Cryptanalysis of Authentication Scheme in IoMT Paradigm

Priyanshi Thakkar, Nishant Doshi, Kapil Sharma

Pandit Deendayal Energy University, Gandhinagar, Gujarat

ABSTRACT – *The integration of the healthcare sector with the Internet of Things (IoT) framework has given rise to the Internet of Medical Things (IoMT). IoMT enables the generation, transmission, and analysis of medical data among interconnected healthcare IT systems, sensors, and management software.Due to the ongoing advancements in IoT and the global impact of the COVID-19 pandemic, IoMT has garnered significant attention for its potential in medical data management, real-time health monitoring, and remote treatment. Yet, the delicate character of medical data within the IoMT landscape has sparked apprehensions about security, underscoring the need for robust security protocols to protect medical systems and IoT devices. This paper presents an in-depth exploration and evaluation of an IoMT scheme that incorporates a hybrid security approach, combining password-based authentication with a fuzzy extractor for biometric authentication. To address limitations identified in previous research, we propose a novel system model and attack model. Through a combination of formal and informal analyses, we assess the security capabilities of the proposed method. Additionally, we conduct a comprehensive examination of computational expenses, highlighting its comparative efficacy in relation to existing approaches.*

Terms of importance– IoMT; remote authentication; Internet of Things, Healthcare.

1. INTRODUCTION

The convergence of the healthcare sector with the extensive functionalities of the Internet of Things (IoT) has spurred the evolution of the Internet of Medical Things (IoMT). This evolution facilitates seamless management, transfer, and analysis of data within healthcare frameworks. This burgeoning field has become increasingly significant, particularly in the context of the current global landscape shaped by technological advancements and the unprecedented challenges posed by the COVID-19 pandemic. IoMT holds the promise of revolutionizing healthcare practices through its potential for personalized medical data management, continuous health monitoring, and remote treatment capabilities. Nevertheless, the inherent vulnerabilities associated with handling sensitive medical information within the IoMT environment have underscored the critical need for robust security measures and lightweight protocols to ensure the protection of medical systems and IoT devices. In this context, this paper delves into the comprehensive examination of an IoMT scheme that integrates both conventional password-based authentication and the innovative application of a fuzzy extractor for biometric authentication. Building upon the findings of the preceding study by Masud et al. [6], we have done cryptanalysis to address the identified limitations. Furthermore, our investigation includes comprehensive formal and informal analyses to evaluate the robustness of the suggested approach. Additionally, we delve into the computational expenses, providing insights into its relative efficacy when compared to existing methodologies.

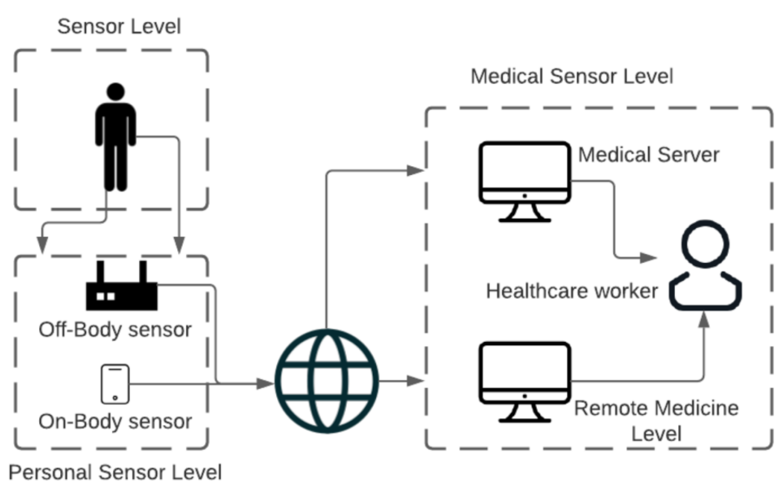

Fig1. Secure and sustainable IoMT Internet of medical things. [2]

1.1 Our Contribution

Within this document, we have conducted an assessment of the Masud et al. system and showcased the resulting weaknesses.

- **Key escrow**: In the transmission phase, the key escrow attack allows the unauthorized interception of ID_i, compromising user identity confidentiality. This highlights the need for secure channels and robust encryption to prevent unauthorized access and safeguard sensitive data during transmission.
- **Session Specific Temporary Information Attack:** It likely refers to a potential exploit targeting temporary data within a user session, potentially compromising the security of the session-based system. Overhead on gateway for each column: The overhead on the gateway for each column denotes the additional computational steps and checks performed at the gateway stage of the protocol, ensuring secure communication and authentication. These checks include verifying the
- **Replay Attack:** A replay attack is characterized as a form of network security breach where a genuine data transmission is intentionally duplicated or delayed in a deceptive manner [3-5]. This could potentially lead to unauthorized access or operations. Such attacks aim to exploit vulnerabilities in communication protocols, compromising the integrity and security of the system.
- **PFS**: Perfect Forward Secrecy (PFS) [5-9] is an encryption feature that guarantees the privacy of previous communications even if long-term secret keys are compromised [15], enhancing security by preventing the decryption of previously intercepted data.

1.2 Paper Organization

Session 1 provides the introduction to the research, Session 2 outlines our specific contributions, Session 3 presents an in-depth analysis of the findings, Session 4 offers acknowledgment and session 5 gives conclusions drawn from the analysis along with proposed future work, and Session 6 includes the references used throughout the research.

2. SCHEME OF MASUD ET AL

Herewith, we have scrutinized the Masud et al. system, with the relevant symbols specified in Table 1.

Notations Used in Table 1

Icon	Represents
$*U_iM^*, GM^*, SN_jM^*$	the i^{th}, gateway, and j^{th} corresponding entities.
ID_j, SID_J	The user's identity is denoted as 'i,' and the specific sensor node is identified by the index 'j.'
PW_i	i^{th} user password
B_i	Biometric of i^{th} user
rU^*, rGW^*, rSN^*	The random number generated by the user, gateway, and individual sensor node is denoted as the '*'-th, respectively.
tsU	Timestamp of the user
S_{i1}	Confidential data of the user and the gateway.
S_{i2}	Sensitive data of the user and the sensor node.
D_{ID}, S_{ID}	User and sensor node identification.
PW_D	Device access code designated by the doctor."
R_{sG}, R_{SN}	Random private key created by the gateway, sensor node, respectively
N_D, N_G, N_s	Random nonce for the user's device, gateway, and sensor node, respectively.
K_{GW}	Gateway's secret key
$h(.)$	One way hash algorithm
k	Concatenation operation
SK	Session key
$\oplus$	Exclusive OR operation

$\|$	String concatenation

The approach outlined in [1] is segmented into different stages as follows.

2.1 User Enrolment Stage

User inputs: ID_i and PWD

a. Generation and Computations:

- Generates a random number: r_{U1}
- Computes the function: *Gen* (*Bi*) to obtain (R_i , RB_i)
- Computes the hash value HPW_i using a hash function hh as follows: $HPW_i = h(PW_i)$

b. Transmission (Target of Key Escrow Attack):

- Attacker gains unauthorized access to ID_i during the transmission from the user to the gateway.

2.2 Sensor Node Transmission:

- The sensor node transmits SID_j to the gateway through a secure channel.

2. Gateway Operations:

- The gateway generates a random number: r_{4GW}
- Computes $TSID_j = h(SID_j \oplus r_{4GW} \oplus KGW)$, where hh represents a hash function.
- Stores SID_j and $TSID_j$
- Transmits $TSID_j$, TID_i, and S_{2i} via a secure channel to the sensor node.
- Deletes S_{2i} from its storage.

- Sensor Node Storage with Perfect Forward Secrecy:
  - Generate a temporary session key for encryption: K_{temp}
  - Encrypt the stored information ($SID_j, TSID_j, TID_i, S_{2i}$) using the temporary session key: $EK_{temp}(SID_j)$

- $EK_{temp}(TSID_j)$
- $EK_{temp}(TID_i)$
- $EK_{temp}(S_{2i})$

- Discard the temporary session key EK_{temp} after the encryption process.

2.3 User Operations:

- The user provides the inputs ID_i and PW_i, then records $B_i$on a device for biometric collection. Subsequently, the user puts ID_i, PW_i and B_i on a smart card device.
- $R_i = Rep(B_i, R_{bi})$
- $r_{U1} = h(PW_i \oplus R_i \oplus ID_i) \oplus U_I M4$
- $HPW_i = h(PW_i \oplus R_i \oplus r)$
- $TID_i = U_i M1 \oplus HPW_i$
- $S_{i1} = U_i M2 \oplus HPW_i$
- $S_{i2} = U_i M3 \oplus HPW_i$
- $U_i M5^* = h(r_{U1} \oplus TID_i \oplus S_{i1} \oplus S_{i2})$
- $Checks\ if\ U_i M5 = U_i M5^*$
- Generates:
- $r_{U2}, r_{U3}, and\ tsU$
- $U_i M6 = TID_i \oplus tsU$
- $2U_i M7 = r_{U2}$
- $U_i M8 = h(TID_i \oplus tsU)$
- $Transmits\ U_i M6, U_i M7, U_i M8, TID_i, and\ tsU\ publicly\ to\ the\ gateway.$

a. Gateway Operations with Overhead:

- $Retrieves\ r_{U2} = U_{iM6} \oplus S_{i6}$
- Computes:

- $TID_{inew} = h(ID_i \oplus KGW)$
- $GM1 = TID_j \oplus r_{5GW}$
- $GM2 = TID_i \oplus r_{5GW}$
- $GM3 = TID_{inew} \oplus r_{5GW}$
- $GM4 = h(TID_j \oplus TID_i \oplus TID_{inew})$
- $Checks\ freshness\ of\ r_{U2}$
- $Checks\ if\ U_iM8 =?\ U_iM8^*$
- $Checks\ if\ tsU\ is\ in\ a\ valid\ range$
- $Transmits\ GM1, GM2, GM3, GM4, and\ U_iM7\ publicly\ to\ the\ sensor\ node.$

b. Sensor Node Operations with Overhead:

- $Retrieves\ r_{5GW} = GM1 \oplus TID_j$
- $Computes$:
- $TID_i = GM2 \oplus r_{5GW}$
- $TID_{inew} = GM3 \oplus r_{5GW}$
- $r_{U3} = U_{iM7} \oplus S_{i2}$
- $GM4^* = h(r_{5GW} \oplus TID_j \oplus TID_i \oplus TID_{inew})$
- $Checks\ if\ GM4 =?\ GM4^*$
- $Computes\ the\ session\ key\ SK$
- $Computes$:
- $SN_{jM1} = SK \oplus S_{i2}$
- $SN_{jM2} = h(SK \oplus TID_{inew})$
- $SN_{jM3} = h(SN_{jM1} \oplus SN_{jM2} \oplus TID_j)$
- $Replaces\ TID_i\ with\ TID_i\ new$
- $Transmits\ SN_{jM1}, SN_{jM2}, and\ SN_{jM3}\ publicly\ to\ the\ gateway.$

c. Gateway Operations (Sensor Node Authentication) with Overhead:

- $Computes\ SN_{jM3}^{*} = h(SN_{jM1} \oplus SN_{jM2} \oplus TID_j)$
- $Checks\ if\ SN_{jM3} =?\ SN_{jM3}^{*}$
- $Computes$:
- $GM5 = h(TID_i \oplus TID_{inew})$
- $GM6 = TID_{inew} \oplus S_i 1$
- $Replaces\ TID_i\ with\ TID_{inew}$
- $Transmits\ GM5, GM6, SN_{jM1}, and\ SN_{jM2}\ publicly\ to\ the\ user$

d. User Operations (Gateway Authentication) with Overhead:

- $Computes$:
- $TID_{inew} = GM6 \oplus S_{i1}$
- $GM5^{*} = h(TID_i \oplus TID_{inew})$
- $U_i M1_{new} = TID_{inew} \oplus HPW_i$
- $Checks\ if\ GM5 =?\ GM5^{*}$
- $Retrieves\ the\ session\ key\ SK$
- $Computes\ SN_{jM2}^{*} = h(SN_{jM1} \oplus SN_{jM2} \oplus TID_j)$

2.4 During this attack we also got two more on the operation:

- $U_i M6', U_i M7', U_i M8', TIDi', and'tsU'$ be the intercepted values by the attacker during the original transmission.

e. The original operation:

- The user generates $rU2, rU3, and\ tsU$.
- Computes:
- U_iM6=$TID_i \oplus tsU$
- $U_i M7 = rU2$

- $U_iM8 = h(TID_i \oplus tsU)$
- Transmits $M6, U_iM7, U_iM8, TID_i, and\ tsU$through a public channel, the information is sent to the gateway.

f. The replay attack:

- The attacker intercepts the previously transmitted values:
- $U_iM6' - value\ of\ U_iM6$ intercepted by the attacker
- U_iM7′ - value of U_iM7 intercepted by the attacker
- U_iM8′ - value of U_iM8 intercepted by the attacker
- $'TID_i'$ - value of TID_i intercepted by the attacker
- $'tsU'$ - value $of\ tsU$ intercepted by the attacker
- The attacker replays these values to the gateway at a later time, impersonating the user's original request.

g. Session specific temporary information attack:

- Given Scenario:
- The sensor node generates SK and computes:
- $SN_jM1 = SK \oplus S_i2,$
- $SN_jM2 = h, (SK \parallel TID_{inew})$
- $SN_jM3 = h(SN_jM1 \parallel SN_jM2 \parallel TSID_j)$. The sensor node replaces TID_i with TID_{inew} and transmits $SN_jM1, SN_jM2, and\ SN_jM3$ through a public channel to the gateway.

h. Potential Attack Scenario:

- Attacker intercepts the values transmitted by the sensor node: $SN_jM1, SN_jM2, and\ SN_jM3$.
- Attacker manipulates the intercepted data, particularly by altering the values of $SN_jM1, SN_jM2, and\ SN_jM3$ using their own values or introducing a malicious payload.
- Attacker transmits the manipulated values to the gateway through the same public channel.

3. ANALYSIS

In this section, we have presented an examination of the Masud et al scheme [1] as follows.

- **Key escrow:** In the transmission phase, the key escrow attack allows the unauthorized interception of ID_i, compromising user identity confidentiality. This highlights the need for secure channels and robust encryption to prevent unauthorized access and safeguard sensitive data during transmission.
- **Attack involving Session-Specific Temporary Information**: The sensor node generates SK and computes SN_jM_1=SK⊕S_i2 [10-15]. Then, it calculates SN_jM_1 using a hash function hh with SK and TID_inew, and SN_JM_3 using h with SN_jM_1, SN_jM_2, and $TSID_j$. An attacker intercepts and manipulates SN_jM_1, SN_jM_2, and SN_jM_3 before transmitting, potentially compromising the integrity of the data.
- **Overhead on gateway for each column:** The overhead on the gateway for each column denotes the additional computational steps and checks performed at the gateway stage of the protocol, ensuring secure communication and authentication. These checks include verifying the freshness of transmitted values, validating the range of specific variables, and confirming the integrity of exchanged data to prevent potential security breaches.
- **Replay Attack:** The attacker seizes the values UiM6 $'$,UiM7 $'$,UiM8 $'$,TID_i $'$, and tsU $'$ during the initial transmission, subsequently reproducing them at a later instance, mimicking the user's genuine request. This security flaw allows unauthorized parties to manipulate the system by reusing intercepted data, potentially leading to unauthorized access or malevolent activities.
- **Perfect forward secrecy**: In the protocol, the sensor node transmits SID_j to the gateway securely, which computes $TSID_j$ using a hash function hh and random number r_{4GW}. During storage, the sensor node employs Perfect Forward Secrecy by generating a temporary session key K_{temp} to encrypt the data, ensuring past communication confidentiality even if long-term keys are compromised.

4. ACKNOWLEGEMENT

The research is backed by the workstation acquired under the GUJCOST/STI/2021-22/3867 grant from the Gujarat Council of Science and Technology, Government of Gujarat, India.

5. CONCLUDING REMARKS AND FUTURE PROSPECTS

The study of an IoMT authentication scheme highlights vulnerabilities including key escrow, session-specific temporary information attacks, and replay attacks, underscoring the need for enhanced encryption and data integrity measures. Future research could explore advanced encryption protocols and blockchain integration to bolster IoMT security.

6. REFERENCES

[1]. Kim, K.; Ryu, J.; Lee, Y.; Won, D. An Improved Lightweight User Authentication Scheme for the Internet of Medical Things. Sensors 2023, 23, 1122. https://doi.org/10.3390/s23031122

[2]. Bhushan, B., Kumar, A., Agarwal, A. K., Kumar, A., Bhattacharya, P., & Kumar, A. (2023). Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends. Sustainability, 15(7), 6177. https://doi.org/10.3390/su15076177

[3]. Jha, N.K. Internet-of-Medical-Things. In Proceedings of the Great Lakes Symposium on VLSI (GLSVLSI), Banff, AB, Canada, 10–12 May 2017; p. 7.

[4]. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis,C. Review of security and privacy for theInternet of Medical Things (IoMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in SensorSystems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 457–464.

[5]. Dilibal, C.; Davis, B.L.; Chakraborty, C. Generative design methodology for internet of medical things (IoMT)-based wearablebiomedical devices. In Proceedings of the 2021 3rd International Congress on Human-Computer Interaction, Optimization andRobotic Applications (HORA), Ankara, Turkey, 11–13 June 2021; pp. 1–4.

[6]. Aman, A.H.M.; Hassan, W.H.; Sameen, S.; Attarbashi, Z.S.; Alizadeh, M.; Latiff, L.A. IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. J. Netw. Comput. Appl. 2021, 174, 102886. [CrossRef] [PubMed]

[7]. Khadidos, A.O.; Shitharth, S.; Khadidos, A.O.; Sangeetha, K.; Alyoubi, K.H. Healthcare Data Security Using IoT Sensors Based onRandom Hashing Mechanism. J. Sens. 2022, 2022, 8457116. [CrossRef]

[8]. Masud, M.; Gaba, G.S.; Choudhary, K.; Hossain, M.S.; Alhamid, M.F.; Muhammad, G. Lightweight and anonymity-preservinguser authentication scheme for IoT-based healthcare. IEEE Internet Things J. 2021, 9, 2649–2656. [CrossRef]

[9]. Lamport, L. Password authentication with insecure communication. Commun. ACM 1981, 24, 770–772. [CrossRef]

[10]. Liao, I.E.; Lee, C.C.; Hwang, M.S. A password authentication scheme over insecure networks. J. Comput. Syst. Sci. 2006, 72,727–740. [CrossRef].

[11]. Wu, Z.Y.; Lee, Y.C.; Lai, F.; Lee, H.C.; Chung, Y. A secure authentication scheme for telecare medicine information systems. J. Med.Syst. 2012, 36, 1529–1535. [CrossRef]

[12]. Debiao, H.; Jianhua, C.; Rui, Z. A more secure authentication scheme for telecare medicine information systems. J. Med. Syst.2012, 36, 1989–1995. [CrossRef]

[13]. Wei, J.; Hu, X.; Liu, W. An improved authentication scheme for telecare medicine information systems. J. Med. Syst. 2012, 36,3597–3604. [CrossRef]

[14]. Wu, F.; Xu, L.; Kumari, S.; Li, X. An improved and provably secure three-factor user authentication scheme for wireless sensornetworks. Peer-Peer Netw. Appl. 2018, 11, 1–20.[CrossRef]Sensors 2023, 23, 1122 17 of 17

[15]. Ryu, J.; Lee, H.; Kim, H.; Won, D. Secure and efficient three-factor protocol for wirelesssensor networks. Sensors 2018, 18, 4481.[CrossRef]

[16]. Mao, D.; Liu, H.; Zhang, W. An enhanced three-factor authentication scheme with dynamic verification for medical multimediainformation systems. IEEE Access 2019, 7, 167683–167695. [CrossRef]

[17]. Li, X.; Peng, J.; Obaidat, M.S.; Wu, F.; Khan, M.K.; Chen, C. A secure three-factor user authentication protocol with forwardsecrecy for wireless medical sensor network systems. IEEE Syst. J. 2019, 14, 39–50. [CrossRef]

[18]. Ebrahimi, S.; Bayat–Sarmadi, S. Lightweight fuzzy extractor based on LPN for device and biometric authentication in IoT. IEEEInternet Things J. 2021, 8, 10706–10713. [CrossRef]

[19]. Satamraju, K.P.; Malarkodi, B. A PUF-based mutual authentication protocol for internet of things. In Proceedings of the 2020 5thInternational Conference on Computing, Communication and Security (ICCCS), Patna, India, 14–16 October 2020; pp. 1–6.

[20]. Abdaoui, A.; Erbad, A.; Al-Ali, A.K.; Mohamed, A.; Guizani, M. Fuzzy Elliptic Curve Cryptography for Authentication in Internetof Things. IEEE Internet Things J. 2021, 9, 9987–9998. [CrossRef]

[21]. Dodis, Y.; Reyzin, L.; Smith, A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Proceedingsof the International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May2004; pp. 523–540.

[22]. Ryu, J.; Lee, H.; Lee, Y.; Won, D. SMASG: Secure Mobile Authentication Scheme for Global Mobility Network. IEEE Access 2022,10, 26907–26919. [CrossRef]

[23]. Kang, D.; Lee, H.; Lee, Y.; Won, D. Lightweight user authentication scheme for roaming service in GLOMONET with privacypreserving. PLoS ONE 2021, 16, e0247441. [CrossRef]

[24]. Ryu, J.; Kang, D.; Lee, H.; Kim, H.; Won, D. A secure and lightweight three-factor-based authentication scheme for smarthealthcare systems. Sensors 2020, 20, 7136. [CrossRef]

[25]. Blanchet, B.; Smyth, B.; Cheval, V.; Sylvestre, M. ProVerif 2.04: Automatic Cryptographic Protocol Verifier, User Manual andTutorial. Available online: https://proverif.inria.fr/manual.pdf (accessed on 30 November 2021).

[26]. Kang, D.; Jung, J.; Lee, D.; Kim, H.; Won, D. Security analysis and enhanced user authentication in proxy mobile IPv6 networks.PLoS ONE 2017, 12, e0181031. [CrossRef]

[27]. Roy, S.; Chatterjee, S.; Das, A.K.; Chattopadhyay, S.; Kumari, S.; Jo, M. Chaotic map–based anonymous user authenticationscheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things. IEEE Internet Things J. 2017, 5, 2884–2895.[CrossRef]

[28]. Lee, H.; Lee, D.; Moon, J.; Jung, J.; Kang, D.; Kim, H.; Won, D. An improved anonymous authentication scheme for roaming inubiquitous networks. PLoS ONE 2018, 13, e0193366. [CrossRef]

[29]. Jung, J.; Kim, J.; Choi, Y.; Won, D. An anonymous user authentication and key agreement scheme based on a symmetriccryptosystem in wireless sensor networks. Sensors 2016, 16, 1299. [CrossRef] [PubMed]

[30]. Xu, L.; Wu, F. Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity forconnected health care. J. Med. Syst. 2015, 39, 1–9. [CrossRef] [PubMed]

[31]. Das, A.K. A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks.Peer-Peer Netw. Appl. 2016, 9, 223–244. [CrossRef]

[32]. Sahoo, S.S.; Mohanty, S.; Majhi, B. An efficient three-factor user authentication scheme for industrial wireless sensor networkwith fog computing. Int. J. Commun. Syst. 2022, 35, 3. [CrossRef]

[33]. Bahache, A.N.; Chikouche, N.; Mezrag, F. Authentication Schemes for Healthcare Applications Using Wireless Medical SensorNetworks: A Survey. SN Comput. Sci. 2022, 3, 1–25. [CrossRef]

[34]. Li, Y.; Tian, Y. A Lightweight and Secure Three-Factor Authentication Protocol With Adaptive Privacy-Preserving Property forWireless Sensor Networks. IEEE Syst. J. 2022, 16, 6197–6208. [CrossRef]