2022

Healthcare 5.0 Security Framework: Applications, Issues and Future Research Directions

Mohammad Wazid

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

Noor Mohd

Youngho Park

Original Publication Citation

Wazid, M., Das, A. K., Mohd, N., & Park, Y. (2022). Healthcare 5.0 security framework: Applications, issues and future research directions. *IEEE Access*, *10*, 129429-129442. https://doi.org/10.1109/ACCESS.2022.3228505

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 November 2022, accepted 7 December 2022, date of publication 12 December 2022,
date of current version 15 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3228505

RESEARCH ARTICLE

Healthcare 5.0 Security Framework: Applications, Issues and Future Research Directions

MOHAMMAD WAZID[1], (Senior Member, IEEE), ASHOK KUMAR DAS[2,3], (Senior Member, IEEE), NOOR MOHD[1], AND YOUNGHO PARK[4], (Member, IEEE)

[1]Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248002, India
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India
[3]Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA
[4]School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, Republic of Korea

Corresponding authors: Ashok Kumar Das (iitkgp.akdas@gmail.com) and Youngho Park (parkyh@knu.ac.kr)

This work was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605.

ABSTRACT Healthcare 5.0 is a system that can be deployed to provide various healthcare services. It does these services by utilising a new generation of information technologies, such as Internet of Things (IoT), Artificial Intelligence (AI), Big data analytics, blockchain and cloud computing. Due to the introduction of healthcare 5.0, the paradigm has been now changed. It is disease-centered to patient-centered care where it provides healthcare services and supports to the people. However, there are several security issues and challenges in healthcare 5.0 which may cause the leakage or alteration of sensitive healthcare data. This demands that we need a robust framework in order to secure the data of healthcare 5.0, which can facilitate different security related procedures like authentication, access control, key management and intrusion detection. Therefore, in this review article, we propose the design of a secure generalized healthcare 5.0 framework. The details of various applications of healthcare 5.0 along with the security requirements and threat model of healthcare 5.0 are provided. Next, we discuss about the existing security mechanisms in healthcare 5.0 along with their performance comparison. Some future research directions are finally discussed for the researchers working in healthcare 5.0 domain.

INDEX TERMS Healthcare 5.0, Internet of Things (IoT), artificial intelligence, cyber security, blockchain.

I. INTRODUCTION

Due to the advancement of the information technology, the idea of healthcare 5.0 has rapidly gained attention. Healthcare 5.0 transforms the conventional medical system in a comprehensive way by making healthcare effective, convenient and more personalised [1]. It does this by utilising a new generation of information technologies, such as the Internet of Things (IoT), artificial intelligence, Big data analytics, blockchain and cloud computing. Healthcare 5.0 is a multi-level transformation that goes beyond basic technological advancements [2]. There are changes in the medical model (for example, it is disease-centered to patient-centered care now). The construction of information technology has been shifted from clinical to regional medical informatization [3]. Moreover, the medical management has become from general to personalised management. The idea of prevention and treatment are all examples of this change. It is focusing not only on disease treatment, but also on the preventive healthcare [4], [5].

A. EVOLUTION OF HEALTHCARE

Various applications of healthcare 5.0 include ‘‘hospital operations management’’, ‘‘remote monitoring of patients’’, ‘‘treatment and detection of diseases’’, etc. [6], [7]. The transition of healthcare system is given Figure 1. It started with the healthcare 1.0, which stood with the production. Healthcare 1.0 focused on evidence based treatment, where the main objective was quality treatment and patient’s survivability. Healthcare 2.0 came into existence, which stood with the

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

industrializing which focused on value chain. Its main objective was responsiveness and end-to-end service coverage. Next, Healthcare 3.0 was introduced, which stood with the automation which focused on operating model. Its main objective was access, cost to serve and efficiency. After that, Healthcare 4.0 was introduced, which stood with the digitalization where the focus was shifted to business model. Its main objective was uniqueness, mass personalization and proactive healthcare. Currently, we are working with Healthcare 5.0, which stands with the personalization which focuses on customer model. Its main objective is lifelong partnership, customer well-being and quality of life [8].

B. SECURITY CHALLENGES IN HEALTHCARE 5.0

Healthcare 5.0 suffers from different issues and challenges i.e., "managing huge data volumes, absence of standards, data security threats, regulatory difficulties", etc [9]. Different information security related attacks, i.e., "replay, man-in-the-middle (MiTM), impersonation, malware injection, Denial-of-Service (DoS)", etc., are possible in healthcare 5.0 [10]. Due to these attacks, the sensitive healthcare data of different patients may be reveled, changed or deleted. Hence, we need a robust security framework to secure the data of healthcare 5.0. Therefore, in this review article, we focus on the designing of security framework for healthcare 5.0.

C. RESEARCH CONTRIBUTIONS

The main research contributions in the paper are highlighted below.

- Various application relevant to the healthcare 5.0 are discussed.
- Various issues and challenges of healthcare 5.0 are highlighted in this work. In addition, Further, various security requirements related to healthcare 5.0 along with their possible threats and attacks are discussed. A threat model relevant to healthcare 5.0 is also provided to build a robust framework for healthcare 5.0.
- Next, we provide a generalized secure healthcare 5.0 framework.
- A detailed comparative study among existing "security schemes in healthcare 4.0 and healthcare 5.0" is also provided.

D. OUTLINE

The remaining part of this review article is organised as follows. Various applications related to the healthcare 5.0 are discussed in Section II. The security requirements of healthcare 5.0 along with possible threats and attacks of healthcare 5.0 with the details of the proposed threat model relevant in healthcare 5.0 are given in Section III. The details of the designed secure generalized healthcare 5.0 framework are provided in Section IV. A discussion on various existing "security schemes in healthcare 4.0 as well as healthcare 5.0" along with their performance comparisons are provided in Section V. Furthermore, a detailed discussion on different issues and challenges of healthcare 5.0 are given in Section VI. Some future research directions are given in Section VII. Finally, the article is concluded in Section VIII.

II. APPLICATIONS OF HEALTHCARE 5.0

Healthcare 5.0 can be used for different facilities and services in the healthcare. Some of the important applications of healthcare 5.0 are given below [2], [6], [7], [11], and [12].

A. HOSPITAL OPERATIONS MANAGEMENT

Hospital operations management is the administration of all hospital operations, including both clinical and non-clinical procedures, in order to maintain a productive workplace. It involves funding, hiring personnel, developing and enforcing policies, buying and maintaining medical equipment, managing health insurance and associated claims, and many other things. It aids in enhancing patient happiness and speeding up the improvement of healthcare service quality. There may be a number of bottlenecks in the hospital setting that could reduce the overall effectiveness and productivity of healthcare services. These bottlenecks could include the availability of physicians and nursing staff for emergency treatment, the ability to care for several sick people at once who really need it, the availability of medications prescribed in adequate dose units and amount, the accessibility of ambulances, hospital beds, ICU beds, lack of sample (i.e., blood) collection (specially in rural areas) and ventilators in emergency cases like COVID'19, etc. Healthcare 5.0 greatly aids in overcoming these operational issues. The hospital's operational team and healthcare professionals can be alerted by the smart medical devices deployed in various areas to supervise and coordinate the hospital's operations. Under these circumstances, the drone-based drugs supply and sample collection feature of Healthcare 5.0 seem very useful. The healthcare 5.0's smart healthcare devices assist in determining when the equipment parts are about to expire and alert the concerned team about the maintenance and or replacement if it is required. Additionally, clinicians may quickly locate specific medical equipment (such as an oxygen cylinder), which is urgently needed that reduces time spent looking for it and perhaps helps to save the patient's life. Healthcare 5.0 also aids in maintaining order and managing the workforce within the network. Hence healthcare 5.0 can be very beneficial to the hospital's general operation in this way [5], [7], [13].

B. REMOTE MONITORING OF PATIENTS

A method of treating and offering healthcare resources and services to patients who are far away is termed as remote patient monitoring. The healthcare profession has traditionally found it difficult to assist the elderly, the physically disabled, people living in rural areas, patients who are seriously ill and immobile at home, and extreme emergencies. Due to a lack of facilities and to stop the corona virus from spreading, remote patient care is still necessary (i.e., in COVID'19 pandemic) [14]. Due to a lack of surveillance, it frequently occurs that even patients who are cured are readmitted to the hospital after their discharging. Healthcare 5.0 uses IoT and associated technologies to provide remote patient monitoring and overcome the associated constrained. Moreover, there is also the facility of drone-based sample (i.e., blood) collection, which specially helps in the underprivileged rural residents. In the healthcare 5.0, implantable or wearable smart healthcare devices assess patients' health-related factors and transmit that information to healthcare professionals (i.e., doctors) for medical treatment. In the event of aberrant health parameters, it also alerts the healthcare providers. With the aid of the healthcare 5.0 communication environment, underprivileged rural residents can also receive advice and medical care from top experts located all over the world. To ensure that no one is denied treatment, it also helps to lower hospitalisation and travel expenses [7], [13].

C. TREATMENT AND DETECTION OF DISEASES

In order to increase life expectancy and to enjoy a meaningful life, timely and precise disease detection, assessment, and medication are crucial. There is a need to constantly improve the medical facilities and services that are readily available to every person, despite the fact that numerous attempts have been made for a long time to handle various emergent health-related difficulties of all ages. Early disease symptoms can sometimes go unrecognised and undiagnosed, leading to chronic and severe sickness that is exceedingly challenging to treat and can even result in the patient's death. Heart attacks, cirrhosis of the liver, cancer, brain seizures, diabetes, asthma, and other illnesses necessitate rapid hospital treatment. With the aid of smart healthcare devices, which continuously monitor the patient's vital signs including blood pressure, temperature, blood sugar level, oxygen level, etc.. Then send the health related data to the practitioner (i.e., doctor) through the communication facility of healthcare 5.0. Healthcare 5.0 aids in recognising the first signs of any serious illness so that it can be handled with extreme caution. Healthcare 5.0's tools and technologies (i.e., machine learning or deep learning algorithms) do this task without any mistake or error. This lessens the likelihood of a number of the previously mentioned life-threatening conditions. This further helps in the prevention of the critical illnesses [9], [13]. However, such features were missing in the earlier versions of the healthcare system.

D. REMOTE SURGERY

Through the use of robotic arms and related technologies, skilled surgeons can operate on a patient from some remote location. The remote surgeon gives commands and controls to robots at the operating site. Through this facility, patients from all around the world can access the knowledge of specialised surgeons without going to the surgery location physically. The widespread adoption of healthcare 5.0 tools and technologies make this possible. It guarantees more accurate and precise real-time remote action and reactions. During times of war or some natural disasters, healthcare 5.0 also contributes to the preservation of numerous lives [13], [15]. The healthcare 5.0's activities and operations are well supported through the tactile Internet. Therefore, remote surgery can be performed without any issue or error. However, such features were not available in the previous versions of the healthcare system.

E. SECURE DRUG SUPPLYCHAIN MANAGEMENT

The planning and management of every step in drug distribution, from production to end point delivery is considered as drug supply chain management. This supply chain's security, safety and dependability must also be maintained because at any time it could be compromised or utilized inappropriately. The drug supply management process is streamlined and improved with the help of healthcare 5.0. Using smart devices like smart tags attached to the drug bags, the tools and technologies of healthcare 5.0 protects the security and safety of delivered medications from being counterfeited. These smart tags aid in the proper dispersion, tracking, and safeguarding of medications from counterfeiting, ensuring that patients are securely given with high-quality prescription medications. Smart devices alert the relevant authority in charge of managing drug supply change management in the event that someone tries to exchange drugs with the counterfeit medications [16]. Moreover, the drone-based drugs supply is another good feature, which is provided by healthcare 5.0. It was not available in the previous versions of the healthcare system.

III. SECURITY OF HEALTHCARE 5.0

The security requirements, threats and attacks of healthcare 5.0 and threat model of healthcare 5.0 are disucssed below [2].

A. SECURITY REQUIREMENTS OF HEALTHCARE 5.0

The security and privacy requirements of healthcare 5.0 are as follows [7], [17], [18], [19], [20], [21], and [22].

- *Confidentiality:* This property offers protection from all types of data release attacks. It also goes by the names secrecy and privacy. In healthcare 5.0, both data transmission and storage secrecy must be attained. To protect the confidentiality of data that is stored and sent, mechanism like, data encryption should be used.
- *Integrity:* The data integrity that is transferred and stored is guaranteed by this attribute. It implies that the transferred and stored healthcare data should not be subject to any unapproved updates. Furthermore, no data should be added or removed without permission. We may employ some mechanisms like "secure hash algorithms to ensure the integrity" (i.e., using "Secure Hash Algorithm (SHA-256)" [23]).
- *Authentication:* It is a process of determining whether a person or object is legitimate. In the case of healthcare 5.0, it may involve "device-to-device, user-to-device, or user-to-user authentication." We employ mechanisms like the "two factor user authentication protocol" or

the "three factor user authentication protocol" for this task. The interacting individuals establish session keys for their secure transmission of information that usually happens when all authentication protocol stages have been successfully completed.

- *Access control:* It is a process of mitigating the unauthorised access attempts to the legitimate devices and resources of Healthcare 5.0. Different kinds of mechanisms can be applied, like device access control and user access control.
- *Non-repudiation:* It is yet another significant necessity. It gives the transferring party the assurance that they should not contest the veracity of anything like the transferred communications. This feature guarantees both the data's integrity and "evidence of the data origin." Therefore, it is difficult to reject "who sent the message" or "from where the message came."
- *Authorization:* Healthcare 5.0 uses authorization to ensure that genuine parties, such as "legitimate smart healthcare device", deliver the data to other parties (for instance, a doctor).
- *Freshness:* It guarantees the messages being exchanged are fresh in order to reduce the re-transmission tries (i.e., mitigation of replay attacks).
- *Availability:* This attribute guarantees that the devices and the associated network services should be made accessible to the real devices/ entities even in the worst circumstances i.e., "scenario of denial-of service (DoS) attacks."
- *Forward secrecy:* It ensures that the messages sent and received are kept confidential. This means that if a smart healthcare device departs healthcare 5.0 system, then it must not get access to any messages, which may be sent in the future.
- *Backward secrecy:* It guarantees the messages, which were exchanged in the past, should remain private. It means that if a smart healthcare device or user that has just joined the network of healthcare 5.0 then he/ she must not have access to any of the previously exchanged messages.

B. POSSIBLE THREATS AND ATTACKS OF HEALTHCARE 5.0

The following types of passive/active attacks can be possible in healthcare 5.0 [5], [22], and [24].

- *Eavesdropping:* The sniffing of transmitted signals is used for eavesdropping attempts. Later, further attacks like credential guessing and impersonation attacks can be launched using the intercepted messages.
- *Traffic analysis:* The adversary in this nefarious act intercepts messages to learn what kind of conversation is occurring on the route. The opponent, for instance, can learn which side is speaking with whom and for how long.
- *Replay attack:* In this threatening attempt, the opponent keeps a record of the messages, which are transmitted and then tries to play them back to deceive the receiving side [25].
- *Man-in-the-middle (MiTM) attack:* In this malicious attempt, the adversary intercepts the communications being sent prior. Then he/ she tries to amend or delete them before sending them to the addressee [26].
- *Impersonation attack:* In this malicious act, $\mathcal{A}$ first attempts to determine "sender's identity" with the help of intercepted messages. He/ she then attempts to change or generate new messages before sending them to the target recipient. Following receipt of such messages, the recipient assumes that the messages are from the original sender [27]. However, in reality, $\mathcal{A}$ has sent them [25].
- *Denial-of-Service (DoS) attack:* In this hostile act, $\mathcal{A}$ prevents authorised users from using the services of healthcare 5.0. $\mathcal{A}$ accomplishes this by setting up an attacker system (or a system running malicious malware), which delivers bogus requests or attack packets to the legitimate healthcare 5.0 devices or services. As a result, the servers or devices cannot offer the service to the original users. The variation of DoS known as "Distributed DoS (DDoS)" can be carried out through numerous attacking systems i.e., botnets [28], [29], [30].
- *Attacks associated with blockchain:* As healthcare 5.0 consists of blockchain, therefore, some attacks associated with blockchain 5.0, i.e., 51% attack and selfish mining are possible. That usually happens if we do not choose a consensus algorithm carefully. When an opponent has a lot of hashing power, these kinds of harmful activities could occur [31]. A 51% attack, in particular, necessitates that $\mathcal{A}$ carries more than half of the hashing power. The 51% attack is typically used against crypto currencies, where $\mathcal{A}$ engages in malicious behaviours like "double spending." Apart from that, another well-known weakness in the blockchain-based system is termed as "selfish mining." Here malicious miners $\mathcal{A}$ can take use of this to steal block rewards. The "Proof-of-Work (PoW)" is vulnerable to a 51% attack, according to the recent observations and discoveries. Therefore, it is advised that we choose the "consensus algorithm" cleverly. Hence, to mitigate these issues, we should employ consensus algorithms, such as "Ripple Protocol Consensus Algorithm (RPCA)" and "practical Byzantine Fault Tolerance (pBFT)" [25].
- *Malware attack:* A remote sitting adversary uses the execution of malicious malware scripts in the remote systems to carry out malware attacks. These malicious operations include information theft, the encryption of sensitive data and the hijacking of the smart healthcare devices [22].
- *Database attack:* Healthcare 5.0 stores healthcare information on a server, or cloud server. The possibility of database-related cyber attacks exists in this communication context. The use of exploits like "Structured Query Language (SQL) injection attack" and "Cross-Site Scripting (XSS) attack" can reveal the sensitive

medical data. In a SQL injection attack, the attacker attempts to insert malicious code into the "existing SQL queries" to trick the database administrator into disclosing the confidential data [32]. While in an XSS attack, $\mathcal{A}$ attempts to insert malicious scripts into legitimate and trustworthy websites in order to steal sensitive data i.e., "identity and password information" [2], [33].

- *Physical device stolen attack:* Because they cannot be monitored continuously, smart healthcare devices are vulnerable to physical theft by the enemy. Then, using complex "power analysis attacks," it will be possible to use these stolen healthcare devices to extract confidential material from them [34], [35]. Additionally, the risk increases if $\mathcal{A}$ attempts to use the knowledge obtained to execute additional attacks like "MiTM, illegal session key computation, impersonation attacks, etc." [36], [37].
- *Privileged-insider attack:* The registration authority's privileged insider user, who has access to the private registration data for multiple users and devices, may cause issues in this illegal activity. "A privileged insider user" may pose as an $\mathcal{A}$ and uses the different users' and devices' obtained registration information to execute prospective attacks on healthcare 5.0. The examples are "offline password guessing attacks, impersonation attack and unauthorised session key computation attack [38], [39].
- *Stolen verifier attack:* In this malicious activity, an adversary $\mathcal{A}$ tries to deduce the sensitive information of legitimate entities i.e., smart healthcare devices, users. Usually, $\mathcal{A}$ uses the secret data stored at the servers. By making the use of this information $\mathcal{A}$ launches other potential attacks, i.e., MiTM, impersonation, session key computation, physical device stolen, etc., on the system. To mitigate this attack, it is recommended to store the secret registration information of various entities in the secured region of the database [37].
- *Online/offline password guessing attack:* In this attack, an $\mathcal{A}$ tries to obtain the passwords of legitimate uses of the Healthcare 5.0. $\mathcal{A}$ does this task with the help of exchanged messages and information stored at the cloud servers. Using this deduced information, $\mathcal{A}$ proceeds for the guessing of password either in the online way or in the offline way. To mitigate this attack, it is recommended to store the secret registration information of various entities in the secured region of the database [37]. Moreover, we should be careful when we exchange any message. In the exchanged messages, we should not exchange any secret information in the plaintext; otherwise, this may be helpful for $\mathcal{A}$ to launch the unauthorised attempts of online/ offline password guessing [40].

C. THREAT MODEL OF HEALTHCARE 5.0

For the scenario of healthcare 5.0, widely followed model, like, Dolev-Yao threat model is taken into consideration [41]. As per the DY model, the entities, for example, smart healthcare devices, servers, users smartphones communicate over the Internet, which is an insecure channel. This communication, which happens through this channel is accessible to everyone even to the hackers (online attackers $\mathcal{A}$) also. Thus $\mathcal{A}$ can get access to the exchanged messages, and he/she gets the opportunity to update/ delete/ disclose/ delay them. $\mathcal{A}$ also can try to deploy botnet (a network of attacker systems) to launch different attacks (i.e., malware) on the systems and devices of healthcare 5.0. Therefore, we need some security mechanisms to detect and mitigate aforementioned attacks. Due to the introduction of these attacks, the online connected devices and servers are always under high risks. For example, the smart healthcare devices may be hijacked or may be shut down. Subsequently, their stored healthcare data can be leaked or altered. $\mathcal{A}$ can also capture some of the deployed smart healthcare devices physically. $\mathcal{A}$ then can deduce secret values (for instance, secret keys, session keys, identities of users and devices), which are stored in their memory with the help of steps of sophisticated power analysis attack [34], [35]. $\mathcal{A}$ also has ability clone other smart healthcare devices, which seem like the captured smart healthcare devices with more devastating attack features, (i.e., ability to launch routing attacks) [42], [43]. $\mathcal{A}$ then uses these malicious devices to perform a number of attacks to disrupt the network's ongoing communication.

IV. PROPOSED GENERALIZED FRAMEWORK: SECURE HEALTHCARE 5.0 FRAMEWORK

The architecture of the proposed generalized secure healthcare 5.0 framework is given in Figure 2. In this architecture, we have patients, who have implantable and wearable medical devices (i.e., smart healthcare devices), which monitor their health parameters. The data, which is collected through the implantable and wearable medical devices is helpful to the medical experts i.e., doctors and nursing staff. The doctors can provide the remote prescription to the patients with the help of the application (APP), which doctors have in their smartphone/ tablet. The nursing staff can also monitors the health of the patients on the basis of received values of health parameters i.e., heart rate, SP-O2 level, level of blood sugar, etc. In the similar the health information is also available to the relatives of the patients. During the pandemic time (i.e., COVID'19), it is difficult for the patients to visit the hospitals physically. In these circumstances, the medical drone can collect the samples (blood, urine, etc.,) of the patients and then deliver them to the laboratory for the testing purpose. The medical drones can also delivery medicines and other healthcare related products to the patients at their home. We also have some deployed smart ambulances, which act as per the alerts send by the system, for example, the ambulance can be called immediately in case of any severe health issue. The patients, which is collected through the smart healthcare devices is stored over the peer-to-peer cloud server (P2PCS) network in the form of a blockchain. Usually, it is like, the private blockchain and maintained the health records in the form of encrypted transactions inside the blocks. It is

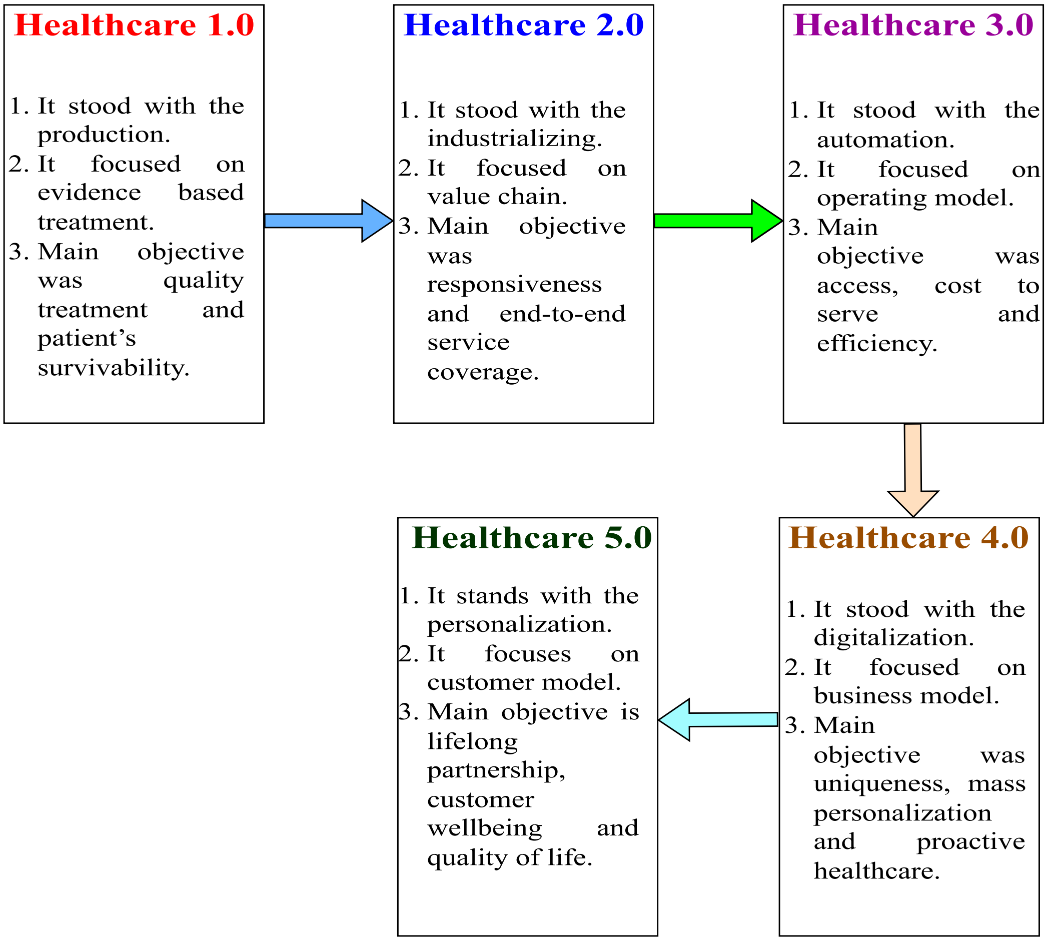
Healthcare 1.0
1. It stood with the production.
2. It focused on evidence based treatment.
3. Main objective was quality treatment and patient's survivability.
Healthcare 2.0
1. It stood with the industrializing.
2. It focused on value chain.
3. Main objective was responsiveness and end-to-end service coverage.
Healthcare 3.0
1. It stood with the automation.
2. It focused on operating model.
3. Main objective was access, cost to serve and efficiency.
Healthcare 4.0
1. It stood with the digitalization.
2. It focused on business model.
3. Main objective was uniqueness, mass personalization and proactive healthcare.
Healthcare 5.0
1. It stands with the personalization.
2. It focuses on customer model.
3. Main objective is lifelong partnership, customer wellbeing and quality of life.

FIGURE 1. Transition of healthcare system.

always preferable to use stored healthcare data for the data analytics purpose. For that purpose, the data, which is stored in the blockchain can be utilized to predict about the patient's illness. For this tasks, some artificial intelligence (AI) based technique (i.e., machine learning/ deep learning algorithm) can be used. Then treatment can be provided to the patients as per his / her health conditions. The health related data, which is exchanged among the smart health devices, servers and users (i.e., doctors) is vulnerable to various information security related attacks as the entire data exchanges through the Internet. The online attackers (i.e., hackers) are always in search of some vulnerabilities in the deployed system to exploit them. Various attacks i.e., replay, man-in-the-middle, impersonation, credentials guessing, hijacking of smart healthcare device, malware injection, stolen verifier, privileged insider, unauthorised session key computation, denial of service (DoS), distributed denial of service (DDoS), spurious flooding, etc. Therefore, security experts try to deploy some security mechanisms to make the system secure against the discussed attacks.

The following security mechanisms can be deployed.

- **Authentication and key establishment protocols:** These protocols are required to provide the secure mutual authentication and key establishment among the communicating entities of healthcare 5.0. After the successful completion of mutual authentication, entities establish session keys for their secure exchange of data.
- **Access control and key establishment protocols:** These protocols are required to achieve secure access control among the communicating entities of healthcare 5.0. After the successful completion of access control process, entities establish session keys for their secure exchange of data.
- **Key distribution and management protocols:** These protocols are required for the secure key distribution as well as key management among the communicating entities of healthcare 5.0. Usually the trusted registration authority does the registration of entities (i.e., smart healthcare devices, users, servers) of the healthcare 5.0 and store registration credentials in their memory/ database. These stored credentials are further utilized in the processes of secure authentication/ access control.

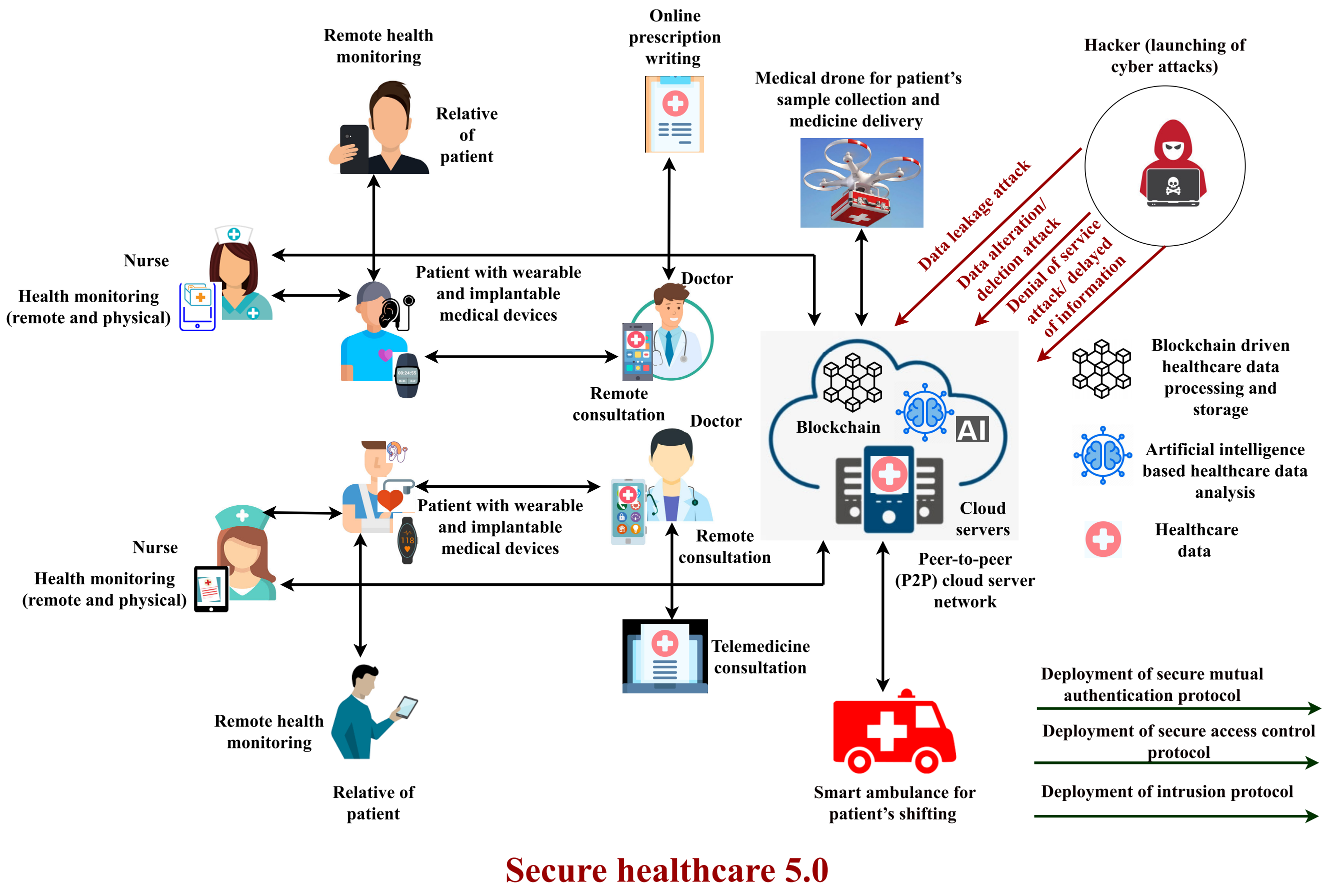
Remote health monitoring
Relative of patient
Online prescription writing
Medical drone for patient's sample collection and medicine delivery
Hacker (launching of cyber attacks)
Data leakage attack
Data alteration/ deletion attack
Denial of service attack/ delayed of information
Nurse
Health monitoring (remote and physical)
Patient with wearable and implantable medical devices
Doctor
Remote consultation
Blockchain
AI
Cloud servers
Blockchain driven healthcare data processing and storage
Artificial intelligence based healthcare data analysis
Healthcare data
Doctor
Patient with wearable and implantable medical devices
Remote consultation
Nurse
Health monitoring (remote and physical)
Peer-to-peer (P2P) cloud server network
Telemedicine consultation
Remote health monitoring
Relative of patient
Smart ambulance for patient's shifting
Deployment of secure mutual authentication protocol
Deployment of secure access control protocol
Deployment of intrusion protocol
Secure healthcare 5.0

FIGURE 2. Architecture of secure healthcare 5.0 system.

- **Intrusion detection protocols:** To make the system more secure authentication, access control and key distribution protocols are not enough. Sometimes the deployed security mechanisms get failed and intrusions get entry into the system. Under these circumstances, the smart healthcare devices, servers and users may be attacked by the hackers through various attacks, i.e., remote hijacking, malware injection, DoS/ DDoS, spurious flooding, etc. To stop these malicious activities, we need deploy some intrusion detection protocols to protect the devices, servers and users of healthcare 5.0. Usually intrusion detection system protects in two ways, i.e., at the network level and at the system (host) level. These two kinds of intrusion detection systems are called as network based intrusion detection system and host based intrusion detection system.

Some of the important features of architecture of secure healthcare 5.0 system are given below.

- **Main entities:** In the given architecture of secure healthcare 5.0 system, the main entities are users (i.e., doctor, nurse, relative of patient), who want to access the data of healthcare 5.0 for their various purposes. Moreover, there are various devices, i.e., implantable medical devices, wearable medical devices, medical drones, smart ambulance, and cloud servers of peer-to-peer cloud server network. These devices have communication capabilities and exchange the information as per the various needs. Cloud servers store the data of healthcare 5.0 in the form of different blocks of blockchain. This data is further analysed to obtain useful outcomes i.e., prediction related to some illness. There are also some unauthorised entities i.e., hackers, who want to launch some cyber attack on the communication of healthcare 5.0. The various potential attacks are possible, i.e., unauthorized data leakage, unauthorized data alteration/ deletion, and denial of or distributed denial of service attacks (DoS or DDoS). Therefore, we need some security mechanisms to protect the data of healthcare 5.0.
- **Available services:** In healthcare 5.0, there are various services available, i.e., remote health monitoring, in which secure access of healthcare data of various patients to the legitimate users like, doctors, nurse, relative of patient is provided. This data is further maintained in the form of blocks in the blockchain, which can later used to obtain important outcomes, i.e. prediction

about the illness of a patient. Moreover, there are other important services available, i.e., drone-based sample collection and medicine delivery, smart ambulance for patient's shifting, telemedicine consultation.

- **Secure data flow management:** For the secure data flow management, various security mechanism can be deployed. For example, for secure authentication, a mechanism of 2-factor or 3-factor user authentication can be used. Apart from that for the secure access control, mechanisms, like, device access control or user access control can be used. For this task methods, like, certificate-based access control or certificate-less access control mechanisms can be deployed. Moreover to protect against the potential intrusion, schemes like, machine learning-based or deep learning-based intrusion detection can be used. For this task, methods, like, signature-based detection, anomaly-based detection or hybrid detection can be deployed.

V. SECURITY SCHEMES IN HEALTHCARE 4.0 AND HEALTHCARE 5.0

In this section, we provide the details of the security schemes applicable to healthcare 4.0 and healthcare 5.0.

A. EXISTING SECURITY SCHEMES IN HEALTHCARE 4.0

In the following, we discuss the following recent schemes proposed in healthcare 4.0. Next, we discuss the performance comparison of the discussed schemes.

- **Qahtan et al.** [50] presented the formulation of fuzzy weighted with zero inconsistency (FWZIC) scheme under the spherical fuzzy environment. Their scheme combined "GRATOPSIS and the BES optimization." They also presented a new security and privacy mechanism i.e., multi-criteria decision-making (MCDM) for blockchain-enabled IoT healthcare Industry 4.0.
- **Aggarwal et al.** [45] presented a blockchain-enabled unmanned aerial vehicle (UAV) path planning system for Healthcare 4.0. They also provided a identity management and privacy preservation scheme for the sharing of medical data in healthcare 4.0. They have also provided a comparative study of their scheme and other potential schemes to found out about the performance improvement of their scheme over the other schemes.
- **Qiu et al.** [46] proposed a user-centric data storage and sharing scheme in cloud-based medical cyber-physical systems (MCPS). Their scheme tried to protect the safety and privacy of users' electronic health record (EHR) data. It could secure the data and maintained its privacy even even in case of cloud servers and keys are compromised. They had also evaluated the feasibility of their scheme on mobile-edge computing (MEC) on a smartphone to observe its performance improvement over the standard encryption algorithms.
- **Bhattacharya et al.** [47] proposed a blockchain-based scheme for deep learning as-a-service to store patient's EHR data in a secured way. They presented a lattice based signature mechanism for the assurance of privacy and authentication of EHR records of various patients.

The performance comparison of security schemes in healthcare 4.0 is given in Table 1. From the information given in Table 1, it is clear that the scheme of Bhattacharya et al. [47] covers most of desired security and funtionality features. However, blockchain related implementation is missing in all schemes.

B. EXISTING SECURITY SCHEMES IN HEALTHCARE 5.0

In the following, we discuss the following recent schemes proposed in healthcare 5.0. Next, we discuss the performance comparison of the discussed schemes.

- **Ghosh et al.** [44] provided a public blockchain network (PBCN) oriented architecture, which includes a layer of validation service providers (VSPs). In the their architecture, multiple validation devices (VDs) participate in the communication. However, some of them could have bad motives, such as inaccurate information validation and information fabrication. They proposed B2H, which was able to predict a malicious validation device and penalizing them as per the situation. Their architecture helped the end-users for the association of limited number of VDs. In their mechanism, an end-user had multiple chooses for the selection of a VSP, which the information validation has done through VDs. Their scheme i.e., B2H helped the end-user for the selection of an optimal VSP. Their scheme reduced the validation latency of PBCN-based system, which was provided to fulfil the healthcare needs of the Society 5.0.
- **Bhavin et al.** [7] examined various security architectures for the security of "electronic health records (EHRs). They have introduced "quantum computing (QC)" for the conventional encryption mechanism. Further, they suggested a "blockchain-based architecture for healthcare 5.0." It enabled users to access database data as per their assigned roles. Furthermore, they have used "quantum blind signature" for the creation of blocks on the "hyperledger Fabric blockchain." This mechanism was used to defend the encryption scheme from the potential quantum attacks, which are possible in the future. They have computed important results i.e., "transaction throughput, resource usage, and network traffic."
- **Shamshad et al.** [48] looked at a case study of an "artificial intelligence (AI), cloud computing, big data technologies, industrial cyber-physical systems (I-CPSs)" based healthcare ecosystem, which could be used for healthcare 5.0 applications. They emphasised its problems with physical and cyber security. They then created a "system-wide key establishment scheme", which was effective and physically secure. Their scheme made the use of "effective cryptographic primitives", i.e., "fuzzy extractor, hash function, and XOR operator." Because

TABLE 1. Performance comparison of security schemes in healthcare 4.0.

Scheme	Task	Available Features	Limitations
Qahtan *et al.* [46]	A blockchain-enabled multi security and privacy benchmarking framework for the security of IoT-based healthcare industry 4.0 was provided.	* They presented the formulation of fuzzy weighted with zero inconsistency (FWZIC) scheme under the spherical fuzzy environment. * Their scheme combined "GRATOPSIS and the BES optimization." * They presented a new security and privacy mechanism i.e., multi-criteria decision-making (MCDM) for blockchain-enabled IoT healthcare Industry 4.0.	* They did not focus on the potential threats/attacks (i.e., replay attack, man-in-the-middle (MiTM) attack, impersonation attack, credentials guessing etc.) of the domain. * There is no blockchain related implementation. Mitigation of potential attacks, i.e., replay attack, man-in-the-middle (MiTM) attack, impersonation attack, credentials guessing etc., is not available. * There is no discussion related to blockchain related attacks. They did not provide any blockchain related implementation of their scheme.
Aggarwal *et al.* [47]	A blockchain-enabled unmanned aerial vehicle (UAV) path planning scheme for healthcare 4.0 was provided.	* They presented a blockchain-enabled UAV path planning system for healthcare 4.0. * They provided an identity management and privacy preservation scheme for the sharing of medical data in healthcare 4.0. * They have provided a comparative study of their scheme and other potential schemes to found out about the performance improvement of their scheme over the other schemes.	* Only few attacks were covered. * Mitigations of potential attacks, i.e., physical drone stolen attack, impersonation attack, stolen verifier attack, credentials guessing, etc., are not available. * There is no discussion related to blockchain related attacks. * They did not provide any blockchain related implementation of their scheme.
Qiu *et al.* [48]	A secure health data sharing scheme for medical cyber-physical systems-enabled healthcare 4.0 was provided.	* They proposed a user-centric data storage and sharing scheme in cloud-based medical cyber-physical systems (MCPS). * Their scheme protects the safety and privacy of users' electronic health record (EHR) data. It secures the data and maintained its privacy even even in case of cloud servers and keys are compromised. * They evaluated the feasibility of their scheme on mobile-edge computing (MEC) on a smartphone to observe its performance improvement over the standard encryption algorithms.	* There is no proper security analysis of their scheme. * Potential security threats were not discussed. * There is no discussion related to blockchain related attacks. * They did not provide any blockchain related implementation of their scheme.
Bhattacharya *et al.* [49]	A lattice based signature mechanism was provided to ensure the authenticity and privacy of electronic health record (EHR) records.	* They proposed a blockchain-based scheme for deep learning as-a-service to store patient's EHR data in a secured way. * They presented a lattice based signature mechanism for the assurance of privacy and authentication of EHR records of various patients.	* Formal security analysis is missing. * Potential security threats were not discussed. * There is no discussion related to blockchain related attacks. * Blockchain related implementation is missing.

of the use of "physically unclonable function (PUF)," the their scheme was resistant to physical attacks as well as cyber attacks. They have also conducted the formal and informal security analyses of their scheme, which identified that their scheme could prevent many potential physical and cyber attacks. A widely endorsed NS3 simulator tool was used to test the effectiveness of their scheme during the realistic network demonstration. It was also observed that their scheme clearly superior in terms of "computing overhead, communication overhead, and functionality characteristics" when compared to the other related existing schemes.

- **Gupta et al.** [49] highlighted the security, privacy, and communication issues of healthcare 5.0 enabled telesurgery system. They introduced "Blockchain-driven Intelligent Scheme for Telesurgery System

TABLE 2. Performance comparison of security schemes in healthcare 5.0.

Scheme	Task	Available Features	Limitations	Security flaws/ attacks
Ghosh *et al.* [46]	Their scheme was able to predict a malicious validation device (VD) and penalizing them as per the situation.	* It helped the end-users for the association of limited number of VDs. * Their scheme reduced the validation latency of PBCN-based system, which was provided to fulfil the healthcare needs of the Society 5.0.	Very few security and functionality features were considered. * They did not focus on the potential threats/attacks (i.e., replay attack, man-in-the-middle (MiTM) attack, impersonation attack, and credentials guessing attack) of the domain. * There is no blockchain related implementation.	* Mitigation of potential attacks, i.e., replay attack, man-in-the-middle (MiTM) attack, impersonation attack, and credentials guessing attack, is not available.
Bhavin *et al.* [50]	They proposed "blockchain-based architecture for healthcare 5.0."	* This scheme examined various security architectures for the security of "electronic health records (EHRs). * They have introduced "quantum computing (QC)" for the conventional encryption mechanism. * Their scheme used "quantum blind signature" for the creation of blocks on the "hyperledger Fabric blockchain." * They have implemented the blockchain for their proposed scheme.	* Security analysis of the proposed scheme is weak. * They did not discuss anything about the defense of blockchain related attacks.	* Mitigation of blockchain related attacks is not available.
Shamshad *et al.* [51]	They have provided a "system-wide key establishment scheme" for "artificial intelligence (AI), cloud computing, big data technologies, industrial cyber-physical systems (I-CPSs)" based healthcare ecosystem applicable for healthcare 5.0 applications.	* A "system-wide key establishment scheme" for healthcare 5.0 application was proposed. * Their scheme made the use of "effective cryptographic primitives", i.e., "fuzzy extractor, hash function, and XOR operator." * Their scheme is resistant to physical attacks as well as cyber attacks.	* They did not provide any implementation of blockchain.	* They did not discuss anything about the potential cyber attacks.
Gupta *et al.* [52]	They proposed "Blockchain-driven Intelligent Scheme for Telesurgery System (BITS)" for the secure communication of telesurgery system applicable to healthcare 5.0.	* They highlighted the security, privacy, and communication issues of healthcare 5.0 enabled telesurgery system. * They introduced "Blockchain-driven Intelligent Scheme for Telesurgery System (BITS)" for the secure and effective functioning of telesurgery system. * They demonstrated how the presented BITS scheme could solve the aforementioned security issues.	* Security analysis of the proposed scheme is weak. * The formal and informal security analysis of the designed scheme is not provided.	* Mitigation of blockchain related attacks is not available.

(BITS)'' for the secure and effective functioning of telesurgery system. Further, they demonstrated how the presented BITS scheme could solve the aforementioned security, privacy and communication issues of the associated system.

The performance comparison of security schemes in healthcare 5.0 is given in Table 2. From the information given in Table 2, it is clear that the scheme of Shamshad et al. [48] provides most of the desirable features. Moreover it also seems secure against the various potential attacks. However, its blockchain implementation is not given. The scheme of Bhavin et al. [7] seems promising from the future perspective. As it was designed with help of ''quantum cryptography (i.e., quantum blind signature).'' However, security analysis of this scheme is not satisfactorily done. They did not discuss anything about the defense of blockchain related attacks.

VI. ISSUES AND CHALLENGES OF HEALTHCARE 5.0

Healthcare 5.0 is applicable for various applications and support the people and society in various ways. However, it also has several issues and challenges, which need to be handled carefully. Some of issues and challenges of healthcare 5.0 are given below [2], [5], [7], [9].

- **Managing huge data volumes:** Large volumes of medical data are exchanged over the healthcare 5.0 from a variety of networked devices. Traditional mechanisms and algorithms cannot process this data. Healthcare 5.0 examines the gathered data to offer an early illness diagnosis. Hence there is a need to establish a technique to manage the enormous volume of data in order to improve the decision-making and diagnosing capabilities of the system. However, to manage huge data more easily, we can deploy some machine learning algorithms and more sophisticated algorithms, which seem a potential solution for this issue.

- **Absence of standards:** In the healthcare 5.0 communication environment, there are the communications among the smart healthcare devices, servers, service provides and users. The different equipments (i.e., smart healthcare devices) are largely purchased from various vendors. Due to the lower cost, some gadgets use bluetooth, while others are online. When transferring data to distant servers, these variances could raise some issues. The security of the data and the stability of the systems are at risk due to the incompatibility of systems problem. To resolve these issues, we should check for the devices for dangers that employees use to access data.
- **Utilization of smart healthcare devices while using outdated infrastructure:** Healthcare 5.0 is a fantastic breakthrough for the healthcare sector, but if it is connected with out-of-date infrastructure, it won't be functioned well. It's challenging to search some right person to upgrade the infrastructure of healthcare facilities with outdated technology. Because of this issue, the majority of IT graduates do not want to work in the medical industry. As a solution to this issue, it is always desirable to make sure that deployed infrastructure should be updated to the newest technologies to draw in the best talent. The information technology devices and appliances should be replaced every ten years as per the suggestions of the industry experts.
- **Data security threats:** Cyber attacks are quite likely to compromise healthcare data of healthcare 5.0. The danger of exposure is greatly increased when the healthcare 5.0's data is added to the already existing pool of clinically sensitive medical data. Data breaches are more likely happen when more devices are connected to the external systems and also to one another [51].
- **Data unification:** Healthcare 5.0 is the collection of heterogeneous devices. If the data from these devices cannot be combined and computed to produce useful and meaningful conclusions then it seems useless. All the healthcare 5.0 devices must be compatible with one another and enable data transmission to all users of the technology, including payers and healthcare service providers, in order to fully acquire the potential advantages of it [51].
- **Regulatory difficulties:** Different countries have different laws (i.e., laws related to privacy of sensitive healthcare data). Clinical grade medical devices must have clearance and permission from national regulatory authority before they are launched in the market. Healthcare 5.0 devices provide new difficulties for legislators and regulatory authority as well [51].
- **Cost factor:** A hefty initial investment is the result of the expense of the hardware, specialised healthcare 5.0 infrastructure, cloud computing and developing a consumer-facing app. Although the eventual return on investment is absolutely there. Hence the deployment and installment of healthcare 5.0 infrastructure is bit expensive [51].
- **Scaling issue:** Scaling is a major issue to healthcare 5.0. In order to improve economics and patient outcomes of healthcare 5.0, it is important to make sure that healthcare organisations, professionals, and patients recognise the added value of connected smart healthcare devices of healthcare 5.0 [51].
- **Trust factor:** Healthcare companies implement strategies on the basis of patient's data. Therefore, these organisations must ensure the patients, the general public and health care professionals how the healthcare data is being used. Hence some trust building is required in this direction [51], [52].

VII. FUTURE RESEARCH ON HEALTHCARE 5.0

Healthcare 5.0 uses new tools and technologies. It becomes very promising and emerging rapidly. However, some of aspects of healthcare 5.0 are still undiscovered. Due to that it requires some new research works. The future research directions of healthcare 5.0 are given below.

A. UNBREAKABLE SECURITY

Various security framework have been developed. However, most of them are not fully secure or lack in functionality features. Different kinds of attacks i.e., blockchain related attacks, malware attacks, credentials guessing, sensitive data leakage, etc., are possible. As a result, it's important to develop security framework for healthcare 5.0 that can withstand numerous simultaneous attacks. Consequently, developing such solutions can be a challenging task.

B. EFFICIENT SECURITY SCHEMES

The devices (i.e., smart healthcare devices) in healthcare 5.0 communication environment are resource-constrained as they have limited processing power, memory, and battery life. As a result, we are unable to use them for tasks that demand a lot of computing, communication, or storage capabilities. Therefore, we cannot use resource intensive complex algorithms to secure the communication of healthcare 5.0. Because of this, it's important to design security schemes, which are low-cost in terms of computing, communication, and storage without sacrificing security.

C. SCALABILITY ISSUES

Healthcare 5.0 is a type of large-scale heterogeneous network of many communication systems/ devices and applications, each of which has its own capabilities and needs. As a result, the designing of security frameworks for Healthcare 5.0 is very difficult. Different healthcare records of specific individuals may be present there, which are stored on an IoT-enabled cloud server for further processing. The many "Body Area Network (BAN)" devices produce data, which then transmitted to the cloud servers. As a result, there exists a heterogeneous network comprising of various communication hardware. We require a certain form of security framework that can safeguard all different kinds of communication devices in such an environment. More in-depth research is therefore required in this area.

D. HETEROGENEITY OF HEALTHCARE 5.0 SYSTEMS

Healthcare 5.0 system is considerably different from traditional healthcare system since it uses a wide range of devices, including "RFID tags, desktop computers, full-edge laptops, and personal digital assistants." Additionally, these devices function in accordance with several communication protocol principles. The fact that these devices differ in terms of their available storage, processing power, communication range, and operating system is also very important to note. From this point forward, we must create a security framework, which can support and defend various devices and underpinning technology types.

E. COMPATIBILITY FOR CROSS-PLATFORMS EXISTENCE IN HEALTHCARE 5.0

When attempting to establish a security framework for healthcare 5.0, the heterogeneity of inbuilt networks poses a challenge. This characteristic makes it easier for different application domains to connect. But it also makes it difficult to design a security framework for healthcare 5.0 that works well. For instance, security framework for healthcare 5.0 needs to be strong and compatible. For example, when a smart home application needs to get data from a smart healthcare device, then the application may get access to the data from the target network without any issue. At the same time, it's crucial to keep in mind that data saved in the cloud servers need strong defense schemes. Therefore, to ensure continuous connectivity across various platforms of healthcare 5.0, we need to create robust and effective security framework for healthcare 5.0.

F. LACK OF LEGAL AND REGULATORY FRAMEWORKS

Most of the tools and technologies, which are used in healthcare 5.0 are in their very early phase. Since healthcare 5.0 handles sensitive healthcare data, therefore, it always has privacy related issues. Moreover, there is the lacking of legal and regulatory frameworks. If somethings wrong happens then it is very difficult to take care about certain things i.e., who will handle this, how this will be handled. Therefore, there is the essential need of design and implementation of legal and regulatory frameworks to mitigate the legal problems of healthcare 5.0 [3].

G. E-HEALTH POLICIES

Healthcare 5.0 is the amalgamation of various technologies and domains, i.e., medical science, machine learning, IoT, blockchain, tactile Internet, 5G communication technologies, etc. Under these circumstances, it is very important to tell that what should be our e-health policies. How the e-health policies should be designed, in what ways policies should be implemented. Therefore, we need some proper mechanisms for the designing of e-health policies in healthcare 5.0 [3].

H. LACK OF FUNDING

Healthcare 5.0 is the amalgamation of various tools and technologies as discussed earlier. For the proper deployment of these tools and technologies, we need some money. However, the countries, which do not have enough funding or have funding issues can not afford the use of these novel and advanced technologies, which seems very costly for them. Therefore, how to tackle these issues has become very important. Can we go for the invention of some cost effective solutions for healthcare 5.0 seem another important future research direction [3].

VIII. CONCLUDING REMARKS

The design of a secure healthcare 5.0 framework has been presented in this article. The details of various application of healthcare 5.0 were then provided. Next, the security requirements of healthcare 5.0 along with possible threats and attacks of healthcare 5.0 were also given. The details of threat model of healthcare 5.0 has been provided. Furthermore, the summary of existing security schemes in healthcare 4.0 and healthcare 5.0 was given, which was also included in their performance comparison. Finally, some future research directions of healthcare 5.0 were provided.

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] D. Saraswat, P. Bhattacharya, A. Verma, V. K. Prasad, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Explainable AI for healthcare 5.0: Opportunities and challenges," *IEEE Access*, vol. 10, pp. 84486–84517, 2022.

[2] M. Wazid, B. Bera, A. K. Das, and D. P. Singh, "IoT and blockchain technology-based healthcare monitoring," in *Blockchain in Digital Healthcare*, G. C. D. M. D. Borah, R. Moro-Visconti, Eds. Boca Raton, FL, USA: Chapman & Hall/ CRC, 2021, pp. 1–24.

[3] E. Mbunge, B. Muchemwa, S. Jiyane, and J. Batani, "Sensors and healthcare 5.0: Transformative shift in virtual care through emerging digital health technologies," *Global Health J.*, vol. 5, no. 4, pp. 169–177, Dec. 2021.

[4] S. Tian, W. Yang, J. M. L. Grange, P. Wang, W. Huang, and Z. Ye, "Smart healthcare: Making medical care more intelligent," *Global Health J.*, vol. 3, no. 3, pp. 62–65, Sep. 2019.

[5] R. Gupta, P. Bhattacharya, S. Tanwar, N. Kumar, and S. Zeadally, "GaRuDa: A blockchain-based delivery scheme using drones for healthcare 5.0 applications," *IEEE Internet Things Mag.*, vol. 4, no. 4, pp. 60–66, Dec. 2021.

[6] B. D. Deebak and F. Al-Turjman, "Smart mutual authentication protocol for cloud based medical healthcare systems using Internet of Medical Things," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 346–360, Feb. 2021.

[7] M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, and N. Kumar, "Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications," *J. Inf. Secur. Appl.*, vol. 56, Feb. 2021, Art. no. 102673.

[8] M. Kowalkiewicz. (2017). *Health 5.0: The Emergence of Digital Wellness*. [Online]. Available: https://medium.com/qut-cde/health-5-0-the-emergence-of-digital-wellness-b21fdff635b9

[9] N. Garg, M. Wazid, J. Singh, D. P. Singh, and A. K. Das, "Security in IoMT-driven smart healthcare: A comprehensive review and open challenges," *Secur. Privacy*, vol. 5, no. 5, p. e235, Sep. 2022.

[10] 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*, London, U.K., 2020, pp. 37–42.

[11] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, "BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for Internet of Medical Things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[12] M. Wazid, A. K. Das, and Y. Park, "Blockchain-envisioned secure authentication approach in AIoT: Applications, challenges, and future research," *Wireless Commun. Mobile Comput.*, vol. 2021, Oct. 2021, Art. no. 3866006.

[13] H. Su, A. Mariani, S. E. Ovur, A. Menciassi, G. Ferrigno, and E. De Momi, "Toward teaching by demonstration for robot-assisted minimally invasive surgery," *IEEE Trans. Autom. Sci. Eng.*, vol. 18, no. 2, pp. 484–494, Apr. 2021.

[14] R. C. Moon, H. Brown, and N. Rosenthal, "Healthcare resource utilization of patients with COVID-19 visiting U.S. hospitals," *Value Health*, vol. 25, no. 5, pp. 751–760, May 2022.

[15] M. Wazid, A. K. Das, and J.-H. Lee, "User authentication in a tactile internet based remote surgery environment: Security issues, challenges, and future research directions," *Pervas. Mobile Comput.*, vol. 54, pp. 71–85, Mar. 2019.

[16] M. Wazid, A. K. Das, M. K. Khan, A. A. D. Al-Ghaiheb, N. Kumar, and A. V. Vasilakos, "Secure authentication scheme for medicine anti-counterfeiting system in IoT environment," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1634–1646, Oct. 2017.

[17] F. Fernandez and G. C. Pallis, "Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective," in *Proc. 4th Int. Conf. Wireless Mobile Commun. Healthcare Transforming Healthcare Through Innov. Mobile Wireless Technol. (MOBIHEALTH)*, Athens, Greece, 2014, pp. 263–266.

[18] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, Mar. 2020.

[19] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S.-J. Lim, "Privacy ensured *e*-healthcare for fog-enhanced IoT based applications," *IEEE Access*, vol. 7, pp. 44536–44543, 2019.

[20] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall Press, 2010.

[21] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the Internet of Medical Things enabled healthcare systems: A survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019.

[22] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019.

[23] *Secure Hash Standard*, Standard FIPS PUB 180-1, Nat. Inst. Standards Technol. (NIST), U.S. Dept. Commerce, Gaithersburg, MD, USA, April 1995, Accessed: Jan. 2019. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[24] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020.

[25] M. Wazid, B. Bera, A. K. Das, S. P. Mohanty, and M. Jo, "Fortifying smart transportation security through public blockchain," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 16532–16545, Sep. 2022, doi: 10.1109/JIOT.2022.3150842.

[26] M. Wazid, A. K. Das, and S. Shetty, "TACAS-IoT: Trust aggregation certificate-based authentication scheme for edge enabled IoT systems," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 1–14, Nov. 2022, doi: 10.1109/JIOT.2022.3181610.

[27] M. Wazid and P. Gope, "BACKM-EHA: A novel blockchain-enabled security solution for IoMT-based e-healthcare applications," *ACM Trans. Internet Technol.*, pp. 1–27, Mar. 2022.

[28] W. Eddy. *TCP SYN Flooding Attacks and Common Mitigations*. Accessed: Mar. 2020. [Online]. Available: https://tools.ietf.org/html/rfc4987

[29] H. Wang, D. Zhang, and K. G. Shin, "Change-point monitoring for the detection of DoS attacks," *IEEE Trans. Depend. Sec. Comput.*, vol. 1, no. 4, pp. 193–208, Oct. 2004.

[30] G. A. Jaafar, S. M. Abdullah, and S. Ismail, "Review of recent detection methods for HTTP DDoS attack," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–10, Jan. 2019, doi: 10.1155/2019/1283472.

[31] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, pp. 1–17, 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/9/1788

[32] (2020). *What is an SQL Injection Attack?* Accessed: Mar. 2020. [Online]. Available: https://sucuri.net/guides/what-is-sql-injection/

[33] (2020). *Cross Site Scripting (XSS)*. Accessed: Mar. 2020. [Online]. Available: https://owasp.org/www-community/attacks/xss/

[34] 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.

[35] J. Ryoo, D. G. Han, S. K. Kim, and S. Lee, "Performance enhancement of differential power analysis attacks with signal companding methods," *IEEE Signal Process. Lett.*, vol. 15, pp. 625–628, 2008.

[36] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, "A multimodal malware detection technique for Android IoT devices using various features," *IEEE Access*, vol. 7, pp. 64411–64430, 2019.

[37] M. Wazid, A. K. Das, K.-K.-R. Choo, and Y. Park, "SCS-WoT: Secure communication scheme for web of things deployment," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10411–10423, Jul. 2022.

[38] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE J. Biomed. Health Informat.*, vol. 22, no. 4, pp. 1299–1309, Jul. 2018.

[39] M. Wazid, A. K. Das, and Y. Park, "Blockchain-enabled secure communication mechanism for IoT-driven personal health records," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 4, p. e4421, 2022.

[40] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 2, pp. 391–406, Dec. 2020.

[41] 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.

[42] M. Wazid and A. K. Das, "A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks," *Wireless Pers. Commun.*, vol. 94, no. 3, pp. 1165–1191, Jun. 2017.

[43] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Designing efficient sinkhole attack detection mechanism in edge-based IoT deployment," *Sensors*, vol. 20, no. 5, p. 1300, Feb. 2020.

[44] T. Ghosh, A. Roy, and S. Misra, "B2H: Enabling delay-tolerant blockchain network in healthcare for society 5.0," *Comput. Netw.*, vol. 210, Jun. 2022, Art. no. 108860.

[45] S. Aggarwal, N. Kumar, M. Alhussein, and G. Muhammad, "Blockchain-based UAV path planning for Healthcare 4.0: Current challenges and the way ahead," *IEEE Netw.*, vol. 35, no. 1, pp. 20–29, Jan. 2021.

[46] H. Qiu, M. Qiu, M. Liu, and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 9, pp. 2499–2505, Sep. 2020.

[47] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, "BinDaaS: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1242–1255, Apr. 2021.

[48] S. Shamshad, K. Mahmood, S. Hussain, S. Garg, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "An efficient privacy-preserving authenticated key establishment protocol for health monitoring in industrial cyber–physical systems," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5142–5149, Apr. 2022.

[49] R. Gupta, U. Thakker, S. Tanwar, M. S. Obaidat, and K.-F. Hsiao, "BITS: A blockchain-driven intelligent scheme for telesurgery system," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Hangzhou, China, Oct. 2020, pp. 1–5, doi: 10.1109/CITS49457.2020.9232662.

[50] S. Qahtan, K. Y. Sharif, A. A. Zaidan, H. A. Alsattar, O. S. Albahri, B. B. Zaidan, H. Zulzalil, M. H. Osman, A. H. Alamoodi, and R. T. Mohammed, "Novel multi security and privacy benchmarking framework for blockchain-based IoT healthcare industry 4.0 systems," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6415–6423, Sep. 2022.

[51] CIFS Health. *Internet of Medical Things: Challenges and Adoptions*. Accessed: Aug. 2022. [Online]. Available: https://cifs.health/backgrounds/internet-of-medical-things-challenges-and-adoptions/

[52] M. Lindström and M. Pirouzifard, "Trust in the healthcare system and mortality: A population-based prospective cohort study in southern Sweden," *SSM Population Health*, vol. 18, Jun. 2022, Art. no. 101109.

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 a 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 at the Department of Computer Science and Engineering, Manipal Institute of Technology, MAHE, Manipal, India. He was also a Postdoctoral Researcher at the Cyber Security and Networks Laboratory, Innopolis University, Innopolis, Russia. His current research interests include information security, remote user authentication, the Internet of Things (IoT), cloud/fog/edge computing, and blockchain. He has published more than 100 papers in international journals and conferences in the above areas. 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 TRANSACTIONS ON CONSUMER ELECTRONICS, 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. He has also received ''Excellent Reviewer'' award from IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING in 2022.

ASHOK KUMAR DAS (Senior Member, IEEE) received the M.Tech. degree in computer science and data processing, the M.Sc. degree in mathematics, and the Ph.D. degree in computer science and engineering from the IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India. He was also a Visiting Faculty with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA, USA. His current research interests include cryptography, system and network security, including security in smart grid, the Internet of Things (IoT), the Internet of Drones (IoD), the Internet of Vehicles (IoV), cyber-physical systems (CPS), cloud computing, intrusion detection, blockchain, and AI/ML security. He has authored over 330 papers in international journals and conferences in the above areas, including over 280 reputed journal papers. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He has been listed in the Web of Science (Clarivate^{TM}) Highly Cited Researcher 2022 in recognition of his exceptional research performance. 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 in 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. His Google Scholar H-index is 72 and i10-index is 204 with over 14,700 citations.

NOOR MOHD received the Ph.D. degree in computer science and engineering from the G. B. Pant Institute of Engineering and Technology, Pauri Garhwal, Uttarakhand, India. He is currently working as an Associate Professor with the Department of CSE, Graphic Era Deemed to be University, Dehradun, India. His research interests include self configurable networks, WSN/IoT, and intrusion detection systems.

YOUNGHO PARK (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. He is currently a Professor at the School of Electronics Engineering, Kyungpook National University. From 1996 to 2008, he was a Professor at the School of Electronics and Electrical Engineering, Sangju National University, South Korea. From 2003 to 2004, he was a Visiting Scholar at the School of Electrical Engineering and Computer Science, Oregon State University, USA. His research interests include information security, computer networks, and multimedia.