Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

# Enhanced Lightweight and Secure Session Key Establishment Protocol for Smart Hospital Inhabitants

**Anshita Dhoot**

Department of Radio Engineering & Computer Technology, Moscow Institute of Physics & Technology, Moscow, Russia – 9 Institutskiy per., Dolgoprudny, Moscow Region, 141701, Russian Federation.E-mail: anshita.dhoot@phystech.edu

**A. N. Nazarov**

Department of Radio Engineering & Computer Technology, Moscow Institute of Physics & Technology, Moscow, Russia – 9 Institutskiy per., Dolgoprudny, Moscow Region, 141701, Russian Federation. E-mail: a.nazarov05@bk.ru

**Tayyab Khan**

School of Computer and Systems Sciences, JNU, New Delhi- 110067, India. E-mail: tayyabkhan.cse2012@gmail.com

## Abstract

In the era of internet technologies, to provide wireless communication and transfer the information in seconds from one place to another has arrived because of the need to consume information technologies. All users desire to quickly access the smart world's life and interact with the entire world socially. This paper proposed an environment for the safe and secure smart patient's room connected to the WSN, BAN, and RFID. All the data will be transferred to the session key, secure and contains the patient's information. The network connected through WSN and data will be sent through the session key to make an smart hospital's patient cabin. The small token is there that will be transferred throughout the network to get authenticated by each network. This proposed scheme is secure enough to overcome the drawbacks of the other protocol in such a way as to make the protocol more secure from the entire adversary's attack may occur.

**Keywords:** Session Key, Cryptanalysis, Smart Hospital Environment, WSN (Wireless Sensor Network), BAN (Body Area Network)

DOI: https://doi.org/10.22059/jitm.2022.86733 Manuscript Type: Research Paper University of Tehran, Faculty of Management

Received: December 12, 2020 Accepted: March 10, 2021

## Introduction

Everywhere in the world, our surrounding concerns for health care issues. Most of them have already solved, but there will be some or more issues that need to be solved. The medical science field considers a lot of significant concerns for the health and patient's security. If there are any data or information that contains a single crucial data that cannot be supposed to get leaked, it should be secure enough that no intruder can get that information. The major problem that has tried to solve through this paper is to secure the environment from such attacks, damaging the data or information. The previous protocol was not good enough to support those attacks concerned by this new protocol. Many loops have been detected and preserved from more attacks. Section III explains the entire attacks, which can destroy the existing protocol's environment and ruin the concept of the session key installation. The designed protocol can easily resist insider attacks, offline and online password guessing attacks, brute force attack, stolen smart card attack, foreign impersonation attack, user impersonation attack, forward secrecy key, compromised key and all the attacks of previous protocol too. These attacks cannot resist the previous protocol. This paper has contributed to resisting the environment from these attacks, which can be attacked able to the environment and make the data insecure. The session key establishment protocol has been already a better protocol than those protocols which exist before the SKE. Even though the SKE protocol is good enough to resist more attacks than previous protocols, this newly designed protocol has compared with this SKE protocol that ensures the existing protocol secure the environment from previous protocols.

The previous protocol has adopted the session key establishment protocol is unsafe from some attacks (Seshadri et al., 2011). This protocol emanates a secured environment that resists a few more attacks using the hash functions, encryption, and decryption technologies. Cryptographically representation of the session key helps to secure each variable that may traverse during authentication. In the case of enhancing the security to get the system vulnerable was the protocol's prior work. Internet of things, WSN, Internet of Things, sensor networking, and BAN become essential things to secure the environment (Jara et al., 2012). Even though all are becoming an important part of mundane life, as much as usages of them are increasing. Accordingly, security ought to be at its height. Confidentiality has become more critical to secure the system (Aghili et al., 2019). This paper has been systemized in this manner that Section II explains the methodology used in this paper. This section also explains the work done till yet in this area and the entire limitations or weaknesses this protocol may occur. In section III introduces the design of the system and its property to make the security system. Section IV compares the existing and proposed method, which will follow the next section, i.e. Section V, which describes analytic methods proposed by this scheme. Then Section VI concludes the paper at its end.

Many papers (Jalal et al., 2014) are there which have predicted to create a smart hospital environment have their advantages as well as disadvantages. As we have gone through the SKE by adding some new constraint in the above protocol, the EASH can apply to healthcare issues. It is becoming a big concern to look after for some severe cases that come to the hospital, as discussed in the literature in (He et al., 2016) proposed an anonymous wireless body area network that isthe anonymous verification process. By modifying this system and proposed a system that is reliable enough with complete update protocol. If people will see the world medical sciences and its services has been increasing rapidly. Wireless networking, even electronics with computer science technologies, has been increased and increasing day by day. Wireless Sensor Network, i.e. WSN, plays a massive role in many software by giving various kinds of several changes. The health care system includes WSN and BAN for communication, even power computation techniques (Al Ameen et al., 2012). World changes and update every year, every month, several information & technologies. Its speedy growth needs to make better security. The smart hospital environment tends to be capable of enhancing its smartness that converted into an innovative hospital. It includes WSN connectivity. Comfort increases by decreasing the operation's cost and ensures its people's security to design the protocol (Almulhim et al., 2018).

The concept behind the smart hospital is capacious. It enables the hospital light system under control. Its appliances with safety and security are important to being control. The people who live in this environment are helpless enough to do their work and ordinary things themselves. Several types of research are undergoing such concepts related to older people and help them look after them to survive their basic needs (Gomez et al., 2010). It is helpful if this scheme uses a lightweight session key. We can establish this scheme to secure the environment. This paper needs legal access as well as takes care of the concern related to access security legally. There is a Silicon identity that helps to create a safe environment by using the cryptography method (Attkan et al., 2020) to exchange the information in between the Home Gateway (HG) as well as Service Devices (SD). It uses a symmetric key method within HG and SD to implement a hospital environment that helps it secure enough from other attacks and make it smart. It is also secure enough over the Dolev-Yao attack model. Its confidentiality takes place to make the system efficiency as well as enhance its performance (Mantas et al., 2011) (Kim et al., 2017).

(Minaie et al., 2013) discussed those issues related to the concept of WSN by implementing this onto the health care system. It has been divided into three categories: clinical settings to monitor patient's health, monitoring as a care centre for older adults, and collecting the long-term clinical databases for the data. It has ended up with issues related to its security and privacy issue's improvement. (Nayak et al., 2013) introduced healthcare applications. It includes that any patient watchable by tracking their records through Wireless Medical Sensor Networks, i.e. WMSNs. It requires enhancing functionality, protocol, technology, as well as the allocation of the network channel. (Balakrishna et al., 2013) discussed the health of older people. In this, we

can monitor any patient's health by using the WSN and BAN. Several health parameters can transmit by capturing the data through handheld devices by the health care providers or any physicians. It includes a wearable health unit that can easily track the patient's record. It also needed security and authentication services to keep the data safe as well as secure. (Kim et al., 2014) discussed the security and privacy threats related to the RFID Authentication protocol that has been extensively studied its embedding in the healthcare system. Security services are not enough, so it will require developing ultra-lightweight primitives of cryptographic. (Pandesswaran et al., 2016) described the monitoring system, which has been base on the WSN. It deals with the medical and hospital assistance centre: wireless network and other existing infrastructure related to any healthcare. In the recent decade, many researchers contributed to making an advanced hospital system to improve patients' health by using various other IoT techniques. Lightweight session key establishment for security purpose, providing higher security with minor damage, yet restricted to many other things. Security over attacks, networks, security, authentication, and many more things have secured in a vast range. Many scientists do these works, and more researchers are exploring this area (Han et al., 2013), (Gubbi et al., 2013). According to the previous work done before this proposed protocol, Enhanced Authentication Smart Healthcare (EASH) protocol can secure the patient data at a higher level. The existing model of Enhanced Lightweight and Secure Session Key Establishment Protocol for Smart Hospital Inhabitants can secure around ten attacks, but this proposed protocol can provide security to the system from seventeen attacks.

## Materials and Methods

This phase's objective is to provide service for $HoG$and Device A. SP sends the parameter to the HoG and Device A to authenticate the gateway identity. It contains three entities HG, SP and Device A, shows in Figure 1. It contains three entities $HoG$, SP and Device A, shows in Figure 5.2.

Phase I: Registration Phase

- SP helps to assign the terms $GW_{id}$, $tok_A$, $r_n$, $KI_A$, $id_A$ and also computes $Q_A=h(tok_A||GW_{id}||S_{id})$ & $h(K) = K'_A$. After this, SP will transfer its data in Device A and HoG to easily access the data by authenticating a user.
- Device A receives the data from the SP and stores them in its storage memory. The data $id_A$, $tok_A$, and K receive from the SP and $S_{id}$ is already stored into Device A such that it is having the information so the valid user can access its data through this $S_{id}$.

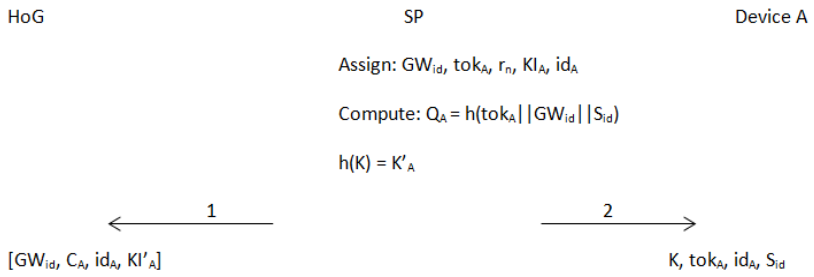


Figure 1. Registration Setup Phase (EASH Protocol)

- In the HoG, it receives data from the SP are $GW_{id}$, $C_A$, $id_A$, $KI'_A$ and store these into its storage memory of database so that it becomes easy to communicate all the valid data to access.

Phase II: Authentication Phase

It contains five sessions for data and message transaction that lies while accessing the HG, Figure 2. As HoG has [$GW_{id}$, $C_A$, ($id_A$, $KI'_A$), $NF_i$] on the other side Device, A has [K, $id_A$, $tok_A$, $S_{id}$] that was stored in HoG and Device A by Phase I.

- In session one (Session 1), it generates $r_n$ (random entity) and computes $S_1$ and $S_2$, where $S_1$ has encrypted in the form of $E_{CA}[GW_{id}, r_n, T_1]$, and $S_2$ has the value that contains hash function $h(S_1||r_n||C_A||T_1||KI'_A)$. After this generation and computation process session1 sends the message to session 2, where the message contains $GW_{id}$, $S_1$, $S_2$, and $T_1$.
- In session two (Session 2), it checks first $T_2$-$T_1 \leq \Delta T$ (here T defines the current time of that instant) to protect the protocol from the replay attack that may occur due to the time variation. Compute $KI'_A = h(K)$ makes the $K_{id}$'s safe and prevents this from insider attack. Then compute $C_A=h(tok_A||GW_{id}||S_{id}||KI'_A)$. It will proceed by decrypting the message $S_1$ with $C_A$to easily get GWid, rn, T1, which will prevent the protocol from the brute force attack such that the adversary will not get $C_A$. All this follow by the computation of $S_2^* = h(S_1^*||r_n^*||C_A||T_1||KI'_A)$ and then verifies $S_2^*$=? $S_2$. By verifying this, then generate $s_n$,which is another random secret number that will follow the computation of $S_3$ that encrypts $E_{KI'A}[id_A, s_n, r_n]$. $S_4$ contains HMAC function that has $HMAC\{C_A, id_A||GW_{id}||s_n||T_3\}$. By preventing S1 and CA by encrypting these, this protocol prevents the offline guessing attack. Now, the message will send session 2 to session three that contains $S_3$, $S_4$, and $T_3$.
- In session three (Session 3), again, $\Delta T$ will get a check, $S_3$ gets decrypted with $KI'_A$to get $id_A^*$, $s_n^*$ and $r_n^*$. Further, this will verify $id_A^*$ =? $id_A$ and $r_n^*$ =? $r_n$, then compute the $S_4^* = HMAC\{C_A||id_A||GW_{id}||s_n^*||T_3\}$ and then verify $S_4^* = S_4$ so that the valid data can be more secure by confirming the $S_4$ again to evaluate data's purity. Now by ting,$\sigma = h(id_A||GW_{id}||s_n||r_n||C_A)$the session key and S5 are encrypted in the form of $E'_{KIA}[\sigma, s_n, T_5]$. After this, session three will sends the message to session four that contains $S_5$ and $T_5$.
- In session four (Session 4), check $\Delta T$ then decrypt the encrypted message $S_5$ with $KI'_A$ to get $\{\sigma, s_n^*, T_5\}$ followed by verification of the $s_n^*$ =? $s_n$. Then compute $\sigma^*$ that contains a message in a terms of hash function $h(id_A||GW_{id}||s_n||r_n||C_A)$. Next, verify $\sigma^*$ =? $\sigma$, so that by verifying the ses-

sion key, we can assure the session key is valid. Then S4 sends the acknowledgement to session five (Session 5) and authenticate access by the keyword $auth\_access$.

In session six (Session 6), a notification will send to the device. Due to this, the Doctor or the user will get the notification, and then it will be able to update the feedback, as per the improvement or any loss they get. $E_\sigma(\alpha_{i)}) = \beta_i$Encrypted information will send to Device A that will decrypt the encrypted message and get $D_\sigma(\beta_i) = \alpha_i$. Then, D id can access the read notification's authority NFi$i \neq d$ and allow $read\_access$ if $i = d$ the user get the authority to modify the notification ($read\_modification\_access$). All the values of device A or HoG will get stored in the storage of the database. By the registration phase, we have added the Notification part, which describes the notification that will get updated by receiving the encrypted key that will get decrypted, only when it will receive the Doctor's id $E_\sigma(\alpha_{i)}) = \beta_i$, where $\alpha_i$ belongs to the id of the Doctor. If encrypted data do not match the authenticated user, then the system will not allow giving modification access to other members that could be relatives of patient or staff members of the hospital. $D_\sigma(\beta_i) = \alpha_i$Where $\beta_i$ is the decryption of the key which has decrypted by the authentication process, suppose this situation comes $D_\sigma(\beta_i) = \alpha_i$, after that the access to read and update will be updated on the notification only and only when $D_{id}(\alpha_i) = NF_i$.

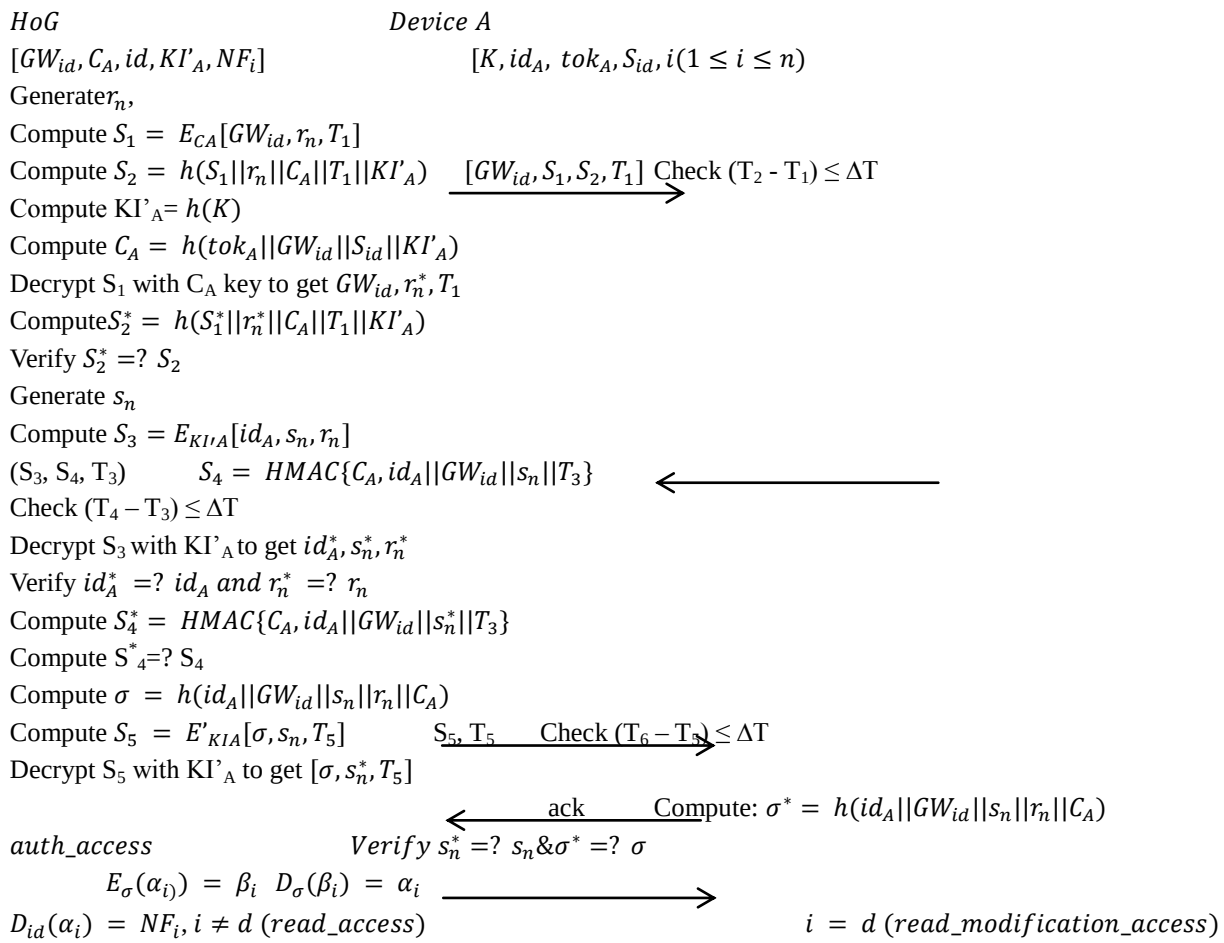


Figure 2.Authentication Phase (EASH Protocol)

## Results

This section contains the comparison between the Session Key Establishment (SKE) protocol and Enhanced Authentication Smart Healthcare (EASH) protocol and other existing protocols. The comparison will be made according to the concern about the storage capacity, communication capacity, computation cost capacity, and the attacks' security analysis. All these comparisons have shown in Table 1 - 5. Table 1 shows that the computation cost is different as well as efficient of EASH from the other protocol that exists

Table 1. Computation Cost Comparison from other Protocols

| Cryptography Method | Communication Cost | | | | |
|---|---|---|---|---|---|
| | (Almulhim et al., 2018) | (Attkan et al., 2020) | (Aghili et al., 2019) | SKE | EASH |
| Point Multiplication | - | 2t | 2t | - | - |
| Hash Operation | 5H | 4H | 4H | 2H | 6H |
| MAC | 7MAC | 1MAC | - | 1MAC | - |
| HMAC | - | - | - | 1HMAC | 2HMAC |
| Cryptosystem | 4E+4D | 1E+1D | - | 1E+1D | 4E+4D |

Table 2 shows the storage capacity that lies in SKE and EASH that how it is efficient from the other. For computing this, we have count n = 1/bit.

Table 2. Storage Capacity

| Storage Capacity | |
|---|---|
| SKE | EASH |
| Device A | Device A |
| 4bit | 4bit |

Table 3 shows the communication cost that lies found during the time of analysis within the SKE and EASH.

Table 3. Communication Cost

| Communication Cost | | |
|---|---|---|
| Communication/Bit | SKE | EASH |
| S1 | 4bit | 4bit |
| S2 | 4bit | 3bit |
| S3 | 2bit | 2bit |
| Total Bits | 10bit | 9bit |

Table 4 shows the computation cost that exists within the host of the protocol of both ends. HoG and Device A are those two hosts of the protocol.

Table 4. Computation Cost

| Cryptography Method | Computation Cost | | | | |
|---|---|---|---|---|---|
| | (Almulhim et al., 2018) | (Attkan et al., 2020) | (Aghili et al., 2019) | (Pandesswaran et al., 2016) | Proposed |
| Point Multiplication | 2t | 2t | - | - | - |
| Hash Operation | 1H | 4H | 5H | 2H | 6H |
| MAC | 1MAC | - | 7MAC | 1MAC | - |
| HMAC | - | - | - | 1HMAC | 2HMAC |
| Cryptosystem | 1E+1D | - | 4E+4D | 1E+1D | 4E+4D |

Finally, Table 5 shows the security analysis within the protocols that existed and the proposed protocol, i.e. SKE and EASH, respectively. It has found that EASH was able to resist seventeen attacks whether SKE protocol can resist seven attacks. So by concluding from this, we can say that protocol EASH are better protocols from the SKE protocol that existed before.

Table 5. Security Analysis

| Security Analysis | | |
|---|---|---|
| Attacks | SKE | EASH |
| Denial-of-Services | YES | YES |
| Eavesdropping | YES | YES |
| Insider Attack | NO | YES |
| Brute Force Attack | NO | YES |
| Offline Guessing Attack | NO | YES |
| Masquerade | YES | YES |
| Message Forgery | YES | YES |
| Message Replay Attack | YES | YES |
| Known-Key Attack | YES | YES |
| Device Compromise | YES | YES |
| Foreign Agent Impersonation Attack | NO | YES |
| User Impersonation Attack | NO | YES |
| Stolen Smart Card Attack | NO | YES |
| Online Password Guessing Attack | NO | YES |
| Adversary Attack | NO | YES |
| Forward Secrecy | NO | YES |
| Compromised Key Attack | NO | YES |

## Conclusion

Many works have done in this field, providing numerous technologies that work on the smart hospital network and security. Many entities are suitable to apply to the environment such that the surrounding can become safe and secure. The environment where patients live should be secure enough and needs to look after them. It has to be secure enough such that none information gets the leak. It is also a severe topic for discussing the security of patients. This

protocol has been proposed for lightweight as well as securing session key. It establishes in the smart hospital environment. It has analyzed formally to assure about its security, efficiency, and confidentiality is better than the existing protocol.

## Acknowledgements

Networking Lab at School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi, India, supported this research at its best. The fundamental part of this research was held at the same university.

## Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

## Funding

This research did not receive any specific grant from agencies in the public, commercial or not for profit sectors.

## References

Seshadri, A., Luk, M., & Perrig, A. (2011). SAKE: Software attestation for key establishment in sensor networks. Ad Hoc Networks, 9(6), 1059-1067.

Aghili, S. F., Mala, H., Shojafar, M., & Peris-Lopez, P. (2019). LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. future generation computer systems, 96, 410-424.

Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. Journal of medical systems, 36(1), 93-101.

Almulhim, M., & Zaman, N. (2018, February). Proposing secure and lightweight authentication scheme for IoT based E-health applications. In 2018 20th International Conference on advanced communication technology (ICACT) (pp. 481-487). IEEE.

Anunobi, C. V., & Okoye, I. B. (2008). The role of academic libraries in universal access to print and electronic resources in the developing countries. Library philosophy and practice, 5(20), 1-5.

Attkan, A., & Ahlawat, P. (2020). Lightweight two-factor authentication protocol and session key generation scheme for WSN in IoT deployment. In Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies (pp. 189-198). Springer, Singapore.

Gomez, C., & Paradells, J. (2010). Wireless home automation networks: A survey of architectures and technologies. IEEE Communications Magazine, 48(6), 92-101.

Mantas, G., Lymberopoulos, D., & Komninos, N. (2011). Security in smart home environment. In Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications (pp. 170-191). IGI global.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

Han, K., Kim, J., Shon, T., & Ko, D. (2013). A novel secure key paring protocol for RF4CE ubiquitous smart home systems. Personal and ubiquitous computing, 17(5), 945-949.

He, D., Zeadally, S., Kumar, N., & Lee, J. H. (2016). Anonymous authentication for wireless body area networks with provable security. IEEE Systems Journal, 11(4), 2590-2601.

Jalal, A., Kamal, S., & Kim, D. (2014). A depth video sensor-based life-logging human activity recognition system for elderly care in smart indoor environments. Sensors, 14(7), 11735-11759.

Jara, A. J., Zamora, M. A., & Skarmeta, A. (2012). Glowbal IP: An adaptive and transparent IPv6 integration in the Internet of Things. Mobile Information Systems, 8(3), 177-197.

Kim, J. E., Barth, T., Boulos, G., Yackovich, J., Beckel, C., & Mosse, D. (2017). Seamless integration of heterogeneous devices and access control in smart homes and its evaluation. Intelligent Buildings International, 9(1), 23-39.

Kim, J. T. (2014). Attacks and threats on the U-healthcare application with mobile agent. International Journal of Security and Its Applications, 8(4), 59-66.

Minaie, A., Sanati-Mehrizy, A., Sanati-Mehrizy, P., & Sanati-Mehrizy, R. (2013, June). Application of wireless sensor networks in health care system. In 2013 ASEE Annual Conference & Exposition (pp. 23-200).

Nayak, M., & Agrawal, N. (2013). Security in Body Sensor Networks for Healthcare applications. IOSR Journal of Computer Engineering, pg, 41-46.

Balakrishna, D., Sujeethnanda, M., & Murthy, G. R. (2013, February). Mobile Wireless Sensor Networks: Healthcare in Hospitals. In ifth International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED 2013).

Pandesswaran, C., Surender, S., & Karthik, K. V. (2016). Remote patient monitoring system based coap in wireless sensor networks. International Journal of Sensor Networks and Data Communications, 5(3).

**Bibliographic information of this paper for citing:**

Dhoot, Anshita; Nazarov, A. N. & Khan, Tayyab (2022). Enhanced Lightweight and Secure Session Key Establishment Protocol for Smart Hospital Inhabitants.*Journal of Information Technology Management*, Special Issue, 225-234.