2022

ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things

Mohammad Wazid

Jaskaran Singh

Ashok Kumar Das
Old Dominion University, adas@odu.edu

Sachin Shetty
Old Dominion University, sshetty@odu.edu

Muhammad Khurram Khan

See next page for additional authors

Original Publication Citation

Wazid, M., Singh, J., Das, A. K., Shetty, S., Khan, M. K., & Rodrigues, J. J. P. C. (2022). ASCP-IoMT: AI-enabled lightweight secure communication protocol for Internet of Medical Things. *IEEE Access*, *10*, 57990-58004. https://doi.org/10.1109/ACCESS.2022.3179418

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 7, 2022, accepted May 28, 2022, date of publication May 30, 2022, date of current version June 6, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3179418

ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things

MOHAMMAD WAZID[1], (Senior Member, IEEE), JASKARAN SINGH[1], (Student Member, IEEE), ASHOK KUMAR DAS[2,3], (Senior Member, IEEE), SACHIN SHETTY[4], (Senior Member, IEEE), MUHAMMAD KHURRAM KHAN[5], (Senior Member, IEEE), AND JOEL J. P. C. RODRIGUES[6,7], (Fellow, IEEE)

[1]Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248 002, India
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
[3]Virginia Modeling, Analysis, and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA
[4]Virginia Modeling, Analysis, and Simulation Center, Department of Computational Modeling and Simulation Engineering, Old Dominion University, Suffolk, VA 23435, USA
[5]Center of Excellence in Information Assurance, King Saud University, Riyadh 12372, Saudi Arabia
[6]College of Computer Science and Technology, China University of Petroleum (East China), Qingdao 266555, China
[7]Instituto de Telecomunicações, 6201-001 Covilhã, Portugal

Corresponding author: Mohammad Wazid (wazidkec2005@gmail.com)

This work was supported in part by the DoD Center of Excellence in AI and Machine Learning (CoE-AIML) with the U.S. Army Research Laboratory under Contract W911NF-20-2-0277, in part by the FCT/MCTES through National Funds and when Applicable Co-Funded EU Funds under Project UIDB/50008/2020, in part by the Brazilian National Council for Research and Development (CNPq) under Grant 313036/2020-9, and in part by the King Saud University, Riyadh, Saudi Arabia under Project RSP-2022/12.

ABSTRACT The Internet of Medical Things (IoMT) is a unification of smart healthcare devices, tools, and software, which connect various patients and other users to the healthcare information system through the networking technology. It further reduces unnecessary hospital visits and the burden on healthcare systems by connecting the patients to their healthcare experts (i.e., doctors) and allows secure transmission of healthcare data over an insecure channel (e.g., the Internet). Since Artificial Intelligence (AI) has a great impact on the performance and usability of an information system, it is important to include its modules in a healthcare information system, which will be very helpful for the prediction of some phenomena, such as chances of getting a heart attack and possibility of a tumor, from the collected and analysed healthcare data. To mitigate these issues, in this paper, a new AI-enabled lightweight, secure communication scheme for an IoMT environment has been designed and named as ASCP-IoMT, in short. The security analysis of ASCP-IoMT is performed in different ways, such as an informal way and a formal way (through the random oracle model). ASCP-IoMT performs better than other similar schemes and provides superior security with extra functionality features as compared those for the existing state of art solutions. A practical implementation of ASCP-IoMT is also performed in order to measure its impact on various network performance parameters. The end to end delay values of ASCP-IoMT are 0.01587, 0.07440 and 0.17097 seconds and the throughput values of ASCP-IoMT are 5.05, 10.88 and 16.41 bits per second (bps) under the different considered cases, respectively. For AI-based Big data analytics phase, the values of computation time (seconds) for decision tree, support vector machine (SVM), and logistic regression are measured as 0.19, 0.23, and 0.27, respectively. Moreover, the different values of accuracy for decision tree, SVM and logistic regression are 84.24%, 87.57%, and 85.20%, respectively. From these values, it is clear that decision tree method requires less time than the other considered techniques, whereas accuracy is high in case of SVM.

INDEX TERMS Internet of Medical Things (IoMT), authentication, key agreement, artificial intelligence (AI), security.

I. INTRODUCTION

Internet of Medical Things (IoMT) envisions a network of smart healthcare devices and users, which use some

The associate editor coordinating the review of this manuscript and approving it for publication was Adnan M. Abu-Mahfouz.

wireless communication technology for the exchange of healthcare data. As the cost and prices of healthcare for various services are now increasing with the growing population, it is important to mention that the combination of IoMT and healthcare can ameliorate the quality of life and provide better care [1], [2]. This can be used to create more cost-effective systems of healthcare [3]. Some of the potential applications of IoMT include complete real-time monitoring of patients, patient information management, medical equipment and drug monitoring, medical device and pharmaceuticals anti-counterfeiting, medical waste information management, medical emergency management, remote surgery, medical equipment and drug tracking and medicine and sample collection through drones [4], [5].

A. MOTIVATION

The healthcare data can be stored over the cloud for further analysis and prediction. In such cases, for the prediction and outcomes, we can use the AI-enabled Big data analytic methods at the authorized cloud server(s). This process is essentially required to predict the health conditions (i.e., chances of getting a heart attack, chances of getting a diabetic shock and possibility of a tumor, etc.) [6]–[8]. Furthermore, although IoMT supports various types of applications as discussed earlier, it also suffers from different security and privacy issues. This may cause the problems with secure transmission and storage of the sensitive healthcare data. The present protocols lack in security and functionality features. The existing protocols are vulnerable to various attacks. Moreover, they do not have important phases, like key revocation phase and AI-enabled big data analytics phase. Thus, it is essential to provide a robust security protocol for the secure communication in an IoMT environment, which should overcome the existing issues. This motivates us to design a new AI-enabled secure communication scheme for the IoMT environment.

B. RESEARCH CONTRIBUTIONS

The following are the research contributions of the paper:

- A new AI-enabled lightweight, secure communication scheme for IoMT environment (in short ASCP-IoMT) is proposed. It provides secure communications among Internet of Things (IoT)-enabled implantable medical devices and personal servers, and personal servers and cloud servers through the provided authentication and key establishment procedure.
- The given network model and threat model provide the details of the associated network arrangement of the devices and users of IoMT and information security threats of the IoMT.
- The performed security analysis confirms the security of ASCP-IoMT against different potential passive as well as active attacks.
- The comparison of ASCP-IoMT with the other similar schemes is also performed. It indicates that ASCP-IoMT performs better than the other similar schemes.
- The practical implementation of ASCP-IoMT is then provided to find out its influence on network performance parameters of the system.

C. PAPER OUTLINE

The rest of the paper is arranged as follows. Various related security schemes in the domain of IoMT are discussed in Section II. The associated system models of ASCP-IoMT are provided in Section III. The various phases of ASCP-IoMT are elaborated in Section IV. The security of ASCP-IoMT is provided in Section V. The comparison of ASCP-IoMT and other similar schemes is then provided in Section VI. The practical implementation of ASCP-IoMT is also done in Section VII. At the last, the paper is concluded in Section VIII.

II. RELATED WORK

Wazid *et al.* [4] proposed a private-blockchain based framework for secure communication in an IoT-enabled drone-aided healthcare environment. Camara *et al.* [9] discussed the safety, security, and privacy risk associated with the use of IMDs.

Cano and Canavate-Sanchez [10] proposed a dual-signature based elliptic curve digital signature algorithm (ECDSA) to protect the privacy in the IoMT environment. Wang *et al.* [11] designed a fog-based access control method to ensure high-level privacy in the cloud/fog-based IoMT environment. However, in their scheme, important security and functionality features like mutual authentication, absence of key agreement, etc., were not provided. Alsubaei *et al.* [12] presented a web-based IoMT security assessment method.

Jang *et al.* [13] proposed a hybrid security scheme that uses both heterogeneous cryptosystems, such as symmetric and asymmetric (public) key cryptographic techniques. However, their scheme fails to provide proper security for the healthcare data exchange.

He and Zeadally [14] presented an authentication mechanism by using the ambient intelligence, specifically for an Ambient Assisted Living (AAL) system. Their scheme helped in the monitoring of healthcare data and it also provided tele-health care services. Merabet *et al.* [15] presented Machine-to-Machine (M2M) and Machine-to-Cloud (M2C) methods, which were required in the IoT-based healthcare systems. However, their presented schemes did not support essential features, like dynamic controller node addition and medical device addition.

Most of the schemes discussed in this section lack in security and functionality features and do not have essential features like AI-based big data analytics. Thus, it is important to provide some AI-based security mechanism for secure healthcare data exchange inside an IoMT environment.

III. SYSTEM MODELS

In this section, we discuss the associated network model and attack model of the proposed ASCP-IoMT algorithm/method.

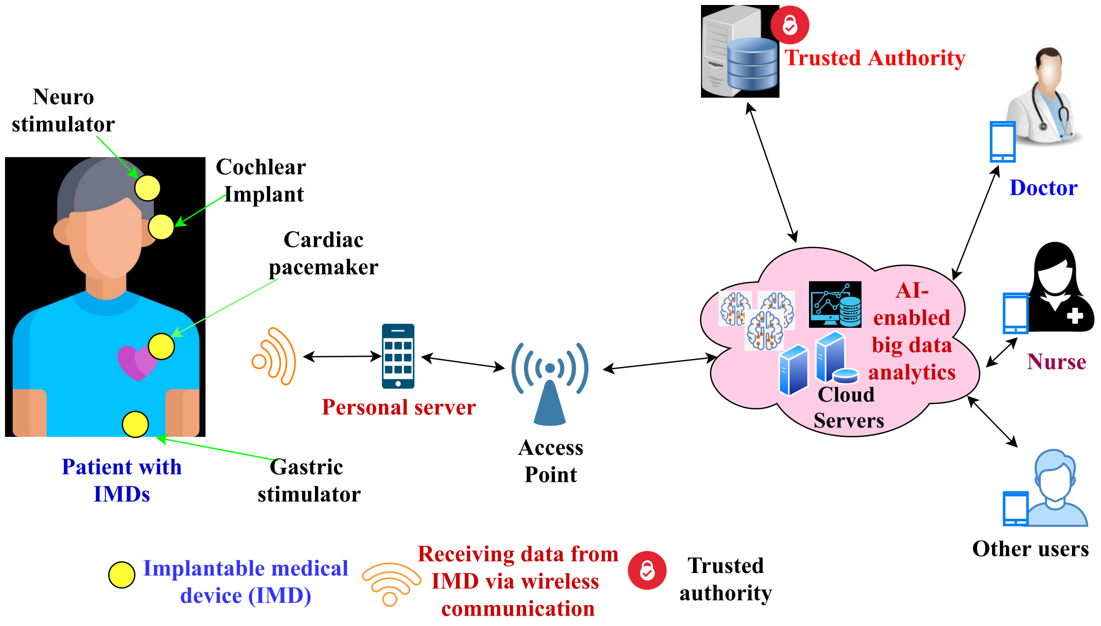

FIGURE 1. Network model of ASCP-IoMT.

A. NETWORK MODEL

In the network model of ASCP-IoMT provided in Figure 1, there is a patient, who is implanted with some medical devices (IMDs), i.e., neurostimulator, cardiac pacemaker, etc. There is also a deployed personal server, which collects data from IMDs through some wireless communication method. Various wireless communication technologies along with protocols can be utilized in order to connect the IoT-enabled smart devices [16]. Some of these include 1) Internet Protocol Version 6 (IPv6), over Low power Wireless Personal Area Networks (6LoWPAN), 2) ZigBee, 3) Bluetooth Low Energy (BLE), and 4) Z-Wave and Near Field Communication (NFC). 6loWPAN is the most commonly used standard in IoT communication protocols, because it is based on IP-based standard internetworking protocol and can be connected directly with other IP networks without any intermediate networking entities such as proxies and translation gateways. ZigBee relies on low-power wireless IEEE802.15.4 networking standard, which also supports various types of topologies including star, mesh, star tree network topologies. BLE is intended for designing and enhancing the short-range, low bandwidth, and low latency for IoT-based applications. On the other hand, NFC is a very short-range wireless communication mechanism which has the ability to transfer the data among IoT devices.

The data, which is collected by the personal server, is forwarded to the associated cloud server via an access point. The cloud servers stores, process, and analyse the received healthcare data of the patients. There are also some users (i.e., doctors) who want to access the health-related data of the patient. A trusted authority is required to deploy for the registration of the various devices, i.e., IMDs, personal server, cloud servers and the users. The healthcare data of the patient can be accessed by the users from the associated cloud server after the execution of required steps of the authentication technique.

The cloud servers are resource-rich entities and have high processing, computation and storage capabilities. All the messages among the communicating devices and users are exchanged in a secure way with the help of established session keys. Here, it is also important to mention that the deployed IMDs are resource constrained entities, which have very low high processing, computation and storage capabilities. Therefore, a deployed authentication and key establishment scheme should use lightweight cryptographic operations such as hash and XOR operations.

In the proposed ASCP-IoMT, we only consider the use of lightweight cryptographic operations. The deployed cloud servers store a huge amount of healthcare data, which can be used in various health-related predictions. For the prediction and outcomes, we can use the AI-enabled big data analytics methods at the authorized cloud server. This process is essentially required to predict the health conditions (i.e., chances of getting a heart attack, chances of getting a diabetic shock and possibility of a tumor) [6], [7]. Therefore, AI-enabled big data analytics phase is also included in ASCP-IoMT. Hence the proposed ASCP-IoMT seems very useful from the healthcare point of view, i.e., for the better treatment, control and prediction of health problems of the patients [4], [17], [18].

B. ATTACK MODEL

We use the guidelines of the widely used Dolev-Yao (DY) threat model [19]. As per the DY model, the communicating entities (i.e., IMDs, servers, users) communicate over the public channel (i.e., Internet). It means that an active or a passive adversary $\mathcal{A}$ of the network/system may intercept, disclose, update, delete, or delay the exchanged messages. Moreover, $\mathcal{A}$ can also capture some of the deployed IMDs physically and use them to extract sensitive information (i.e., secret keys) from their memory under the execution of steps of advanced power analysis attacks [20]. The guidelines of another important model, "Canetti and Krawczyk's adversary model is also known as CK-adversary model, which is the current *de facto* standard model in the modeling of an authenticated key agreement security protocol, has been also followed in the designing of ASCP-IoMT. As per the "CK-adversary model, $\mathcal{A}$ can have all the capabilities like the DY model, along with that he/she can compromise the secret credentials and with the session keys or the session states in the sessions." Furthermore, trusted authority (*TA*) is considered as the trusted entity of the network and this will not be compromised in any case; Otherwise, the security of the entire network will be compromised. The personal servers are considered as semi-trusted entities of the network, they are kept inside some physical locking system to prevent against the physical device capture attack. The cloud servers used for the AI-enabled big data analytics are considered as the semi-trusted entities.

TABLE 1. Notations used in the paper.

Notation	Meaning
$\mathcal{A}$	An adversary
TA	Trusted authority performs registration of devices and servers
IMD_i	i^{th} implantable medical device (IMD)
PS_j	j^{th} personal server
CS_k	k^{th} cloud server
TS_l	Different timestamp values
rn_l	Different random nonce values
$h(\cdot)$	Operation through hash function
$\psi_{X,Y}$	Session key of party X and party Y
$\|\|$	Operation through concatenation
$\oplus$	Operation through bitwise exclusive-OR (XOR)

IV. PROPOSED PROTOCOL: ASCP-IoMT

In this section, we discuss various phases of ASCP-IoMT. ASCP-IoMT consists of the following important phases: a) registration phase, b) authentication and key management phase, c) dynamic device addition phase d) key revocation phase and e) AI-based Big data analytics phase.

We assume that the various entities involved in the network are synchronized with their clocks in order to prevent relay attack protection against an adversary. This assumption is realistic as it is used in designing the security protocols for IoT-enabled networking environments [21]–[25]. The details of various notations are given in Table 1.

A. REGISTRATION PHASE

In this phase, a trusted authority (*TA*) does the registration of different communicating parties, like IMDs, personal servers and cloud servers.

1) REGISTRATION OF IMDs

The registration of an IMD_i is performed as follows:

- **RGIMD1:** ID_{IMD_i} is chosen as a "unique identity for the implantable medical device IMD_i" by *TA*. Further, *TA* computes its pseudo identity $RID_{IMD_i} = h(ID_{IMD_i}||\ \mu_{TA}||\ \mu_{IMD_i})$, where μ_{TA} is the secret key of *TA* and μ_{IMD_i} is the secret key of IMD_i.
- **RGIMD2:** Further *TA* calculates temporal credentials of IMD_i as $TC_{IMD_i} = h(ID_{IMD_i}||\ \phi_{IMD_i}||\ \mu_{IMD_i})$, where ϕ_{IMD_i} is the registration timestamp value of device IMD_i. *TA* again generates the temporary identity as TID_{IMD_i} and deployment area identity as f_{IMD_i} for IMD_i.
- **RGIMD3:** After completing these steps, TA stores $\{RID_{IMD_i}, TC_{IMD_i}, TID_{IMD_i}, f_{IMD_i}, h(\cdot)\}$ in the memory of IMD_i before its deployment.

2) REGISTRATION OF PERSONAL SERVERS

The *TA* performs the registration of the personal server PS_j as follows:

- **RGPS1:** ID_{PS_j} is chosen as a "unique identity for the personal server PS_j" by *TA*. Further *TA* calculates $RID_{PS_j} = h(ID_{PS_j}||\mu_{TA}||\mu_{PS_j})$ as the pseudo-identity for the same PS_j, where μ_{PS_j} is the secret key of PS_j. *TA* also generates a shared secret key of PS_j and CS_k as μ_{PS_j,CS_k}, which is used for their secure communication. It is also note that the value of μ_{PS_j,CS_k} is different for different PS_j and CS_k.
- **RGPS2:** After the generations of these values, the TA stores $\{(TID_{IMD_i},\ RID_{IMD_i}, TC_{IMD_i},\ f_{IMD_i})|i = 1, 2, \cdots, num_{IMD_i}\}$, RID_{PS_j}, μ_{PS_j,CS_k}, $h(\cdot)\}$ in the memory of PS_j before its deployment.

3) REGISTRATION OF CLOUD SERVERS

The registration of cloud server CS_k is performed as follows:

- **RGCS1:** ID_{CS_k} is chosen as a unique identity for the cloud server CS_k by *TA*. Again *TA* calculates $RID_{CS_k} = h(ID_{CS_k}||\ \mu_{TA}||\ \mu_{CS_k})$ as the pseudo-identity for the same CS_k, where μ_{CS_k} is the secret key of CS_k.
- **RGCS2:** After these generation of these values, *TA* stores $\{(RID_{PS_j}|j = 1, 2, \cdots, num_{PS_j})\}$, RID_{CS_k}, $\{\mu_{PS_j,CS_k}|j = 1, 2, \cdots, num_{PS_j}\}$, $h(\cdot)\}$ in the memory of CS_k, where num_{PS_j} are the total number of personal servers. Here, it is important to mention that $\{\mu_{PS_j,CS_k}|j = 1, 2, \cdots, num_{PS_j}\}$ mean that we have different shared secret keys for different personal servers and cloud server CS_k.

B. AUTHENTICATION AND KEY MANAGEMENT (AKM) PHASE

This procedure is required for the secure messages exchange between the legitimate IMD_i and PS_j, and also between legitimate PS_j and CS_k.

1) AKM BETWEEN IMD_i AND PS_j

The authentication and key establishment between IMD_i and PS_j is performed as follows:

IMD_i	PS_j
Generate rn_1 & TS_1. Compute $M_1 = rn_1 \oplus h(RID_{IMD_i}\|\| TS_1)$, $M_2 = h(rn_1\|\| RID_{IMD_i}\|\| TC_{IMD_i}\|\| TS_1\|\| f_{IMD_i})$. $\underrightarrow{\langle MSG_1 = \{TID_{IMD_i}, M_1, M_2, TS_1\}\rangle}$ (via open channel)	
Check if $\|TS_2 - TS_2^*\| \leq \Delta T$? If so, compute $h(rn_2\|\| RID_{PS_j}) = M_3 \oplus h(RID_{IMD_i}\|\| TS_1\|\| TS_2)$, $\psi_{IMD_i,PS_j} = h(h(rn_2\|\| RID_{PS_j})\|\|$ $RID_{IMD_i}\|\| TC_{IMD_i}\|\| rn_1\|\| TS_1\|\| TS_2)$ $M_4' = h(\psi_{IMD_i,PS_j}\|\| TS_1\|\| TS_2)$. Check if $M_4' = M_4$? If so, compute $TID_{IMD_i}^{new} = M_5$ $\oplus h(RID_{IMD_i}\|\| TC_{IMD_i}\|\| h(rn_2\|\| RID_{PS_j}))$. Replace $TID_{IMD_i}^{new}$ with TID_{IMD_i}.	Check if $\|TS_1 - TS_1^*\| \leq \Delta T$? If so, fetch RID_{IMD_i}, TC_{IMD_i}, f_{IMD_i}. Compute $rn_1 = M_1 \oplus h(RID_{IMD_i}\|\| TS_1)$, $M_2' = h(rn_1\|\| RID_{IMD_i}\|\| TC_{IMD_i}\|\| TS_1\|\| f_{IMD_i})$. Check if $M_2' = M_2$? If so, generate rn_2 & TS_2. Compute $M_3 = h(rn_2\|\| RID_{PS_j})\oplus h(RID_{IMD_i}\|\| TS_1\|\| TS_2)$, $\psi_{PS_j,IMD_i} = h(h(rn_2\|\|RID_{PS_j})\|\| RID_{IMD_i}$ $\|\|TC_{IMD_i}\|\| rn_1\|\| TS_1\|\| TS_2)$, $M_4 = h(\psi_{PS_j,IMD_i}\|\| TS_1\|\| TS_2)$. Generate $TID_{IMD_i}^{new}$. Compute $M_5 = TID_{IMD_i}^{new} \oplus h(RID_{IMD_i}\|\|$ $TC_{IMD_i}\|\| h(rn_2\|\| RID_{PS_j}))$. $\underleftarrow{\langle MSG_2 = \{M_3, M_4, M_5, TS_2\}\rangle}$ (via open channel)
Generate TS_3 Compute $M_6 = h(\psi_{IMD_i,PS_j}\|\|$ $TID_{IMD_i}^{new}\|\| TS_3)$. $\underrightarrow{\langle MSG_3 = \{M_6, TS_3\}\rangle}$ (via open channel)	Check if $\|TS_3 - TS_3^*\| \leq \Delta T$? If so, compute $M_6' = h(\psi_{PS_j,IMD_i}\|\| TID_{IMD_i}^{new}\|\| TS_3)$. Check if $M_6' = M_6$? If so, update TID_{IMD_i} with $TID_{IMD_i}^{new}$.
Both IMD_i and PS_j store $\psi_{IMD_i,PS_j} = (\psi_{PS_j,IMD_i})$.	

FIGURE 2. Summary of AKE between IMD_i and PS_j.

- **AKEIP1:** IMD_i starts the process and generates a random nonce rn_1 and the current timestamp TS_1 and then generates following values $M_1 = rn_1 \oplus h(RID_{IMD_i}|| TS_1)$, $M_2 = h(rn_1|| RID_{IMD_i}|| TC_{IMD_i}|| TS_1|| f_{IMD_i})$. Later on IMD_i sends $\langle MSG_1 = \{TID_{IMD_i}, M_1, M_2, TS_1\}\rangle$ to PS_j via public channel. After receiving MSG_1 from IMD_i, PS_j verifies the timestamp value TS_1 through condition $|TS_1 - TS_1^*| \leq \Delta T$, where TS_1^* represents the receiving timestamp value of MSG_1. If this verification happens successfully, then PS_j fetches $RID_{IMD_i}, TC_{IMD_i}, f_{IMD_i}$ from its memory corresponding to received TID_{IMD_i} value. PS_j then calculates values like $rn_1 = M_1 \oplus h(RID_{IMD_i}|| TS_1)$ and $M_2' = h(rn_1|| RID_{IMD_i}|| TC_{IMD_i}|| TS_1||f_{IMD_i})$. PS_j again verifies $M_2' = M_2$? If these values matches then IMD_i is authenticated with PS_j. In different circumstances, IMD_i's authentication is failed.
- **AKEIP2:** Further PS_j generates a random nonce rn_2 along with a current timestamp TS_2 and calculates values like, $M_3 = h(rn_2|| RID_{PS_j}) \oplus h(RID_{IMD_i}|| TS_1|| TS_2)$, session key $\psi_{PS_j,IMD_i} = h(h(rn_2||RID_{PS_j})|| RID_{IMD_i}|| TC_{IMD_i}|| rn_1|| TS_1|| TS_2)$ and $M_4 = h(\psi_{PS_j,IMD_i}|| TS_1|| TS_2)$. After the computing these parameters, PS_j generates new temporary identity for IMD_i as $TID_{IMD_i}^{new}$ and estimates $M_5 = TID_{IMD_i}^{new} \oplus h(RID_{IMD_i}|| TC_{IMD_i}|| h(rn_2|| RID_{PS_j}))$. Then PS_j sends $\langle MSG_2 = \{M_3, M_4, M_5, TS_2\}\rangle$ to IMD_i via public channel.
- **AKEIP3:** Upon the arrival of MSG_2, IMD_i first verifies the timeliness of TS_2 through condition $|TS_2 - TS_2^*| \leq \Delta T$, where TS_2^* is the receiving timestamp value of MSG_2. If it verifies successfully then IMD_i calculates $h(rn_2|| RID_{PS_j}) = M_3 \oplus h(RID_{IMD_i}|| TS_1|| TS_2)$, session key $\psi_{IMD_i,PS_j} = h(h(rn_2|| RID_{PS_j})|| RID_{IMD_i}|| TC_{IMD_i}|| rn_1|| TS_1|| TS_2)$ and $M_4' = h(\psi_{IMD_i,PS_j}|| TS_1|| TS_2)$. IMD_i goes for the verification of $M_4' = M_4$? If that happens successfully then PS_j is authenticated with IMD_i. In other circumstances the authentication of PS_i is failed with IMD_i. Further IMD_i calculates its new temporary identity through $TID_{IMD_i}^{new} = M_5 \oplus h(RID_{IMD_i}|| TC_{IMD_i}|| h(rn_2|| RID_{PS_j}))$ and replaces $TID_{IMD_i}^{new}$ with TID_{IMD_i}. IMD_i again generates another fresh timestamp TS_3 and calculates $M_6 = h(\psi_{IMD_i,PS_j}|| TID_{IMD_i}^{new}|| TS_3)$. Then IMD_i sends $\langle MSG_3 = \{M_6, TS_3\}\rangle$ to PS_j via public channel. Upon the arrival of MSG_3, PS_j verifies the timeliness of TS_3 as per the condition explained earlier. If that happens successfully then PS_j computes $M_6' = h(\psi_{PS_j,IMD_i}|| TID_{IMD_i}^{new}|| TS_3)$. Again PS_j goes for the verification of $M_6' = M_6$? If it matches, then the session key calculated by IMD_i is correct and IMD_i has successfully updated the $TID_{IMD_i}^{new}$. PS_j also updates TID_{IMD_i} with $TID_{IMD_i}^{new}$ in its database. Finally, both IMD_i and PS_j

establish session key $\psi_{IMD_i,PS_j} = (\psi_{PS_j,IMD_i})$ for their secure communication.

After the completion of the above discussed steps, both IMD_i and PS_j establish a session key for their secure communication. The summary of authentication and key establishment between IMD_i and PS_j is also given in Figure 2.

2) KEY MANAGEMENT BETWEEN PS_j AND CS_k

For the secure exchange of messages, both PS_j and CS_k can use the stored μ_{PS_j,CS_k} shared secret key. PS_j can encrypt the message μ_{PS_j,CS_k}, which will be further decrypted by the recipient, i.e., CS_k through the same key μ_{PS_j,CS_k}. It is also important to mention that freshly generated timestamp values can also be included in the exchanged messages for the prevention of replay attack.

C. DYNAMIC DEVICE ADDITION PHASE

IoMT may suffer from the failures of a certain number of IMDs. Therefore, it is always required to add a new device (i.e., IMD_i^{new}) in the network. TA does the tasks of addition of a new IMD_i^{new} as follows:

- **DAIMD1:** $ID_{IMD_i^{new}}$ is chosen as a unique identity for IMD_i^{new} by TA. Further, TA calculates $RID_{IMD_i^{new}} = h(ID_{IMD_i^{new}} || \mu_{TA} || \mu_{IMD_i^{new}})$ as the pseudo identity for IMD_i^{new}, where μ_{TA} is the secret key of TA and $\mu_{IMD_i^{new}}$ is the secret key of IMD_i^{new}.
- **DAIMD2:** Further TA calculates temporal credentials of IMD_i^{new} as $TC_{IMD_i^{new}} = h(ID_{IMD_i^{new}} || \phi_{IMD_i^{new}} || \mu_{IMD_i^{new}})$, where $\phi_{IMD_i^{new}}$ is the registration timestamp IMD_i^{new}. TA again generates the temporary identity as $TID_{IMD_i^v}$ and deployment area identity as $f_{IMD_i^v}$ for IMD_i. Furthermore, $f_{IMD_i^v}$ may be equal to f_{IMD_i}.
- **DAIMD3:** After computing these values, TA stores $\{RID_{IMD_i^{new}}, TC_{IMD_i^{new}}, TID_{IMD_i^v}, f_{IMD_i^v}, h(\cdot)\}$ in the memory of IMD_i^{new} before its deployment. TA also informs the other devices, like personal servers about the addition of new IMD in a secure way. In the similar way the addition of new PS_j can be done, if it is desired.

Remark 1: Here, it is also important to mention that PS_j, and CS_k store all secret information, for example, secret keys and identities in the secured region of their database. Thus these values are not available to $\mathcal{A}$ to launch further attacks, i.e., "stolen verifier attack, MiTM, impersonation attack and illegal session key computation attack" on ASCP-IoMT. Such kind of strong assumptions are also considered in RSA/ECC-based secure communication systems, which are deployed in recent times.

D. KEY REVOCATION PHASE

Using this phase, the trusted authority TA can update the shared secret key of personal server PS_j and cloud server CS_k as it is required in case of any key leakage or if key is in use from the long time. For that purpose TA generates new shared secret key $\mu^v_{PS_j,CS_k}$ and then replace it with the old key μ_{PS_j,CS_k} in the database of PS_j and CS_k securely in the online mode. Here it is important to mention that TA communicates securely with PS_j and CS_k through the secret keys i.e., MK_{TA,PS_j} and MK_{TA,CS_k}. Therefore, all information exchange happens through MK_{TA,PS_j} and MK_{TA,CS_k} in between TA and PS_j, and TA and CS_k, respectively. Finally, PS_j have information $\{(TID_{IMD_i}, RID_{IMD_i}, TC_{IMD_i}, f_{IMD_i})|i = 1, 2, \cdots, num_{IMD_i}\}$, RID_{PS_j}, $\mu^v_{PS_j,CS_k}$, $h(\cdot)\}$ in its database. Moreover, CS_k have information $\{(RID_{PS_j}|j = 1, 2, \cdots, num_{PS_j}\}$, RID_{CS_k}, $(\mu^v_{PS_j,CS_k}|j = 1, 2, \cdots, num_{PS_j})$, $h(\cdot)\}$ in its database.

E. AI-ENABLED BIG DATA ANALYTICS PHASE

Big data is the heterogeneous collection of data that generates a huge amount of volume. In AI-enabled big data analytics, AI methods execute on this diverse data through some machine learning (ML) algorithms. This process examines a large amount of data (i.e., healthcare data) to uncover hidden patterns and other useful information from it [8]. This is further helpful for the prediction of some phenomena. The huge amounts of diverse data make it possible for the ML algorithms to learn and predict with negligible errors. Thus the overall performance (i.e., accuracy) of the system can be improved if a huge amount of data is made available to the AI module. Because in that situation, it can learn in a better way that also improves its pattern recognition capabilities. AI-enabled big data analytics phase is required for the forecast of useful outcomes (i.e., the possibility of a tumor) [26], [27]. This task is supposed to happen at the authorized cloud server, i.e., CS_k. CS_k calls the steps of big data analytics. CS_k first executes the necessary steps of data aggregation. This accumulated information is useful for the big data analysis process. The deployed AI module will learn and predict on the basis of available training and testing data. Furthermore, CS_k executes other essentials steps like "data analysis," "data visualization & prediction on the accumulated data". The final results of this phase come out in the form of some significant results (predictions) as explained earlier [4].

The process flow diagram of the proposed ASCP-IoMT is depicted in Figure 3. This provides an overview of various processes (for example, registration of devices and server, authentication and key establishment between IMD and personal server, key management between personal server and cloud server, AI-enabled big data analytics and key revocation), which are associated with the proposed ASCP-IoMT.

V. SECURITY ANALYSIS

In this section, we first provide the correctness of the proposed scheme. Next, we provide both informal (heuristics) and formal security analysis for the proposed scheme (ASCP-IoMT) to show its robustness against various attacks.

A. CORRECTNESS PROOF

In Theorem 1, we provide the correctness of the proposed ASCP-IoMT by showing that two entities always establish the same common key between them.

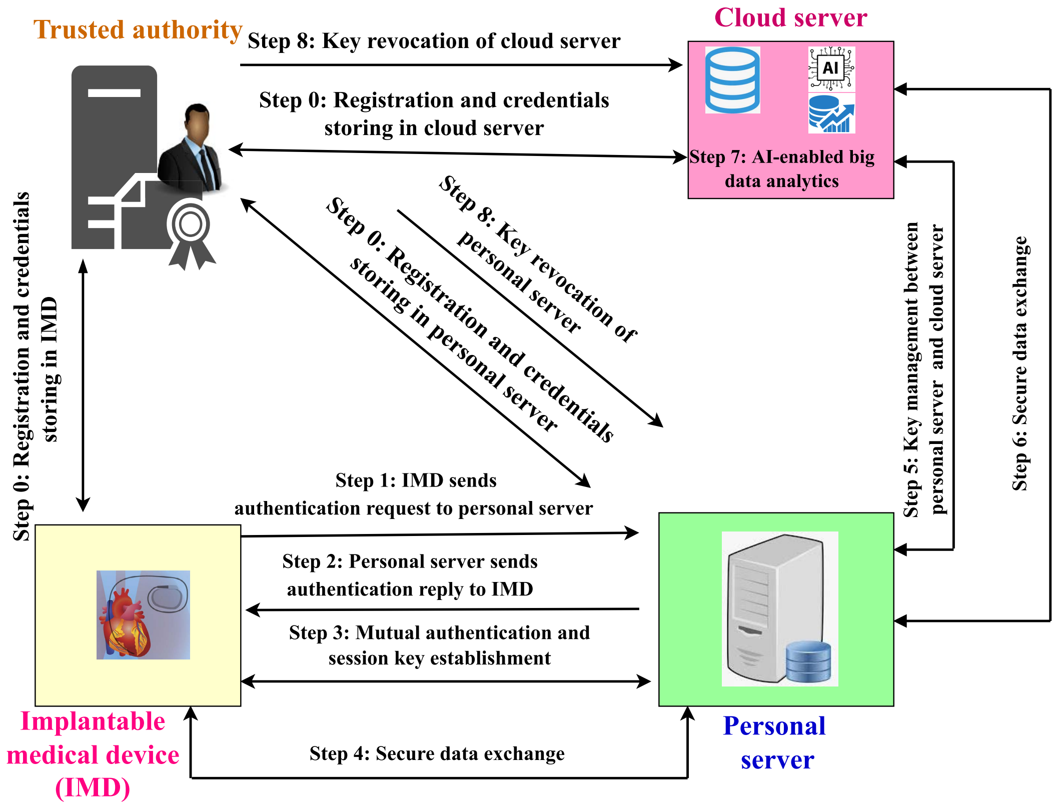
Trusted authority
Cloud server
Step 8: Key revocation of cloud server
Step 0: Registration and credentials storing in cloud server
Step 7: AI-enabled big data analytics
AI
Step 8: Key revocation of personal server
Step 0: Registration and credentials storing in personal server
Step 0: Registration and credentials storing in IMD
Step 5: Key management between personal server and cloud server
Step 6: Secure data exchange
Step 1: IMD sends authentication request to personal server
Step 2: Personal server sends authentication reply to IMD
Step 3: Mutual authentication and session key establishment
Step 4: Secure data exchange
Implantable medical device (IMD)
Personal server

FIGURE 3. Process flow diagram of ASCP-IoMT.

Theorem 1: In the proposed ASCP-IoMT, during the authentication and key management phase the session keys established between IMD_i and PS_j are the same.

Proof: At the time of authentication and key establishment between IMD_i and PS_j, PS_j calculates the session key shared with IMD_i as $\psi_{PS_j,IMD_i} = h(h(rn_2||RID_{PS_j})|| RID_{IMD_i}|| TC_{IMD_i}|| rn_1|| TS_1|| TS_2)$. After mutual authentication, IMD_i calculates the session key shared with PS_j as $\psi_{IMD_i,PS_j} = h(h(rn_2|| RID_{PS_j})|| RID_{IMD_i}|| TC_{IMD_i}|| rn_1|| TS_1|| TS_2)$. It is worth noticing that PS_j derives $rn_1 = M_1 \oplus h(RID_{IMD_i}|| TS_1)$ from the message $\langle MSG_1 = \{TID_{IMD_i}, M_1, M_2, TS_1\}\rangle$, whereas IMD_i derives $h(rn_2|| RID_{PS_j}) = M_3 \oplus h(RID_{IMD_i}|| TS_1|| TS_2)$ from the message $\langle MSG_2 = \{M_3, M_4, M_5, TS_2\}\rangle$. It is then follows that $\psi_{PS_j,IMD_i} = \psi_{IMD_i,PS_j}$. □

B. INFORMAL SECURITY ANALYSIS

ASCP-IoMT is able to defend the following types of attacks.

1) REPLAY ATTACK

In ASCP-IoMT messages, like MSG_1, MSG_2, and MSG_3 were exchanged. These messages are Incorporated with different freshly generated timestamp values, i.e., TS_1, TS_2, and TS_3. These timestamp values are also verified at the receiver's end, when a message arrives. Due to this procedure of timestamp generation and verification, $\mathcal{A}$ is not able to launch the replay attack on ASCP-IoMT. Therefore, ASCP-IoMT provides protection for a replay attack.

2) MAN-IN-THE-MIDDLE (MiTM) AND IMPERSONATION ATTACKS

In ASCP-IoMT messages, like MSG_1, MSG_2, and MSG_3 were exchanged. These messages are incorporated with different randomly generated nonce values, i.e., rn_1, and rn_2. Apart from that, each message contains various secret key and identity values (i.e., ID_{IMD_i}, ID_{PS_j}, ID_{CS_k}, ϕ_{IMD_i}, μ_{IMD_i}, μ_{PS_j}, μ_{CS_k}, μ_{TA}, μ_{PS_j,CS_k}). These secret values are not known to $\mathcal{A}$. Therefore, $\mathcal{A}$ can not update the exchanged messages. Moreover, in such a situation $\mathcal{A}$ is also not able to generate the same message on behalf of a legitimate entity of the network. Due to the aforementioned procedure, $\mathcal{A}$ is not able to launch in MiTM and impersonation attacks on ASCP-IoMT. Thus, ASCP-IoMT provides protection for MiTM and impersonation attacks.

3) EPHEMERAL SECRET LEAKAGE (ESL) ATTACK

It is preferable to check the possibility of "Ephemeral Secret Leakage (ESL) attack" on a newly designed authentication and key establishment scheme. It proves the resilience of that scheme whether $\mathcal{A}$ has ability to compute the session key or not. We contemplate "short term secrets (for example, random secrets) and long term secrets (for example, secret keys and various real identities)'' in the proposed ASCP-IoMT. In each session, parties compute a new session key and then establish that key for their secure communication. However, $\mathcal{A}$ is not aware of these secret values. Thus, he/she can not compute the correct session key on behalf of a legitimate entity of the network. Hence, ASCP-IoMT provides protection against ``unauthorized session key computation attack under CK-adversary model''. In this way, ESL attack is protected in the proposed ASCP-IoMT.

4) PRIVILEGED INSIDER ATTACK

In ASCP-IoMT, it is considered that all registered secret information should be deleted from the database of *TA*. Therefore, this secret information is not available to the insider user of *TA*. Hence, required information is not available to the malicious insider user for the launching of associated attacks, like ``MiTM, impersonation attack, secret credentials guessing, and illegal session key computation attacks.'' Thereafter ASCP-IoMT provides protection for a privileged insider attack.

5) PHYSICAL IMD CAPTURE ATTACK

In ASCP-IoMT, any secret information is not stored in the plaintext in the memory of IMDs. Even if $\mathcal{A}$ physically captures an IMD and tries to deduce some secret information (i.e., its stored session key) from its memory through the application of an advanced power analysis attack [20]. However, such kind of malicious tasks will only reveal the session key of this particular IMD not the session keys of other IMDs. Because as per the arrangements of ASCP-IoMT each device computes and establishes different session keys for the different sessions. Thus such kind of compromising does not affect the remaining part of the communication and it is still safe and secure. Hence ASCP-IoMT provides protection for physical IMD compromised attacks.

6) STOLEN VERIFIER ATTACK

Stolen verifier attack is another important attack that an authentication and key establishment should defend it. In the presence of this attack, $\mathcal{A}$ has an ability to perform other potential attacks. For example, $\mathcal{A}$ can launch MiTM, impersonation, unauthorised credentials guessing, illegal session key computation attacks on a newly designed scheme. In proposed ASCP-IoMT, as per the aforementioned mechanism, all sensitive values are stored in the secured region of the databases residing in the personal server and cloud server. Moreover, a personal server is also maintained inside a physical locking system in order to protect against the physical stealing and other associated attacks [28]. Therefore, the sensitive information is not available to the adversary $\mathcal{A}$ for launching potential attacks, like ``MiTM, impersonation, unauthorised credentials guessing, illegal session key computation'' attacks. Hence, ASCP-IoMT provides protection for stolen verifier attack (see also Remark 1).

7) ANONYMITY AND UNTRACEABILITY

In ASCP-IoMT, we do not exchange any identity in the plaintext. The identities of the devices and users are anonymous. Further, all exchanged messages are calculated via ``freshly generated timestamp values and random nonce values''. Therefore, the aforementioned procedure produces distinct messages in different sessions. Thus, $\mathcal{A}$ is not able to trace the exchanged messages. After a while, ASCP-IoMT supports the essential anonymity and untraceability properties.

C. FORMAL SECURITY ANALYSIS THROUGH REAL-OR-RANDOM (ROR) MODEL

We formally analyze the proposed ASCP-IoMT to prove its security against other potential attacks. We conduct formal security analysis through ``Real-Or-Random (ROR) random oracle model''. Here it is important to discuss that ROR model [29] is the standard model, which is used to provide the proof of security of session key (SK) in the proposed ASCP-IoMT. This model is also used in some recently published ``authentication schemes'' to provide the proof of security of session key.

There are two participants in proposed ASCP-IoMT, i.e., IMD_i and PS_j, during the ``authentication and key management (AKM) phase of ASCP-IoMT'' (for the secure of communication of IMD_i and PS_j). We express $\mathcal{O}^t_{IMD_i}$ and $\mathcal{O}^v_{PS_j}$ as the instances t and v of IMD_i and PS_j, respectively. These considered instances are also taken as the *oracles*. The ROR model has following essential terminologies.

- **Participants.** We express $\mathcal{O}^t_{IMD_i}$ and $\mathcal{O}^v_{PS_j}$ as the instances t and v of IMD_i and PS_j, respectively. These instances are also considered as the *oracles*.
- **Accepted state.** At the receiving of the last protocol message, an instance $\mathcal{O}^t$ is in the accept state then we understand that $\mathcal{O}^t$ goes to the accepted state. If all communicated messages, for example, send and receive messages by $\mathcal{O}^t$) are concatenated according to the order. (sid) of $\mathcal{O}^t$ is taken as session identification for a particular session.
- **Partnering.** Instance $\mathcal{O}^{l_1}$ and $\mathcal{O}^{l_2}$ are considered as the partner of each other. In case if following three conditions provides assurance: 1) ``both instances are in the accepted states'', 2) ``both instances mutually authenticate each other and share the same session id sid'', and 3) ``both instances are mutual partners''.
- **Freshness.** Suppose that session key SK_{ij} does not disclose under the deployment of reveal query $\mathcal{R}$. Under these circumstances, it can be said that $\mathcal{O}^t_{IMD_i}$ or $\mathcal{O}^v_{PS_j}$ are fresh and latest.
- **Adversary.** The adversary $\mathcal{A}$ is executed through Dolev-Yao (DY) model. Under such circumstances, it is considered as $\mathcal{A}$ has control over the communication, which is happening through the public channel. Therefore, $\mathcal{A}$ can perform some unauthorised activities i.e., eavesdrop, delete, update, or injection of false messages with the help of following queries.

- $\mathcal{E}$ $(\mathcal{O}^t, \mathcal{O}^v)$: The eavesdropping attack, which is passive in nature, can be executed with this *execute* query. With query $\mathcal{A}$ can eavesdrop the exchanged messages of entities IMD_i and PS_j.
- $\mathcal{S}$ $(\mathcal{O}^t, msg)$: It is executed like the active attack. $\mathcal{A}$ sends or receives messages to or from $\mathcal{O}^t$ via *send* query.
- $\mathcal{R}$ $(\mathcal{O}^t)$: It is one of the important query. *reveal* query tries to reveal session key SK_{ij} reckoned by $\mathcal{O}^t$ and the other associated entity to the attacker $\mathcal{A}$ for a particular session.
- $\mathcal{T}$ $(\mathcal{O}^t)$: Before starting the game, an unbiased coin c is flipped, which is executed via *test* query. Then there is the flipping of coin, which may produce different outcomes (results). On the basis of the results of coin flipping, following decisions are made. If the result of coin flipping is, $c = 1$ then $\mathcal{O}^t$ returns session key SK_{ij}. Otherwise, in case of $c = 0$, then it returns a null value ($\perp$). Here it is important to mention that $\mathcal{A}$ can perform the execution of an unlimited number of $\mathcal{T}$ $(\mathcal{O}^t)$ queries.

- **Semantic security:** Semantic security of session key SK_{ij} is another important parameter. The semantic security of session key ψ_{PS_j,IMD_i} $(= \psi_{IMD_i,PS_j})$, which is established in between IMD_i and PS_j is analysed through ROR model. It depends on the adversary $\mathcal{A}$'s capabilities to discover the difference between the real session key and a random number. The result of $\mathcal{T}$ $(\mathcal{O}^t)$ query should be compatible with random bit c. Let say $\mathcal{A}$ guesses c' bit. If *Succ* is the expression of winning probability, the advantage of $\mathcal{A}$ in breaking the semantic security of ψ_{PS_j,IMD_i} $(= \psi_{IMD_i,PS_j})$ of ASCP-IoMT is given by $Adv_{\mathcal{A}}^{ASCP-IoMT} = |2.Pr[Succ]-1|$, where the probability of an event X is $Pr[X]$.
- **Random oracle:** In proposed ASCP-IoMT cryptographic one-way hash function $h(\cdot)$ is utilized. It is executed like a random oracle, i.e., *Hash* value of $h(\cdot)$ is public. In which all participants including $\mathcal{A}$, are able to access the *Hash* oracle.

Theorem 2: Suppose a probabilistic polynomial time (PPT) adversary $\mathcal{A}$ exists which runs in polynomial time t_p and attempts to obtain the session key ψ_{PS_j,IMD_i} $(= \psi_{IMD_i,PS_j})$ between an IMD device IMD_i and its associated personal server PS_j during the AKE phase of the proposed scheme (ASCP-IoMT). Let q_h and $|Hash|$ represent the number of Hash queries and the range space of a one-way collision-resistant hash function $h(\cdot)$, respectively. Then, the advantage of $\mathcal{A}$ denoted by $Adv_{\mathcal{A}}^{ASCP-IoMT}$, in breaking the semantic security of the ASCP-IoMT for deriving the session key ψ_{PS_j,IMD_i} $(= \psi_{IMD_i,PS_j})$ is $Adv_{\mathcal{A}}^{ASCP-IoMT} \leq \frac{q_h^2}{|Hash|}$.

Proof: In this proof, the four games $Gm_j, j \in [0, 3]$ are considered. The event is formulated in which $\mathcal{A}$ can guess the random bit c in the Gm_j correctly and its success probability can be written as $Succ_{\mathcal{A}}^{Gm_j}$. The advantage of $\mathcal{A}$ to win a game Gm_j is written as $Adv_{\mathcal{A},Gm_j}^{ASCP-IoMT} = Pr[Succ_{\mathcal{A}}^{Gm_j}]$.

Game Gm_0: This game is executed initially. It is the identical game with an actual scheme running under the fundamentals of ROR model. Under such assumptions following equation can be achieved:

$$Adv_{\mathcal{A}}^{ASCP-IoMT} = |2.Adv_{\mathcal{A},Gm_0}^{ASCP-IoMT} - 1|. \tag{1}$$

Game Gm_1: Game Gm_1 simulates the eavesdropping attack. In Gm_1 query, $\mathcal{E}$ is executed. Further, $\mathcal{A}$ performs the execution of query $\mathcal{T}$ at the end of this game. $\mathcal{A}$'s task is to the inequality of session key SK_{ij} and a random number when the output of query $\mathcal{T}$ is received. In proposed ASCP-IoMT, session key established by IMD_i and PS_j is $\psi_{PS_j,IMD_i} = h(h(rn_2||RID_{PS_j})||\ RID_{IMD_i}||\ TC_{IMD_i}||\ rn_1||\ TS_1||\ TS_2)$. In the calculation of session key both "long term secrets, i.e., secret keys and identities, as well as the short term secrets, i.e., freshly generated timestamp values and random secret values" are utilized. Hence through the eavesdropping of messages MSG_1, MSG_2 and MSG_3, winning probability of the game Gm_1 does not change and is not again helping in the computation of session key SK_{ij}. According to the "indistinguishability of Gm_0 and Gm_1" we can achieve:

$$Adv_{\mathcal{A},Gm_1}^{ASCP-IoMT} = Adv_{\mathcal{A},Gm_0}^{ASCP-IoMT} \tag{2}$$

Game Gm_2: This game simulates another active attack (other active attacks). Here $\mathcal{A}$ does the simulation of $\mathcal{S}$ and *Hash* queries to misguide the communicating entity to obtain the fake messages. $\mathcal{A}$ does exercises with some *Hash* queries to find out the collision in hash outcomes for MSG_1, MSG_2, and MSG_3 messages. For the estimation of these messages, we use both long term secrets, i.e., secret keys and identities as well as short term secrets, i.e., freshly generated timestamp values and random secret values, which produce distinct messages for distinct sessions. However, if $\mathcal{A}$ launches several $\mathcal{S}$ queries, then again he/ she does not have the capability to find out any collision in the outputs of hash. Therefore, with the birthday paradox following result is achieved:

$$|Adv_{\mathcal{A},Gm_1}^{ASCP-IoMT} - Adv_{\mathcal{A},Gm_2}^{ASCP-IoMT}| \leq \frac{q_h^2}{2|Hash|}. \tag{3}$$

After execution of these queries, $\mathcal{A}$ needs to guess the correct bit c. It then follows that

$$Adv_{\mathcal{A},Gm_2}^{ASCP-IoMT} = \frac{1}{2}. \tag{4}$$

Using Eqs. (1) and (2), subsequent result is produced:

$$\begin{aligned} \frac{1}{2}.Adv_{\mathcal{A}}^{ASCP-IoMT} &= |Adv_{\mathcal{A},Gm_0}^{ASCP-IoMT} - \frac{1}{2}| \\ &= |Adv_{\mathcal{A},Gm_1}^{ASCP-IoMT} - \frac{1}{2}| \\ &= |Adv_{\mathcal{A},Gm_1}^{ASCP-IoMT} \\ &\quad - Adv_{\mathcal{A},Gm_2}^{ASCP-IoMT}| \end{aligned} \tag{5}$$

The "triangular inequality" and Eqs. (3) and (5) provide subsequent result:

$$\frac{1}{2}.Adv_{\mathcal{A}}^{ASCP-IoMT} = |Adv_{\mathcal{A},Gm_1}^{ASCP-IoMT}$$

$$\begin{aligned} & - Adv^{ASCP-IoMT}_{\mathcal{A},Gm_2}| \\ \leq\ & |Adv^{ASCP-IoMT}_{\mathcal{A},Gm_1} \\ & - Adv^{ASCP-IoMT}_{\mathcal{A},Gm_2}| \\ \leq\ & \frac{q_h^2}{2|Hash|} \end{aligned} \tag{6}$$

Finally, if we multiply both sides of Eq. (6) with a factor of 2, then the desired result is achieved: $Adv^{ASCP-IoMT}_{\mathcal{A}} \leq \frac{q_h^2}{|Hash|}$. □

VI. COMPARATIVE STUDY

The comparative study of ASCP-IoMT and other related existing schemes like Merabet *et al.* [15], Jang *et al.* [13] and He-Zeadally [14] is conducted for the comparisons of computation costs, communication costs and security and functionality features. The rough estimated time for different cryptographic can be obtained as per the scenarios given in [30]. The approximate computation time (seconds) for various operations, i.e., "One-way hash function T_h", "ECC point multiplication T_{ecm} ", "ECC point addition T_{eca}", "Symmetric key encryption T_{senc}", "Symmetric key decryption T_{sdec}", "Modular exponentiation T_{me}", "Fuzzy extractor function T_{fe} " are 0.00032, 0.0171, 0.0044, 0.0056, 0.0056, 0.0192 and 0.0171 [30].

TABLE 2. Comparison of various computation costs.

Scheme	Computation cost (in milliseconds)
Jang *et al.* [13]	$25T_{ecm} + 15T_{eca} + 5T_h \approx 495.10$ ms
He-Zeadally [14]	$4T_h$ $+8T_{senc}$ $+6T_{ecm} \approx 148.68$ ms
Merabet *et al.* [15] (Protocol-I)	$6T_{ecm} + 6T_h + T_{eca} \approx 108.92$ ms
Merabet *et al.* [15] (Protocol-II)	$4T_{ecm} + 4T_h \approx 69.68$ ms
ASCP-IoMT	$15T_h \approx 4.80$ ms

TABLE 3. Comparison of various communication costs.

Scheme	No. of messages	No. of bits
Jang *et al.* [13]	8	5920
He-Zeadally [14]	4	2944
Merabet *et al.* [15] (Protocol-I)	3	1472
Merabet *et al.* [15] (Protocol-II)	3	1472
ASCP-IoMT	3	1792

Table 2 has the comparison of computational costs of proposed ASCP-IoMT and other similar techniques. The computation cost for the scheme of Jang *et al.* [13] is calculated as $25T_{ecm} + 15T_{eca} + 5T_h \approx$ 495.10 ms. In case of scheme of Merabet *et al.* [15] (in Protocol-I), it is calculated as $6T_{ecm} + 6T_h + T_{eca}$ $\approx$ 108.92 ms and for their second protocol, i.e., Protocol-II it is calculated as $4T_{ecm} + 4T_h \approx$ 69.68 ms. Again for the scheme of He-Zeadally [14] as $4T_h$ $+8T_{senc}$ $+6T_{ecm}$ $\approx$ 148.68 ms. However, for ASCP-IoMT, it is calculated as $15T_h \approx 4.80$ ms. During the analysis, we have identified that ASCP-IoMT requires low computational cost as compared to the other similar techniques, i.e., Jang *et al.*' scheme [13], Merabet *et al.*' scheme [15] and He-Zeadally's scheme [14].

Further, Table 3 has the comparison of communication costs of ASCP-IoMT and other similar techniques. It is under the assumption that size of identity, a timestamp, a random number (nonce) and a hash output (if SHA-256 hashing algorithm is applied) are 160 bits, 32 bits, 160 bits and 256 bits, respectively. Entities in ASCP-IoMT communicates via three different messages, which are of sizes 704 bits, 800 bits and 288 bits. Therefore, the final communication cost of ASCP-IoMT is computed as 704 +800 +288 = 1792 bits.

During the analysis, we have identified that proposed ASCP-IoMT requires less communication cost as compared to Jang *et al.*' scheme [13] and He-Zeadally' scheme [14]. Though the communication cost of ASCP-IoMT is little higher than Merabet *et al.*' scheme but it can be accepted as ASCP-IoMT provides higher security and more functionality features.

In Table 4, a comparison of security and functionality features among ASCP-IoMT and other techniques against the best recognized security and functionality features is provided. From the conducted analysis, it has been observed that ASCP-IoMT provides better security with additional functionality features as compared to the techniques of Jang *et al.* [13], Merabet *et al.* [15] and He-Zeadally [14].

TABLE 4. Security and functionality attributes comparison.

Feature	Merabet *et al.* [15]	Jang *et al.* [13]	He-Zeadally [14]	Proposed ASCP-IoMT
ψf_1	✓	✓	✓	✓
ψf_2	✓	×	✓	✓
ψf_3	✓	✓	✓	✓
ψf_4	✓	✓	✓	✓
ψf_5	×	✓	✓	✓
ψf_6	✓	✓	✓	✓
ψf_7	✓	✓	✓	✓
ψf_8	×	✓	✓	✓
ψf_9	✓	✓	✓	✓
ψf_{10}	×	×	×	✓
ψf_{11}	✓	✓	✓	✓
ψf_{12}	×	×	×	✓
ψf_{13}	×	×	×	✓
ψf_{14}	✓	×	×	✓

Note: ψf_1: "mutual authentication/access control"; ψf_2: "anonymity"; ψf_3: "untraceability"; ψf_4: "session-key agreement"; ψf_5: "session key security under CK adversary model"; ψf_6: "confidentiality"; ψf_7: "integrity"; ψf_8: "strong replay attack"; ψf_9: "man-in-the-middle attack"; ψf_{10}: "dynamic IMD addition"; ψf_{11}: "protection against impersonation attack"; ψf_{12}: "AI-enabled big data analytics phase"; ψf_{13}: "key revocation phase"; ψf_{14}: "practical impelmentaion".

×: "a scheme is insecure against a particular attack or it does not support a particular feature"; ✓: "a scheme is secure against a particular attack or supports a particular feature"; N/A: "not applicable in a scheme".

VII. PRACTICAL IMPLEMENTATION

In this section, we provide the details of the practical implementation of the proposed ASCP-IoMT. It is conducted in two ways, firstly, we implement proposed ASCP-IoMT using the widely used widely-used NS2 2.35 simulation software tool [31] for measuring the impact of authentication and key establishment procedure on the performance of important performance parameters, i.e., end-to-end delay, throughput and packet loss rate. After that, we simulate "AI-based big data analytics phase" of proposed ASCP-IoMT. As it is important to find out the performance of various machine learning techniques for the considered scenarios in ASCP-IoMT.

A. DETAILS OF NS2 SIMULATION STUDY

NS2-based simulations are desirable for measuring the impact of newly designed scheme on the performance network parameters. This tool is among the popular simulation tools, which are used to measure the network performance parameters in different types of networks. The simulations of various protocols, i.e., Transmission Control Protocol (TCP)/ User Datagram Protocol (UDP), wireless body area network (WBAN), routing protocols and multicast protocols can be performed through NS2. In Table 5, we provide the details of various parameters, which are used during the NS2 simulation. Ubuntu 18.04 LTS platform was used to perform the simulation through the NS2 2.35 simulation tool. The wireless protocol IEEE 802.15.4 was chosen to perform the simulation. Three different cases are taken in the simulation. We consider one, two and three personal servers for Case-1, Case-2, and Case-3, respectively. The number of IMDs is considered as 5 (in Case 1) 10 (in Case 2) and 15 (in Case 3). We have taken 1800 seconds as the simulation time. The communication ranges of IMD and personal server are considered as 25 and 100 meters, respectively. "Ad-hoc on-demand distance vector routing (AODV)" [32] designed by Perkins and Royer is taken as the routing protocol. The other associated parameters are taken with the standard values.

TABLE 5. NS2 simulation parameters and their values.

Parameter	Description
Platform	Ubuntu 18.04 LTS
Simulation tool	NS2 2.35
Wireless protocol	802.15.4
Number of personal servers	01 (Case-1), 02 (Case-2), 03 (Case-3)
Number of IMDs	05 (Case-1), 10 (Case-2), 15 (Case-2)
Simulation time	1800 seconds
Communication range of IMDs	25 meters
Communication range of personal server	100 meters
Routing protocol	AODV [32]

The communication costs (bits) of messages exchanged among various entities are calculated with the following details. In the "authentication and key establishement" procedure of IMD_i and PS_j, we have the following messages exchanged:

- The message $< MSG_1 = TID_{IMD_i}, M_1, M_2, TS_1 >$ from IMD_i to PS_j requires = 704 bits.
- The message $< MSG_2 = M_3, M_4, M_5, TS_2 >$ from PS_j to IMD_i requires = 800 bits.
- The message $< MSG_3 = M_6, TS_3 >$ from IMD_i to PS_j requires = 288 bits.

B. DISCUSSION ON NS2 SIMULATION OUTCOMES

In the experimentation, network performance parameters like, end-to-end delay (in seconds), throughput (in bits per second) and packet loss rate are computed.

1) IMPACT ON END-TO-END DELAY

End-to-End Delay (*EED*) is the average time needed by the messages to reach the destination from the source point. In an authentication and key establishment procedure, it is essentially required to compute the value of *EED*, as it gives the rough estimate of time required to complete the authentication and key establishment procedure for various communicating entities, i.e., IMS_i and PS_j. In case of an efficient authentication and key establishment scheme the value of *EED* should be as less as possible. The *EED* values for the proposed ASCP-IoMT for different considered cases (for example, Case-1, Case-2, Case-3) are given in Figure 4. The *EED* values are 0.01587, 0.07440 and 0.17097 seconds for Case-1, Case-2 and Case-3, respectively. Here it is important to discuss that the value of *EED* increases with the increasing number of *IMD* and *PS* devices as it causes the increment in the number of exchanged messages. Therefore, *EED* increases accordingly from Case-1 to Case-2 and Case-2 to Case-3.

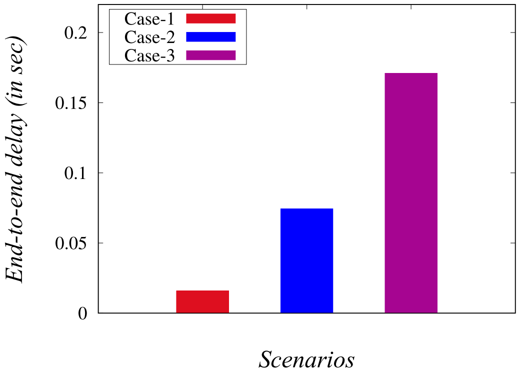

FIGURE 4. End-to-end delay (in seconds) in various scenarios.

2) IMPACT ON THROUGHPUT

Throughput is also an important network performance parameter. It is the estimation of number of bits transmitted per unit of time. The Throughput values of ASCP-IoMT for various considered cases are given in Figure 5. The throughput values of ASCP-IoMT are 5.05, 10.88 and 16.41 *bps* for Case-1, Case-2 and Case-3, receptively. Here it is important to discuss that the value of the throughput increases with the increasing number of *IMD* and *PS* devices as it causes the increment in the number of exchanged messages. Therefore, network throughput increases accordingly from Case-1 to Case-2 and Case-2 to Case-3.

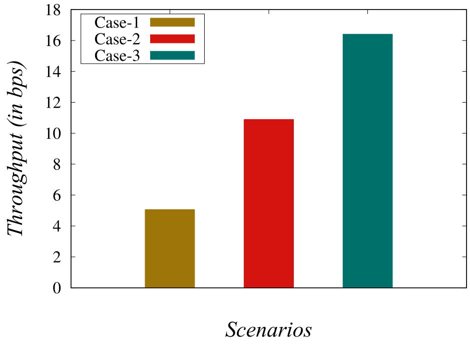

FIGURE 5. Throughput (in bps) in various scenarios.

3) IMPACT ON PACKET LOSS RATE

For a reliable communication scheme, it is desirable to estimate the value of the packet loss rate. The packet loss rate is the estimation of number of packets loss per unit time. It is the total number of lost packets for a given duration of time. An authentication and key establishment scheme is treated as reliable if it has less packet loss rate. The packet loss rates of ASCP-IoMT for various considered cases are given in Figure 6. The values of packet loss rate of ASCP-IoMT are 0.00166, 0.00222 and 0.00333 for Case-1, Case-2 and Case-3, respectively. Here it is important to discuss that the value of "Packet loss rate" increases with the increasing number of *IMD* and *PS* devices as it causes the increment in the number of exchanged messages. That again causes traffic congestion, and therefore, packet loss rate also increases from Case-1 to Case-2 and Case-2 to Case-3. However, the increased value of packet loss rate is marginal as ASCP-IoMT is designed with lightweight cryptographic techniques.

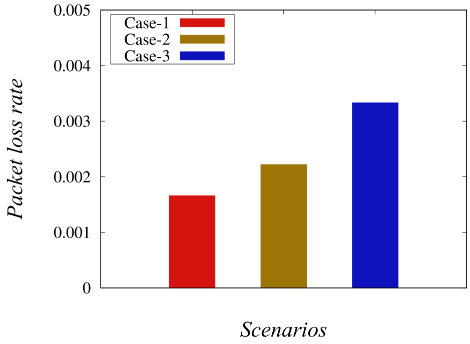

FIGURE 6. Packet loss rate in various scenarios.

C. SIMULATION STUDY ON AI-BASED BIG DATA ANALYTICS

We have simulated the AI-based big data analytics phase of ASCP-IoMT. As it is essential to find out the performance of various machine learning techniques for the considered scenarios in ASCP-IoMT. The dataset of "Heart Disease Dataset", which is available on the IEEE Dataport [33] are utilized for this work. This database is taken because it can be used for machine learning and data mining techniques for diagnosis of coronary artery disease. In this dataset, there are five heart datasets that are combined over eleven common features. The required steps of AI-based big data analytics can be executed at the authorized cloud server (say CS_k).

The following simulation environment and settings were considered. The simulation environment of "AI-based big data analytics phase" is set up as follows.

- **Platform set up:** $i5$ with 11^{th} generation processor is considered for the implementation. 8 GB RAM size with 2 GB Nvidia MX 450 Graphic Card is taken.
- **Deployed tools and libraries:** Google colab platform (environment) is considered. The different libraries, like, "pandas is used to import and read data in tabular form", "seaborne and matplotlib is used to visualize data" and "scikit learn was used to pre-process data and perform machine learning".
- **Data:** The dataset, which is used, is taken from IEEE Dataport [33]. This dataset has medical details of 1190 patients, which have their details recorded. They may or may not have heart-related disease. The dataset has various attributes, like, age, sex, chest pain type (ranging from 1 to 4), resting bp, cholesterol levels, resting ECG level, whether that patient has got heart disease or not. The dataset is prepared for the machine learning process by splitting the data in 70%- 30% for training and testing tasks. After that, the implementation of various models to classify and predict the possibility of "getting a heart attack" is done.
- **Used machine learning algorithms:** The machine learning algorithms like, decision tree, support vector machine (SVM), and logistic regression, which are closely associated with this task, are considered. The summary of these algorithms is given below.
- **Decision tree algorithm:** The decision tree algorithm is a supervised learning technique, which is used to solve problems like classification and regression. It is, nonetheless, preferred for classification problems. In this algorithm, the internal nodes represent dataset attributes, branches represent decision rules, and each leaf node provides the outcome in this tree-structured classifier. The decision node and the leaf node are the two sorts of nodes. The decision nodes are used to make any decision and have numerous branches, whereas the leaf nodes are the decisions' outputs and do not have any more branches. The decisions are made based on the characteristics of the dataset [34].
- **Support vector machine:** Support vector machine (SVM) is very popular supervised learning algorithm. Usually, people prefer to use SVM as it generates great accuracy while using less computing power. SVM can be used for regression as well as classification. However, it is widely used in classification tasks. The goal of the SVM algorithm is to find a hyperplane in an N-dimensional space that classify data points clearly. The hyperplane's size is determined by the number of

features. If there are only two input features, the hyperplane is merely a line. When the number of input features reaches three, the hyperplane transforms into a two-dimensional plane. If the number of input features is three, then the hyperplane becomes a 2-D plane. However, it becomes difficult to imagine when the number of features exceeds three. The hyperplane is the optimal decision boundary in SVM. SVM chooses the extreme points or vectors, which further help in creating the hyperplane. These extreme cases are refers as the support vectors [35], [36].

- **Logistic regression:** Logistic regression is a supervised learning classification algorithm used to predict the probability of a target variable. In this algorithm, the nature of target (dependent variable) is dichotomous. It indicates that there would be only two possible classes. For example, the dependent variable is binary in nature having data coded as either 1 (i.e., in case of success or yes) or 0 (i.e., in case of failure or no). It is one of the simplest machine learning algorithms, which is used for various classification problems for example, cancer detection, spam detection, etc., [37].

During the implementation and analysis following results are obtained.

1) COMPUTATION TIME

It is the time, which is required for a particular model to predict about something. For a "good prediction system," its value should be as less as possible. The values of computation time (seconds) for decision tree, support vector machine (SVM), and logistic regression are 0.19, 0.23, and 0.27, respectively. Hence, it is clear that decision tree method has taken the lesser time than the other considered techniques. The different values of computation time under different techniques are given in Figure 7.

2) ACCURACY

It is one of the important matrices, it is the measure of all the correctly identified cases. For a "good prediction system," its value should be as high as possible. We have computed the accuracy of "getting a heart attack" for the various considered techniques. The different values of accuracy for decision tree, support vector machine (SVM) and logistic regression are 84.24%, 87.57%, and 85.20%, respectively. From these values, it is clear that accuracy is high in case of SVM. The different values of accuracy under different techniques are given in Figure 8.

From the obtained results, it has been clear that the performance of SVM is better than other techniques as it achieves high accuracy with less computation time (refer Figure 7 and Figure 8).

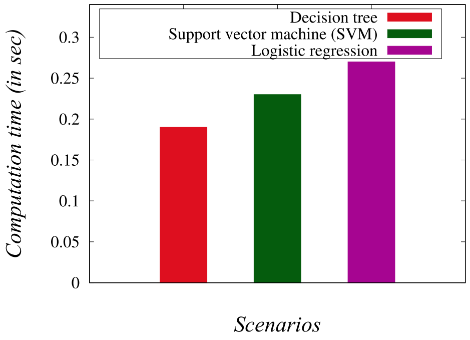

FIGURE 7. Computation time (in seconds) under various scenarios.

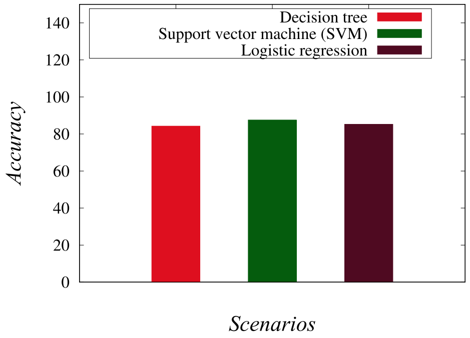

FIGURE 8. Accuracy under various scenarios.

VIII. CONCLUSION

An IoMT environment suffers from different security and privacy related issues because it can be attacked through various methods. Under the presence of these attacks, the sensitive health data can be leaked or altered. Therefore, we need a strong security mechanism to mitigate these attacks in IoMT. Hence, a new AI-enabled secure communication protocol for an IoMT environment has been presented. The discussed network and threat models of the proposed ASCP-IoMT provided the details of the arrangements of various network devices and the associated attacks of the IoMT. The conducted security analysis proved the security of ASCP-IoMT against various potential attacks. During the comparative performance analysis, it has been observed that the proposed ASCP-IoMT provides better security with additional functionality features as compared to existing similar techniques. The pragmatic study of ASCP-IoMT was then provided to find out ASCP-IoMT's influence on the considered parameters. In future, we would like to add more functionality features (i.e., Blockchain) to the presented scheme.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the associate editor for providing their valuable suggestions and comments which helped us to improve the paper significantly.

REFERENCES

[1] X. Yang, L. Guan, Y. Li, W. Wang, Q. Zhang, M. U. Rehman, and Q. H. Abbasi, "Contactless finger tapping detection at C-band," *IEEE Sensors J.*, vol. 21, no. 4, pp. 5249–5258, Feb. 2021.

[2] J. Kim, "Energy-efficient dynamic packet downloading for medical IoT platforms," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1653–1659, Dec. 2015.

[3] F. Al-Turjman, M. H. Nawaz, and U. D. Ulusar, ''Intelligence in the Internet of Medical Things era: A systematic review of current and future trends,'' *Comput. Commun.*, vol. 150, pp. 644–660, Jan. 2020.

[4] M. Wazid, B. Bera, A. Mitra, A. K. Das, and R. Ali, ''Private blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services,'' in *Proc. 2nd ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond (DroneCom)*, London, U.K., Sep. 2020, pp. 37–42.

[5] X. Yang, D. Fan, A. Ren, N. Zhao, and M. Alam, ''5G-based user-centric sensing at C-band,'' *IEEE Trans. Ind. Informat.*, vol. 15, no. 5, pp. 3040–3047, May 2019.

[6] Y. Kumar, A. Koul, R. Singla, and M. F. Ijaz, ''Artificial intelligence in disease diagnosis: A systematic literature review, synthesizing framework and future research agenda,'' *J. Ambient Intell. Humanized Comput.*, pp. 1–28, Jan. 2022, doi: 10.1007/s12652-021-03612-z.

[7] P. N. Srinivasu, J. G. Sivasai, M. F. Ijaz, A. K. Bhoi, W. Kim, and J. J. Kang, ''Classification of skin disease using deep learning neural networks with MobileNet v2 and LSTM,'' *Sensors*, vol. 21, no. 8, p. 2852, Apr. 2021.

[8] S. Dash, S. Verma, Kavita, S. Bevinakoppa, M. Wozniak, J. Shafi, and M. F. Ijaz, ''Guidance image-based enhanced matched filter with modified thresholding for blood vessel extraction,'' *Symmetry*, vol. 14, no. 2, p. 194, Jan. 2022.

[9] C. Camara, P. Peris-Lopez, and J. E. Tapiador, ''Security and privacy issues in implantable medical devices: A comprehensive survey,'' *J. Biomed. Inform.*, vol. 55, pp. 272–289, Jun. 2015.

[10] M.-D. Cano and A. Cañavate-Sanchez, ''Preserving data privacy in the Internet of Medical Things using dual signature ECDSA,'' *Secur. Commun. Netw.*, vol. 2020, pp. 1–9, Jun. 2020.

[11] X. Wang, L. Wang, Y. Li, and K. Gai, ''Privacy-aware efficient fine-grained data access control in Internet of Medical Things based fog computing,'' *IEEE Access*, vol. 6, pp. 47657–47665, 2018.

[12] F. Alsubaei, A. Abuhussein, V. Shandilya, and S. Shiva, ''IoMT-SAF: Internet of Medical Things security assessment framework,'' *Internet Things*, vol. 8, Dec. 2019, Art. no. 100123.

[13] C. S. Jang, D. G. Lee, J.-W. Han, and J. H. Park, ''Hybrid security protocol for wireless body area networks,'' *Wireless Commun. Mobile Comput.*, vol. 11, no. 2, pp. 277–288, Feb. 2011.

[14] D. He and S. Zeadally, ''Authentication protocol for an ambient assisted living system,'' *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 71–77, Jan. 2015.

[15] F. Merabet, A. Cherif, M. Belkadi, O. Blazy, E. Conchon, and D. Sauveron, ''New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications,'' *Peer-Peer Netw. Appl.*, vol. 13, no. 2, pp. 439–474, Mar. 2020.

[16] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, ''Internet of Things (IoT) communication protocols: Review,'' in *Proc. 8th Int. Conf. Inf. Technol. (ICIT)*, Amman, Jordan, May 2017, pp. 685–690.

[17] K. Sha, T. A. Yang, W. Wei, and S. Davari, ''A survey of edge computing-based designs for IoT security,'' *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 195–202, 2020.

[18] Y. Zhen and H. Liu, ''Distributed privacy protection strategy for MEC enhanced wireless body area networks,'' *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 229–237, May 2020.

[19] D. Dolev and A. C. Yao, ''On the security of public key protocols,'' *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[20] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, ''Examining smart-card security under the threat of power analysis attacks,'' *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[21] D. Chattaraj, B. Bera, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, ''Designing fine-grained access control for software-defined networks using private blockchain,'' *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1542–1559, Jan. 2022.

[22] A. K. Das and B. Bruhadeshwar, ''An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system,'' *J. Med. Syst.*, vol. 37, no. 5, pp. 1–17, 2013.

[23] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K. R. Choo, and Y. Park, ''Certificateless-signcryption-based three-factor user access control scheme for IoT environment,'' *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3184–3197, Apr. 2020.

[24] S. Malani, J. Srinivas, A. K. Das, K. Srinathan, and M. Jo, ''Certificate-based anonymous device access control scheme for IoT environment,'' *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9762–9773, Dec. 2019.

[25] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park, ''Provably secure ECC-based device access control and key agreement protocol for IoT environment,'' *IEEE Access*, vol. 7, pp. 55382–55397, 2019.

[26] M. F. Ijaz, M. Attique, and Y. Son, ''Data-driven cervical cancer prediction model with outlier detection and over-sampling methods,'' *Sensors*, vol. 20, no. 10, pp. 1–22, 2020.

[27] M. Mandal, P. K. Singh, M. F. Ijaz, J. Shafi, and R. Sarkar, ''A tri-stage wrapper-filter feature selection framework for disease classification,'' *Sensors*, vol. 21, no. 16, pp. 1–24, 2021.

[28] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ''DDoS in the IoT: Mirai and other botnets,'' *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[29] M. Abdalla, P. A. Fouque, and D. Pointcheval, ''Password-based authenticated key exchange in the three-party setting,'' in *Proc. 8th Int. Workshop Theory Pract. Public Key Cryptogr. (PKC)*, in Lecture Notes in Computer Science, Les Diablerets, Switzerland, vol. 3386, 2005, pp. 65–84.

[30] D. He, N. Kumar, J.-H. Lee, and R. S. Sherratt, ''Enhanced three-factor security protocol for consumer USB mass storage devices,'' *IEEE Trans. Consum. Electron.*, vol. 60, no. 1, pp. 30–37, Feb. 2014.

[31] *The Network Simulator-ns-2*. Accessed: Mar. 2021. [Online]. Available: http://www.isi.edu/nsnam/ns/

[32] C. E. Perkins and E. M. Royer, ''Ad-hoc on-demand distance vector routing,'' in *Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl. (WMCSA)*, New Orleans, LA, USA, Feb. 1999, pp. 90–100.

[33] M. Siddhartha, ''Heart disease dataset (comprehensive),'' Liverpool John Moores Univ., Liverpool, U.K., Tech. Rep., 2020, doi: 10.21227/dz4t-cm36.

[34] J. Ye, J. Yang, J. Yu, S. Tan, F. Luo, Z. Yuan, and Y. Chen, ''A chi-MIC based adaptive multi-branch decision tree,'' *IEEE Access*, vol. 9, pp. 78962–78972, 2021.

[35] A. R. Subhani, W. Mumtaz, M. N. B. M. Saad, N. Kamel, and A. S. Malik, ''Machine learning framework for the detection of mental stress at multiple levels,'' *IEEE Access*, vol. 5, pp. 13545–13556, 2017.

[36] F. Borges, A. Pinto, D. Ribeiro, T. Barbosa, D. Pereira, R. Magalháes, B. Barbosa, and D. Ferreira, ''An unsupervised method based on support vector machines and higher-order statistics for mechanical faults detection,'' *IEEE Latin Amer. Trans.*, vol. 18, no. 6, pp. 1093–1101, Jun. 2020.

[37] L. Liu, ''Research on logistic regression algorithm of breast cancer diagnose data by machine learning,'' in *Proc. Int. Conf. Robots Intell. Syst. (ICRIS)*, Changsha, China, May 2018, pp. 157–160.

MOHAMMAD WAZID (Senior Member, IEEE) received the M.Tech. degree in computer network engineering from Graphic Era deemed to be University, Dehradun, India, and the Ph.D. degree in computer science and engineering from the International Institute of Information Technology, Hyderabad, India. He is currently working as an Associate Professor with the Department of Computer Science and Engineering, Graphic Era deemed to be University, where he is also the Head of the ''Cyber Security and IoT Research Group.'' Prior to this, he was worked as an Assistant Professor with the Department of Computer Science and Engineering, Manipal Institute of Technology, MAHE, Manipal, India. He was also a Postdoctoral Researcher with the Cyber Security and Networks Laboratory, Innopolis University, Innopolis, Russia. He has published more than 100 papers in international journals and conferences in the above areas. His current research interests include information security, remote user authentication, the Internet of Things (IoT), cloud/fog/edge computing, and blockchain. Some of his research findings are published in top cited journals, such as the IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Smart Grid, IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, IEEE Journal of Biomedical and Health Informatics (formerly IEEE Transactions on Information Technology in Biomedicine), *IEEE Consumer Electronics Magazine*, IEEE Access, *Future Generation Computer Systems* (Elsevier), *Computers & Electrical Engineering* (Elsevier), *Computer Methods and Programs in Biomedicine* (Elsevier), *Security and Communication Networks* (Wiley), and *Journal of Network and Computer Applications* (Elsevier). He has also served as a program committee member for many international conferences. He was a recipient of the University Gold Medal and the Young Scientist Award by UCOST, Department of Science and Technology, Government of Uttarakhand, India. He has received Dr. A. P. J. Abdul Kalam Award for his innovative research works. He has also received *ICT Express* (Elsevier) journal ''Best Reviewer'' Award, in 2019.

JASKARAN SINGH (Student Member, IEEE) is currently pursuing the Bachelor of Technology degree in computer science and engineering with specialization in data science with the Department of Computer Science and Engineering, Graphic Era Deemed to be University Dehradun, India. His research interests include machine learning, data science, machine learning security, and intrusion detection systems.

ASHOK KUMAR DAS (Senior Member, IEEE) received the M.Tech. degree in computer science and data processing, the M.Sc. degree in mathematics from IIT Kharagpur, India, and the Ph.D. degree in computer science and engineering. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India, and also a Visiting Faculty with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA, USA. He has authored over 300 papers in international journals and conferences in the above areas, including over 260 reputed journal articles. His Scholar H-index is 65 and i10-index is 66 and 192 with over 12,400 citations. His current research interests include cryptography, system and network security, including security in smart grid, the Internet of Things (IoT), internet of drones (IoD), internet of vehicles (IoV), cyber-physical systems (CPS) and cloud computing, intrusion detection, blockchain, and AI/ML security. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He was/is on the Editorial Board of IEEE Systems Journal, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *Journal of Cloud Computing* (Springer), *Cyber Security and Applications* (Elsevier), *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience). He has served as a program committee member for many international conferences. He also served as one of the Technical Program Committee Chair of the First International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, in June 2019, and Second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, in October 2020.

SACHIN SHETTY (Senior Member, IEEE) received the Ph.D. degree in modeling and simulation from Old Dominion University, in 2007. He was an Associate Professor with the Electrical and Computer Engineering Department, Tennessee State University, USA. He is currently an Associate Professor with the Virginia Modeling, Analysis, and Simulation Center, Old Dominion University. He holds a joint appointment with the Department of Modeling, Simulation and Visualization Engineering and the Center for Cybersecurity Education and Research. He has authored and coauthored over 125 research papers in journals and conference proceedings and two books. His research interests include the intersection of computer networking, network security, and machine learning. He was a recipient of the DHS Scientific Leadership Award. He has served on the Technical Program Committee for ACM CCS, IEEE INFOCOM, IEEE ICDCN, and IEEE ICCCN.

MUHAMMAD KHURRAM KHAN (Senior Member, IEEE) is currently working as a Professor in cybersecurity with the Center of Excellence in Information Assurance, King Saud University, Saudi Arabia. He is also the Founder and the CEO of the "Global Foundation for Cyber Studies and Research" (http://www.gfcyber.org), an independent, and non-partisan cybersecurity think-tank in Washington D.C., USA. He has published more than 450 papers in the journals and conferences of international repute. In addition, he is an Inventor of ten US/PCT patents. He has edited ten books/proceedings published by Springer-Verlag, Taylor & Francis, and IEEE. His research interests include cybersecurity, digital authentication, IoT security, biometrics, multimedia security, cloud computing security, cyber policy, and technological innovation management. He is a fellow of the IET (U.K.), BCS (U.K.), and FTRA (South Korea). He is the Vice Chair of IEEE Communications Society Saudi Chapter. He is a Distinguished Lecturer of the IEEE. He is the Editor-in-Chief of *Telecommunication Systems* (Springer-Nature) with its recent impact factor of 2.314 (JCR 2021). He is on the editorial board of several journals, including, IEEE Communications Surveys and Tutorials, *IEEE Communications Magazine*, IEEE Internet of Things Journal, IEEE Transactions on Consumer Electronics, *Journal of Network & Computer Applications* (Elsevier), IEEE Access, *IEEE Consumer Electronics Magazine*, *PLOS One*, and *Electronic Commerce Research*. His detailed profile can be visited at (http://www.professorkhurram.com).

JOEL J. P. C. RODRIGUES (Fellow, IEEE) is currently with the College of Computer Science and Technology, China University of Petroleum, Qingdao, China, and a Senior Researcher with the Instituto de Telecomunicações, Portugal. He has authored or coauthored over 1000 papers in refereed international journals and conferences, three books, two patents, and one ITU-T Recommendation. He is also the Leader of the Next Generation Networks and Applications Research Group (CNPq), the Director for Conference Development—IEEE ComSoc Board of Governors, an IEEE Distinguished Lecturer, the Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the President of the Scientific Council at ParkUrbis—Covilhã Science and Technology Park, a Past-Chair of the IEEE ComSoc Technical Committee on eHealth, a Past-Chair of the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee Member of the IEEE Life Sciences Technical Community, the Publications Co-Chair, and a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He is a member of the Internet Society and a Senior Member of ACM. He has been the general chair and the TPC chair of many international conferences, including IEEE ICC, IEEE GLOBECOM, IEEE HEALTHCOM, and IEEE LatinCom. He had been awarded several outstanding leadership and outstanding service awards by IEEE Communications Society and several best papers awards. He is the Editor-in-Chief of the *International Journal on E-Health and Medical Communications* and an editorial board member of several high-reputed journals.

• • •