Computers, Materials & Continua
DOI:10.32604/cmc.2022.019442
Article

Tech Science Press

Optimal Confidential Mechanisms in Smart City Healthcare

R. Gopi[1,*], P. Muthusamy[2], P. Suresh[3], C. G. Gabriel Santhosh Kumar[4], Irina V. Pustokhina[5], Denis A. Pustokhin[6] and K. Shankar[7]

[1]Department of Computing Science and Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, 621212, India
[2]School of Computing Science and Engineering, Galgotias University, NCR, Delhi, 203201, India
[3]Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore, 641407, India
[4]Department of Electrical and Electronics Engineering, K. Ramakrishnan College of Engineering, Tiruchirappalli, 621112, India
[5]Department of Entrepreneurship and Logistics, Plekhanov Russian University of Economics, Moscow, 117997, Russia
[6]Department of Logistics, State University of Management, Moscow, 109542, Russia
[7]Department of Computer Applications, Alagappa University, Karaikudi, 630001, India
[*]Corresponding Author: R. Gopi. Email: gopircse@gmail.com

Received: 13 April 2021; Accepted: 27 June 2021

Abstract: Smart City Healthcare (SHC^2) system is applied in monitoring the patient at home while it is also expected to react to their needs in a timely manner. The system also concedes the freedom of a patient. IoT is a part of this system and it helps in providing care to the patients. IoT-based healthcare devices are trustworthy since it almost certainly recognizes the potential intensifications at very early stage and alerts the patients and medical experts to such an extent that they are provided with immediate care. Existing methodologies exhibit few shortcomings in terms of computational complexity, cost and data security. Hence, the current research article examines SHC^2 security through Light Weight Cipher (LWC) with Optimal S-Box model in PRESENT cipher. This procedure aims at changing the sub bytes in which a single function is connected with several bytes' information to upgrade the security level through Swam optimization. The key contribution of this research article is the development of a secure healthcare model for smart city using SHC^2 security via LWC and Optimal S-Box models. The study used a nonlinear layer and single 4-bit S box for round configuration after verifying SHC^2 information, constrained by Mutual Authentication (MA). The security challenges, in healthcare information systems, emphasize the need for a methodology that immovably concretes the establishments. The methodology should act practically, be an effective healthcare framework that depends on solidarity and adapts to the developing threats. Healthcare service providers integrated the IoT applications and medical services to offer individuals, a seamless technology-supported healthcare service. The proposed SHC^2 was implemented to demonstrate its security levels in terms of time and access policies. The model was tested under different parameters such as encryption time, decryption time, access time and response time in minimum range. Then, the level of the model and throughput were analyzed by maximum value i.e., 50 Mbps/sec and 95.56% for PRESENT-Authorization cipher to achieve smart city security. The proposed model achieved better results than the existing methodologies.

Keywords: Smart city; healthcare; security; block cipher; LWC

1 Introduction

Smart urban areas are important for a number of players in the society. The advantages and challenges, associated with the incorporation of smart cities, have drawn critical consideration from different players in multiple aspects. A number of analysts poses an important question about the components involved in smart city development such as Internet of Things (IoT), Information Systems (IS), standard software engineering and designing controls [1]. At this point, various urban communities have started embracing the idea of smart urban areas. There are four zones dictated by Amsterdam, around the idea of manageability, such as the incorporation of mobility, working, open space, and living [2]. Healthcare (HC) IoT supports the patient commitment and service fulfillment by enabling the healthcare providers to invest more energy on doctors associated with them [3–5]. In healthcare domain, a combination of detection devices and consumer hardware innovation remains a valuable application since it helps in monitoring a patient's health [6]. These applications encompass assistive conditions that do not require any communication devices or wearables for the consumer. But, they can still overcome the potential difficulties of monitoring different remotely-located individuals [7]. The most significant challenge, faced by developing as well as developed nations, is the utilization of remote healthcare facilities. This may decrease a large portion of the administration of chronic diseases and likely to improve the satisfaction of old age people [8,9]. Incorporation of remote sensor networks, in healthcare systems, is a developing field for logical examination. Present day healthcare systems require real-time monitoring of patients in terms of vital status with less communication between specialists and the patients [10]. Powerful as well as strong cryptographic techniques are crucial to develop a safety-driven application. Because, the remote sensor systems for Smart Cities Health care (SC-HC) are prone to cyberattacks that target highly confidential information of the patients such as their personal and physiological details [11]. Various stakeholders should be involved in upgrading the infrastructure security required for a remote healthcare service. Healthcare information is reliable, whereas the exchange of information over local network and wireless networks/cloud through internet to server should be secured [12,13].

The key contribution of this research article is the development of a novel light weight cryptographic technique i.e., PRESENT cipher with S-Box optimization model. Smart city healthcare information is encrypted and decrypted for security purposes. S-box utilizes a similar S-box during every round. This is primarily required or else the dynamic S-Box gets changed in the round of S-box itself, as it relies on key and number of rounds. Dynamic as well as ward key calculation are performed to build the cryptographic quality of security level. To optimize the number of slaps, maximum throughput is achieved in data security and minimum execution time. These reasons made swarm optimization, a preferable method for the current study. Strict Avalanche Criteria is a cryptographic capacity that fulfills the above condition. The major contributions of this work are summarized herewith.

- A secure healthcare model is proposed for smart city with the help of SHC^2 security via LWC and optimal S-Box model

- Salp Swarm Optimization (SWO) algorithm is used for effective optimization of S-Box
- Entire system is privacy-protected with secure data storage for every patient

Rest of the paper is organized as follows. Section 2 analyzes the works related to current topic. Section 3 explains the proposed methodology whereas section analyzes the model and the results are discussed in detail. Finally, the paper is concluded in Section 5.

2 Review of Recent Articles

People inhabiting the smart urban areas utilize information technology innovations to improve their living conditions. Smart urban areas bring personal satisfaction for its natives, native economy, easy and affordable green transportation, living conditions, and cooperation with government. Ismagilova et al. [14] mentioned that the smart urban communities are becoming a reality in today's life, thanks to ever-changing information communication technologies that transform the traditional urban communities into smart urban areas. IoT makes these smart urban areas, effective and responsive. Ghani et al. [15] mentioned that the medical technologists can go ahead to develop a new healthcare industry in such smart urban areas since it is easy for them due to the prevalence of conventional types of mechanical developments in previous times.

Smart healthcare, within smart urban areas, introduces a concept of optoelectronic controller chip. This concept intends to control the micro Light-Emitting Diode (LED) framework utilized in retinal prosthesis. It also includes a separately-addressable low power, small and micro LED cluster, while its outcomes are exemplary. A wireless sensor system is utilized in collecting the medical information, for example, vital signs and a patient's individual information, which are then transmitted to the cloud server. Hence, Alami et al. [16] mentioned that such crucial and personal information of the individuals, especially medical data, should be handled with utmost privacy. Information security enables restricted access to data, while it has provisions for permitted individuals to have free and simple access to information beyond the security measures. Since the medical information of individuals is sensitive in nature, it becomes inevitable for healthcare service providers to maintain a strong and dependable data security administration in place. The methodologies should be well ahead of, in terms of responding to queries raised by medical fraternity, securing the social insurance information, predicting the requirements and preventing any form of cyberattacks by hackers.

In spite of the developments achieved so far, the penetration of IoT is low in healthcare applications. There are potential applications that can incorporate IoT such as patient monitoring, resource detectability, and medication organization systems, as opined by Sanchez et al. [17]. Rani et al. [18] devised a Lightweight SIMON block cipher to protect the healthcare information with the help of IoT sensor system. The clients in IoHT are selected through metaheuristic algorithm called Hybrid Teaching and Learning Based Optimization (HTLBO). In this case, the current set of healthcare service providers provide full access to medical services to IoT-integrated individuals.

Secure Healthcare Model (SHM) was proposed by Parah et al. [6] for smart cities. The communication of medical data and safety & privacy concerns regarding the patient's data are crucial parameters in smart healthcare models. It is pertinent to contain a secure, effective and accessible healthcare system for a smart city. In smart city ecosystem, secure and privacy-preserved smart medical system is important with different elements of technology-enabled healthcare services. A privacy-preserved, secure and mutually-authenticated key agreement protocol was proposed by Khatoon et al. [19] to provide healthcare in smart city environment. Telecare and telemedicine are the two factors that drive the adoption of smart homes. For the past two decades, Telecare Medicine Information System (TMIS) has drawn global attention. Multidisciplinary application and research with TMIS include smart technologies, artificial intelligence, bio-sensing, telecommunications and information processing.

After reviewing the literature, few research gaps were found which are discussed herewith. The studies conducted earlier proposed the methods that primarily lag behind in performance due to poor data security, worst privacy preservation, high computational complexity, high time consumption, high costs, etc. In order to overcome these drawbacks, the current article proposes SHC^2 security via LWC with optimal S-Box model.

Purpose of Healthcare for Smart Cities (SHC^2)

The primary aim of this application i.e., Healthcare for smart cities, is to monitor the vital signs of patients remotely using sensors, devices, and equipment that can capture the required information. Smart gadgets are utilized in healthcare domain to store and predict the fluctuations in vital parameters and to deal with disease data. For most of the cases in all actuality, smart gadgets possess in-built fixed sensors [20]. Nowadays, due to the increased awareness about healthcare and wellness, various activities have been included to provide an extensive perspective on wellbeing and prosperity. The penetration of wearable IoT devices has increased among health-conscious individuals in terms of wellness tracker, wellness groups and healthcare evaluation applications in cell phones. These gadgets are simple yet highly useful in screening the vital signs that can lead to necessary medical advice and other arrangements at the right time based on requirement. An example of SHC^2 is graphically represented in Fig. 1 and this procedure share some significant terms as given herewith.

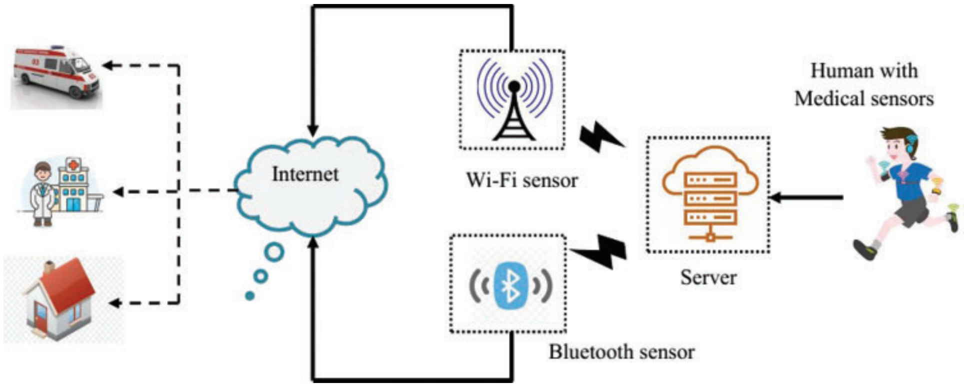

Figure 1: The healthcare system

- Mobile sensors: Dynamic sensors are increasingly applied these days, thanks to its suitability in monitoring a person's wellbeing or health without interfering his or her day-to-day activities. The sensors can measure few physiological signs/parameters through his or her actions, while a person's growth can be tracked by fixing sensors in different parts of the body [21].
- Engaging patients in health monitoring: In this scenario, old age patients with or without chronic disease can benefit in terms of treatment and medical monitoring without any need to physically meet the emergency clinic, once in a while. The specialists can focus and monitor a patient's wellbeing remotely and help her/him in case of a crisis. Further, they can constantly keep in touch with the patient for recuperation and long term care [13,22,23].

- External and internal health information: The external data is alluded to and investigated by the data collection device. By and large, the IoT framework has detection layer, vehicle layer, and the application layer. The sensors execute a significant job in identification layer. This information gets transmitted through IoT and is accessed by the customer through web application.

3 The Proposed SHC^2 Methodology

The current research work proficiently addresses the information security and client protection issues in SHC^2 by presenting Light Weight Cipher (LWC) model in cloud security. The proposed SHC^2 model is illustrated in Fig. 2. The recommended model builds both integrity and confidentiality of the HC so that a patient's information is secure and protected from unapproved client access. Majority of the components, present in this security model, depend on private and public key generation. So, the information should be encrypted and decrypted to protect and store it in cloud servers installed in smart urban areas. At first, the information is gathered from sensor system of the individuals through sensor components and the data is stored after processing.

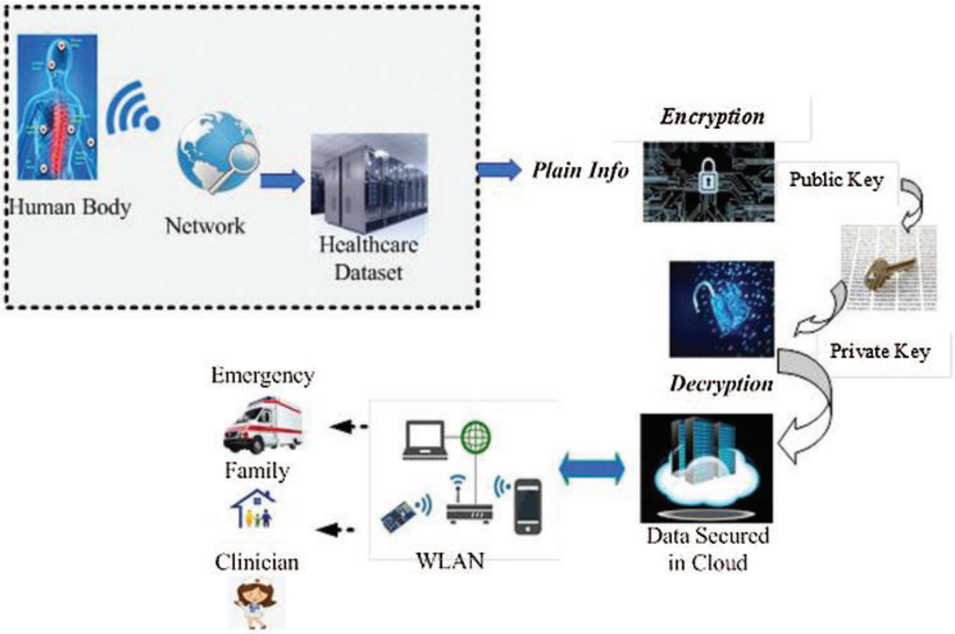

Figure 2: The proposed SHC^2 model

This information contains constant and patient-centered records and is made available to the main approved client by PRESENT cipher optimal S-Box. After the healthcare information is secured in a framework, it is then stored in cloud for authentication and approval. The proposed secure model performs cost-effective tasks and expands the viability of SHC^2, a security solution that minimizes the asset utilization and maximizes the security in healthcare information of smart urban communities.

3.1 Security Threats in the Suggested Model

Healthcare, offered in smart urban areas, is expected to face security threats through its sensors, wireless channel correspondence, and cloud condition. Healthcare systems cannot protect itself from malicious attacks and deliberate hacking attempts for monetary benefits [24]. So, securing the healthcare information is a significant task to accomplish. Various disturbing influences are exerted in security model as discussed herewith.

- Unauthorized access: There is a drastic increase in the number of threats from malware and ransomware in the recent years. These threats can duplicate the information in remote servers prior to genuine encryption execution and anticipation of the unapproved dissemination of information. A patient's information and his or her medical data is accessed without any substantial authentication. This scenario causes issues, for example, harming significant information [25,26].
- Attack on SH: Health supplier or the patients themselves control the access of records who holds all the rights to access/deny. There exists a simple way to create a patient's health records. The attackers tamper the encrypted messages between sensor nodes by duplicating it with the help of fake sequence number and captures the information from one of the two endpoints in functioning association of wireless sensors.
- Network security problem: Most of the patients' information are uploaded in the web. When health data is transferred over web, it is prone to cyberattacks. In today's world, internet has become a hub for cyber attackers regardless of the security level and how much ever secure, the health or medical information is maintained at. Specialists and healthcare professionals encourage the online access of framework with all fundamental information. However, a vast majority of the health information is prepared and affirmed by specialists or health experts.

3.2 LWC for Healthcare Security

Lightweight cryptographic technique ensures the reduction in usage cost and increases the speed, security, execution, and low energy consumption on asset-constrained gadgets. This work verifies the healthcare information in smart urban areas using PRESENT block cipher with ideal S-Box. The proposed lightweight block cipher demonstrated optimal results in SHC process. Two ciphers offer a scope of key size and width; however, at any rate, the encryption should be done for 22 rounds to achieve adequate performance. Medical health records are profoundly sensitive and must be encrypted at both capacity and during transmission. So, the clients cannot access the information without the correct keys [27].

3.3 S-Box Optimization by Swarm Approach

At most of the times, simple models are preferred rather than complicated ones. Being a simple one, the proposed model is also preferred for security and proficient usage. A block cipher algorithm with less size and execution is utilized in this study since it makes use of substitution and stage squares that has just 4 bits. Likewise, the key size is mildly contrasted with different algorithms of a similar kind. This feature, along with its diminished number of rounds, makes it a preferred algorithm. In S-box optimization process, the number of salps is fixed and the direction of that cipher round key is significant for SCHC model. So, the current model has been proved to enhance the outcome.

3.3.1 Swarm Optimization

Salps are grouped under the family, Salpidae [28] in animal kingdom. They possess a transparent barrel-molded body, while its tissues exceedingly look like jellyfishes. They move fundamentally alike the jellyfish, wherein the water is siphoned off through the body as an impetus to push ahead. The condition of all salps is verified in two-dimensional system called $S\text{-}Box(H)$. Normally, when there is a prey available nearby, it is engulfed by the Salps which forms the inquiry space for swarm's objective. To update the situation of a leader, the following condition is proposed:

3.3.2 Initialization

At first, the number of salps (number of S-box) should be introduced. Here, the weights of the system structure are deemed to be the initial solution. The quantity of assignments depends on the number of excess common sub term events in S-box portrayal and the function is represented in condition (1).

$$\text{Initialization} = \begin{cases} 1 \oplus \text{XY} \oplus \text{XYZ} \\ 1 \oplus \text{XY}(1 \oplus \text{Z} \end{cases} \tag{1}$$

From condition (1), the S-box term, in XYZ directions of the cipher, improves the security of healthcare information in smart urban communities. From this stage, both encryption and decryption of PRESENT are roughly equivalent to that of the physical prerequisites.

3.3.3 Condition Evaluation

This progression is significant for information security, in any place, which implies that a condition achieves the maximum throughput to secure the information. Its fitness is shown in condition (2).

$$\text{Condition} = \text{MAX}\{\text{Throughput}\} \tag{2}$$

It is given as some successful packets (maximum) received per unit time during the transmission and is straightforwardly related to each other.

3.3.4 New s-Box Solution Updating Procedure

Non-direct layer utilizes a single 4-bit S-box which is connected multiple times in parallel during every round. Normally, a food source F_s is procured as swarm's objective for the hunt space [5]. To update the situation of the leader, the conditions (3–5) are proposed:

$$\text{S-box (New)}_j^1 = \begin{cases} \text{T}_\text{j} + \text{Q}_1[(\text{H}_\text{j} - \text{L}_\text{j})\text{Q}_2 + \text{L}_\text{j}] & \text{Q}_3 \geq 0 \\ \text{T}_\text{j} - \text{Q}_1[(\text{H}_\text{j} - \text{L}_\text{j})\text{Q}_2 + \text{L}_\text{j}] & \text{Q}_3 < 0 \end{cases} \tag{3}$$

$$Q_{1\ldots3} = 2e^{(-4l/L)} \tag{4}$$

$$weight_j^i = \frac{1}{2}[w_j^i + w_j^{i-1}] \tag{5}$$

In the above Eqs. (3)–(5), T_j^1 signifies the position of first part (leader) in j^{th} cell, the position of machines in j^{th} cell is symbolized by T_i; the upper bound and lower bound are indicated by H_j and L_j; $\text{Q}_1, \text{Q}_2,$ *and* Q_3 indicate the random numbers generated in the interval of [0, 1].

Similarly, for the next level i.e., finding the weight, the coefficient Q_1 is the most critical parameter in SSO since it adjusts both exploration and exploitation as shown in Eq. (4). It should be noticed that the food source gets refreshed during optimization, since the salp chain is incredibly liable to find a superior solution by investigating and abusing the space around it [21].

3.4 Optimal S-Box in PRESENT Cipher

The real objective behind the structuring of PRESENT is simplicity in addition to security and proficient execution. A completely pipelined usage of PRESENT, with encryption stages, accomplishes a throughput of 64 bit during every clock cycle. This can be converted to encryption throughputs more than 50 G bit/s. The optimal S-box procedure is shown in Tab. 1. This substitution table is created via a table with 4 bit covers. Majority of the table contents depend on the information of a microcontroller with heavy-sized healthcare information [29].

Table 1: Optimal S-Box in PRESENT cipher

S	0	1	2	3	4	5	6	7	8	9	X	Y	Z	P	Q	R
S(T)	Z	5	6	Y	9	0	X	P	3	Q	R	8	4	7	1	2

In the upgraded security model for smart urban areas, the combinational structure can be additionally improved to arrive at a performance. An effective PRESENT cipher scientific articulation is shown in condition (6).

$$\text{Optimal S-Box PRESENT} = \begin{cases} X \oplus Y \oplus P \oplus YZ \\ X \oplus Z \oplus XY \oplus XYQ \\ 1 \oplus X \oplus Y \oplus XZ \oplus XYQ \oplus XZQ \end{cases} \tag{6}$$

In block ciphers, the round activity occurs such as securing the information by algorithm based on unpredictability of these tasks. Meanwhile, the number of rounds that are expected to cipher, tend to increase. The structure of this cipher, with round activity, is shown in Fig. 3. It abuses the high likelihood of specific events of input differences and output differences in order to find the non-arbitrary behavior and utilize its properties to recoup the secret key [6].

3.5 Security Terms of the Proposed Model

During the generation of round keys, both encryption and decryption processes are started. However, a moderate security requirement reflects the limited gain of the attacker, in place. This security model has some terms which are clarified herewith.

3.5.1 Key Generation

It is one of the most significant blocks, since it generates new keys for each round. For this particular usage, an execution of 80-bit key is given herewith.

$$K_i = K_{63}, K_{62}, K_{61}, \ldots, K_0 \tag{7}$$

Thus, the key register is rotated by 61-bit positions to the left, while four left-most bits are passed through present S-box. The round counter value is present with more bits. The main inputs of key generation are health data key “HK”, database and secret key “SK”.

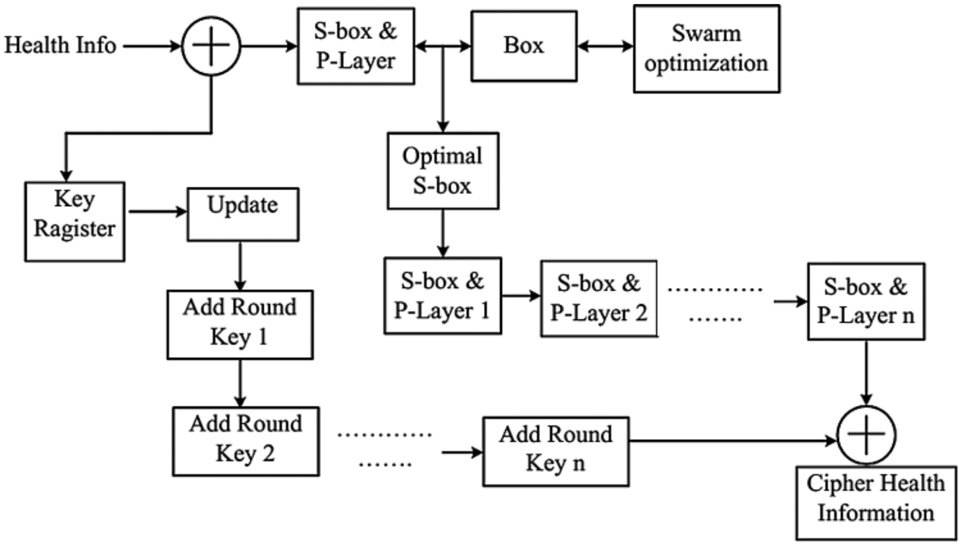

Figure 3: The structure of PRESENT cipher

3.5.2 Add Round Key

Round key activity must be performed in every essential round to cipher the information; else, it becomes critical at the top of priority list. At the time of deciphering, all key rounds must be made, until the last Ki is attained by making an opposite procedure back to the first key. The numerical expression of this model is given herewith.

$$S(SHC^2) = \sum (-1)^{(b, S(k)+(a,s)} \tag{8}$$

3.5.3 Encrypt & Decrypt

Fundamentally, the encryption algorithm is taken as optimal S-box capacity, while the public key is denoted by PK. Both characteristic information and output are health information in cipher position. Decryption denotes the process of separating the ciphered data using a private or secret key [28].

3.5.4 Server Storage

With the help of above procedure, the healthcare information is stored in a server for authentication purpose. Optimal S-BOX PRESENT is constantly kept equivalent at zero, while the worth must be equivalent to two for S-box protection from differential cryptanalysis in case of weight being equivalent to one [17].

3.6 *Authentication of Secured SC-HC*

Strong security measures ought to be ensured against any physical or distant access. The information proprietor provides the instructions to the receiver to create a private key. At that point, the service requests access the private cloud for successful authentication. Here MA (Mutual Authentication) is considered for smart urban communities' information security model [5,30].

3.6.1 Mutual Authentication

This model mediates the communication between medical clinic workers and the patients based on the information shared. The information shared among the tag, reader, and server are traded ahead of time. It produces a similar worth and look while it also checks the same to authenticate the process. The above discussed cipher-based security model confirms the server information with unapproved client [31].

3.6.2 Authorization Control

The security system must be able to appropriately authorize distinctive access rights for various clients. The access control component must be flexible enough to assaults from plotting enemies and from cloned devices. The framework should have the option to check the client and offer authorization to access. For every entrance, the system must check the validity of the client. With regards to information security, when an attacker tries to encrypt the SHRs transmitted on open channels and access SC-HC, it should be restricted.

4 Results and Analysis

The proposed SHC^2 approach was implemented in JAVA programming language JDK 1.7.0 using a PC with windows configuration and Intel (R) Core i5 processor, 1.6 GHz and 4 GB RAM. To evaluate the model, some of the metrics such as encryption, decryption, response, and access time in terms of (ms) were compared against existing cipher methods, for instance, SIMON [18].

Tab. 2 depicts the confusion and diffusion levels (in %) in the form "mean±variance". The proposed model was validated in terms of protecting the healthcare information. The gathered information was changed to packets so that it can be transmitted to sensors. The proposed ideal S-Box with PRESENT cipher achieved the least encryption and decryption times in smart urban areas as indicated in Fig. 4. This examination is dependent on access arrangement *vs.* healthcare information time. For instance, in case of access policy being 60, the time taken for encryption and decryption were 300 ms and 1874 ms by the proposed model against the existing model i.e., SIMON with TLBO model. The proposed security model also took less encryption time for information encryption than alarm-net, thanks to the usage of external keys. SHC^2 required high number of cycles to produce arbitrary keys than the proposed methodology. Fig. 5 shows the access time.

Table 2: Confusion and diffusion levels (in %), written in the form **"**mean ± variance"

Cryptosystem (key size/block size)	Confusion level	Diffusion level
LBlock (80/64)	50.1510 ± 0.0038	0.9448 ± 0.0002
KLEIN (64/64)	50.2531 ± 0.0072	1.0281 ± 0.0001
LILLIPUT (80/64)	49.9990 ± 0.0069	0.9677 ± 0.0001
PRESENT (80/64)	50.5125 ± 0.0078	0.9833 ± 0.0002
IPRESENT (80/64)	49.9729 ± 0.0048	50.1719 ± 0.0076

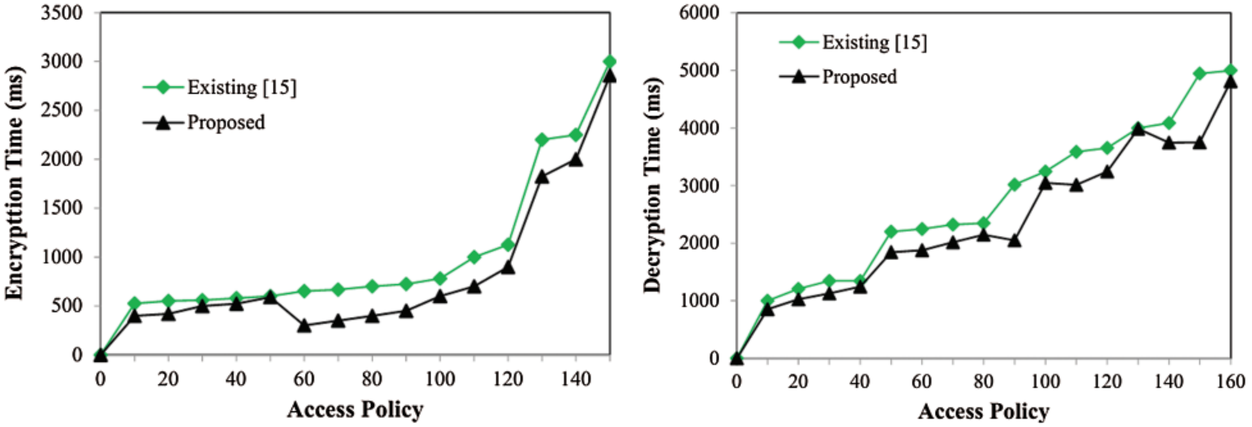

Figure 4: Encryption and decryption time evaluation

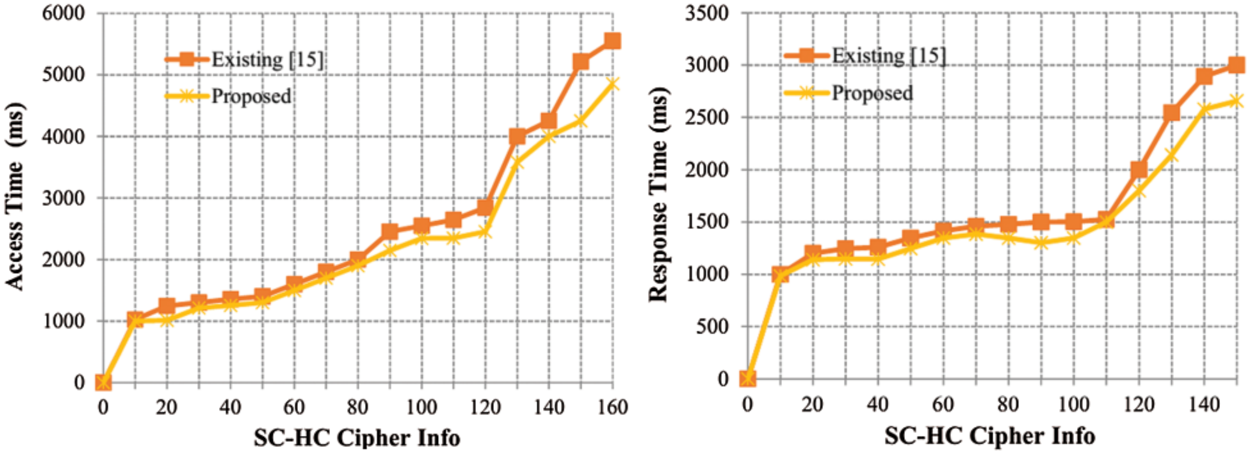

Figure 5: Response and access time evaluation

Fig. 6 shows the objective analysis of optimization in which the number of cycles got shifted and the most extreme throughput was 50 Mbps/sec for 120 age of swarm optimization process. This figure was plotted against time period. As shown in the graph, the throughput got expanded bit-by-bit after some time and achieved a stature of 30 Mbps/sec. The area throughput was higher, when the density of sensor nodes was heavier. When using a contention-based protocol, the thickness of the nods influenced the capacity of the protocol fundamentally to evade the packet collisions. The communication channel might be wired or wireless based on the application. In wireless sensor systems, the throughput initially increases to a specific value. Towards the end, the level of the proposed framework was assessed with the help of reference chart. Here, three kinds of security models were referred such as SIMON, PRESENT and the PRESENT with ideal authentication process. The maximum security level was accomplished in the proposed model than the existing techniques. Information size got expanded in case of diminishing degree of system. This implies that in case of high information size, some disturbances may be present. From the experimentation procedure, it is established that the proposed strategy is effective in securing the healthcare information of smart urban communities with 98.22% accuracy. Fig. 7 shows the level of security. The former differs with the quantity of SHC^2 ciphertexts. The reaction time was 1345 ms for ideal PRESENT cipher and 2348 ms was the access time taken by 40 cipher information in ideal S-Box.

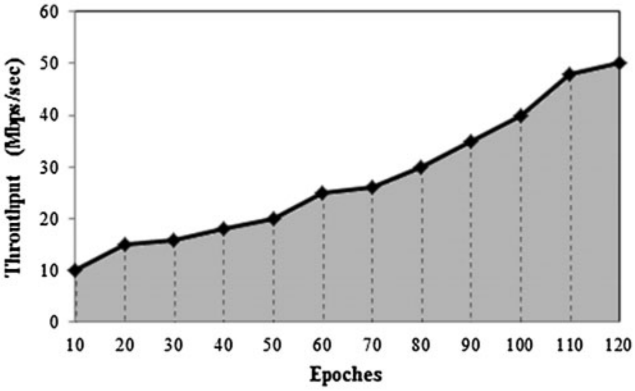

Figure 6: Throughput *vs.* epoch

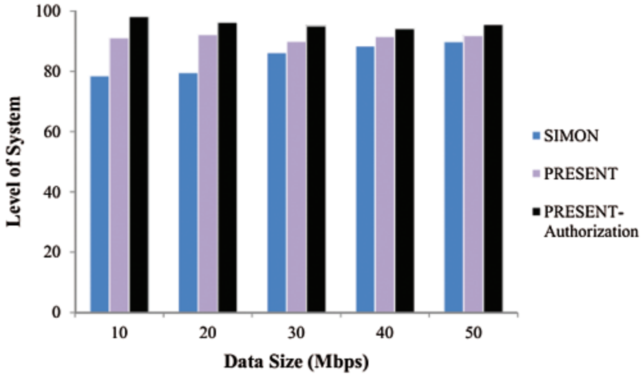

Figure 7: Level of security in SHC^2

5 Conclusion

In this research article, the authors discussed about the security of SHC^2 model with the help of optimal S-Box ciphers. In healthcare domain, data protection and privacy of the information are crucial. Access to data, authentication, approval, availability, and responsibility for information are important, because of the application of data and security of an individual's information. The proposed model proved to have improved the security level of healthcare information in sensor networks through system measurements. It reduced the security and resource consumption requirements progressively, during emergency situations. Further, the proposed model also mitigated the costs incurred upon healthcare solutions. Additionally, it also ensured the protected transmission of medical information between patients and the doctors. The PRESENT Cipher performed key scheduling for which two distinctive estimated keys such as 80 and 128 bit keys were chosen and designed. At that point, the proposed model was compared with other cryptographic algorithms to improve the security of hybrid algorithm for more information. The proposed system reduced the heavy computational cost. In future, the researchers recommend to use effective deep learning models to achieve better results. Besides, the block ciphers can also be used in enhancing the security level of healthcare information.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren *et al.*, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 122–129, 2017.

[2] S. Oueida, M. Aloqaily and S. Ionescu, "A smart healthcare reward model for resource allocation in a smart city," *Multimedia Tools and Applications*, vol. 78, pp. 24573–24594, 2019.

[3] Z. O. Omogbadegun, "Security in healthcare information systems," in *2006 ITI 4th Int. Conf. on Information & Communications Technology*, IEEE, Cairo, Egypt, pp. 1–2, 2006.

[4] A. Onasanya, S. Lakkis and M. Elshakankiri, "Implementing IoT/WSN based smart Saskatchewan healthcare system," *Wireless Networks*, vol. 25, pp. 3999–4020, 2019.

[5] A. A. A. E. Latif, B. A. E. Atty, M. S. Hossain, S. Elmougy and A. Ghoneim, "Secure quantum steganography protocol for fog cloud internet of things," *IEEE Access*, vol. 6, pp. 10332–10340, 2018.

[6] S. A. Parah, J. A. Sheikh, J. A. Akhoon and N. A. Loan, "Electronic health record hiding in images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," *Future Generation Computer Systems*, vol. 108, pp. 935–949, 2020.

[7] M. A. Ameen, J. Liu and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.

[8] K. Shankar, M. Ilayaraja and K. S. Kumar, "Technological solutions for health care protection and services through internet of things (IoT)," *International Journal of Pure and Applied Mathematics*, vol. 118, no. 7, pp. 277–283, 2018.

[9] Z. Chen, W. Fan, Z. Xiong, P. Zhang and L. Luo, "Visual data security and management for smart cities," *Frontiers of Computer Science in China*, vol. 4, no. 3, pp. 386–393, 2010.

[10] S. S. M. Aldabbagh and I. F. T. A. Shaikhli, "Security of PRESENT S-box," in *2012 Int. Conf. on Advanced Computer Science Applications and Technologies*, IEEE, Kuala Lumpur, Malaysia, pp. 219–222, 2012.

[11] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Int. Workshop on Cryptographic Hardware and Embedded Systems. Proc.: Lecture Notes in Computer Science Book Series (LNCS, Volume 4727)*, New York City, NY, USA, pp. 450–466, 2007.

[12] N. Kothawade, A. Biradar, K. Kodmelwar, K. P. Tambe and V. Deshpande, "Performance analysis of wireless sensor network by varying reporting rate," *Indian Journal of Science and Technology*, vol. 9, no. 26, pp. 1–6, 2016.

[13] M. Elhoseny and K. Shankar, "Optimal bilateral filter and convolutional neural network based denoising method of medical image measurements," *Measurement*, vol. 143, pp. 125–135, 2019.

[14] E. Ismagilova, L. Hughes, Y. K. Dwivedi and K. R. Raman, "Smart cities: Advances in research—An information systems perspective," *International Journal of Information Management*, vol. 47, pp. 88–100, 2019.

[15] A. Ghani, "Healthcare electronics—A step closer to future smart cities," *ICT Express*, vol. 5, no. 4, pp. 256–260, 2019.

[16] A. Alami, L. Benhlima and S. Bah, "A study of security requirements in smart home healthcare systems using wireless sensor networks," in *Third Int. Conf. on Smart City Applications SCA 2018. Proc.: Lecture Notes in Intelligent Transportation and Infrastructure Book Series (LNITI)*, Springer, Cham, pp. 645–655, 2018.

[17] P. P. Sanchez, N. Bagheri, P. P. Lopez and J. E. Tapiador, "Two RFID standard-based security protocols for healthcare environments," *Journal of Medical Systems*, vol. 37, no. 5, pp. 1–12, 2013.

[18] 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 and Applications*, vol. 79, pp. 35405–35424, 2020.

[19] S. Khatoon, S. M. M. Rahman, M. Alrubaian and A. Alamri, "Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment," *IEEE Access*, vol. 7, pp. 47962–479712, 2020.

[20] K. Shankar, M. Elhoseny, S. K. Lakshmanaprabu, M. Ilayaraja, R. M. Vidhyavathi *et al.*, "Optimal feature level fusion based ANFIS classifier for brain MRI image classification," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 1, pp. e4887, 2020.

[21] M. Elhoseny, K. Shankar and J. Uthayakumar, "Intelligent diagnostic prediction and classification system for chronic kidney disease," *Scientific Reports*, vol. 9, no. 1, pp. 1–14, 2019.

[22] M. Elhoseny, G. B. Bian, S. K. Lakshmanaprabu, K. Shankar, A. K. Singh *et al.*, "Effective features to classify ovarian cancer data in internet of medical things," *Computer Networks*, vol. 159, pp. 147–156, 2019.

[23] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in internet of things," *Neural Computing and Applications*, vol. 32, pp. 10979–10993, 2020.

[24] K. Shankar, M. Elhoseny, E. D. Chelvi, S. K. Lakshmanaprabu and W. Wu, "An efficient optimal key based chaos function for medical image security," *IEEE Access*, vol. 6, pp. 77145–77154, 2018.

[25] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[26] W. Wu and L. Zhang, "LBlock: A lightweight block cipher," in *Int. Conf. on Applied Cryptography and Network Security – ACNS 2011. Proc.: Lecture Notes in Computer Science Book Series (LNCS, Volume 6715)*, New York City, NY, USA, pp. 327–344, 2011.

[27] O. Hyncica, P. Kucera, P. Honzik and P. Fiedler, "Performance evaluation of symmetric cryptography in embedded systems," in *Proc. of the 6th IEEE Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems*, Prague, Czech Republic, IEEE. vol. 1, pp. 277–282, 2011.

[28] Mirjalili, S., Gandomi, A. H., Mirjalili, S. Z., Saremi, S., Faris, H. *et al.*, "Salp swarm algorithm: A bio-inspired optimizer for engineering design problems," *Advances in Engineering Software*, vol. 114, pp. 163–191, 2017.

[29] T. P. Berger, J. Francq, M. Minier and G. Thomas, "Extended generalized feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput," *IEEE Transactions on Computers*, vol. 65, no. 7, pp. 2074–2089, 2015.

[30] N. Tsafack, J. Kengne, B. A. E. Atty, A. M. Iliyasu, K. Hirota *et al.*, "Design and implementation of a simple dynamical 4-d chaotic circuit with applications in image encryption," *Information Sciences*, vol. 515, pp. 191–217, 2020.33.

[31] Y. Zhang, D. Zheng and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.