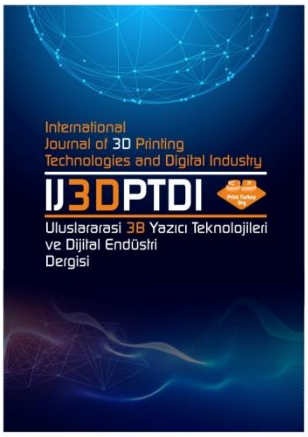

International
Journal of 3D Printing
Technologies and Digital Industry
IJ3DPTDI
Uluslararası 3B Yazıcı Teknolojileri
ve Dijital Endüstri
Dergisi

ULUSLARARASI 3B YAZICI TEKNOLOJİLERİ
VE DİJİTAL ENDÜSTRİ DERGİSİ

INTERNATIONAL JOURNAL OF 3D PRINTING
TECHNOLOGIES AND DIGITAL INDUSTRY

ISSN:2602-3350 (Online)
URL: https://dergipark.org.tr/ij3dptdi

CYBER ATTACKS FOR DATA BREACH AND POSSIBLE DEFENSE STRATEGIES IN INTERNET OF HEALTHCARE THINGS ECOSYSTEM

Yazarlar (Authors): Ahmet Ali Süzen*

Bu makaleye şu şekilde atıfta bulunabilirsiniz (To cite to this article): *Süzenş A. A., "Cyber Attacks For Data Breach and Possible Defense Strategies in Internet of Healthcare Things Ecosystem" Int. J. of 3D Printing Tech. Dig. Ind., 7(1): 55-63, (2023).*

DOI: 10.46519/ij3dptdi.1240743

Araştırma Makale/ Research Article

Erişim Linki: (To link to this article): https://dergipark.org.tr/en/pub/ij3dptdi/archive

CYBER ATTACKS FOR DATA BREACH AND POSSIBLE DEFENSE STRATEGIES IN INTERNET OF HEALTHCARE THINGS ECOSYSTEM

Ahmet Ali Süzen[a*]

[a*] Isparta University of Applied Sciences, Faculty of Technology, Department of Computer Engineering, TURKEY

Corresponding Author: *ahmetsuzen@isparta.edu.tr*

(**Received:** 23.01.2023; **Revised:** 02.02.2023; **Accepted:** 25.04.2023)

ABSTRACT

In this study, the IoT devices used for home patient care have been evaluated for the sources of data leaks and possible security measures that may be experienced in the process from the data owner to data storage stage. In order to identify possible risks and threats, 4 different target scenarios were created. These scenarios include home internet connection resources, data transfer, data storage, and access. 8 different attacks were applied to these possible scenarios where data leakage could occur. In addition, recently, blockchain applications and smart contract transmissions are preferred for data security. Among the attack scenarios, Short Address Attacks and Smart Contract Overflow are attack methodologies used for blockchain security. In particular, denial of service was encountered in all attacks on wireless. Configuration errors, wrong product selection, use of weak passwords, and default configurations in the IOT ecosystem seem to be the main sources of data leaks. As a result, the study includes possible attacker scenarios and possible vulnerabilities have been extracted within the scope of real scenarios. In addition, the measures to be taken against these vulnerabilities were evaluated and recommendations were given to take maximum security measures to prevent data leaks from within the IoT ecosystem.

Keywords: IoT, Healthcare, Cyber Security, Data Leak.

1. INTRODUCTION

Health services can be defined as the whole of services performed by experts to prevent, diagnose and treat diseases, injuries, physical and mental disorders experienced by people [1]. The improvement of health services is one of the most important factors that increase the comfort of human life [2]. The improvement and development of health services day by day are carried out simultaneously with technological developments. The reason for this is based on the need for critical data and instant intervention in healthcare services [3]. Almost all of the developed systems are used to store or process the health information of the patient followed by the internet infrastructure. These developments seem to form the basis of IoT systems in the field of health [4].

The widespread use and rapid growth of the IoT ecosystem in the field of health has enabled the increase of sensitive data in digital environments today [5]. It is a great threat for sensitive and critical health data to fall into the hands of attackers. Recently, it has been discussed how the developed systems are secure in terms of personal data privacy and data leakage threats [6]. When the devices in the systems used are examined, it is seen that they do not apply sufficient security procedures. The widespread and rapid use of IoT devices reveals security vulnerabilities in these devices and creates question marks in data security, integrity, and confidentiality criteria in health data [7].

In this study, the resilience, risks, and possible importance of IoT devices and data transfer layers used in-home patient care services against possible cyber-attacks were evaluated. First, attack matrices for different layers were developed and attacks were carried out in test environments. The risks and data leakage sources obtained as a result of these attacks were evaluated and information about possible precautions were given.

2. INTERNET OF HEALT CARE THINGS ECOSYSTEM

Along with the use and advantages of IoT systems in Industry 4.0, it has also created a vision in the follow-up of people in need of care at home [8,9]. Increasing healthcare costs, rapid response, and instant monitoring make IoT devices preferred in-home patient care. Regular follow-up and monitoring of the person's health information also increases the determination of the experts to diagnose [10]. The increase in the amount of data collected has also paved the way for the spread of artificial intelligence systems. With this, the data has brought with it problems regarding the protection and privacy of this data. Transferring and storing data sources at home to experts via the internet brings security measures to the fore [11].

Recently, blockchain technology has been preferred for the protection of health data due to its security and integrity capabilities. When the literature studies are examined, it is seen that the storage of blockchain-based health data will minimize the possible risks. In this part of the study, studies in the literature that use blockchain technology for data privacy are examined. In their study, Adanur et al. used fog computing and blockchain technology together. A blockchain-based system has been proposed for the confidentiality and transmission of analysis and laboratory results obtained from individuals in the field of health. In this way, it is said that the concerns about the confidentiality and security of the transmitted data are avoided [12]. Rathee et al. proposed a model for the protection of data created with IoT technology in the field of health. The values obtained from the patients, the transfer of these values, the processes of guaranteeing the unchangeability of the drugs in the prescriptions created for treatment were provided with a model they named Healthchain Multimedia. The proposed model has been tested with Falsification Attraction and Wormhole attacks and successful results have been obtained [13]. Dwivedi et al. propose a distributed blockchain structure to eliminate the potential danger of privacy and security after medical data is obtained with IoT technology. Biological values obtained from the patient through sensors are included in the blockchain system by wrapping them with symmetric encryption methods known as the ARX algorithm to the physician [14]. Griggs et al. proposed a secure system, the infrastructure of which was prepared with IoT technology and supported by smart contracts, which can perform real-time follow-up of patients. All processes of patient records can be easily followed without being manipulated. According to the status of the data received from the wireless body sensors, a notification will be sent to the relevant physician through solid contracts. In this way, correct and early intervention opportunities will be provided for the patient [15]. Srivastava et al. proposed a model that shows how the remote patient monitoring system established with the IoT infrastructure is secured with blockchain technology. The proposed model promises secure data communication over the network. Data is stored on the cloud with the ARX encryption method. Also, a double encryption scheme is used to make the symmetric key more secure over the network, and they use the Concept Diffie-Hellman Key Exchange Technique on the blockchain base, which protects the public key from an intruder [16].

The control of the systems in the house has been provided by electronic systems with the introduction of smart houses into our lives. Especially in the first systems, the controls that started with the command and sound were shaped by joint movements and autonomous systems [17]. Wired and wireless networks established in the house collect data and provide remote control. Together with IoT devices, interconnected devices can process their own data and make autonomous decisions [18]. The increase in systems and the production of data also attract the attention of attackers. Possible configuration errors, use of vulnerable systems or technologies increase data leaks [19]. In this study, it is aimed to identify threats and measures to ensure the security of health records within the IoT ecosystem. In this context, studies carried out for home patient care in order to create the attack matrix were examined and the technologies used were determined. As seen in Table 1, the technologies preferred by the studies related to the production, processing, monitoring, and storage of health data are listed. Thus, the framework of the attack matrix to be used in our study was formed.

Table 1. Examination of home healthcare practices in terms of the technologies they use.

Study	Study Purpose	Technology
[20]	Early Diagnosis of Heart Attack	MMS and EGPRS
[21]	System of care and emergency medical assistance of chronic lung patients	WIFI and GPRS
[22]	Remote Follow-up of Patients in Coma	GSM and WIFI
[23]	Correct location of faults	Arduino Uno and GPS
[24]	To be able to store the basic health parameters of patients	Raspberry Pi 3, Sensors, BLE Adapter, GSM Module
[25]	Remote Follow-up of Patients in Coma	Arduino Uno, GSM Module, Cloud Storage
[26]	Continuous monitoring of patients	Arduino and WIFI
[27]	Storage of medical data	Zigbee and WBAN
[28]	Storage and monitoring of medical data	Intel Galileo Gen 2, XBEE S2 Sensor
[12]	Secure transmission of medical data	Sensors and Blockchain
[13]	Ensuring the security of medical data and prescriptions	Sensors, IoT, Blockchain
[14]	Keeping medical data encrypted on a distributed blockchain structure	Sensors, IoT, Blockchain
[15]	Real-time secure patient follow-up thanks to smart contracts	IoT, smart contracts, Blockchain
[16]	Developing a secure remote patient monitoring system	IoT, smart contracts, Blockchain

3. CYBER ATTACKS FOR DATA BREACH IN INTERNET OF HEALTHCARE THINGS ECOSYSTEM

IoT networks basically consist of 4 layers: devices, data, connection and users. In particular, the device and data layers face more attacks. In-network short-distance networks (Bluetooth, NFC, WIFI, Zigbee, etc.) are used in the creation of sensitive health records within the IoT ecosystem. After the data is collected in the network, it is transferred to the wide network with different protocols as shown in Table 2. During this process, it may face data leaks and system blockages. In this study, the risks and possible precautions against leaks of patient care data produced within the IoT ecosystem were evaluated. In the tests performed to detect the potential risks of the ecosystem, mock test data were used.

Table 2. Network technologies used in the transmission of health records in the IOT ecosystem

Communication	Standard
WIFI	IEEE 802.11 a/c/b/ d/g/n
WiMAX	IEEE 802.16
WSN	IEEE 802.15.4
LR-WPAN	IEEE 802.15.4 (ZigBee)
Mobile	2G-GSM, CDMA 3G-UMTS, CDMA2000 4G-LTE
LoRa WAN	LoRaWAN R1.0

3.1. Cyber Attacks for Data Breach in Internet of Healthcare Thinks Ecosystem

A practical attack scenario has been developed, as shown in Figure 1, in order to detect possible vulnerabilities in Call Control or SMS controlled systems where the internet connection in the house is via GPRS. HackRF Dongles are used for this. In the attack scenario, a temporary GSM line was purchased and tests were carried out with the open-source mobile communication called osmocon. The test phone was connected to the computer via USB-TTL and mobile communication was started via osmocon. Basically, it is aimed to capture the information and wireless traffic transmitted by GSM within the IoT ecosystem. The first goal of this attack is to capture the International Mobile Subscriber Identity (IMSI). Used to receive IMSI data, IMSI Catcher acts as a base station and allows the target to connect to itself. The following tools are preferred for attacking IoT networks using GSM-based communication. Application tests were carried out on the Kali operating system.

- Wireshark
- HackRF
- kalibrate
- gr-gsm

Wireshark is an open source software that enables the examination and monitoring of the network data it is connected to from the interface. Network packets can be monitored or recorded instantly with Wireshark. Detailed analysis of the recorded network data can be performed later.

The system created as a result of the hardware and software requirements given above for obtaining GPRS and SMS data is called IMSI-Catcher. It stands midway between the station and the telephone, as shown in Figure 1.

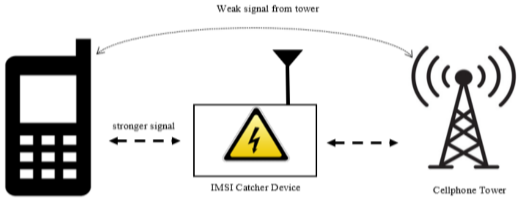


Figure 1. Example attack scenario diagram.

After the applications are installed on the system, first of all, the frequency band ranges should be known in order to monitor the GSM traffic (Turkey: 900 MHz -1800 MHz). When the scenario runs, base stations close to the test environment are detected. Then, GSM traffic was captured with Wireshark. The following filtering is used to see the data of GSMTAP protocol in the Wireshark packet monitor.

wireshark -k -f udp -Y gsmtap -i lo

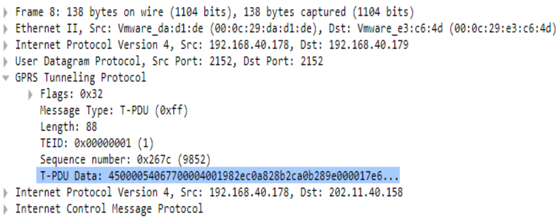
The airprobe_rtlsdr_capture tool was used to capture the SMS traffic. The tool is used to capture SMS data in traffic with the following parameter.

airprobe_SMS.py -c capture.pcap -s 1000000 -f 949200000 -m SDCCH8 -t 2 -e 1 -k 0x0E,0x10,0xEA,0xF3,0x02,0x99,0xF2,0xC4

Here -e 1 specifies the A5/1 algorithm and -k specifies 0x0E,0x10.0xEA,0xF3.0x02.0x99.0xF2.0xC4 Kc. It is the key used to wirelessly encrypt the KC telephone network.

GPRS Tunneling Protocol (GTP) traffic was monitored for possible threats in the transmission of health data via GPRS within the IOT ecosystem, as seen in Figure 2. There are two different types of traffic in the scenario, GTP Policy Out and GTP Policy In. By examining the GTP traffic, it has been seen that it is possible to access the data of the GPRS flow.

- GTP Policy Out is traffic from client to server
- GTP Policy In is the traffic from the server to the client



```
▸ Frame 8: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
▸ Ethernet II, Src: Vmware_da:d1:de (00:0c:29:da:d1:de), Dst: Vmware_e3:c6:4d (00:0c:29:e3:c6:4d)
▸ Internet Protocol Version 4, Src: 192.168.40.178, Dst: 192.168.40.179
▸ User Datagram Protocol, Src Port: 2152, Dst Port: 2152
▾ GPRS Tunneling Protocol
    ▸ Flags: 0x32
      Message Type: T-PDU (0xff)
      Length: 88
      TEID: 0x00000001 (1)
      Sequence number: 0x267c (9852)
      T-PDU Data: 4500005406770000400198 2ec0a828b2ca0b289e000017e6...
▸ Internet Protocol Version 4, Src: 192.168.40.178, Dst: 202.11.40.158
▸ Internet Control Message Protocol
```

Figure 2. Wireshark monitoring of GPRS traffic.

3.2. Attack for Wireless Networks Controlled IOT Ecosystems

The use of wireless networks in smart home systems and IOT ecosystem is carried out with many technologies as shown in Table 1. WIFI offers an average data transfer rate of 1 Mb/s – 6.75 Gb/s and WiMAX offers a data transfer rate between 1 Mb/s – 1 Gb/s. Recently, especially the large number and size of data has brought the widespread use of WIFI and WiMAX to the fore. In the scheme shown in Figure 3, first of all, 8 processes were created on the attack computer and DDOS attacks were made on the detected wireless networks. In the second stage, it has been determined whether it is possible to access the health records and sensitive data in the IOT network with the attack types given below.

- Access Control Attacks
- Confidentiality Attacks
- Integrity Attacks
- Authentication Attacks

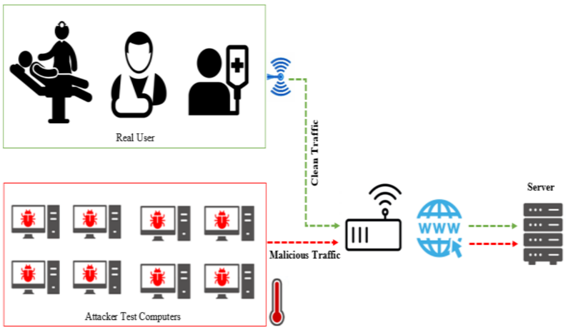
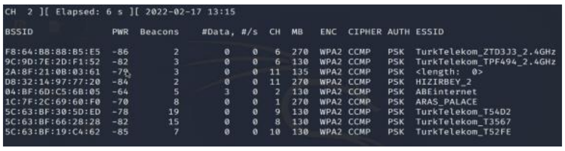


Figure 3. Anomaly diagram for WIFI and WIMAX networks.

First, the attacking computer was put in the USB WIFI adapter monitoring mode, and the WIFI and WIMAX network devices around were listed as shown in Figure 4. For attack targets, wireless network signals within 5 km of average open area were scanned. As a result of the scanning, the ESSIDs of the sample IoT networks were determined.



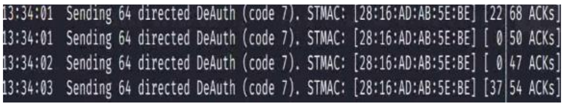
```
CH  2 ][ Elapsed: 6 s ][ 2022-02-17 13:15

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

F8:64:B8:88:B5:E5  -86        2        0    0   6  270  WPA2 CCMP   PSK  TurkTelekom_ZTD3J3_2.4GHz
9C:9D:7E:2D:F1:52  -82        3        0    0   6  130  WPA2 CCMP   PSK  TurkTelekom_TPF494_2.4GHz
2A:8F:21:0B:03:61  -79        3        0    0  11  135  WPA2 CCMP   PSK  <length:  0>
D8:32:14:97:77:20  -84        2        0    0  11  270  WPA2 CCMP   PSK  HIZIRBEY_2
04:BF:6D:C5:6B:05  -64        5        3    0   2  130  WPA2 CCMP   PSK  ABEinternet
1C:7F:2C:69:60:F0  -70        8        0    0   1  270  WPA2 CCMP   PSK  ARAS_PALACE
5C:63:BF:30:5D:ED  -78       19        0    0   9  130  WPA2 CCMP   PSK  TurkTelekom_T54D2
5C:63:BF:66:28:28  -82       15        0    0   8  130  WPA2 CCMP   PSK  TurkTelekom_T3567
5C:63:BF:19:C4:62  -85        7        0    0  10  130  WPA2 CCMP   PSK  TurkTelekom_T52FE
```

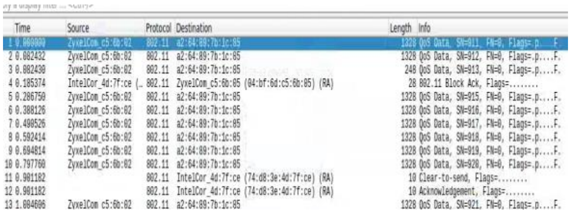
Figure 4. Monitoring Mode Scanner.

Basically, in the IoT ecosystem with WIFI and WIMAX networks, firstly, the selected user is dropped from the network by sending deaulth packets as seen in Figure 5, in order to determine the passwords of the devices belonging to the users. When the active device wants to connect to the network again, its packets are captured and saved as a cap file. Thus, in the registered packets, sensitive data and network password information are searched by performing packet analysis with Wireshark, as in Figure 6.



```
13:34:01  Sending 64 directed DeAuth (code 7). STMAC: [28:16:AD:AB:5E:BE] [22|68 ACKs]
13:34:01  Sending 64 directed DeAuth (code 7). STMAC: [28:16:AD:AB:5E:BE] [ 0|50 ACKs]
13:34:02  Sending 64 directed DeAuth (code 7). STMAC: [28:16:AD:AB:5E:BE] [ 0|47 ACKs]
13:34:03  Sending 64 directed DeAuth (code 7). STMAC: [28:16:AD:AB:5E:BE] [37|54 ACKs]
```

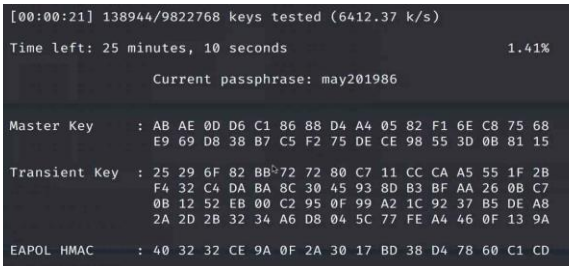
Figure 5. Sending deauth packets.



```
   Time        Source               Protocol Destination                                Length Info
 1 0.000000    ZyxelCom_c5:6b:02    802.11   a2:64:89:7b:1c:85                            1328 QoS Data, SN=911, FN=0, Flags=.p....F.
 2 0.082432    ZyxelCom_c5:6b:02    802.11   a2:64:89:7b:1c:85                            1328 QoS Data, SN=912, FN=0, Flags=.p....F.
 3 0.082430    ZyxelCom_c5:6b:02    802.11   a2:64:89:7b:1c:85                             248 QoS Data, SN=913, FN=0, Flags=.p....F.
 4 0.185374    IntelCor_4d:7f:ce (… 802.11   ZyxelCom_c5:6b:05 (04:bf:6d:c5:6b:05) (RA)     28 802.11 Block Ack, Flags=........
 5 0.286750    ZyxelCom_c5:6b:02    802.11   a2:64:89:7b:1c:85                            1328 QoS Data, SN=915, FN=0, Flags=.p....F.
 6 0.388126    ZyxelCom_c5:6b:02    802.11   a2:64:89:7b:1c:85                            1328 QoS Data, SN=916, FN=0, Flags=.p....F.
 7 0.490526    ZyxelCom_c5:6b:02    802.11   a2:64:89:7b:1c:85                            1328 QoS Data, SN=917, FN=0, Flags=.p....F.
 8 0.592414    ZyxelCom_c5:6b:02    802.11   a2:64:89:7b:1c:85                            1328 QoS Data, SN=918, FN=0, Flags=.p....F.
 9 0.694814    ZyxelCom_c5:6b:02    802.11   a2:64:89:7b:1c:85                            1328 QoS Data, SN=919, FN=0, Flags=.p....F.
10 0.797760    ZyxelCom_c5:6b:02    802.11   a2:64:89:7b:1c:85                            1328 QoS Data, SN=920, FN=0, Flags=.p....F.
11 0.901182                         802.11   IntelCor_4d:7f:ce (74:d8:3e:4d:7f:ce) (RA)     10 Clear-to-send, Flags=........
12 0.901182                         802.11   IntelCor_4d:7f:ce (74:d8:3e:4d:7f:ce) (RA)     10 Acknowledgement, Flags=........
13 1.004696    ZyxelCom_c5:6b:02    802.11   a2:64:89:7b:1c:85                            1328 QoS Data, SN=921, FN=0, Flags=.p....F.
```

Figure 6. Examination of packets with Wireshark.

The network password HASH value obtained after the packet analysis of the target IoT devices should be estimated. As shown in Figure 7, the hash matching process has been completed by uploading the wordlist with the software named aircrack and hashcat.



```
[00:00:21] 138944/9822768 keys tested (6412.37 k/s)

Time left: 25 minutes, 10 seconds                           1.41%

                 Current passphrase: may201986

Master Key     : AB AE 0D D6 C1 86 88 D4 A4 05 82 F1 6E C8 75 68
                 E9 69 D8 38 B7 C5 F2 75 DE CE 98 55 3D 0B 81 15

Transient Key  : 25 29 6F 82 BB 72 72 80 C7 11 CC CA A5 55 1F 2B
                 F4 32 C4 DA BA 8C 30 45 93 8D B3 BF AA 26 0B C7
                 0B 12 52 EB 00 C2 95 0F 99 A2 1C 92 37 B5 DE A8
                 2A 2D 2B 32 34 A6 D8 04 5C 77 FE A4 46 0F 13 9A

EAPOL HMAC     : 40 32 32 CE 9A 0F 2A 30 17 BD 38 D4 78 60 C1 CD
```

Figure 7. Brute force attack on IOT networks.

Hashcat is an attack software with GPU and CPU support that enables the detection of open data from the obtained hash data. In decoding the hash data obtained from WIFI and WIMAX networks, a wordlist consisting of seven million data was used by using hashcat GPU support.

An Evil Twin attack was carried out by simultaneously creating a fake wireless network while IoT devices were exposed to the deauth attack. In the IoT ecosystem, due to the communication network and its protocols between devices, the device automatically connects to the network device that signals closer to it. However, since they both have the same name, the user cannot notice it. Thus, it is aimed to connect IoT devices to the fake network and collect data packets. In addition, a Man in the Middle – MITM attack was carried out on IoT devices whose passwords were detected. With this attack, tests of accessing the data flow of IoT devices, manipulating and blocking the data were carried out.

3.3. Attack For Blockchain-based IOT Ecosystems

Although the blockchain was first mentioned with cryptocurrencies, it has recently been widely used to ensure data security. In particular, ensuring the security and integrity of sensitive data is carried out with blockchain applications. It provides its own security with the mechanisms used in the blockchain structure. However, although it is not possible to provide 100% security, there are possible attacks and risks in the blockchain [29]. Due to its blockchain structure, it can face the following attacks and risks [30].

- 51% Attack
- Long-Range Attack
- P+ Epsilon Attack
- Brute Force Attack
- Distributed Denial-of-Service (DDoS)
- Border Gateway Protocol Hijacking (BGP)

- Balance Attack
- Mining Pool Attacks
- Sybil Attack

The attacks carried out within the scope of the study were carried out in the transfer of the health records shown in Figure 8, which we previously developed, to the expert with the smart contract and their storage in the blockchain [31]. In the case study, data storage is stored in BlockChainDB and Mongodb. C# programming language interface software has been developed to monitor the collected data.

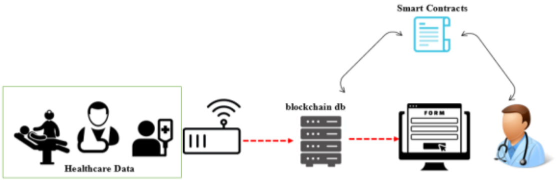


Figure 8. Blockchain-based attack testnet.

First, the Smart Contract Overflow and Underflow method was tested for accessing the data stored in the blockchain. With this method, it occurs in transactions that accept unauthorized health data or value. A smart contract overflow basically occurs when more than the maximum value is supplied. Commonly smart contracts are written in Solidity, which can handle numbers up to 256 bits, where an increment of 1 causes overflow.

As the second attack, a short address attack was made. A Short Address Attack is basically similar to a SQL injection error and occurs when an insufficient data flow is detected. This vulnerability is an input validation error and is mostly exposed by the sender due to weak transaction generation code. Finally, a DDOS attack was applied to test the continuity of communication in all possible scenarios.

3.4. Potential Post-Attack Threat and Risks

The results obtained as a result of attacks on the test environment where devices are controlled by call, sms and GPRS in the IoT ecosystem are given in Table 3. As a result of four different attacks, it was observed that GSM operator headers, call and SMS information were accessed, especially in attacks with IMSI Catcher hardware. In GSM-based systems, it has been determined that there are cases where access to API or database is performed in the target system and session verification is not used. As a result, it is possible to send parameters to IoT devices or to monitor and copy incoming sensitive data. The attacks on the target system and the results show that the security structures in GSM-based systems are insufficient.

Table 3. Attack evaluation of GSM, SMS and GPRS based IoT systems.

Attack Type	Result
IMSI Catcher	Data Leak - MCC (Mobile Country Code), MNC (Mobile Network Code) and MSIN (Mobile Subscriber Identification Number)
GSMTAP	Data Leak (Call Parameters)
GTP	Data Leak (SMS DATA)
DDOS	Success (service is blocked)

Five different attack modeling has been carried out on WIFI and WIMAX networks, which are more commonly preferred in the communication of IoT devices. Incomplete configuration of IoT devices and edge devices in the data collection and transfer process is one of the most common mistakes. Table 4 shows the attacks on target systems and their results. Although the passwords of the default wireless networks meet the strong password criteria, it is seen that modem, access point (AP), or switch interface configurations are not made. With the MITM attack, access to the data produced by IoT devices is provided. In addition, it has been determined that devices can be dropped from the network with a deauth attack and redirected to fake connections with an Evil Twin attack. In cases where continuous data flow is made and critical health data is monitored instantly, data flow can be interrupted by DDOS attacks. This is expected to result in life-threatening risks.

Table 4. Attack evaluation of WIFI and WIMAX-based IoT systems

Attack Type	Result	Password Detection
Brute Force (aircrack)	-	Fail
Hashcat	-	Yes
MITM	Data Leak	-
Evil Twin	Data Leak	Yes
DDOS	Success (service is blocked)	-

In order to ensure data security, data is stored in the blockchain structure in wired and wireless communication solutions and transferred to experts with smart contracts. Data from within the IoT ecosystem is mostly transferred to the wide network with web services. For this reason, possible risks in WIFI and WIMAX networks are predicted to be a threat within blockchain-based systems. Three different attacks were applied to the test blockchain network as shown in Table 5. It is seen that the probability of data leakage in blockchain-based systems is very low. However, in these attacks, data access problems are experienced during the transfer of health data to specialists.

Table 5. Attack evaluation of blockchain IoT systems.

Attack Type	Result	Password Detection
Brute Force (aircrack)	-	Fail
Hashcat	-	Yes
MITM	Data Leak	-
Evil Twin	Data Leak	Yes
DDOS	Success (service is blocked)	-

In order to ensure data security, data is stored in the blockchain structure in wired and wireless communication solutions and transferred to experts with smart contracts. Data from within the IoT ecosystem is mostly transferred to the wide network with web services. For this reason, possible risks in WIFI and WIMAX networks are predicted to be a threat within blockchain-based systems. Three different attacks were applied to the test blockchain network as shown in Table 5. It is seen that the probability of data leakage in blockchain-based systems is very low. However, in these attacks, data access problems are experienced during the transfer of health data to specialists.

4. MEASURES TO PROTECT SENSITIVE HEALT RECORDS IN THE IOT ECOSYSTM

The process of collecting, transferring, and monitoring sensitive health data in the IoT ecosystem needs to be carefully structured. Many of the possible risks and threats appear to be caused by configuration errors. Data leaks and risks have been determined as a result of different attack types and aggressive behavior in test environments. Basically, security requirements must include confidentiality, integrity, source verification, data up-to-date, service integrity, and key management. In the light of the data obtained, the precautions to be taken for the protection and secure communication of sensitive health records produced within the framework of IoT home patient care services are listed as follows.

- In general, using a Virtual Private Network (VPN) to prevent web traffic from being monitored by attackers helps prevent MITM attacks.
- Data flow of IoT sensors configured in the house is provided by WIFI. Here, the wireless passwords of the modem and AP devices must be at least 10 characters long and a combination of letters-numbers-special characters. In addition, the default configuration of the device interface login screens needs to be adjusted individually.
- Update and security patches of devices used in IoT networks should be checked periodically.
- Firewall should be preferred in order to instantly monitor wired and wireless network traffic and detect possible anomalies.
- IoT devices must be registered to the network with MAC authentication.
- A secure data transfer environment should be created by using strong encryption in Bluetooth, Zigbee, Wi-Fi, GPRS, LoRa, NFC and similar IoT protocols.
- Network capacity and bandwidth should be limited to the lowest value that will be sufficient for the IoT system to operate.
- The daily internet used in the home and the internet networks used by IoT devices should be partitioned.
- IoT protocols such as Message Queue Telemetry Transport (MQTT), Data Distribution Service (DDS), Extensible Messaging and Presence Protocol (XMPP), Advanced Message Queuing Protocol (RestFull HTTP), or Constrained Application Protocol (CoAP) should be preferred.

5. CONCLUSION

Collecting and processing sensitive health records with IoT devices has become a life abandonment. In this and beyond, low-complexity and high-reliability solutions should be configured for IoT networks. In this study, the current risks, potential threats, and security measures of the IoT ecosystem used in home patient care processes are evaluated. First of all, IoT studies related to patient care were examined and the IoT technologies used were determined. An attack matrix was created and test attacks were made with the findings obtained. The risks, threats, and possible precautions obtained after the attacks are reported. Today, it is seen that the basis of threats is wrong and incomplete configurations. While designing security mechanisms in the IoT ecosystem, each IoT device layer should be arranged with security requirements in mind. Methods that are resistant to denial of service and eavesdropping attacks should be developed at the physical and media access layers.

REFERENCES

1. Thimbleby, H., "Technology and the future of healthcare", Journal of public health research, Vol. 2, Issue 3, Pages 160-167, 2013.

2. Bhavnani, S. P., Narula, J., & Sengupta, P. P., "Mobile technology and the digitization of healthcare", European heart journal, Vol. 37, Issue 18, Pages 1428-1438, 2016.

3. Strudwick, G., "Predicting nurses' use of healthcare technology using the technology acceptance model: an integrative review" CIN: Computers, Informatics, Nursing, Vol. 33, Issue 5, Pages 189-198, 2015.

4. Farahani, B., Firouzi, F., & Chakrabarty, K., "Healthcare iot", In Intelligent internet of things , Pages 515-545, Springer, 2020.

5. Zakaria, H., Bakar, N. A. A., Hassan, N. H., & Yaacob, S., "IoT security risk management model for secured practice in healthcare environment", Procedia Computer Science, Vol. 161, Pages 1241-1248, 2019.

6. Chacko, A., & Hayajneh, T., "Security and privacy issues with IoT in healthcare", EAI Endorsed Transactions on Pervasive Health and Technology, Vol. 4, Issue 14, Pages 1-7, 2018.

7. Gopalan, S. S., Raza, A., & Almobaideen, W., "IoT Security in Healthcare using AI: A Survey", In 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Pages 1-6, IEEE, 2021.

8. Nausheen, F., & Begum, S. H., "Healthcare IoT: benefits, vulnerabilities and solutions", In 2018 2nd International Conference on Inventive Systems and Control (ICISC), Pages 517-522, IEEE, 2018.

9. Gürfidan, R., Ersoy, M., "A new approach with blockchain based for safe communication in IoT ecosystem", J. of Data, Inf. and Manag. Vol. 4, Pages 49–56, 2022.

10. Moosavi, S. R., Nigussie, E., Levorato, M., Virtanen, S., & Isoaho, J., "Performance analysis of end-to-end security schemes in healthcare IoT", Procedia computer science, Vol. 130, Pages 432-439, 2018.

11. Pradhan, B., Bhattacharyya, S., & Pal, K., "IoT-based applications in healthcare devices", Journal of healthcare engineering, Vol. 2021, Pages 1-18, 2021.

12. Adanur, B., Bakir-Güngör, B., & Soran, A., "Blockchain-based fog computing applications in healthcare", In 2020 28th Signal processing and communications applications conference (SIU), Pages 1-4, IEEE, 2020.

13. Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R., "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology", Multimedia Tools and Applications, Vol. 79, Issue 15, Pages 9711-9733, 2020.

14. Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R., "A decentralized privacy-preserving healthcare blockchain for IoT", Sensors, Vol. 19, Issue 2, Pages 326, 2019.

15. Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T., "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring", Journal of medical systems, Vol. 42, Issue 7, Pages 1-7, 2018.

16. Srivastava, G., Crichigno, J., & Dhar, S., "A light and secure healthcare blockchain for iot medical devices", In 2019 IEEE Canadian conference of electrical and computer engineering (CCECE), Pages 1-5. IEEE, 2019.

17. Jie, Y., Pei, J. Y., Jun, L., Yun, G., & Wei, X., "Smart home system based on IOT technologies", In 2013 International conference on computational and information sciences, Pages 1789-1791, IEEE, 2013.

18. Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M., "A review of smart home applications based on Internet of Things", Journal of Network and Computer Applications, Vol. 97, Pages 48-65, 2017.

19. Santoso, F. K., & Vun, N. C., "Securing IoT for smart home system", In 2015 international

symposium on consumer electronics (ISCE), Pages 1-2, IEEE, 2015.

20. Fidan, U., Aktürk, T. B., “Application of GPRS Based 12 Derivation EKG Telemonitoring System For 112 Emergency Service”, Engineering Sciences, Vol. 5, Issue 1, Pages 79-87, 2010.

21. Işık, A. H., “Development of Intelligent Care and Emergency Medical Assistance System for the Follow-up of Chronic Lung Patients with Mobile Communication Technology”. Pages 107. Gazi University, Informatics Institute, Turkey, 2012.

22. Fatih, S. M., Muneer, A., Mungur, D., & Badawi, A., “Integrated health monitoring system using GSM and IoT”, In 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Pages 1-7, IEEE, 2018.

23. Kanani, P., & Padole, M., “Real-time Location Tracker for Critical Health Patient using Arduino, GPS Neo6m and GSM Sim800L in Health Care”, In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Pages 242-249, IEEE, 2020.

24. Swaroop, K. N., Chandu, K., Gorrepotu, R., & Deb, S., “A health monitoring system for vital signs using IoT. Internet of Things”, Vol. 5, Pages 116-129, 2019.

25. Tamilselvi, V., Sribalaji, S., Vigneshwaran, P., Vinu, P., & GeethaRamani, J., “IoT based health monitoring system”, In 2020 6th International conference on advanced computing and communication systems (ICACCS), Pages 386-389, IEEE, 2020.

26. Yeri, V., & Shubhangi, D. C., “IoT based real time health monitoring”, In 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Pages 980-984, IEEE, 2020.

27. Akkaş, M. A., Sokullu, R., & Cetin, H. E., “Healthcare and patient monitoring using IoT”, Internet of Things, Vol. 11, Issue 100173, Pages 1-12, 2020.

28. Kodali, R. K., Swamy, G., & Lakshmi, B., “An implementation of IoT for healthcare”, In 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Pages 411-416, IEEE, 2015.

29. Huynh, T. T., Nguyen, T. D., & Tan, H., “A survey on security and privacy issues of blockchain technology”, In 2019 international conference on system science and engineering (ICSSE), Pages 362-367, IEEE, 2019.

30. Sayeed, S., & Marco-Gisbert, H., “Assessing blockchain consensus and security mechanisms against the 51% attack”, Applied Sciences, Vol. 9, Issue 9, Pages 1788, 2019.

31. Süzen, A.A., & Duman, B., “Protecting the Privacy of IoT-Based Health Records Using Blockchain Technology” In Internet of Medical Things, Pages 35-54, Springer, Cham, 2021.