shown in Table 5.

The main motivation of proposed work is to select the best lightweight cryptographic primitive for lightweight authentication for IoHT. This research work completes in phase-wise fashion such as in first phase, the selection problem is identified then alternatives and criteria or properties for lightweight crypto security are identified. In this phase, security evaluation criteria is built based upon security requirements, which are collected from three different sources such as literature, ISO light weight security standard and NIST security characteristics. After, building the security evaluation criteria, 10 ciphers are selected for assessment and among these ciphers, one cipher is selected as best choice for light weight security in IoHT based system.

In second phase, CRITIC method has been employed to assign weights to the security criteria or properties related to lightweight cryptography. In 3rd phase, the alternatives are ranked by using TOPSIS method. TOPSIS method selects the best cipher among the list of 10 lightweight ciphers. All of phases involved in the research procedure are depicted diagrammatically in Fig 7.

D. CRITIC METHOD

CRITIC stands for "CRiteria Importance Through Intercriteria Correlation" and it was introduced by Diakoulaki *et al.* [65] in 1995. It is MCDM method which is applied for assigning weights to criteria in this research work. This method assigns weights to the criteria objectively such that without the judgements of decision makers or using pairwise

TABLE 4. Summary and detail of all ciphers selected for security evaluation.

Ref(s)	Cipher	Block size	Key size	Number of rounds	Structure	Attack against ciphers	Pros and Cons
[46] [20] [42]	PRESENT	64	80 128	31	SPN	▪ Side channel attacks ▪ Biclique attacks ▪ Related key attacks	**Pros:** ▪ Less code size ▪ Ideal for limited power and memory devices ▪ Energy efficient ▪ Ultra-light weight **Cons:** ▪ More vulnerable to side channel attacks
[46]	SEA	64	96	Variable	Feistal	----	**Pros:** ▪ Ease of use ▪ Easy to upgrade ▪ Low cost of development ▪ Flexibility ▪ Low latency **Cons:** ▪ Slow in software implementation ▪ Limited ability to protect private key ▪ Too slow for critical time applications
[46] [42] [49]	HIGHT	64	128	32	ARX+GFN	▪ Impossible differential Attack ▪ Zero-correlation attacks	**Pros:** ▪ Provide high security ▪ Good for limited and low resource system ▪ Composed of simple operations **Cons:** ▪ Higher power requirements ▪ Vulnerable to saturation attacks
[50] [46]	LEA	128	128 192 256	24 28 32	ARX	▪ Power analysis ▪ Side channel attack	**Pros** More ideal for resistance against side channel attacks **Cons.** It suffers from vulnerabilities
[45] [27] [42] [24]	AES	64	128 192 256	10 12 14	SPN	▪ Biclique cryptanalysis ▪ Man in middle	**Pros:** ▪ Supports large size of keys ▪ Efficient in both hardware and software ▪ It can be used as security solution at all IoT layers **Cons:** ▪ Not ideal for resource constrained devices ▪ Works on table based implementation, vulnerable to cache timing attack
[46]	mCrypton	64	64 96 128	13	SPN	▪ Rectangle attack	**Pros:** ▪ Low latency ▪ Ideal for RFID tags and sensors ▪ Low power consumptions ▪ Compact in both hardware and software implementations **Cons:** ▪ Not ideal for Electronic Product Code (EPC) encryption
[24, 46]	NOEKEON	128	28	16	SPN	▪ Related key cryptanalysis	**Pros:** ▪ Using bit-slicing technique ▪ Better performance ▪ Less number of rounds ▪ Less energy consumption **Cons:** ▪ High energy consumption per bit ▪ High latency ▪ Low hardware efficiency
[46, 57]	KLEIN	64	64 80 96	12 16 20	SPN	▪ Chosen-plaintext key-recovery attacks ▪ Biclique cryptanalysis	**Pros:** ▪ Compact hardware implementation ▪ Good performance on legacy system in software implementation ▪ Well balanced in key schedule ▪ Secure against potential related key attacks **Cons:** ▪ Consumes more energy per bit for 80 bits key
[46] [45] [19]	Camellia	128	128 192 256	18 24	Feistel	▪ Cache timing attacks in software implementations ▪ Impossible differential Square attack ▪ Boomerang attack ▪ Collision attack	**Pros:** ▪ More resistant against brute force attacks on keys ▪ Provides equal security of AES ▪ Heterogeneous system support **Cons** ▪ Focus needed for sensitivity applications ▪ It faces serious threats against cache timing attacks
[27, 46]	TEA	64	128	Variable	Feistel	▪ Key related attacks	**Pros:** ▪ Simple and easy to implement ▪ Suitable for wireless communication ▪ Less size of code **Cons:** ▪ More power consumption ▪ Poor performance as hash function ▪ High energy per bit

comparison [66]. CRITIC method is the type of correlation method [67].

For "m" number of possible alternatives such as A_i, when $i = 1, 2, 3 \ldots .m$, and "n" number of evaluation criteria

TABLE 5. Profiles of ciphers.

Profile 1				
Primitive	**PRESENT-80**			
Physical characteristics	**Chip area**	**Code size**	**Implementation**	**RAM Size**
	1075	1000	Hardware+Software	18
Performance characteristics	**Throughput**	**Power**	**Energy**	**Latency**
	11.7	1.61	137.81	547
Security characteristics (Key size)	80 bit security			
Profile 2				
Primitive	**SEA**			
Physical characteristics	**Chip area in**	**Code size**	**Implementation**	**RAM size**
	2569	426	Hardware+Software	24
Performance characteristics	**Throughput**	**Power**	**Energy**	**Latency**
	3.29	3.85	1170.50	243
Security characteristics (Key size)	96 bit security			
Profile 3				
Primitive/Cipher	**HIGHT**			
Physical characteristics	**Chip area in**	**Code size**	**Implementation**	**RAM size**
	3048	402	Hardware+Software	32
Performance characteristics	**Throughput**	**Power**	**Energy**	**Latency**
	188	5.48	29.14	34
Security characteristics (Key size)	128 bit security			
Profile 4				
Primitive	**LEA**			
Physical characteristics	**Chip area in**	**Code size**	**Implementation**	**RAM size**
	3826	590	Hardware+Software	32
Performance characteristics	**Throughput**	**Power**	**Energy**	**Latency**
	76.19	3.82	50.22	168
Security characteristics (Key size)	128 bit security			
Profile 5				
Primitive	**AES Block cipher**			
Physical characteristics	**Chip area**	**Code size**	**Implementation**	**RAM size**
	2400	1659	Software+Hardware	33
Performance characteristics	**Throughput**	**Power**	**Energy**	**Latency**
	56.64	2.4	42.38	226
Security characteristics (Key size)	128 bit security			
Profile 6				
Primitive	**mCrypton**			
Physical characteristics	**Chip area**	**Code size**	**Implementation**	**RAM size**
	2760	3108	Hardware+Software	24
Performance characteristics	**Throughput**	**Power**	**Energy**	**Latency**
	33.51	4.14	122.90	190
Security characteristics (Key size)	128 bit security			
Profile 7				
Primitive	**NOEKEON**			
Physical characteristics	**Chip area**	**Code size**	**Implementation**	**RAM size**
	2862	364	Hardware+Software	32
Performance characteristics	**Throughput**	**Power**	**Energy**	**Latency**
	3.44	4.30	1247.65	3720
Security characteristics (Key size)	128 bit security			
Profile 8				
Primitive	**KLEIN**			

TABLE 5. ***(Continued.)*** **Profiles of ciphers.**

Physical characteristics	**Chip area in**	**Code size**	**Implementation**	**RAM size**
	1478	1268	Hardware+Software	`18
Performance characteristics	**Throughput**	**Power**	**Energy**	**Latency**
	23.62	2.21	93.87	271
Security characteristics (Key size)	80 bit security			
Profile 9				
Primitive	**Camellia**			
Physical characteristics	**Chip area in**	**Code size**	**Implementation**	**RAM size**
	6511	1262	Hardware+Software	12
Performance characteristics	**Throughput**	**Power**	**Energy**	**Latency**
	290.1	9.76	33.57	44
Security characteristics (Key size)	128 bit security			
Profile 10				
Primitive	**TEA**			
Physical characteristics	**Chip area in**	**Code size**	**Implementation**	**RAM size**
	2355	1354	Hardware+Software	13
Performance characteristics	**Throughput**	**Power**	**Energy**	**Latency**
	100	3.53	35.32	64
Security characteristics (Key size)	128 bit security			

such as C_j for $j = 1, 2, 3 \ldots n$, in a problem. This method is composed of the following steps [66], [68].

Step-1 (Building a Decision Matrix): In the first step of this method a decision matrix X is created.

$$X = [X_{ij}] = \begin{bmatrix} X_{11} & X_{12} & \ldots & X_{1n} \\ X_{21} & X_{22} & \ldots & X_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ X_{m1} & X_{m2} & \ldots & X_{mn} \end{bmatrix} \times (\text{for } i = 1, 2, 3 \ldots m \text{ and } J = 1, 2, 3 \ldots n) \quad (1)$$

In equation (1), X_{ij} shows the performance value of it^{h} alternative on jth criterion.

Step-2 (Decision Matrix Normalization): The normalization of the decision matrix is done by using the following equation.

$$X^*_{ij} = \frac{X_{ij} - \min(X_{ij})}{\max\left(X_{ij}\right) - \min(X_{ij})} \quad i = 1, 2 \ldots m \text{ and } j = 1, 2 \ldots n \quad (2)$$

X^*_{ij} is the normalized performance value of *i*th alternative on *j*th criterion.

Step-3 (Calculation of Standard Deviation and Its co-Relation With Other Criteria for Criteria Weights): In this step, the weights of jth criterion can be found with the following equation.

$$W_j = \frac{C_j}{\sum_{j=1}^{n} C_j} \quad (3)$$

In equation (3), C_j is the amount of information contained in jth criterion. C_j is calculated as follow.

$$C_j = \sigma_j \sum\nolimits_{j'=1}^{n} \left(1 - rjj'\right) \quad (4)$$

where, σ_j is standard deviation of the j^{th} criterion and r'_{jj} is the correlation coefficient between the two criteria.

E. CRITIC NUMERICAL WORK

In this section, weights are assigned to the criteria by using CRITIC method. The main purpose of the proposed work is to find the best light weight cryptographic primitive or cipher by using hybrid MCDM approach. The profiles of lightweight ciphers as (previously mentioned) have been used as alternative such as P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9 and P_{10} for the purpose of decision making. Security requirements, performance and physical characteristics are used as criteria such as chip area (C_1), Throughput (C_2), power consumption (C_3), energy (C_4), latency (C_5), program code size (C_6), RAM size (C_7) and security strength (C_8). All the selected criteria are quantitative in nature. Criteria can be divided into two types: beneficial and non-beneficial. In this table beneficial criteria are C2 and C8 and remaining are non-beneficial criteria. Decision matrix is established for ten (10) type of different lightweight crypto ciphers with respect to defined security properties/criteria as are given in Table 6.

Decision matrix is normalized by applying equation (2) and results is given in Table 7.

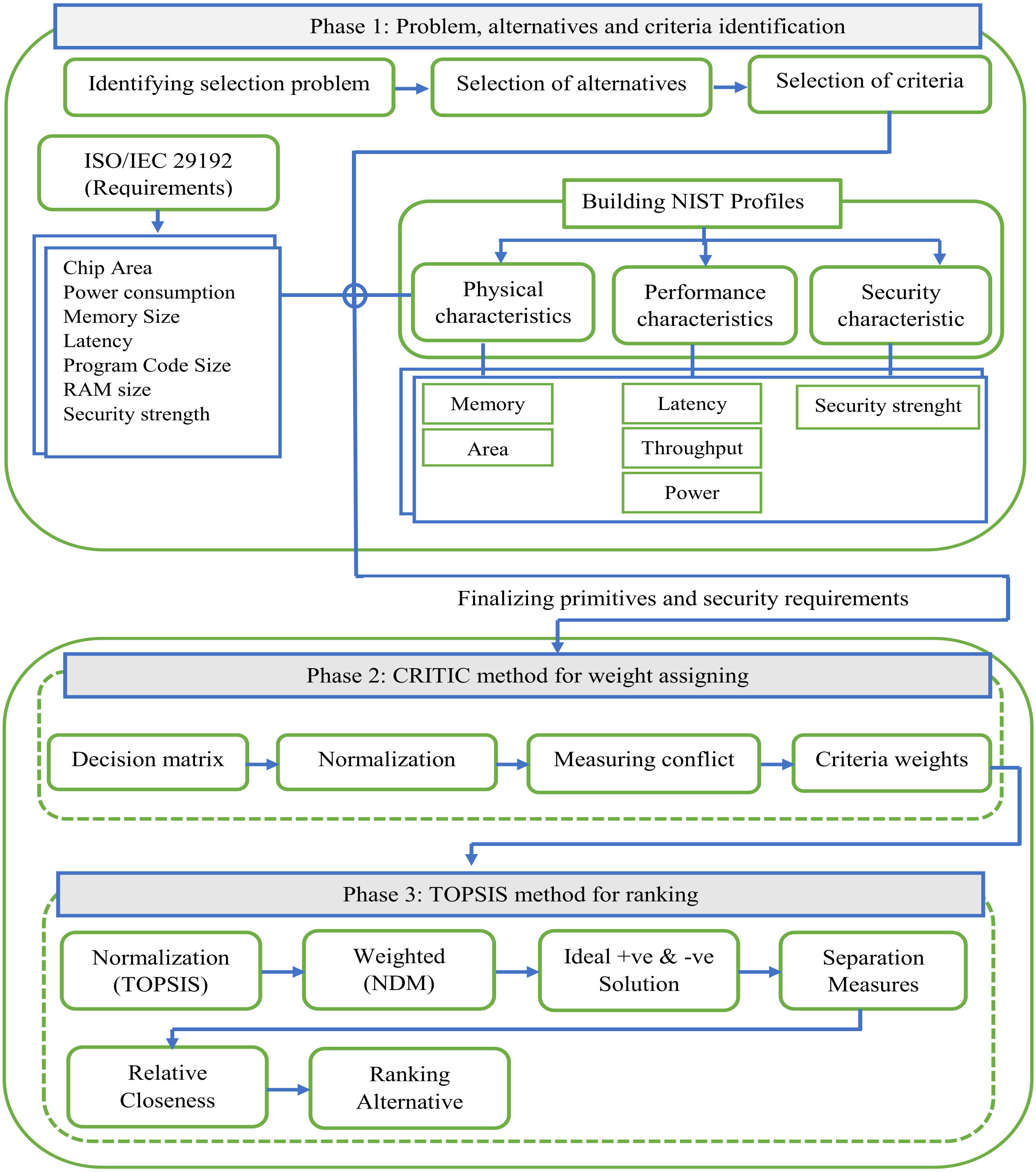

FIGURE 7. **Proposed evaluation framework.**

Correlation coefficient of each criteria is calculated as shown in Table 8.

Measure of conflict, quantity of information, criteria weights and standard deviation are shown in Table 9.

The weights assigned to the security criteria after applying the CRITIC method and results are displayed in Fig 8.

F. TOPSIS METHOD

This method "Technique for Order Preference by Similarity to Ideal Solution" (TOPSIS) was presented by Krohling and Pacheco [69]. This method works on by using ideal solution, if alternative is closer towards the positive ideal solution then it will considered as best solution. TOPSIS

TABLE 6. Decision matrix [46].

Alternative	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
	Chip Area (GE)	Throughput @ 100 KHz (Kbps)	Power Consumption (μw)	Energy (μJ/ bit)	Latency (Cycles/block)	Program code size (Bytes)	RAM size (Bytes)	Key size (bits)
P_1	1075	11.7	1.61	137.81	547	1000	18	80
P_2	2569	3.29	3.85	1170.5	243	426	24	96
P_3	3048	188	5.48	29.14	34	402	32	128
P_4	3826	76.19	3.82	50.22	168	590	32	128
P_5	2400	56.64	2.4	42.38	226	1659	33	128
P_6	2760	33.51	4.14	122.9	190	3108	24	128
P_7	2862	3.44	4.3	1247.65	3720	364	32	128
P_8	1478	23.62	2.21	93.87	271	1268	18	80
P_9	6511	290.1	9.76	33.57	44	1262	12	128
P_{10}	2355	100	3.53	35.32	64	1354	13	128

TABLE 7. Normalized decision matrix.

Alternatives	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
P_1	0.000	0.029	0.000	0.089	0.139	0.232	0.286	1.000
P_2	0.275	0.000	0.275	0.937	0.057	0.023	0.571	0.667
P_3	0.363	0.644	0.475	0.000	0.000	0.014	0.952	0.000
P_4	0.506	0.254	0.271	0.017	0.036	0.082	0.952	0.000
P_5	0.244	0.186	0.097	0.011	0.052	0.472	1.000	0.000
P_6	0.310	0.895	0.310	0.077	0.042	1.000	0.571	0.000
P_7	0.329	0.999	0.330	1.000	1.000	0.000	0.952	0.000
P_8	0.074	0.929	0.074	0.053	0.064	0.329	0.286	1.000
P_9	1.000	0.000	1.000	0.004	0.003	0.327	0.000	0.000
P_{10}	0.235	0.663	0.236	0.005	0.008	0.361	0.048	0.000

TABLE 8. Correlation coefficient of criteria.

	C1	C2	C3	C4	C5	C6	C7	C8
C1	1.000	0.515	0.725	-0.078	-0.849	-0.422	0.794	-0.798
C2	0.515	1.000	0.760	-0.536	-0.763	-0.295	0.656	-0.702
C3	0.725	0.760	1.000	0.092	-0.883	-0.730	0.539	-0.549
C4	-0.078	-0.536	0.092	1.000	0.081	-0.398	-0.402	0.472
C5	-0.849	-0.763	-0.883	0.081	1.000	0.364	-0.860	0.853
C6	-0.422	-0.295	-0.730	-0.398	0.364	1.000	0.099	-0.075
C7	0.794	0.656	0.539	-0.402	-0.860	0.099	1.000	-0.995
C8	-0.798	-0.702	-0.549	0.472	0.853	-0.075	-0.995	1.000

method follows simple computation procedure, it is well established and reliable [69]. In TOPSIS method the selected alternative should have the minimum distance from the positive ideal solution and the maximum distance from the negative-ideal solution. This method follows the following procedure [69], [70].

Step-1 (Building Decision Matrix): In this step, a decision matrix such as D is constructed by using multiple criteria and alternatives. For example for "n" number of alternatives and criteria, the decision matrix can be found as.

$$D = \begin{array}{c|ccc|} & C_1 & \cdots\cdots\cdots & C_n \\ A_1 & X_{11} & \cdots\cdots & X_{1n} \\ \vdots & & & \\ A_n & \vdots & \ddots & \vdots \\ & X_{m1} & \cdots\cdots\cdots & X_{mn} \end{array} \tag{5}$$

where A_1, A_2, A_3......A_n, are variable alternatives and C_1, C_2, C_3......C_n are the criteria.

TABLE 9. **Criteria weights.**

Criteria	Measure of conflict	Standard Deviation	Quantity of information	Criteria weights
C1	7.114	0.274	1.948	**0.089**
C2	7.366	0.408	3.008	**0.137**
C3	7.045	0.281	1.978	**0.090**
C4	7.769	0.396	3.079	**0.140**
C5	9.058	0.305	2.761	**0.125**
C6	8.457	0.302	2.558	**0.116**
C7	7.170	0.392	2.810	**0.128**
C8	8.795	0.439	3.860	**0.175**

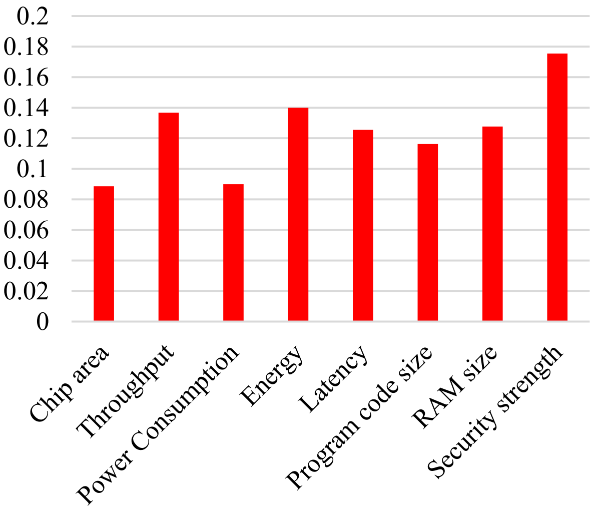

FIGURE 8. **Weights of criteria.**

Step-2 (Building Normalized Decision Matrix): The input data of the decision matrix *D* originated from different sources, therefore, it has to be normalized to convert it into a dimensionless matrix.

The comparison of different criteria is done via Dimension matrix. A normalized decision matrix is built by using the following formula.

$$R_{i_j} = \frac{X_{i_j}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \qquad (6)$$

For i = 1 . . . . .m and j = 1 . . . . . . n

Step-3 (Determining the Weighted Normalized Decision Matrix): It is not necessary that all attributes must be of same importance. Therefore, a weighted normalized decision matrix can be obtained by multiplying the each element of normalized decision matrix with a random weight number as given in formula below.

$$V = V_{ij} = W_j \times R_{ij}$$

$$V = \begin{bmatrix} V_{11} & V_{12} & V_{1j} & V_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ V_{i1} & V_{i2} & V_{ij} & V_{in} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ V_{m1} & V_{m2} & V_{mi} & V_{mn} \end{bmatrix}$$
$$= \begin{bmatrix} w_1r_{11} & w_1r_{11} & w_1r_{11} & w_1r_{11} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ w_1r_{11} & w_1r_{11} & w_1r_{11} & w_1r_{11} \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ w_1r_{11} & w_1r_{11} & w_1r_{11} & w_1r_{11} \end{bmatrix} \qquad (7)$$

Step-4 (Finding Ideal Positive and Negative Solutions): The positive ideal solutions are denoted by A^+ and negative ideal solutions are represented by A^-. These are determined by using weighted decision matrix.

$$A^+ = \left\{V_1^+, V_2^+, V_3^+, V_n\right\}, \quad \text{Where}$$
$$V_j^+ = \left\{((\text{maxi}\left(V_{ij}\right) \text{ if } j \in J);\ (\text{mini } V_{ij} \text{ if } j \in J^{'})\right\} \qquad (8)$$
$$A^- = \left\{V_1^-, V_2^-, V_3^-, V_n^-\right\}, \quad \text{Where}$$
$$V_j^- = \left\{(\text{mini}\left(V_{ij}\right) \text{ if } j \in J);\ (\text{maxi}V_{ij}\text{if } j \in J^{'})\right\} \qquad (9)$$

where, J denotes the beneficial attributes and J' is shows non-beneficial attributes.

Step-5 (Determining the Separation Measures): Ideal and no ideal separation are calculated by the following formulae.

$$S^+ = \sqrt{\sum_{J=1}^{n} (V_{ij} - V+)^2} \quad \text{For } i = 1 \ldots \text{m} \qquad (10)$$

$$S^{-} = \sqrt{\sum_{J=1}^{n} (V_{ij} - V^{-})^2} \quad \text{For } i = 1 \ldots .m \qquad (11)$$

Step-6 (Finding of Relative Closeness): It is determined with respect to the ideal solutions by using the following equation.

$$C_i = \frac{S_{i^-}}{(S_i^+ + S_i^-)} \quad 0 \le C_i \le 1 \qquad (12)$$

Step-7 (Ranking of Alternatives): The ranking is done by using Ci value, the maximum value of Ci means the higher the ranking order and alternative can be described as better in terms of performance. Ranking of preferences can be performed in ascending or descending order. The descending order of preferences can be used for comparing the better performance.

1) APPLICATION OF TOPSIS METHOD

In context of decision making, the TOPSIS method is applied for ranking alternatives. TOPSIS method selects the profile that describes the best light weight authentication algorithm or cipher among the ten alternatives. The decision matrix as mentioned in Table (5) is normalized by using equation (6) and output is shown in Table 9. The criteria weights obtained from CRITIC method are also written in Table 10.

Ideal positive solution ($A^{+)}$ and Ideal negative solution (A^{-}) are determined from weighted normalized data table and results are given in Table 11.

Ideal separation measure, non-ideal separation measures, value of relative closeness are calculated by equation (10), (11) and (12) respectively and results are depicted in Table 12.

Ranking of alternatives is performed based upon the values of relative closeness. The higher value of C_i indicates the best alternative among the five alternatives. The alternatives are ordered according the values of relative closeness and best alternative among the all alternatives is given in Table 13.

From Table 13, it is clear that P_8 alternative has the highest value among all alternatives so it best option of security for lightweight cryptography. The comparison of alternative is given in Fig 9.

Alternatives in chronological orders are $\mathbf{P_8} > \mathbf{P_3} > \mathbf{P_7} > \mathbf{P_9} > \mathbf{P_2} > \mathbf{P_5} > \mathbf{P_4} > \mathbf{P_6} > \mathbf{P_{10}} > \mathbf{P_1}$. It is clear from Fig 8 that P_8 is profile of KLEIN cipher, which is considered to be best lightweight cryptographic cipher against the security requirements for light weight security in internet of health things.

2) CRYPTO ANALYSIS OF KLEIN CIPHER

Our proposed evaluation framework ranks and selects the KLEIN cipher among the different ciphers and hence, it can be used for light weight cryptographic security in IoHT environment. KLEIN cipher is ideal for healthcare environment as the following crypto-analysis which validates the reason for selection of KLIEN cipher among the list of selected ciphers by our proposed evaluation framework intended to select best choice among the list of lightweight cryptographic authentication ciphers.

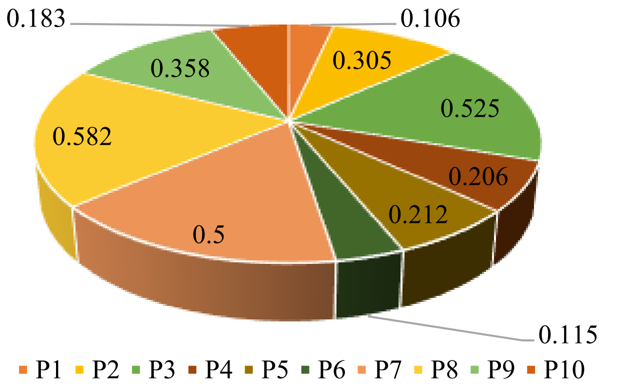

FIGURE 9. Alternatives comparisons.

- KLEIN cipher is well suited for low-resource applications such as IoT and wireless sensor and actuators based networks. This is the main reason that it can be used as light weight security option for IoHT system.
- It provides good security in full rounds. KLEIN offers a variety of key sizes, which makes it more flexible.
- Besides, KLEIN can be implemented on both hardware and software like legacy sensors systems.
- KLEIN uses byte-oriented structure like AES for better software performances.
- The S-box nature of KLEIN provides strong resistant against side channel attacks [57].
- Similarly, Gong *et al.* [57] also studied the performance of KLEIN cipher with other lightweight ciphers such as AES, NOEKEON, SEA, HIGHT, PRESENT and mCrypton on different platforms such as IRIS and TelosB and according to the results obtained they suggested that KLEIN cipher shows better performance among the mentioned ciphers. They also compared the hardware implementation of KLEIN and it showed good results, comparatively.
- KLEIN cipher is selected as best option for lightweight authentication as it provides best results among the selected algorithm for different assessment parameters like size of memory, code size, RAM size, chip area, latency, throughput, power consumption, memory usage and type of implementation.
- From the decision matrix (Input table), it is quite clear that KLEIN cipher requires less chip area and low power consumption and low latency as compared to all other ciphers.

In light of above discussion, we believe that KLEIN cipher is better choice as light weight security option in IoHT environment. Several studies are available regarding different aspects of security [71]–[78].

3) SIGNIFICANCE OF USING CRITIC AND TOPSIS

In the proposed evaluation framework both CRITIC and TOPSIS methods have been used to support the validity of framework. The main idea of using CRITIC method

TABLE 10. Normalized data with TOPSIS.

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
P_1	0.1057	0.0312	0.1095	0.0799	0.1442	0.2278	0.2272	0.2164
P_2	0.2527	0.0088	0.2619	0.6784	0.0641	0.0970	0.3030	0.2596
P_3	0.2998	0.5018	0.3728	0.0169	0.0090	0.0916	0.4040	0.3462
P_4	0.3763	0.2034	0.2599	0.0291	0.0443	0.1344	0.4040	0.3462
P_5	0.2360	0.1512	0.1633	0.0246	0.0596	0.3779	0.4166	0.3462
P_6	0.2715	0.0894	0.2817	0.0712	0.0501	0.7080	0.3030	0.3462
P_7	0.2815	0.0092	0.2926	0.7231	0.9806	0.0829	0.4040	0.3462
P_8	0.2088	0.0767	0.2083	0.8875	0.9613	0.5652	0.7132	0.4042
P_9	0.6404	0.7743	0.6640	0.0195	0.0116	0.2875	0.1515	0.3462
P_{10}	0.2316	0.2669	0.2402	0.0205	0.0169	0.3084	0.1641	0.3462
Weights	**0.089**	**0.137**	**0.090**	**0.140**	**0.125**	**0.116**	**0.128**	**0.175**

TABLE 11. Weighted normalized data.

Alternatives	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
P_1	0.009	0.004	0.010	0.011	0.018	0.026	0.029	0.038
P_2	0.022	0.001	0.024	0.095	0.008	0.011	0.039	0.045
P_3	0.027	0.076	0.061	0.000	0.001	0.035	0.168	0.120
P_4	0.033	0.028	0.023	0.004	0.006	0.016	0.052	0.061
P_5	0.021	0.021	0.015	0.003	0.007	0.044	0.053	0.061
P_6	0.024	0.019	0.008	0.020	0.016	0.013	0.016	0.031
P_7	0.025	0.001	0.026	0.101	0.123	0.010	0.052	0.061
P_8	0.019	0.011	0.019	0.124	0.120	0.066	0.091	0.071
P_9	0.057	0.106	0.060	0.003	0.001	0.033	0.019	0.061
P_{10}	0.021	0.037	0.022	0.003	0.002	0.036	0.021	0.061
$A+$	**0.057**	**0.106**	**0.061**	**0.124**	**0.123**	**0.066**	**0.168**	**0.120**
A^-	**0.009**	**0.001**	**0.008**	**0.000**	**0.001**	**0.010**	**0.016**	**0.031**

TABLE 12. Ideal separation measure, non-ideal separation measure and relative closeness of alternatives.

Alternatives	Ideal separation measure	Non-ideal separation measure	$S^+ + S^-$	Relative closeness
P_1	0.258	0.031	0.289	0.106
P_2	0.230	0.101	0.330	0.305
P_3	0.182	0.201	0.383	0.525
P_4	0.236	0.061	0.297	0.206
P_5	0.236	0.064	0.300	0.212
P_6	0.260	0.034	0.294	0.115
P_7	0.167	0.167	0.333	0.500
P_8	0.144	0.201	0.345	0.582
P_9	0.237	0.132	0.369	0.358
P_{10}	0.251	0.056	0.307	0.183

for assigning weights to criteria or requirements is, this method uses statistical techniques to validate the proposed framework empirically. Similarly, CRITIC method assigns uniform weight values to the criteria and it is based upon analytical testing of decision matrix [67]. CRITIC method also uses co-relational analysis and standard deviation for finding the contrast among all the criteria [68].

TABLE 13. Ranking alternatives.

Alternatives	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}
Final score	0.106	0.305	0.525	0.206	0.212	0.115	0.500	**0.582**	0.358	0.183
Ranking	10	5	2	7	6	8	3	**1**	4	9

Similarly, TOPSIS method has been used for evaluation and ranking of lightweight authentication ciphers against the defined criteria or requirements. TOPSIS performs ranking based on similarity to the ideal solution. It avoids the same similarity index to both negative and positive ideal solutions. TOPSIS is more practical and more ideal techniques for ranking of alternatives [71]. TOPSIS provides ease and efficient computation. It is mathematical model which measures both best and worst alternatives by considering the relative performance.

In light of above discussion, we can say that both multi criteria decision making techniques such as CRITIC and TOPSIS are adequate enough to be fit in this framework for the purpose of assigning weights to criteria and evaluating alternatives against the criteria defined for lightweight authentication ciphers.

VII. LIMITATIONS AND CHALLENGES

- This proposed evaluation framework is applied on data collected from microcontroller technology for 10 lightweight security ciphers. The performance and evaluation results may change with the changes in the technology used for running these ciphers. The proposed framework is using limited number of ciphers and it can be extended for more number of ciphers.
- Although, we have made a vigorous attempt to formulate the best security evaluation criteria based on most vital security requirements but relatively, these requirements get changed from one platform to other platform. These requirements are not absolute as security parameters for some other frameworks or plateforms. Like some authors used different evaluation metrics, but still the main focus was to include the most fundamental security requirements.
- There are some important security requirements like side channel attacks, short input performance, size of file, encryption and decryption time, avalanche effect, block size, efficiency, figure of merit, technology used and execution time. These parameters can also be used as evaluation metric for selection of light weight authentication cipher.

VIII. CONCLUSION

Light weight cryptographic security of IoT based system in health care environment is important due to nature of wearable devices, nodes and sensors. In modern world there are enormous number of lightweight authentication ciphers but the selection and ranking of these algorithm becomes an issue due to the number of factors and conflicting objectives involved. This issued become more significant in healthcare environment due to the nature of sensitive and fragile data related to patient's record. Hence, the selection of most appropriate and best authentication cipher providing a solution towards light weight authentication security issues is the most challenging task due to the rapidly changing in the number of evaluation parameters. For this purpose a proposed evaluation framework is presented to address the issued related to the decision making and evaluation of lightweight ciphers. Light weight cryptographic cipher is considered for authentication based upon different physical, performance and security parameters or requirements, extracted from ISO lightweight cryptography standard and National Institute of Standards and Technology (NIST). The proposed framework works in two folds: in first evaluation metric or criteria and profiles are built based on different requirements and in second fold, the hybrid MCDM methods such as CRITIC and TOPSIS methods are applied for the purpose of objective weight assignment to criteria and ranking the alternatives respectively. Weights are assigned to the criteria by using CRITIC method and then TOPSIS method is used to rank the profiles of lightweight authentication ciphers based upon security requirements. The results obtained after the empirical work suggest that KLEIN cipher is ranked as first among the lightweight ciphers such as PRESENT-80, SEA, HIGHT, LEA, AES Block cipher, mCrypton, NOEKEON, Camellia and TEA ciphers. KLEIN cipher can used as lightweight authentication option for IoT devices operating in healthcare system. Results obtained from the evaluation framework are impactful and have been thoroughly revised by the experts in the field of IoT security evaluation. The ranking of ciphers is done based upon the quantitative and empirical data after applying both MCDM methods. These are the standard methods and results obtained from these methods are impactful and recognizable. These methods have variety of applications in other domains as well like industry, transportation, agricultural, production, business, engineering and banking.

The proposed evaluation framework selects the most suitable of lightweight authentication cipher and hence, it can be used as benchmark for assessment and ranking of lightweight cryptographic ciphers in healthcare or in any other environment. This framework provides a comprehensive guideline for security policy makers and IoT network administrator in healthcare environment to select and use the most suitable authentication cipher against the defined security criteria. The security evaluation criteria covers all the dimensions of lightweight cryptographic security to provide a full pledged secure IoHT based system.

The proposed evaluation framework for lightweight cryptographic authentication cipher focuses basically upon the physical and performance characteristics of ciphers. Our future work is to extend this framework by adding security requirements such as resistance against side channel attacks, relevant attack models, encryption and decryption time, block size, number of rounds, key scheduling and structure. In future, we will focus on bringing these security requirements for considering the most suitable and appropriate lightweight authentication cipher to address the authentication issues prevailing in healthcare environment. Our focus is also to use fuzzy approach for decision making and setting a new benchmark related to security requirements of IoHT devices.

IX. CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding this article.

REFERENCES

[1] S. Makkar, A. K. Singh, and S. Mohapatra, "Challenges and opportunities of Internet of Things for health care," in *A Handbook of Internet of Things in Biomedical and Cyber Physical System*. Cham, Switzerland: Springer, 2020, pp. 301–314.

[2] S. Polat, *Performance Evaluation of Lightweight Cryptographic Algorithms for Internet of Things Security*. Ankara, Turkey: Middle East Technical Univ., 2019.

[3] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of IoT devices using blockchain-enabled fog nodes," in *Proc. IEEE/ACS 15th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Oct. 2018, pp. 1–8.

[4] A. W. Atamli and A. Martin, "Threat-based security analysis for the Internet of Things," in *Proc. Int. Workshop Secure Internet Things*, Sep. 2014, pp. 35–43.

[5] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6LoWPAN based Internet of Things," in *Proc. IEEE 9th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2013, pp. 600–607.

[6] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in *Proc. Int. Conf. Modeling, Identificat. Control*, Jun. 2011, pp. 563–566.

[7] W. J. Buchanan, S. Li, and R. Asif, "Lightweight cryptography methods," *J. Cyber Secur. Technol.*, vol. 1, nos. 3–4, pp. 187–201, Sep. 2017.

[8] A. Shah and M. Engineer, "A survey of lightweight cryptographic algorithms for IoT-based applications," in *Smart Innovations in Communication and Computational Sciences*. Singapore: Springer, 2019, pp. 283–293.

[9] *Information technology—Security techniques—Lightweight cryptography—Part 1: General*, document ISO/IEC 29192-1:2012, 2012. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:29192:-1:ed-1:v1:en

[10] N. Dimitrioglou, D. Kardaras, and S. Barbounaki, "Multicriteria evaluation of the Internet of Things potential in health care: The case of dementia care," in *Proc. IEEE 19th Conf. Bus. Informat. (CBI)*, Jul. 2017, pp. 454–462.

[11] J. I. Drake, J. C. T. de Hart, C. Monleón, W. Toro, and J. Valentim, "Utilization of multiple-criteria decision analysis (MCDA) to support healthcare decision-making FIFARMA, 2016," *J. Market Access Health Policy*, vol. 5, no. 1, Jan. 2017, Art. no. 1360545.

[12] Y. Liu, Y. Yang, Y. Liu, and G.-H. Tzeng, "Improving sustainable mobile health care promotion: A novel hybrid MCDM method," *Sustainability*, vol. 11, no. 3, p. 752, Jan. 2019.

[13] N. A. Nabeeh, M. Abdel-Basset, H. A. El-Ghareeb, and A. Aboelfetouh, "Neutrosophic multi-criteria decision making approach for IoT-based enterprises," *IEEE Access*, vol. 7, pp. 59559–59574, 2019.

[14] S. S. Rani, J. A. Alzubi, S. K. Lakshmanaprabu, D. Gupta, and R. Manikandan, "Optimal users based secure data transmission on the Internet of healthcare things (IoHT) with lightweight block ciphers," *Multimedia Tools Appl.*, vol. 79, pp. 1–20, May 2019.

[15] T. D. C. Frazão, D. G. G. Camilo, E. L. S. Cabral, and R. P. Souza, "Multicriteria decision analysis (MCDA) in health care: A systematic review of the main characteristics and methodological steps," *BMC Med. Informat. Decis. Making*, vol. 18, no. 1, p. 90, Dec. 2018.

[16] S. Kerckhof, F. Durvaux, C. Hocquet, D. Bol, and F.-X. Standaert, "Towards green cryptography: A comparison of lightweight ciphers from the energy viewpoint," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2012, pp. 390–407.

[17] C. Pei, Y. Xiao, W. Liang, and X. Han, "Trade-off of security and performance of lightweight block ciphers in industrial wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, p. 117, Dec. 2018.

[18] P. Patil, P. Narayankar, N. D. G., and M. S. M., "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish," *Procedia Comput. Sci.*, vol. 78, pp. 617–624, Jan. 2016.

[19] P. M. M. Girija and M. Ramaswami, "Comprehensive analysis on lightweight cryptographic algorithms for low resource devices," *Test Eng. Managment*, vol. 81, p. 14, Dec. 2019.

[20] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 24, no. 6, pp. 522–533, Nov. 2007.

[21] T. K. Goyal, V. Sahula, and D. Kumawat, "Energy efficient lightweight cryptography algorithms for IoT devices," *IETE J. Res.*, pp. 1–14, Nov. 2019.

[22] S. Rajesh, V. Paul, V. Menon, and M. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 293, Feb. 2019.

[23] J. Figueroa-Hernandez, Jr, *A Comparison of Lightweight Ciphers Meeting NIST Lightweight Cryptography Requirements to the Advanced Encryption Standard*. Pomona, CA, USA: California State Polytechnic Univ., 2019.

[24] J. A. C. S. Fernandes. (Jun. 19, 2020). *Choosing the Future of Lightweight Encryption Algorithms [Thesis]*. Available: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://fenix.tecnico.ulisboa.pt/downloadFile/281870113704550/Extended_Abstract-Choosing_the_Future_of_Lightweight_Encryption_Algorithms.pdf

[25] B. Chaitra, V. Kumar, and R. Shatharama, "A survey on various lightweight cryptographic algorithms on FPGA," *IOSR J. Electron. Commun. Eng.*, vol. 12, no. 1, pp. 45–59, 2017.

[26] S. Rana, S. Hossain, H. I. Shoun, and M. A. Kashem, "An effective lightweight cryptographic algorithm to secure resource-constrained devices," *Spectrum*, vol. 9, no. 11, pp. 1–9, 2018.

[27] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight cryptography: A solution to secure IoT," *Wireless Pers. Commun.*, vol. 112, pp. 1–34, Jan. 2020.

[28] P. Singh and K. Deshpande, "Performance evaluation of cryptographic ciphers on IoT devices," 2018, *arXiv:1812.02220*. [Online]. Available: http://arxiv.org/abs/1812.02220

[29] F. Mollaie, M. Alizadeh, S. Dadsetan, and A. Rashno, "Implementation and evaluation of lightweight encryption algorithms suitable for RFID," *J. Next Gener. Inf. Technol.*, vol. 4, no. 1, pp. 65–77, Feb. 2013.

[30] J. Awotunde, A. Ameen, I. Oladipo, A. Tomori, and M. Abdulraheem, "Evaluation of four encryption algorithms for viability, reliability and performance estimation," *Nigerian J. Technol. Develop.*, vol. 13, no. 2, pp. 74–82, 2016.

[31] F. Ullah, M. A. Habib, M. Farhan, S. Khalid, M. Y. Durrani, and S. Jabbar, "Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare," *Sustain. Cities Soc.*, vol. 34, pp. 90–96, Oct. 2017.

[32] R. Sadhukhan, S. Patranabis, A. Ghoshal, D. Mukhopadhyay, V. Saraswat, and S. Ghosh, "An evaluation of lightweight block ciphers for resource-constrained applications: Area, performance, and security," *J. Hardw. Syst. Secur.*, vol. 1, no. 3, pp. 203–218, Sep. 2017.

[33] J. Hosseinzadeh and M. Hosseinzadeh, "A comprehensive survey on evaluation of lightweight symmetric ciphers: Hardware and software implementation," *Adv. Comput. Sci., Int. J.*, vol. 5, no. 4, pp. 31–41, 2016.

[34] M. A. KARADAYI and E. E. KARSAK, "Fuzzy MCDM approach for health-care performance assessment in Istanbul," in *Proc. 18th World Multi-Conf. Systemics, Cybern. Inform.*, 2014, pp. 228–233.

[35] H. Akdag, T. Kalaycı, S. Karagöz, H. Zülfikar, and D. Giz, "The evaluation of hospital service quality by fuzzy MCDM," *Appl. Soft Comput.*, vol. 23, pp. 239–248, Oct. 2014.

[36] Ž. Stevic, D. Pamučar, A. Puška, and P. Chatterjee, "Sustainable supplier selection in healthcare industries using a new MCDM method: Measurement of alternatives and ranking according to COmpromise solution (MARCOS)," *Comput. Ind. Eng.*, vol. 140, Feb. 2020, Art. no. 106231.

[37] H.-C. Liu, J.-X. You, C. Lu, and Y.-Z. Chen, "Evaluating health-care waste treatment technologies using a hybrid multi-criteria decision making model," *Renew. Sustain. Energy Rev.*, vol. 41, pp. 932–942, Jan. 2015.

[38] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA evaluation framework for security of Internet of health things system using AHP-TOPSIS methods," *IEEE Access*, vol. 8, pp. 152316–152332, 2020.

[39] G. Buyukozkan, O. Feyzioglu, and F. Gocer, "Evaluation of hospital Web services using intuitionistic fuzzy AHP and intuitionistic fuzzy VIKOR," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM)*, Dec. 2016, pp. 607–611.

[40] H. Khemissa and D. Tandjaoui, "A lightweight authentication scheme for E-Health applications in the context of Internet of Things," in *Proc. 9th Int. Conf. Next Gener. Mobile Appl., Services Technol.*, Sep. 2015, pp. 90–95.

[41] A. Biryukov and L. P. Perrin, "State of the art in lightweight symmetric cryptography," Univ. Luxembourg, Luxembourg City, Luxembourg, Tech. Rep. 2017/511, 2017.

[42] M. S. Zouheir Labbi, A. Maarof, and M. Belkasmi, "Lightweight cryptographic for securing constrained resource IoT devices," *Int. J. Innov. Technol. Exploring Eng.*, vol. 9, p. 8, Feb. 2020.

[43] O. Khomlyak, *An Investigation of Lightweight Cryptography and Using the Key Derivation Function for a Hybrid Scheme for Security in IoT*. Karlskrona, Sweden: Blekinge Institute of Technology, 2017.

[44] K. McKay, L. Bassham, M. Sönmez Turan, and N. Mouha, *Report on Lightweight Cryptography*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2016.

[45] S. P. Jadhav, "Towards light weight cryptography schemes for resource constraint devices in IoT," *J. Mobile Multimedia*, vol. 15, pp. 91–110, Jan. 2020.

[46] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, "A review of lightweight block ciphers," *J. Cryptograph. Eng.*, vol. 8, no. 2, pp. 141–184, 2018.

[47] M. Kosug, M. Yasuda, and A. Satoh, "FPGA implementation of authenticated encryption algorithm minalpher," in *Proc. IEEE 4th Global Conf. Consum. Electron. (GCCE)*, Oct. 2015, pp. 572–576.

[48] T. Kußmaul, J. Löffler, and A. Wiesmaier, "Block ciphers PRESENT and SEA in comparison," Technische Univ. Darmstadt, Darmstadt, Germany, Tech. Rep. TUD-CS-2016-14739, 2015.

[49] B. J. Mohd, T. Hayajneh, Z. A. Khalaf, and K. M. Ahmad Yousef, "Modeling and optimization of the lightweight HIGHT block cipher design with FPGA implementation," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 2200–2216, Sep. 2016.

[50] J. Choi and Y. Kim, "An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system," in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA)*, Dec. 2016, pp. 1–4.

[51] J. Hosseinzadeh and A. G. Bafghi, "Evaluation of lightweight block ciphers in hardware implementation: A comprehensive survey," 2017, *arXiv:1706.03878*. [Online]. Available: http://arxiv.org/abs/1706.03878

[52] K. Jeong, H. Kang, C. Lee, J. Sung, S. Hong, and J. I. Lim, "Weakness of lightweight block ciphers mCrypton and LED against biclique cryptanalysis," *Peer-to-Peer Netw. Appl.*, vol. 8, no. 4, pp. 716–732, Jul. 2015.

[53] S. Wang, Q. Cui, X. Gao, L. Zhang, and X. Duan, "Differential power analysis attack and countermeasures on MCrypton," in *Proc. IEEE Adv. Inf. Manage., Communicates, Electron. Autom. Control Conf. (IMCEC)*, Oct. 2016, pp. 167–172.

[54] S. F. Abdul-Latip, M. R. Reyhanitabar, W. Susilo, and J. Seberry, "On the security of NOEKEON against side channel cube attacks," in *Proc. Int. Conf. Inf. Secur. Pract. Exper.*, May 2010, pp. 45–55.

[55] S. B. Sinaga, "Message security using criptography noekeon algorithm," Academia, San Francisco, CA, USA, Tech. Rep., 2018, doi: 10.13140/RG.2.2.27168.28165.

[56] D. Sehrawat and N. S. Gill, "Lightweight block ciphers for IoT based applications: A review," *Int. J. Appl. Eng. Res.*, vol. 13, no. 5, pp. 2258–2270, 2018.

[57] Z. Gong, S. Nikova, and Y. W. Law, "KLEIN: A new family of lightweight block ciphers," in *Int. Workshop Radio Freq. Identification: Secur. Privacy Issues*, vol. 2011, pp. 1–18.

[58] V. Lallemand and M. Naya-Plasencia, "Cryptanalysis of KLEIN," in *Proc. Int. Workshop Fast Softw. Encryption*, 2014, pp. 451–470.

[59] L. Zhou, C. Su, Y. Wen, W. Li, and Z. Gong, "Towards practical white-box lightweight block cipher implementations for IoTs," *Future Gener. Comput. Syst.*, vol. 86, pp. 507–514, Sep. 2018.

[60] H. Jiang, M. Fujishiro, H. Kodera, M. Yanagisawa, and N. Togawa, "Scan-based side-channel attack on the camellia block cipher using scan signatures," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. E98.A, no. 12, pp. 2547–2555, 2015.

[61] L. Li, K. Jia, X. Wang, and X. Dong, "Meet-in-the-middle technique for truncated differential and its applications to CLEFIA and camellia," in *Proc. Int. Workshop Fast Softw. Encryption*, Mar. 2015, pp. 48–70.

[62] Z. Liu, D. Gu, B. Sun, Q. Wang, and K. Varici, "Improved zero-correlation linear cryptanalysis of reduced-round camellia under weak keys," *IET Inf. Secur.*, vol. 10, no. 2, pp. 95–103, Mar. 2016.

[63] R. Rahim, D. Adyaraka, S. Sallu, E. Sarimanah, M. M. Rahman, N. L. Chusna, and N. Kurniasih, "Tiny encryption algorithm and pixel value differencing for enhancement security message," *Int. J. Eng. Technol*, vol. 7, nos. 2–9, pp. 82–85, 2018.

[64] R. Anusha and V. V. D. Shastrimath, "LCBC-XTEA: High throughput lightweight cryptographic block cipher model for low-cost RFID systems," in *Proc. Comput. Sci. Line Conf.*, 2019, pp. 185–196.

[65] D. Diakoulaki, G. Mavrotas, and L. Papayannakis, "Determining objective weights in multiple criteria problems: The critic method," *Comput. Oper. Res.*, vol. 22, no. 7, pp. 763–770, Aug. 1995.

[66] A. Tuş and E. Aytaç Adalı, "The new combination with CRITIC and WASPAS methods for the time and attendance software selection problem," *Opsearch*, vol. 56, no. 2, pp. 528–538, Jun. 2019.

[67] M. Vujicic, M. Papic, and M. Blagojevic, "Comparative analysis of objective techniques for criteria weighing in two MCDM methods on example of an air conditioner selection," *Tehnika*, vol. 72, no. 3, pp. 422–429, 2017.

[68] E. A. Adalı and A. T. Işık, "CRITIC and MAUT methods for the contract manufacturer selection problem," *Eur. J. Multidisciplinary Stud.*, vol. 2, pp. 93–101, 2017.

[69] R. A. Krohling and A. G. C. Pacheco, "A-TOPSIS—An approach based on TOPSIS for ranking evolutionary algorithms," *Procedia Comput. Sci.*, vol. 55, pp. 308–317, Jan. 2015.

[70] P. Wang, B. Li, H. Shi, Y. Shen, and D. Wang, "Revisiting anonymous two-factor authentication schemes for IoT-enabled devices in cloud computing environments," *Secur. Commun. Netw.*, vol. 2019, pp. 1–13, May 2019.

[71] E. Roszkowska, "Multi-criteria decision making models by applying the TOPSIS method to crisp and interval data," *Multiple Criteria Decis. Making/Univ. Econ. Katowice*, vol. 6, no. 6, pp. 200–230, 2011.