

Review

Exploring Authentication Protocols for Secure and Efficient Internet of Medical Things Systems

Seungbin Lee , Kyeong A Kang, Soowang Lee and Jiyeon Kim * 

Department of Computer Science and Engineering, Gyeongsang National University,
Jinju 52828, Republic of Korea; dltmdqls1526@gnu.ac.kr (S.L.); kka2418@gnu.ac.kr (K.A.K.);
id0311sw@gnu.ac.kr (S.L.)

* Correspondence: jykim92@gnu.ac.kr

Abstract

The Internet of Medical Things (IoMT) comprises the application of traditional Internet of Things (IoT) technologies in the healthcare domain. IoMT ensures seamless data-sharing among hospitals, patients, and healthcare service providers, thereby transforming the medical environment. The adoption of IoMT technology has made it possible to provide various medical services such as chronic disease care, emergency response, and preventive treatment. However, the sensitivity of medical data and the resource limitations of IoMT devices present persistent challenges in designing authentication protocols. Our study reviews the overall architecture of the IoMT and recent studies on IoMT protocols in terms of security requirements and computational costs. In addition, this study evaluates security using formal verification tools with Scyther and SVO Logic. The security requirements include authentication, mutual authentication, confidentiality, integrity, untraceability, privacy preservation, anonymity, multi-factor authentication, session key security, forward and backward secrecy, and lightweight operation. The analysis shows that protocols satisfying a multiple security requirements tend to have higher computational costs, whereas protocols with lower computational costs often provide weaker security. This demonstrates the trade-off relationship between robust security and lightweight operation. These indicators assist in selecting protocols by balancing the allocated resources and required security for each scenario. Based on the comparative analysis and a security evaluation of the IoMT, this paper provides security guidelines for future research. Moreover, it summarizes the minimum security requirements and offers insights that practitioners can utilize in real-world settings.

Keywords: Internet of Medical Things; authentication protocol; formal verification



Academic Editors: Sajjad Dadkhah,
Xichen Zhang, Euclides Neto and
Mahdi Daghmehchi Firoozjaei

Received: 8 September 2025

Revised: 21 October 2025

Accepted: 21 October 2025

Published: 24 October 2025

Citation: Lee, S.; Kang, K.A.; Lee, S.;
Kim, J. Exploring Authentication
Protocols for Secure and Efficient
Internet of Medical Things Systems.
Electronics **2025**, *14*, 4164. <https://doi.org/10.3390/electronics14214164>

Copyright: © 2025 by the authors.
Licensee MDPI, Basel, Switzerland.
This article is an open access article
distributed under the terms and
conditions of the Creative Commons
Attribution (CC BY) license
(<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The rising average age of the global population is accompanied by an increasing incidence of chronic disease. This trend is significantly increasing the demand for efficient healthcare services. The adoption of intelligent healthcare systems is essential if systems are to meet this demand. In this landscape, the Internet of Medical Things (IoMT) is emerging as a next-generation technology for healthcare services. The IoMT supports patient-health management through remote consultations and timely interventions. It is expected to play a significant role in improving the quality, efficiency, and sustainability of healthcare services.

First, the IoMT is transforming service delivery across both clinical and home settings. Point-of-care diagnostic tools enable clinicians to perform rapid tests in hospitals and

outpatient facilities, while remote monitoring extends these benefits to home care, allowing continuous health tracking without disruption of daily life [1]. In addition, the IoMT enhances the efficiency of hospital operations and resource management by monitoring various resources, including equipment, medicines, and consumables, in real time. This enhances the efficiency of supply-chain management through intuitive status monitoring and automated ordering and linking. The IoMT provides interoperability by integrating medical devices with different standards. This allows for a consistent supply of medical data, enabling clinicians to access necessary information in real time. These capabilities enable the delivery of high-quality healthcare services such as preventive medicine, management of chronic disease, emergency response, and continuous monitoring.

However, despite these advantages, the scalability of the IoMT exposes new security vulnerabilities. Because most IoMT devices are network-connected, the attack surface is significantly expanded compared to traditional healthcare environments. Attacks on medical data go beyond simple information leaks and directly impact patient lives. These threats clearly demonstrate the need for a security framework tailored to the IoMT environment. Existing IT security systems are inadequate for the unique needs of healthcare environments and the characteristics of IoMT devices, requiring the development of an encryption strategy tailored to IoMT systems [2].

Secure and reliable data transmission is a key element supporting IoMT performance. Sensors and medical devices continuously generate sensitive health data. This data flow must simultaneously meet needs related to confidentiality, integrity, low latency, and energy efficiency. Some errors can pose threats to patient health. Furthermore, inadequate security measures to ensure authentication, confidentiality, and integrity make data exchange vulnerable, posing a serious threat to the protection of sensitive medical information [3]. Therefore, it is essential to verify the efficiency and security of IoMT communication protocols. The main contributions of the paper are as follows:

- (i) Conducting systematic and objective comparative analysis of recent IoMT security protocols to quantitatively evaluate their performance and security metrics.
- (ii) Verifying the recent IoMT security protocols to derive essential security requirements for IoMT environments.
- (iii) Providing security guidelines for future research based on the results of comparative analysis and security assessment.

Section 2 describes IoT, IoMT, and IoMT communications. Section 3 analyzes recent research and conducts an objective evaluation. Section 4 formally verifies the proposed protocol using SVO Logic and Scyther. Section 5 discusses security requirements and safety, and Section 6 concludes this work.

2. Background

The IoMT has evolved in recent years through the integration of IoT technology into medical device systems and services. While the general IoT connects common objects such as home appliances and vehicles, the IoMT specifically links clinical devices that monitor vital signs and administer treatments [4]. This evolution has been driven by advances in low-power wireless communication and edge computing technologies, which hospitals and healthcare institutions have adopted to enhance service quality and accessibility [5].

2.1. IoT and IoMT

Figure 1 shows IoMT device classification. The IoT interconnects distinct physical entities, enabling embedded sensors and software to exchange data with edge and cloud platforms. Extending these principles into the clinical domain, the IoMT operates within care workflows to enable real-time monitoring, remote patient management, and early

detection of anomalies, thereby improving patient outcomes through continuous monitoring, personalized treatment, and telemedicine [6,7]. The IoMT encompasses patient-worn devices (e.g., smartwatches, biosensor patches), hospital-deployed assets (e.g., smart beds, infusion pumps), and implantable systems that stream remote telemetry or deliver closed-loop therapies (e.g., pacemakers, neurostimulators) [8]. The IoMT sector continues to expand as companies consistently release specialized sensors and advanced monitoring tools. Unlike the general-purpose IoT, the IoMT handles sensitive health data, making robust security essential.

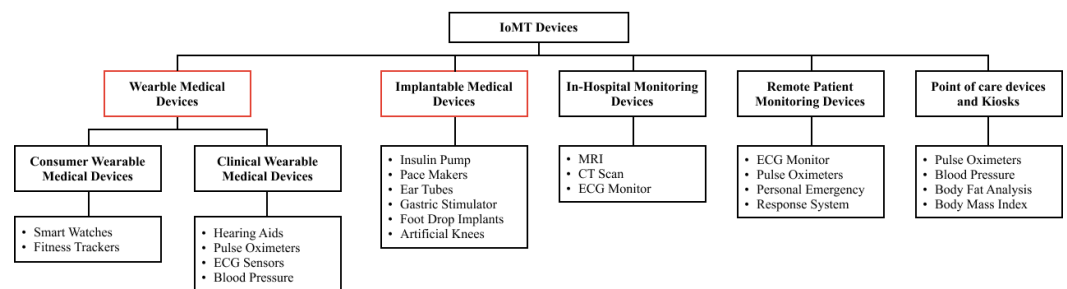


Figure 1. Classification of IoMT devices.

IoMT devices can fall into two main categories: Implantable Medical Devices (IMDs) and Internet of Wearable Devices (IoWDs) [9]. IMDs primarily support long-term monitoring or treatment by directly interfacing with human tissue, whereas IoWDs operate externally to collect and transmit physiological data [10,11].

Cardiovascular IMDs: Implantable cardioverter defibrillators (ICDs) detect and correct arrhythmias [12]. Left ventricular assist devices (LVADs) help maintain blood circulation in patients with severe heart failure [13].

Neurological IMDs: Deep brain stimulators (DBS) send electrical impulses to targeted brain regions to treat conditions such as Parkinson’s disease and epilepsy. Clinicians use spinal cord stimulators (SCS) to manage chronic pain. Vagus nerve stimulators (VNS) assist in managing seizures and mood disorders [14–16].

Metabolic and Endocrine IMDs: Implantable insulin pumps regulate blood glucose in diabetic patients [17,18].

Respiratory and Pulmonary IMDs: Diaphragm stimulators aid patients with respiratory conditions. Implantable airway sensors monitor airflow and detect abnormalities [19,20].

The use of IMDs involves challenges, including limited battery life, vulnerabilities associated with wireless communication interfaces, and risks to patients’ data privacy. The advancement of IMDs depends on reliable energy management, secure low-power communication, and compliance with healthcare safety and cybersecurity requirements. These factors remain critical challenges throughout the design, certification, and deployment of IMDs [21,22].

IoWDs function externally as a noninvasive alternative, collecting physiological data for continuous, near-real-time monitoring. They transmit this data to clinical information systems to support preventive care, long-term management of chronic conditions, and remote oversight. This process provides patients with timely feedback and reduces reliance on in-person visits [10].

Vital-Sign-Monitoring Wearables: Devices such as smartwatches and fitness trackers measure heart rate. They also track oxygen saturation (SpO₂), body temperature, and sleep patterns. Wearables equipped with ECG functions detect irregular heart activity [23].

Glucose-Monitoring Wearables: Continuous glucose monitoring (CGM) sensors measure blood glucose levels. They provide real-time feedback to diabetic patients [24].

Smart Clothing and Adhesive Health Patches: ECG-enabled garments, such as smart shirts, monitor cardiovascular activity. Smart patches measure hydration, detect temperature variations, and analyze sweat composition [25,26].

Neurological Wearables: Brain–computer interface (BCI) devices analyze brain activity to support cognitive training and neurotherapy [27].

Although IoWDs are noninvasive, they present challenges, most notably in measurement accuracy, which varies depending on wearing conditions and device-specific characteristics. Furthermore, security threats such as data leakage and tampering, which can directly impact patient safety, must also be addressed. In this context, IoMT systems continuously generate vast amounts of patient-specific clinical data. To manage the complexity of IoMT systems, a layered architecture has been adopted. While various architectures exist, their components can be categorized into three core layers: perception, network, and application [28,29].

Figure 2 shows the hierarchical architecture of the IoMT. Patients access medical devices through the perception layer. This layer collects data and transmits it to the application layer via the network layer. The application layer stores the data and preprocesses it so that medical professionals can effectively utilize it.

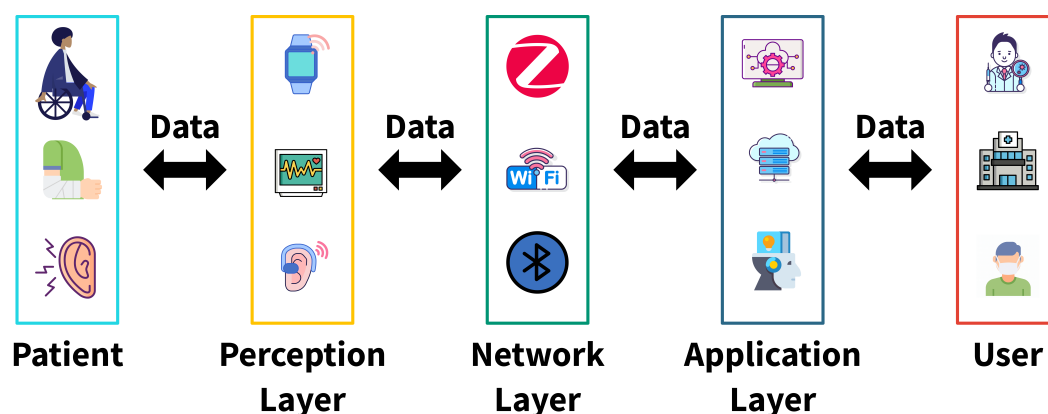


Figure 2. Layered architecture of the IoMT.

The perception layer handles all components that capture medical data at the source. It includes wearable health monitors, implantable devices, and hospital-grade diagnostic machines. These instruments collect raw physiological data, such as heart rate, oxygen saturation, glucose concentration, and other vital indicators. Wearable sensors play a central role in this layer. Devices such as smartwatches and biosensor patches continuously track the condition of a patient without disrupting daily routines. In addition to acquisition, many devices perform basic processing by filtering noise, compressing signals, and detecting abnormalities before transferring the processed information to the network layer [29].

The network layer is the intermediate layer connecting the perception layer and the application layer in the IoMT architecture. It securely and quickly transmits data collected by sensors to hospital servers, cloud platforms, or healthcare service providers. The primary purpose of this layer is to ensure data confidentiality, integrity, and availability during transmission while maintaining the real-time performance essential in healthcare environments and ensuring seamless connectivity. These functions are essential for ensuring uninterrupted data transmission, especially in life-threatening situations. In addition, edge computing devices are deployed at the network layer to reduce communication delays with cloud servers and enable immediate local processing of urgent data [30].

As the upper layer, the application layer aggregates data received from the network layer and delivers it to healthcare providers. This layer enables remote monitoring and control in medical settings, facilitates real-time assessment of a patient's condition, and sup-

ports physicians in making data-driven diagnoses and treatment decisions. User interfaces, including the software and applications used at the application layer, play a critical role in managing the increasing complexity of system administration [31].

2.2. IoMT Communication Protocols

IoMT systems employ multiple communication protocols to connect devices, networks, and applications. Each component requires a suitable method for data transmission. At the perception layer, where data collection occurs, short-range protocols are common. RFID tags track medical equipment in hospitals. They are small and inexpensive and do not require batteries. A reader emits a signal, and the tag returns the information. NFC operates in a similar way but requires close contact (within a few centimeters). Bluetooth Low Energy (BLE) is widely used in wearable devices because it minimizes power consumption. Most fitness trackers and health monitors rely on BLE to connect with smartphones [32]. ZigBee conserves energy and supports mesh networking, making it suitable for large-scale IoMT integration [33]. For longer distances, Wi-Fi is frequently deployed in hospitals due to its high transmission speed, although it consumes more power. Remote monitoring systems often adopt cellular networks such as 4G and 5G, especially for patients at home [34]. These connections enable clinicians to observe a patient's condition without in-person visits. At the application layer, different protocols manage collected data. MQTT provides lightweight many-to-many communication through a publish–subscribe model. It reduces network overhead and supports three quality-of-service (QoS) levels for varying reliability requirements [35]. Constrained Application Protocol (CoAP) serves as another option and is particularly effective for devices with limited processing capacity [36]. Healthcare systems also apply standards such as Health Level 7 (HL7) to ensure consistent interpretation of medical information across institutions [37]. Standardization plays a critical role in enabling interoperability among hospitals and healthcare providers.

Protocol selection depends on device power capacity, data volume, and security requirements. Security remains a central concern due to the sensitivity of medical data. Each system layer must apply strong encryption and authentication mechanisms to guarantee secure access. An appropriate combination of these protocols enables real-time monitoring, health-trend analysis, and remote care delivery while meeting strict regulatory standards.

3. Recent Research

3.1. Literature Review

In this section, we review recent research on the IoMT. The papers cover the architecture of the IoMT, future directions, security requirements, and the authentication protocol or enhanced authentication protocol. A description of each paper is provided below, and Table 1 summarizes these results.

According to Askar et al. [38], the IoMT is a concept that uses IoT technology to improve healthcare systems to make them smarter and more proactive. The IoMT can integrate new technologies such as ML, Blockchain, Fog, and edge computing to provide benefits such as faster treatment, improved communication, and cost reduction. This research analyzes various IoMT technologies and solutions built on these paradigms and presents possible directions for future development and applications.

Table 1. Summary.

Type	Ref.	Purpose	Description	Advantages	Challenges
IoMT Survey	[38]	- Description of the challenges associated with IoMT	- Integrates new-generation tech. (such as ML, blockchain, fog, and edge computing)	- Enables analysis of medical data using machine learning - Achieves low latency and efficient data processing through fog and edge computing	- Mobility - Security and privacy - Interoperability and scalability - Real-time operation - Low-power operation
IoMT Survey	[39]	- Design of an IoMT security framework and application of an e-healthcare system	- Investigates PUF, blockchain, AI, and SDN - Validated through three case studies evaluating authentication, security, performance, and data collection	- Proposes an IoMT architecture - Applies new technology for security and performance - Maps real-life applicability - Conducts experimental validation through case studies	- Difficulty in activating SDN - Black-box problem in AI (XAI) - Blockchain scalability
IoMT Survey	[40]	- Design of a web-based security-assessment framework	- Uses an ontology- and scenario-based approach to create a web-based security-assessment framework (IoMT-SAF) - Supports the evaluation of protection and deterrence capabilities	- Utilizes real-world security-threat cases and cyberattack data - Evaluates framework performance using the CVE list	- Security-profile definition is lengthy and complex
IoMT Survey	[41]	- Research on recent advances in IoMT security	- Proposes a three-stage IoMT security framework addressing data collection, data in transit, and data storage	- Analyzes IoMT security requirements - Proposes an IoMT security framework	- Blockchain scalability - Securing remote setup and providing alternative access methods
IoMT Survey	[42]	- Review of IoMT security models and various key algorithms	- Discusses security requirements of the IoMT model - Discusses symmetric-key algorithms - Discusses keyless algorithms	- Identifies security weaknesses in IoMT systems - Details methods to accomplish end-to-end security - Presents mechanisms that protect privacy and anonymity	- High infrastructure cost - Strain on existing networks - Lack of standardization
IoMT Survey	[43]	- Survey of IoMT security requirements, design issues, methods, and future trends	- Analyzes IoMT background and security threats - Investigation of security requirements - Reviews design challenges associated with the IoMT environment - Presents various security technologies	- Offers detailed classification of device sensors associated with the IoMT - Presents security requirements - Investigates security techniques	- Security and privacy issues - Design complexity - Network-connectivity limitations

Table 1. Cont.

Type	Ref.	Purpose	Description	Advantages	Challenges
Protocol	[44]	- Lightweight authentication and key-agreement protocol	- Introduces a lightweight authenticated key-agreement scheme for IoMT systems - Verified security via Scyther - Outperforms existing methods in cost and security	- Reduces encryption overhead through Hashing and XOR - Performance optimization	- Persistent threats and security/privacy challenges
Protocol	[45]	- Proposes a lightweight mutual-authentication protocol using blockchain	- Employs ECC and CRT for efficient identity verification - Integrates NFTs to provide immutable and verifiable identity records on the blockchain	- Verified against replay and MITM attacks via AVISPA - In performance evaluation, low communication and storage costs	- Risk of device hijacking - Vulnerabilities in centralized identity management - Residual delays in NFT registration
Protocol	[46]	- Proposes a lightweight authentication protocol based on post-quantum cryptography	- Replaces current authentication methods used in the IoMT, which rely on simple passwords and lack additional layers of protection, posing a risk of data breaches. - Introduces a lightweight authentication protocol based on post-quantum cryptography	- Strong security against quantum attacks - Efficient key generation to support the performance and scalability of the IoMT device	- Entity verification - Authentication of medical devices
Protocol	[47]	- Proposes an ultra-lightweight and secure RFID authentication scheme	- Uses the solutions of homogeneous linear equations as keys - Minimizes tag costs and allows tags to encrypt and decrypt data through lightweight computations	- Minimizes costs - Enables mutual authentication - Suitable for emergency-response applications	- Limited applicability to realistic medical scenarios - High scanning cost
Protocol	[48]	- Privacy-protection authentication-management protocol	- Employs three-factor authentication to ensure user identity is verified on login. - Employs the Chebyshev chaotic map to support the authentication process and key security	- Verified via BAN logic - Resists attacks and results in various security attributes.	- Lightweight blockchain limitations - Need for a reliable authentication and verification mechanism without a TA - Lack of research on quantum-resistant cryptography algorithms

Table 1. Cont.

Type	Ref.	Purpose	Description	Advantages	Challenges
Protocol	[49]	- Proposed authentication and key management based on blockchain	- Need for a secure authentication key-management protocol leveraging tamper-resistant and decentralized blockchain mechanisms to secure communications in IoMT environments.	- Robust against attacks (replay, MITM, impersonation, ESL attacks, etc.) - Formally verified for security using AVISPA.	- Not mentioned in this paper.
Protocol	[50]	- Proposes a multifactor user-authentication protocol using blockchain and elliptic curve cryptography (ECC)	- Implements a multi-authentication protocol based on blockchain and ECC. - Demonstrates resistance to various attacks in security verification	- Low computational cost - Enhanced security and computational performance	- High cost due to blockchain usage - Higher communication overhead.
Protocol	[51]	- Analysis of Chen et al. [52] authentication protocol - Improves on Chen et al.'s authentication protocol	- Addresses the shortcomings of Chen et al. with an improved authentication protocol using elliptic curve discrete-logarithms, encryption and hashing methods.	- Robust against attacks (replay, MITM, impersonation, ESL attacks, etc.) - Formally verified for security using AVISPA.	- Limited application of emerging technologies, machine learning, quantum cryptography, and blockchain technology
Protocol	[53]	- User-authentication protocol (3ECAP)	- Uses three-factor authentication (passwords, biometrics, smart cards) and mitigates privilege-escalation attacks with Merkle tree-based access control.	- Verified security via ProVerif - Resistant to attacks (replay, MITM, Sensor hijacking etc.)	- Not mentioned in this paper.
Authentication framework	[54]	- Lightweight two-factor authentication framework (L2FAK)	- Addresses gap: existing approaches fail to address several security vulnerabilities, such as user and gateway tampering	- Improves transmission efficiency and reduces overhead compared to existing methods. - Enhances authentication accuracy in medical applications using federated learning.	- Not mentioned in this paper.

Razdan et al. [39] noted that IoMT-based healthcare systems improve the quality of life of all stakeholders, not just patients. However, there are challenges such as power consumption, energy efficiency, security and privacy, high data-transmission rates, and low latency. To solve these problems, researchers are developing technologies that integrate ML, blockchain, fog, and edge computing, and emphasize that these technologies are essential if we are to improve the performance and enhance the security of IoMT healthcare systems. This paper analyzes the current status and potential future applications of IoMT systems that leverage the latest technologies and suggests future research directions and innovative application cases to advance the healthcare industry.

Ghubaish et al. [41] find that the rapid development of micro-computing, mini-hardware manufacturing, and M2M communication has made it possible to reconfigure many networking applications with new IoT solutions. An IoMT system can remotely monitor patients with chronic diseases. Therefore, the IoMT can provide timely patient diagnoses that can save lives in emergency situations. However, the security of these critical systems is a major challenge facing their widespread use.

Hatzivasilis et al. [42] show that security threats are increasing because patients and healthcare professionals process healthcare data using their own devices through Bring Your Own Device (BYOD) use cases. The latest security and privacy controls in the IoMT environment aim to address this problem. On combining IoMT and CE, users can expect improved accessibility, cost reduction, rapid implementation, and improved efficiency. In conclusion, this paper presents key security-control measures to protect CE-based IoMT systems and provides practical guidelines for enhancing security and privacy.

Bhushan et al. [43] show that the use of the IoMT has brought about great changes in healthcare through the deployment of universal and inexpensive devices. However, they suggest limitations on the adoption of IoMT devices due to security and privacy issues. This paper emphasizes the importance of core security measures for securing IoMT systems and enhancing interconnectivity between healthcare domains to address these limitations. The paper identifies three principal security technologies applicable to the IoMT environment: asymmetric key algorithms, which ensure robust data protection and authentication; symmetric key algorithms, which offer fast and efficient data encryption; and keyless algorithms, which fulfill the security requirements of IoMT systems through non-traditional mechanisms.

Alsubaei et al. [40] assert that in the IoMT environment, security and privacy issues are considered serious due to the presence of various IoMT devices that transmit sensitive medical data to the cloud. Consequently, IoMT security assessments and the selection of appropriate protection measures are important, but can be difficult for users who lack security knowledge. To address this, the authors propose a security-assessment framework that can recommend security features for the IoMT and evaluate their protection and deterrence capabilities. This provides practical experience in IoMT security, promotes competition by enabling security solution providers to verify and evaluate product security, and promotes the design of IoMT solutions that reflect the security measures required by consumers.

Abdussami et al. [44] argue that sensitive data related to patient health are vulnerable to attacks. The authors propose an architecture utilizing cloud servers and edge-computing technologies suitable for local and emergency scenarios. The Provably Secured Lightweight Authenticated Key Agreement Protocol (PSLA2P) is a lightweight authentication and key-agreement protocol that can be deployed in the proposed network architecture for the modern health industry. It protects data privacy by providing anonymity, untraceability, and integrity to the patient. In this paper, we prove that the PSLA2P protocol is secure through Scyther formal verification. Through performance evaluation, we show that

it is superior to other approaches in terms of computational cost, communication cost, and security features.

Qiu et al. [45] propose a lightweight mutual-authentication method using blockchain to improve privacy protection and secure communication. The protocol uses elliptic curve cryptography (ECC) and the Chinese remainder theorem (CRT) to perform identity authentication efficiently. It also uses non-fungible tokens (NFTs) to make identity information on the blockchain immutable and verifiable. To enhance security, it applies two-factor authentication by combining certificate-based verification with physically unclonable functions (PUF). Security analysis using AVISPA confirms resistance to replay attacks and man-in-the-middle attacks. Performance evaluation shows low communication and storage costs, making it usable on resource-limited devices. Ethereum-based simulations and hyperledger caliper load tests were conducted to verify practicality. However, risks such as device hijacking, vulnerabilities in centralized identity management, and delays in NFT registration remain.

According to Lo et al. [46], current authentication methods used in the IoMT in the healthcare sector rely on simple passwords. They lack additional layers of protection, posing a risk of data breaches. Furthermore, they are inadequately protected against threats posed by quantum computing. To address this issue, we propose a lightweight authentication protocol based on post-quantum cryptography. This aims to ensure the confidentiality and integrity of medical data while verifying the identities of users and devices. To defend against quantum computing attacks, lattice-based cryptography, a quantum-safe encryption method, can be utilized. The structure of lattices is based on mathematical challenges such as the shortest vector problem (SVP), closest vector problem (CVP), and learning with errors (LWE), which can serve as the foundation for future post-quantum cryptography. By applying lightweight lattice-based cryptography (LBC) to IoMT authentication protocols, the protocol can not only withstand quantum attacks, but also provide strong security against them. It also offers the key-generation efficiency critical for the performance and scalability of IoMT devices, enhances two-factor authentication, and improves user convenience during authentication.

Masud et al. [47] proposes the MASK (mutual authentication and secret key) protocol, which verifies the reliability of sensor nodes and users and defends against physical attacks using PUF. The MASK protocol guarantees key security properties such as mutual authentication, data confidentiality, integrity, anonymity, untraceability, and physical security. Performance evaluation shows that the protocol minimizes computation based on PUF, reducing the burden and keeping sensor nodes' energy consumption and memory usage lower than they are in existing protocols. It also reduces the number of message exchanges to minimize network delay and power consumption. However, the MASK protocol has some limitations.

Miao et al. [48] propose a blockchain-based privacy-protection authentication-management protocol to address IoMT device vulnerabilities in open network environments. The proposed protocol introduces blockchain into the protocol to store device identity and authentication-key information. In addition, security is guaranteed through Chebyshev chaos maps. In this paper, security is proven through a random oracle model and BAN logic. The protocol is shown to resist attacks and result in various security properties. The results of functional comparison and performance analysis show that the proposed protocol has advantages for IoMT devices in terms of security, computational overhead, communication overhead, and storage overhead. However, the consideration is limited to the storage aspect through the application of blockchain. The response time, the efficiency of the blockchain consensus algorithm, and the method of bypassing TA to fully utilize a distributed ledger technology are not considered. Therefore, it is shown that

blockchain mechanisms should be thoroughly studied in the future and that an efficient and secure authentication protocol should be designed.

Garg et al. [49] propose a new blockchain-based authentication and key-management protocol (BAKMP) for IoMT environments. The BAKMP provides secure key management between different communication entities. Authorized users can access medical data in a secure manner from the cloud server. All of the medical data are stored in a blockchain maintained by the cloud server. The BAKMP can resist security-vulnerability attacks such as replay attacks, man-in-the-middle attacks, impersonation attacks, and ephemeral secret leakage (ESL) attacks. The proposed protocol demonstrates security against various types of attacks through AVISPA. In addition, it shows better performance in terms of communication and communication costs in the security, authentication, and key-management phases compared to existing schemes.

Pradhan et al. [50] proposes a multi-authentication protocol based on blockchain and ECC. For security verification, ProVerif and BAN logic were used to demonstrate resistance against various attacks. Slither was utilized for smart contract-vulnerability analysis, and no known security vulnerabilities were found. Experimental results comparing the proposed method with existing approaches showed improved computational and communication performance, demonstrating its applicability in resource-constrained environments. However, limitations remain, such as transaction costs due to blockchain usage, higher communication overhead compared to competing protocols, and difficulties in resetting biometric authentication data if compromised. Therefore, further optimization and expansion are needed to enhance applicability in real medical environments.

Gautam et al. [51] thoroughly analyzed the authentication protocol for IoMT remote patient monitoring proposed by Chen et al. [52] and found that Chen's protocol is vulnerable to various security threats. Chen et al. relies on a random Nonce generated by all entities for the security of the session key. Since any random Nonce can be computed by utilizing publicly transmitted messages, the protocol is vulnerable to session key attacks. The protocol proposed here addresses these shortcomings through the use of an ECC algorithm and encryption and hashing methods. The improved protocol shows resistance to various attacks such as insider attacks, replay attacks, impersonation attacks, man-in-the-middle attacks, ephemeral secret leakage attacks, and session key-disclosure attacks.

Su et al. [53] propose a new user-authentication protocol, 3ECAP, which considers both security and efficiency in the IoMT environment. To these ends, 3ECAP adopts a three-factor authentication method combining passwords, biometric information, and smart cards and prevents privilege-escalation attacks through fine-grained access control using a Merkle tree. Here's a lightly polished version of your sentence for clarity and flow while keeping all technical details:

Furthermore, 3ECAP primarily relies on hash operations to minimize computational and communication overhead, and its security has been validated through formal analysis using ProVerif. A comparative analysis with existing authentication protocols confirmed that 3ECAP maintains low computational and communication costs while providing higher security. In particular, it allows users to update their biometric information and passwords, supports the addition of new sensor devices, and maintains both forward and backward security, which are important in the IoMT environment.

Deebak et al. [54] proposed a lightweight two-factor authentication framework (L2FAK) with privacy-preserving capability that utilizes mobile sinks for smart eHealth. In the S-IoMT environment, data-privacy protection and device security are essential factors. L2FAK utilizes mobile sinks to manage these security issues. L2FAK prevents potential threats such as privileged insider. Additionally, L2FAK ensures secure mutual authentication and session key agreement, demonstrating resistance to user and gateway

impersonation, privileged insider attacks, and replay attacks. L2FAK reduces computational costs and minimizes operational expenses, enhancing the performance of real-time systems. It employs lightweight computations to improve efficiency in system authentication and key agreement stages, achieving superior transmission efficiency and lower overhead compared to conventional methods.

3.2. Evaluation

Security requirements provide the foundation for evaluating the robustness of authentication protocols in IoMT environments. The core security requirements typically encompass authentication, mutual authentication, confidentiality, integrity, untraceability, privacy preservation, anonymity, multi-factor authentication, session key security, forward/backward secrecy, and lightweight operation. In addition, advanced requirements—including quantum resistance and emergency response mechanisms—are becoming increasingly important in healthcare scenarios, where the protection of sensitive medical data and the capacity for timely response to urgent situations are critical.

As shown in Table 2, most existing protocols consistently support authentication, integrity, and confidentiality, which are regarded as the fundamental security properties. However, only a limited number of protocols implement mutual authentication, indicating that many designs still rely on one-way authentication, in which the server verifies the user but the user cannot validate the server. Such asymmetry increases susceptibility to phishing and man-in-the-middle attacks. Consequently, achieving two-way trust through mutual authentication is indispensable for practical and secure deployment.

Table 2. Security requirements supported by each protocol [44–51,53,54].

Security Requirement	Abdussami et al. [44]	Qiu et al. [45]	Lo et al. [46]	Masud et al. [47]	Miao et al. [48]	Garg et al. [49]	Pradhan et al. [50]	Gautam et al. [51]	Su et al. [53]	Deebak et al. [54]
Authentication ✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mutual Authentication ✓	✓	×	×	✓	✓	✓	✓	×	×	×
Confidentiality ✓	×	×	✓	✓	✓	×	✓	×	✓	✓
Integrity ✓	✓	×	✓	✓	✓	×	✓	✓	✓	✓
Untraceability	×	✓	×	✓	✓	✓	×	×	✓	✓
Privacy Preservation ✓	×	×	×	×	×	×	×	✓	×	✓
Anonymity	✓	✓	×	✓	✓	✓	×	×	✓	✓
Multi-Factor Authentication	×	×	×	×	✓	×	✓	×	×	✓
Freshness ✓	✓	×	×	×	✓	✓	✓	✓	✓	×
Secure Session Key ✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓
Forward/Backward Secrecy ✓	✓	×	×	×	✓	×	×	✓	×	×
Lightweight Operation ✓	×	×	✓	✓	✓	✓	×	✓	✓	✓
Post-Quantum Security	×	×	✓	×	×	×	×	×	×	×
Emergency	✓	×	×	×	×	×	×	×	✓	✓

✓: Support, ×: Not Support.

The elements listed under Security Requirement in Table 2 represent the minimum recommended attributes tailored for IoMT scenarios. The essential security elements that must be satisfied include authentication, confidentiality, and integrity. In addition, considering the characteristics of IoMT devices, secure session key, lightweight operation, privacy preservation, mutual authentication, and freshness are also included. These attributes can be more practically beneficial when practitioners use the devices. A secure session key is necessary to ensure the security of messages exchanged within the session, while lightweight operation is included because IoMT devices have limited resources in practice. Privacy preservation is required because the information involved pertains to personal health data. Mutual authentication and freshness are also included to ensure mutual verification and secure communication during operation.

Privacy protection is addressed in [51,54]. This highlights that safeguarding users' sensitive information requires not only cryptographic encryption but also system-level mechanisms that mitigate metadata exposure and behavioral pattern tracking. Similarly,

only a limited number of protocols [44,48–51,53] implement freshness to prevent replay attacks. In addition, only protocols [44,48,51] provide forward and backward secrecy, thereby ensuring the confidentiality of both past and future sessions even if a session key is compromised.

Beyond these classical requirements, emerging threats call for additional considerations. The rapid progress of quantum computing poses fundamental risks to ECC- and RSA-based systems, underlining the need for quantum-resistant cryptographic algorithms in future protocol designs. Moreover, emergency security requirements—such as authentication bypass or rapid identification in urgent scenarios—are largely overlooked in existing works, despite their practical relevance in medical contexts where emergencies are frequent.

These observations underscore the point that while current protocols address fundamental security requirements, future designs must evolve to incorporate advanced properties—including mutual authentication, privacy preservation, quantum resistance, and emergency handling—to achieve comprehensive security in IoMT environments.

Table 3 lists the types and number of operations used in this papers [44–51,53,54], and Table 4 shows hardware specifications and software configurations. The protocols commonly include hash operations and XOR operations and additionally include operations such as public key-based operations, symmetric key operations, and key exchange, as needed. Some protocols also introduce special operations such as fuzzy extractors for biometric information security, modular operation PUFs, and Merkle tree operations.

Table 3. Comparison of computational overhead.

Ref.	C_{HH}	C_{XOR}	C_{RSAE}	C_{RSAD}	C_{AESE}	C_{AESD}	C_{DH}	C_{FZ}	C_{MOD}	C_{KG}	C_{MT}	C_{PUF}	Computation Time
[44]	43	22	1	1	-	-	-	-	-	-	-	-	2.691 μ s
[45]	15	13	3	3	-	-	17	-	-	6	-	-	30.631 μ s
[46]	8	4	4	4	-	-	10	-	-	-	-	-	6.678 μ s
[47]	39	27	-	-	-	-	-	-	-	-	-	-	1.15 μ s
[48]	28	13	-	-	2	2	-	3	2	-	-	-	12.657 μ s
[49]	57	6	1	1	5	5	-	-	-	1	-	-	32.01 μ s
[50]	12	2	-	-	1	1	-	2	-	-	-	-	6.176 μ s
[51]	17	3	-	-	4	4	3	-	-	-	-	-	23.989 μ s
[53]	35	1	2	2	3	3	4	-	-	1	4	-	21.609 μ s
[54]	42	12	1	1	3	3	-	-	-	-	3	2	19.973 μ s

C_{HH} : cost of hash operation (e.g., SHA-256); C_{XOR} : cost of XOR operation (bitwise exclusive-or); C_{RSAE} : cost of RSA encryption (asymmetric encryption using public key); C_{RSAD} : cost of RSA decryption (asymmetric decryption using private key); C_{AESE} : cost of AES encryption (symmetric encryption); C_{AESD} : cost of AES decryption (symmetric decryption); C_{DH} : cost of Diffie–Hellman key exchange (e.g., ECC scalar multiplication); C_{FZ} : cost of fuzzy extractor or matching (e.g., biometric feature processing); C_{MOD} : cost of modular exponentiation (e.g., RSA or DH); C_{KG} : cost of ECC key generation (key pair generation); C_{MT} : cost of Merkle tree computation (e.g., path proof or update); C_{PUF} : cost of simulated Physical Unclonable Function (PUF) response generation;

Table 4. Experimental Environment.

Equipment	Specification
CPU	Intel i7-12700 (2.1 GHz)
RAM	DDR-4 16 GB
VGA	NVIDIA GeForce RTX 2080
OS	Microsoft Windows 11 Pro
Compiler	MSVC

Looking at the characteristics of each protocol, Abdussami et al. [44] mostly use only hash and XOR operations to simplify the operation structure and pursues lightweight operation by performing RSA operations only once. Qiu et al. [45] provide high-level asymmetric security with many ECC-based key-generation and exchange operations, but the

number of operations is large. Lo et al. [46] also use Diffie–Hellman and RSA operations in a balanced manner and show intermediate complexity. On the other hand, the work by Masud et al. [47] consists of only hash and XOR, so it can be said to be the most lightweight protocol.

Miao et al. [48] combine various elements in authentication by adding biometric information extraction (fuzzy extractor) and modular operations with the basic operations, and Garg et al. [49] strengthen basic security security primarily using hash operations, supplementing them by AES symmetric encryption and digital signature verification. Pradhan et al. [50] proposed a protocol that utilizes AES encryption along with hash functions and XOR operations. Gautam et al. [51] chose a structure that secures basic integrity and confidentiality by using only hash operations, AES, and a small number of DH operations in a relatively simple way.

Su et al. [53] developed a complex structure including ECC key exchange, AES, RSA, and signature verification, aiming to increase defense against various attacks at the same time. Finally, Deebak et al. [54] use PUF and Merkle tree operations in addition to hash operations, XOR, AES, and RSA to additionally ensure security and integrity in special environments such as the IoMT.

Figure 3 graphs the relationship between the computational time of each protocol and the number of security requirements satisfied. The x-axis represents the computational time (in milliseconds) required for each protocol, and the y-axis represents the number of security requirements satisfied. The trendline of the graph was derived by calculating the average slope of all data points. This provides an overall metric for evaluating the tradeoff between security and efficiency.

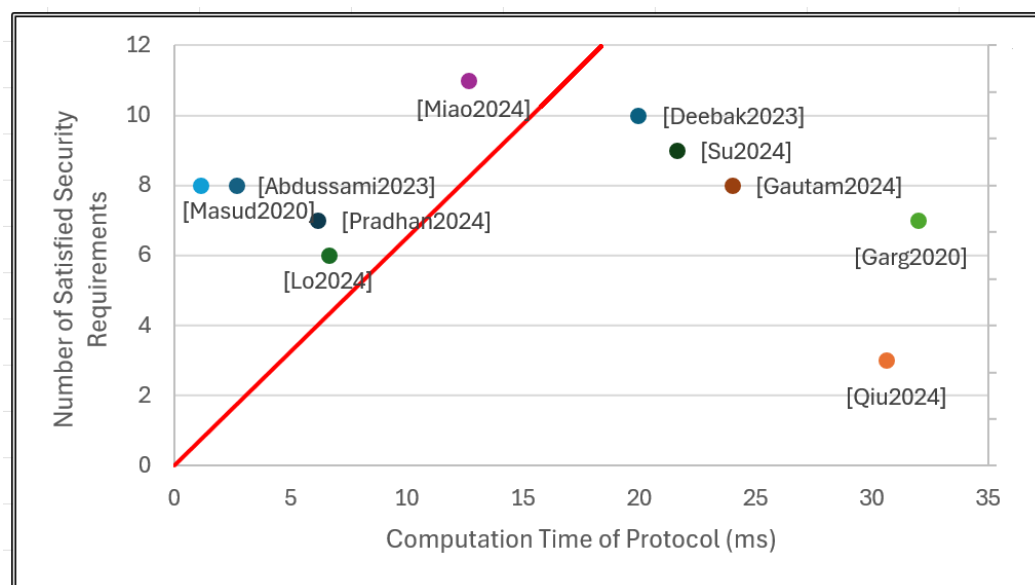


Figure 3. Comparison of protocols by computational time and satisfaction of security requirements [44–51,53,54].

From the graph, it can be observed that protocols positioned closer to the upper left side of the trendline achieve both higher security and greater computational efficiency. A position above and to the left of the trendline suggests that a protocol satisfies a relatively large number of security requirements while maintaining a lower computational burden, thus demonstrating superior performance. According to the graph, the protocol proposed by Miao et al. is especially notable.

This protocol satisfies a wide range of security requirements, demonstrating a high level of security. In addition, this protocol shows excellent efficiency, with a relatively low

computational time compared to other protocols that provide similar security coverage. The balance between security strength and efficiency highlights the practical benefits of this protocol, making it a suitable candidate for environments where both high security and lightweight operation are important. In particular, the combination of lightweight design and meeting comprehensive security requirements shows that this protocol is well-suited for resource-constrained systems in IoMT or next-generation mobile networks.

4. Security Verification

In this section, we evaluate the security of existing proposed protocols and use formal verification tools to check whether each protocol satisfies the main security requirements. Formal verification is a method to comprehensively analyze the validity, safety, and reliability of a protocol through logical reasoning and checking via mathematical models [55]. In this paper, we verify various IoMT authentication protocols using representative formal techniques such as Scyther and SVO Logic. The verification procedure follows the Dolev–Yao adversary model, which assumes that the adversary can eavesdrop on, intercept, and synthesize any message.

For the detailed derivation of the SVO Logic reasoning steps and the Scyther verification process, please refer to the Supplementary Materials.

4.1. SVO Logic

SVO Logic has two rules of inference [56]:

- Modus Ponens: From φ and $\varphi \supset \psi$ infer ψ .
- Necessitation: From $\vdash \varphi$ infer $\vdash P$ believes φ .

‘ $\vdash$ ’ is a meta-lingual symbol that is used in a logical system. ‘ $\Gamma \vdash \varphi$ ’ means that φ can derive from the formula Γ (and the axioms given below), and this indicates that φ can be proven using Γ and axioms. On the other hand, ‘ $\vdash \varphi$ ’ means that φ is a theorem that can be derived using only axioms without additional assumptions or formulas, and this indicates that φ can be proven by itself in the logical system. Evaluation was carried out using SVO Logic notations in Table 5 and the axioms in Table 6, as follows.

Table 5. SVO Logic Notation.

Notation	Meaning
$P \models X$	P believes X
$P \triangleleft X$	P has received a message containing X .
$P \mid \sim X$	P believes X when P sent it.
$P \mid \approx X$	P has saying X
$P \blacktriangleleft X$	Owens X or received it from another entity.
$P \Rightarrow X$	P has a control on X
$\#(X)$	X is newly generated and has never been transmitted before
$P \xrightarrow{K} Q$	P and Q communicate securely through the common key K
$\xrightarrow{PK_P} P$	PK_P is P 's public key, and only P can decrypt message with P 's private key
$\{X\}_K$	X encrypted by K
$[X]_K$	X signed with key K
$\langle X \rangle_{*P}$	The received message X is unrecognized by P

In this section, we present the result of Formal verification using SVO Logic for the 10 authentication protocols presented in this paper. In [44,48,49], the designed protocols clearly prove security through formal verification based on SVO Logic. The logical basis for secure session key exchange in each protocol is clearly presented. This is achieved through a structured reasoning process based on SVO Logic.

Table 6. SVO Logic Axioms.

Axioms	Formula
Believing Axioms (BA)	$P \models \varphi \wedge P \models (\varphi \supset \psi) \rightarrow P \models \psi$ $P \models \varphi \supset P \models (P \models \varphi)$
Source Association Axiom (SAA)	$(P \xleftarrow{K} Q \wedge P \triangleleft \{X\}_K) \rightarrow (Q \approx X \wedge Q \blacktriangleleft X)$
Receiving Axioms (RA)	$P \triangleleft (X_1, \dots, X_n) \supset P \triangleleft X_i$ $(P \triangleleft \{X\}_K \wedge P \blacktriangleleft \tilde{K}) \supset P \triangleleft X$
Possession Axioms (PA)	$P \triangleleft X \rightarrow P \blacktriangleleft X$ $P \blacktriangleleft (X_1, \dots, X_n) \rightarrow P \blacktriangleleft X_i$ $(P \blacktriangleleft X_1 \wedge \dots \wedge P \blacktriangleleft X_n) \rightarrow P \blacktriangleleft F(X_1, \dots, X_n)$
Comprehension Axioms (CA)	$P \models (P \blacktriangleleft F(X)) \supset P \models F(X)$
Saying Axioms (SA)	$P \sim (X_1, \dots, X_n) \rightarrow P \sim X_i \wedge P \blacktriangleleft X_i$ $P \sim (X_1, \dots, X_n) \rightarrow (P \approx X_1, \dots, X_n) \wedge P \sim X_i$
Freshness Axioms (FA)	$\#(X_i) \rightarrow \#((X_1, \dots, X_n))$ $\#((X_1, \dots, X_n)) \rightarrow \#(F(X_1, \dots, X_n))$
Jurisdiction Axiom (JR)	$(P \Rightarrow \varphi \wedge P \sim \varphi) \rightarrow \varphi$
Nonce-Verification Axioms (NV)	$(\#(X) \wedge P \sim X) \rightarrow P \approx X$
Diffie-Hellman Key Exchange Axioms (DH)	$(P \models Q \xrightarrow{\sim PK_Q} Q \wedge P \models \xrightarrow{PK_P} P) \rightarrow P \models S$

First, Abdussami et al. [44] supports mutual authentication and sharing of the secure session key with systematically derived steps such as (DA.4), (DA.5), (DA.9), (DA.13), (DA.17), and (DA.18), as given in the Appendix A of this study. These derivation steps validate that the session key is securely established between both entities. Specifically, in [48], steps (DE.11), (DE.16), and (DE.17), as given in the Appendix E of this study confirm the correctness of the key-exchange process. In particular, although the MSN's indirect belief is not explicitly shown in the derivation step, it is confirmed that the authentication is stated as an assumption in (AE.14) of the Appendix E. This indicates that the MSN trusted the session key during the message-exchange process after the key had been shared.

Finally, in the case of [49], mutual authentication and secure session key exchange are clearly demonstrated. These properties are verified through a series of derivation steps, including (DF.5), (DF.10), (DF.15), (DF.20), (DF.21), and (DF.25), as given in the Appendix F of this study. As a result, the protocol is shown to be robust against key forgery and man-in-the-middle attacks.

In addition, each protocol satisfies forward/backward secrecy by deriving the session key through a combination of a hash function and a randomly generated number for each session. As illustrated in the session key-agreement process in [44], (DA.4), (DA.8), (DA.13), and (DA.17), as given in the Appendix A, from the derivation process, it can be inferred that each session key is generated independently using fresh randomness. This ensures that session keys are cryptographically isolated, preserving both forward and backward secrecy. In the [48], it is also derived in (DE.11), as given in the Appendix E of this study and (DE.16) that the session key is generated by a hash function with a new random number, which ensures key independence between sessions. In [49], the derivation steps (DF.5), (DF.10), (DF.15), and (DF.20), as given in the Appendix F of this study, confirm that the session key is freshly generated for each session. As the new key is not logically linked to any

previous session, the protocol satisfies both forward and backward secrecy. In [50], the key agreement steps (DG.5) and (DG.12), as given in the Appendix G of this study, employ the session timestamp to generate a unique key value for each session. Consequently, the newly generated key value differs from that of the previous session, ensuring that the proposed protocol satisfies both PFS and PBS. In addition, by incorporating a mutual key verification process based on the session key in subsequent steps, the protocol is also verified to achieve the mutual authentication.

Whereas the protocols proposed in [45,51,53,54] appear to verify user identity through an authentication process on the surface, they lack a proper mutual authentication structure. This is revealed in the fact that session key verification was not performed, as the mutual trust in key sharing, which is one of the main security goals defined in SVO Logic, was not derived.

The SVO Logic verification of the protocols set goals for sharing and verifying session keys such as (GB.2), (GB.4), (GH.4), (GH.9), (GI.2), (GI.4), (GJ.3), and (GJ.6), as given in the Appendix B, Appendix H, Appendix I, and Appendix J of this study, but failed to derive the goals in the message-derivation phase.

In addition, the protocols proposed in [45–47,54] omit verification of the random numbers or timestamps included in messages, resulting in structural flaws that fail to prove message freshness. Consequently, these protocols are vulnerable to replay attacks. As a result of the formal verification, freshness-related assumptions were not explicitly adopted during the assumption phase in these protocols. Instead, they were expressed as hypotheses in forms such as (HB.1), (HB.2), (HB.3), (HC.1), (HC.2), (HD.1), (HD.2), (HD.3), and (HJ.1), as given in the Appendix B, Appendix C, Appendix D, and Appendix J of this study, indicating a lack of clear justification or evidence that these elements represent truly fresh values.

In SVO Logic, a hypothesis is treated as an assumption that lacks formal proof. As such, it cannot serve as a valid basis for deriving goals related to freshness, such as replay attack resistance or session key reliability. In other words, if freshness—one of the core security requirements—is not formally established, the protocol may become vulnerable to attacks involving the reuse of past messages, leading to threats such as session key exposure and authentication bypass.

In conclusion, the protocols proposed in [45–47,54] lack a systematic mechanism to formally prove message freshness. This limitation is evident in the SVO Logic analysis, where freshness-related assumptions are treated merely as unproven hypotheses. As a result, these protocols fail to achieve freshness-based security goals through formal reasoning, making them vulnerable to replay and time-based attacks and ultimately undermining their reliability as secure authentication protocols.

For transparency and reproducibility, we have included in the Appendices A–J the security verification we performed for all 10 protocols using SVO Logic: annotation, comprehension, interpretation, assumption, goal, and derivation.

4.2. Scyther

The Scyther tool is used to automatically verify the security properties of the protocol. For this purpose, the protocol is transformed into the Security Protocol Description Language (SPDL) and the participants (roles) are defined along with their corresponding behaviors, such as nonce generation, session key computation, and message transmission. Furthermore, `claim()` events are inserted within each role to determine whether the specified security requirements have been satisfied. Verification is carried out by modeling the protocol in SPDL and validating the achievement of the intended security goals through queries expressed in the form of `claim()` statements [57].

The Secret attribute is used to verify whether the confidentiality of a target element is preserved. When the Secret attribute is satisfied, the element is not exposed to the attacker even if it is transmitted over a public channel. The Secret attribute is used to check whether the confidentiality of specific data items is maintained within a protocol. The SKR attribute is similar to the Secret attribute, but it is specifically applied when verifying the confidentiality of a session key. The Alive attribute denotes the liveness of a role. It indicates that all agents participating in the protocol actively perform their roles until the end of communication. The Weakagree attribute ensures that when two agents believe that they have executed the protocol, they mutually agree on that fact. In other words, the communication counterpart must be the legitimate entity and not an attacker. The Nisynch attribute denotes non-injective synchronization. Non-injective synchronization verifies that everything occurs in execution exactly as intended by the protocol. The Niagree attribute refers to non-injective agreement on messages. It ensures that the messages exchanged within the protocol match exactly in their content.

The protocol [44] first allows the IoMT sensor and the medical server to authenticate each other. Then, it enables mutual authentication between the doctor and the medical server. We modeled the sensor–server and doctor–server communications as two separate files. In the sensor–server analysis, Alive and Weakagree claims for both entities returned “OK.” However, the Nisynch and Niagree claims failed. This indicates that the protocol does not guarantee correct message order or exact correspondence between transmitted and received messages. This result shows that the sensor–server communication requires stronger authentication mechanisms. In contrast, the doctor–server analysis showed that all Alive claims for both entities returned “OK.” These findings confirm the security of communication between the doctor and the medical server.

To evaluate the security of [45], we verified the Alive, Weakagree, Nisynch, and Niagree attributes of the participating entities. Participating entities include patients and doctors. Additionally, we analyzed whether the CID exchanged between them maintained confidentiality. Since IPFS functions solely as a medium for storage and transmission and does not perform any cryptographic operations, it was not defined as a separate role in the model. The lack of such measures creates a vulnerability that allows messages modified by a malicious patient to go undetected.

The analysis confirmed the confidentiality of the CID, as well as the Alive, Weakagree, Nisynch, and Niagree attributes for doctors and the Alive and Weakagree attributes for patients. However, the patient’s Nisynch and Niagree attributes failed to meet the security requirements, indicating vulnerabilities in synchronization and agreement.

They modeled the protocol [46] by combining the registration and authentication phases into a single file. As certain steps rely on public key encryption, they were represented using the pk function. The protocol does not establish a session key, so we did not test the SKR claim and instead examined only the confidentiality of the medical data $SData$. The analysis shows that Alive, Nisynch, Niagree, and Weakagree claims for the doctor, the Service Provider (SP), and the gateway all return “OK”. This outcome confirms their activities and mutual authentication.

Masud et al. [47] proposed a protocol in which each agent generates a PUF through the const declaration. The Scyther model includes the registration phase without omission. It also represents the registration and authentication processes within a single file. The gateway, sensor node, and doctor show “OK” for Alive, Nisynch, Niagree, and Weakagree claims. These results confirm liveness and mutual authentication among the entities. The SKR claim for the session keys also returns “OK,” verifying that the confidentiality of the session key remains intact. Therefore, the protocol meets essential security requirements.

In the modeling of the protocol [48], the registration phase operates over a secure channel. It is therefore simplified to highlight the essential information exchange. The Diffie–Hellman key exchange used in this process is modeled through a helper protocol. Claims such as Alive, Nisynch, Niagree, and Weakagree for both the gateway node and the user are all marked “OK”. This confirms liveness and mutual authentication between the entities. The SKR claim between the medical sensor node and the user is also marked “OK”. This result verifies that the confidentiality of the session key is preserved. No attacks were detected during the communication. These outcomes demonstrate that the protocol ensures secure transmission.

In the Scyther modeling of the protocol [49], we included only the user registration, login, and authentication with key-agreement phases. The preliminary phase defines a Trusted Authority (TA) responsible for distributing the required elements. For the user, Alive, Nisynch, Niagree, and Weakagree claims all return “OK.” These results confirm liveness and successful authentication. The SKR claim between the user and the cloud server also returns “OK,” ensuring user authentication and session key confidentiality from the server’s perspective. In contrast, the cloud server shows “Fail” for Alive, Nisynch, Niagree, and Weakagree claims. This result indicates that the protocol does not authenticate the server. However, because Scyther cannot accurately verify timestamps, cross-validation must be conducted with another tool, namely SVO as employed in this paper.

During the modeling of the [50], ambiguity arose in the computation involving the fog node’s private key SK_F . This issue was addressed by treating SK_F as equivalent to a nonce rn_i . In addition, we corrected several typing errors identified in the original text and reflected them in the Scyther code to ensure analytical accuracy. The verified properties included Alive, Weak Agreement, Nisynch, and Niagree for both the User (U) and the Fog Node (FN), along with the secrecy of the session key exchanged between them. The analysis revealed that the user’s Nisynch and Niagree properties, as well as the session key secrecy, failed to satisfy the security criteria. The fog node also failed to meet the Nisynch and Niagree properties, indicating vulnerabilities in synchronization and agreement assurance. This result reveals that the protocol does not provide server authentication. Given that Scyther cannot ensure accurate timestamp verification, cross-checking is required with an alternative method, in this case, the SVO, as utilized in this paper.

The proposed protocol [51] consists of message exchanges among the user, the gateway, and the sensor node. During the user-registration phase, we analyzed the use of the Diffie–Hellman key-exchange method and incorporated it into the modeling process by adding a supplementary protocol. We conducted the security verification by examining the Alive, Weakagree, Nisynch, and Niagree properties for each entity. We also verified the confidentiality of the session key exchanged among the entities. The analysis showed that all verification claims returned “OK”, which confirmed both the liveness of each entity and the satisfaction of mutual authentication. Furthermore, the results demonstrated the confidentiality of the session key, thereby proving that the proposed protocol ensures reliable security.

We modeled the registration phase of the protocol [53] by assuming it had already been completed. In this setting, the gateway transmitted all required elements together. The verification results indicate that the user satisfied all Alive, Nisynch, Niagree, and Weakagree claims. We also confirmed the confidentiality of both the session key and the gateway’s master key x . However, the gateway did not satisfy the AliveAlive and Weakagree claims, and the sensor device did not satisfy any of the Alive, Nisynch, Niagree, and Weakagree claims. These results indicate that the authentication of the gateway and the sensor device is ineffective during communication. The proposed protocol often relies on XOR functions. However, because Scyther is unable to process XOR operations, manual modeling becomes

necessary; this can introduce unintended false positives. Thus, protocols containing XOR must be cross-validated with alternative verification tools.

The protocol [54] specified a single file that sequentially includes the registration and authentication steps. Analysis using Scyther revealed that the Alive, Nisynch, Niagree, and Weakagree claims for the Mobile Equipment (ME), Access Gateway (AG), and Medical Server (MS) all returned “OK.” This confirms that each participant’s activities were normal and that mutual authentication was successfully achieved.

5. Discussion

The analysis presented in Figure 2 shows that there is a trade-off relationship between computational cost efficiency and robust security among the proposed protocols. In general, protocols that satisfy many security requirements have higher computational costs. Other protocols with lower computational overhead have lower security. This relationship is very important in real environments, especially in resource-constrained environments and in environments where security and responsiveness are equally critical.

Table 7 briefly summarizes the formal verification results. This table indicates whether the authors of each paper conducted the verification and the results of our verification via SVO-Logic and Scyther. We observed that most protocols satisfied fundamental security requirements such as authentication, confidentiality, and integrity. However, many protocols are found to be inadequate in meeting the main security requirements, including key agreement, the consistency of communication objectives, and confidentiality assurance. Despite these limitations, the protocols presented in [44,48] demonstrated robustness in both verification approaches, indicating a comparatively higher level of security than the other protocols.

Table 7. Security Verification Result.

Ref.	Verification by the Authors’ Own	SVO	Scyther	Scyther Properties					
				Niagree	Nisynch	Weakagree	Secret	SKR	Alive
[44]	$O(\text{Scyther})$	×	×	✓	✓	✓	✓	✓	✓
[45]	$O(\text{AVISPA})$	×	×	×	×	✓	✓	✓	✓
[46]	—	×	O	✓	✓	✓	×	✓	✓
[47]	—	×	O	✓	✓	✓	✓	✓	✓
[48]	$O(\text{BAN} - \text{Logic})$	O	O	✓	✓	✓	✓	✓	✓
[49]	$O(\text{AVISPA})$	O	×	×	×	×	✓	✓	×
[50]	$O(\text{ProVerif}, \text{BAN} - \text{Logic})$	O	×	×	×	✓	×	✓	✓
[51]	—	×	O	✓	✓	✓	✓	✓	✓
[53]	$O(\text{ProVerif})$	×	×	×	×	×	✓	✓	×
[54]	—	×	O	×	×	×	×	×	×

O : Passed, $\times$: Unpassed/Unsatisfied, $\checkmark$: Satisfied.

Among the protocols reviewed in this paper, the scheme proposed by Miao et al. [48] stands out. This protocol shows a relaxation of the trade-off relationship between security and efficiency. The proposed scheme satisfies a wide range of security requirements. The proposed method maintains relatively low computational time compared to other protocols that achieve similar security levels. This shows that the protocol proposed by Miao et al. [48]. The protocol is suitable for environments such as IoMT systems that require both strong security and a lightweight protocol.

Miao et al. [48]’s protocol was formally verified using SVO Logic and Scyther. The analysis confirmed logical derivations of mutual authentication, session freshness, key agreement, and key confirmation. These results indicate that the protocol satisfies critical security properties while maintaining computational efficiency.

The verification results further emphasize the practical value of the protocol. It not only demonstrates mutual authentication, key agreement, and efficiency, but also shows potential applicability in real-world deployments. In particular, its strengths suggest that it may be well-suited for resource-constrained environments or scenarios requiring strong security guarantees. Nonetheless, moving from theoretical validation to practical adoption requires careful consideration of its limitations.

6. Conclusions

IoT technology has led to significant transformations in the medical sector. In particular, the growth of the elderly population and the increasing prevalence of chronic diseases have continuously heightened the demand for personalized medical services. To address these emerging challenges, the need for intelligent medical systems capable of supporting real-time patient monitoring and data-driven medical decision-making is becoming increasingly critical.

The IoMT is revolutionizing the provision of healthcare services across diverse environments by interconnecting MDs, wearable devices, and point-of-care diagnostic equipment. Furthermore, IoMT technologies are being integrated into hospital-management systems to facilitate the real-time monitoring of medical assets and facilities and to enable seamless sharing of health data between patients and healthcare providers. This integration enhances the delivery of various medical services, including preventive care, management of chronic disease, and emergency response.

Within IoMT environments, data transmission serves as a fundamental determinant of overall system efficiency and reliability. Health data collected by sensors and medical devices must meet stringent requirements concerning security, reliability, latency, and energy efficiency. Given the sensitive nature of medical information, any compromise in data integrity or transmission reliability could pose direct threats to patient safety. Consequently, the development of secure and efficient data-transmission methods is of paramount importance.

In practice, the selection of an authentication protocol must balance the importance of security requirements with the available computational resources. Lightweight schemes may be preferable for resource-constrained IoMT nodes, whereas critical systems require protocols with stronger security guarantees despite higher costs.

In this context, this paper comprehensively analyzes recently proposed authentication protocols in terms of security requirements, computational costs, and formal verification results to explore protocols suitable for the IoMT environment. The results highlighted the protocol proposed by Miao et al. [48], confirming the importance of balancing environmental characteristics and security in future IoMT protocol development.

This evaluation has several limitations. First, it assumed that all security requirements are equivalent and did not consider that their importance may vary depending on the application scenario. Second, the computational time was collected under general conditions, and actual performance may differ across hardware platforms and operational environments.

In future research, we plan to design an authentication protocol that optimizes the trade-off between security and computational efficiency by systematically categorizing diverse use cases and prioritizing security requirements according to their relative importance in each application environment.

Supplementary Materials: The following supporting information can be downloaded at: https://github.com/lb0207/IoMT_SupplementFile (accessed on 2 October 2025).

Author Contributions: Conceptualization, S.L. (Seungbin Lee) and J.K.; methodology, J.K.; validation, S.L. (Seungbin Lee), K.A.K. and J.K.; formal analysis, S.L. (Soowang Lee) and J.K.; investigation, S.L. (Seungbin Lee) and S.L. (Soowang Lee); data curation, K.A.K. and J.K.; writing—original draft preparation, S.L. (Seungbin Lee) and J.K.; writing—review and editing, S.L. (Seungbin Lee) and J.K.; visualization, S.L. (Seungbin Lee); supervision, J.K.; project administration, J.K.; funding acquisition, J.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) [grant number RS-2023-00210767].

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

3ECAP	Three-Factor Efficient and Cost-Aware Authentication Protocol
3-Factor	Three-Factor Authentication
4G/5G	4th Generation/5th Generation
AES	Advanced Encryption Standard
AVISPA	Automated Validation of Internet Security Protocols and Applications
BAKMP	Blockchain-based Authentication and Key Management Protocol
BAN-Logic	Burrows–Abadi–Needham Logic
BCI	Brain–Computer Interface
BLE	Bluetooth Low Energy
BYOD	Bring Your Own Device
CE	Consumer Electronics
CGM	Continuous Glucose Monitoring
CoAP	Constrained Application Protocol
CRT	Chinese Remainder Theorem
CVE	Common Vulnerabilities and Exposures
CVP	Closest Vector Problem
DBS	Deep Brain Stimulator
DH	Diffie–Hellman
ECC	Elliptic Curve Cryptography
ECG	Electrocardiogram
EHRs	Electronic Health Records
ESL	Ephemeral Secret Leakage
HL7	Health Level Seven
ICDs	Implantable Cardioverter Defibrillators
IMD	Implantable Medical Device
IoMT	Internet of Medical Things
IoMT-SAF	Internet of Medical Things – Security Assessment Framework
IoT	Internet of Things
IoWD	Internet of Wearable Devices
L2FAK	Lightweight Two-Factor Authentication Framework
LBC	Lightweight Lattice-Based Cryptography
LTE	Long Term Evolution
LVADs	Left Ventricular Assist Devices
LWE	Learning with Errors
M2M	Machine-to-Machine
MASK	Mutual Authentication and Secret Key
MDs	Medical Devices

MITM	Man-In-The-Middle (Attack)
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
NFC	Near Field Communication
NFT	Non-Fungible Token
ProVerif	Protocol Verification Tool
PSLA2P	Provably Secured Lightweight Authenticated Key Agreement Protocol
PUF	Physically Unclonable Function
QoS	Quality of Service
RFID	Radio-Frequency Identification
RSA	Rivest–Shamir–Adleman (Public Key Cryptosystem)
SCS	Spinal Cord Stimulator
SDN	Software Defined Networking
Slither	Solidity Static Analysis Tool
S-IoMT	Smart Internet of Medical Things
SpO ₂	Peripheral Capillary Oxygen Saturation
SVP	Shortest Vector Problem
TA	Trusted Authority
VNS	Vagus Nerve Stimulator
Wi-Fi	Wireless Fidelity
XAI	Explainable Artificial Intelligence
XOR	Exclusive OR

Appendix A. Formal Verification Result for Abdussami et al. [44]

Annotation

$$\begin{aligned}
 (RA.1) \quad MS &\triangleleft \{B_s, n_1, T_1, \$1\}_{K_{psk}} \\
 (RA.2) \quad IoMT &\triangleleft \{n_1, n_2, T_2, \$2\}_{K_{psk}} \\
 (RA.3) \quad MS &\triangleleft \{ID_{ms}, M, n_3, T_3, \$3\}_{K_{psk_2}} \\
 (RA.4) \quad Doc &\triangleleft \{M, n_3, n_4, T_4, \$4, \$5\}_{K_{psk_2}}
 \end{aligned}$$

Comprehension

$$\begin{aligned}
 (CA.1) \quad MS &| \equiv MS \triangleleft \{B_s, n_1, T_1, \$1\}_{K_{psk}} \\
 (CA.2) \quad IoMT &| \equiv IoMT \triangleleft \{n_1, n_2, T_2, \$2\}_{K_{psk}} \\
 (CA.3) \quad MS &| \equiv MS \triangleleft \{ID_{ms}, M, n_3, T_3, \$3\}_{K_{psk_2}} \\
 (CA.4) \quad Doc &| \equiv Doc \triangleleft \{M, n_3, n_4, T_4, \$4, \$5\}_{K_{psk_2}}
 \end{aligned}$$

Interpretation

$$\begin{aligned}
 (PA.1) \quad MS &| \equiv MS \triangleleft \{B_s, n_1, T_1, \$1\}_{K_{psk}} \\
 &\rightarrow MS | \equiv MS \triangleleft \{B_s, n_1, \#(T_1), IoMT \xleftrightarrow{K_{psk}} MS\}_{K_{psk}} \\
 (PA.2) \quad IoMT &| \equiv IoMT \triangleleft \{n_1, n_2, T_2, \$2\}_{K_{psk}} \\
 &\rightarrow IoMT | \equiv IoMT \triangleleft \{n_1, n_2, \#(T_2), IoMT \xleftrightarrow{K_{psk}} MS\}_{K_{psk}} \\
 (PA.3) \quad MS &| \equiv MS \triangleleft \{ID_{ms}, M, n_3, T_3, \$3\}_{K_{psk_2}} \\
 &\rightarrow MS | \equiv MS \triangleleft \{ID_{ms}, M, n_3, \#(T_3), MS \xleftrightarrow{K_{psk_2}} Doc\}_{K_{psk_2}} \\
 (PA.4) \quad Doc &| \equiv Doc \triangleleft \{M, n_3, n_4, T_4, \$4, \$5\}_{K_{psk_2}} \\
 &\rightarrow Doc | \equiv Doc \triangleleft \{M, n_3, n_4, \#(T_4), MS \xleftrightarrow{K_{psk_2}} Doc, MS \xleftrightarrow{S_2} Doc\}_{K_{psk_2}}
 \end{aligned}$$

Assumption

$$\begin{aligned}
 (AA.1) \quad MS &\blacktriangleleft IoMT \xleftrightarrow{K_{psk}} MS \\
 (AA.2) \quad MS &\blacktriangleleft n_2
 \end{aligned}$$

$$\begin{aligned}
(AA.3) \quad MS &\equiv \#(T_2) \\
(AA.4) \quad IoMT &\blacktriangleleft IoMT \xleftrightarrow{K_{psk}} MS \\
(AA.5) \quad IoMT &\equiv MS \Rightarrow S_1 \\
(AA.6) \quad MS &\blacktriangleleft MS \xleftrightarrow{K_{psk_2}} Doc \\
(AA.7) \quad MS &\blacktriangleleft n_3 \\
(AA.8) \quad MS &\equiv (T_4) \\
(AA.9) \quad Doc &\blacktriangleleft MS \xleftrightarrow{K_{psk_2}} Doc
\end{aligned}$$

Goal

$$\begin{aligned}
(GA.1) \quad MS &\equiv S_1 \\
(GA.2) \quad IoMT &\equiv S_1 \\
(GA.3) \quad IoMT &\equiv MS \equiv S_1 \\
(GA.4) \quad MS &\equiv IoMT \equiv S_1 \\
(GA.5) \quad MS &\equiv S_2 \\
(GA.6) \quad MS &\equiv Doc \approx S_2 \\
(GA.7) \quad Doc &\equiv S_2 \\
(GA.8) \quad Doc &\equiv MS \approx S_2
\end{aligned}$$

Derivation

$$\begin{aligned}
(DA.1) \quad MS &\equiv MS \triangleleft \{B_s, n_1, \#(T_1), IoMT \xleftrightarrow{K_{psk}} MS\}_{K_{psk}} && \text{by Modusponens, (CA.1), (PA.1)} \\
(DA.2) \quad MS &\equiv IoMT \sim (B_s, n_1, \#(T_1), IoMT \xleftrightarrow{K_{psk}} MS) && \text{by (DA.1), (AA.1), SAA, BA} \\
(DA.3) \quad MS &\equiv IoMT \approx (B_s, n_1, \#(T_1), IoMT \xleftrightarrow{K_{psk}} MS) && \text{by (DA.2), FA, NV, BA} \\
(DA.4) \quad MS &\equiv S_1 && \\
&\text{where } S_1 = H(K_{psk} || n_1 || n_2 || T_2) && \text{by (DA.3), (AA.2), (AA.3), BA} \\
(DA.5) \quad IoMT &\equiv IoMT \triangleleft \{n_1, n_2, \#(T_2), IoMT \xleftrightarrow{K_{psk}} MS\}_{K_{psk}} && \text{by Modusponens, (CA.2), (PA.2)} \\
(DA.6) \quad IoMT &\equiv MS \sim (n_1, n_2, \#(T_2), IoMT \xleftrightarrow{K_{psk}} MS) && \text{by (DA.5), (AA.4), SAA, BA} \\
(DA.7) \quad IoMT &\equiv MS \approx (n_1, n_2, \#(T_2), IoMT \xleftrightarrow{K_{psk}} MS) && \text{by (DA.6), FA, NV, BA} \\
(DA.8) \quad IoMT &\equiv MS \equiv S_1 && \\
&\text{where } S_1 = H(K_{psk} || n_1 || n_2 || T_2) && \text{by (DA.6), FA, NV, BA} \\
(DA.9) \quad IoMT &\equiv S_1 && \text{by (DA.8), (AA.8), JR} \\
(DA.10) \quad MS &\equiv MS \triangleleft \{ID_{ms}, M, n_3, \#(T_3), MS \xleftrightarrow{K_{psk_2}} Doc\}_{K_{psk_2}} && \text{by Mondusponens, (CA.3), (PA.3)} \\
(DA.11) \quad MS &\equiv Doc \sim (ID_{ms}, M, n_3, \#(T_3), MS \xleftrightarrow{K_{psk_2}} Doc) && \text{by (DA.10), (AA.6), SAA, BA} \\
(DA.12) \quad MS &\equiv Doc \approx (ID_{ms}, M, n_3, \#(T_3), MS \xleftrightarrow{K_{psk_2}} Doc) && \text{by (DA.11), FA, NV, BA} \\
(DA.13) \quad MS &\equiv Doc \approx S_2 && \\
&\text{where } S_2 = H(M || n_3 || n_4 || T_4) && \text{by (DA.12), (AA.7), (AA.8), BA} \\
(DA.14) \quad Doc &\equiv Doc \triangleleft \{M, n_3, n_4, \#(T_4), MS \xleftrightarrow{K_{psk_2}} Doc, MS \xleftrightarrow{S_2} Doc\}_{K_{psk_2}} && \text{by Modusponens, (CA.4), (PA.4)} \\
(DA.15) \quad Doc &\equiv MS \sim (M, n_3, n_4, \#(T_4), MS \xleftrightarrow{K_{psk_2}} Doc, MS \xleftrightarrow{S_2} Doc) && \text{by (DA.14), (AA.9), SAA, BA} \\
(DA.16) \quad Doc &\equiv MS \approx (M, n_3, n_4, \#(T_4), MS \xleftrightarrow{K_{psk_2}} Doc, MS \xleftrightarrow{S_2} Doc) && \text{by (DA.15), FA, NV, BA} \\
(DA.17) \quad Doc &\equiv MS \approx MS \xleftrightarrow{S_2} Doc && \text{by (DA.16), BA} \\
(DA.18) \quad Doc &\equiv S_2 && \\
&\text{where } S_2 = H(M || n_3 || n_4 || T_4) && \text{by (DA.16), BA}
\end{aligned}$$

Appendix B. Formal Verification Result for Qiu et al. [45]

Annotation

$$\begin{aligned}
(RB.1) \quad D &\triangleleft \{A_j, B_j, Cert_j\}_{PU_D} \\
(RB.2) \quad P &\triangleleft \{C, Cert_i\}_{PU_P} \\
(RB.3) \quad D &\triangleleft \{CID_{J,K}\}_{PU_D}
\end{aligned}$$

Comprehension

$$(CB.1) D \models D \triangleleft \{A_j, B_j, Cert_j\}_{PU_D}$$

$$(CB.2) P \models P \triangleleft \{C, Cert_i\}_{PU_P}$$

$$(CB.3) D \models D \triangleleft \{CID_{J,K}\}_K$$

Interpretation

$$(GB.1) D \models D \triangleleft \{A_j, B_j, Cert_j\}_{PU_D}$$

$$\rightarrow D \models D \triangleleft \{addr, AID, r_3, Cert_j\}_{PU_D}$$

$$(GB.2) P \models P \triangleleft \{C, Cert_i\}_{PU_P}$$

$$\rightarrow P \models P \triangleleft \{addr, r_3, Cert_i\}_{PU_P} \quad (GB.3) D \models D \triangleleft \{CID_{J,K}\}_{PU_D}$$

$$\rightarrow D \models D \triangleleft \{P \xleftrightarrow{CID_{J,K}} D\}_K$$

Assumption

$$(AB.1) D \xleftarrow{PU_D} D$$

$$(AB.2) D \models D \xleftrightarrow{addr} P$$

$$(AB.3) D \models P \Rightarrow Cert_j$$

$$(AB.4) P \xleftarrow{PU_P} P$$

$$(AB.5) P \models D \xleftrightarrow{addr} P$$

$$(AB.6) P \models D \Rightarrow Cert_i$$

$$(AB.7) P \xleftarrow{PU_D} P$$

$$(HB.1) D \models \#(r_3)$$

$$(HB.2) P \models \#(addr, r_3, cert_i)$$

$$(HB.3) D \models \#(CID_{J,K})$$

Goal

$$(GB.1) D \models K$$

$$(GB.2) D \models P \xleftarrow{K} K$$

$$(GB.3) P \models K$$

$$(GB.4) P \models P \xleftarrow{K} K$$

$$(GB.5) D \models P \approx CID_{J,K}$$

Derivation

$$(DB.1) D \models D \triangleleft \{addr, AID, r_3, Cert_j\}_{PU_D} \quad \text{by Modusponens using (CB.1), (GB.1)}$$

$$(DB.2) D \models P \sim (addr, AID, r_3, Cert_j) \quad \text{by (DB.1), (AB.1), (AB.2) SAA, BA}$$

$$(DB.3) D \models P \approx (addr, AID, r_3, Cert_j) \quad \text{by (DB.2), (HB.1), FA, NV, BA}$$

$$(DB.4) D \models (addr, AID, r_3, Cert_j) \quad \text{by (DB.3), (AB.3), JR, BA}$$

$$(DB.5) D \models K$$

$$\text{where } K = r_3 \cdot PU_D$$

$$\text{by (DB.4), (AB.1), BA}$$

$$(DB.6) P \models P \triangleleft \{addr, r_3, Cert_i\}_{PU_P}$$

$$\text{by Modusponens using (CB.2), (PB.2)}$$

$$(DB.7) P \models D \sim (addr, r_3, Cert_i)$$

$$\text{by (DB.6), (AB.4), (AB.5), SAA, BA}$$

$$(DB.8) P \models D \approx (addr, r_3, Cert_i)$$

$$\text{by (DB.7), (HB.2), FA, NV}$$

$$(DB.9) P \models (addr, r_3, Cert_i)$$

$$\text{by (DB.8) JR, BA}$$

$$(DB.10) P \models K$$

$$\text{where } K = r_3 \cdot PU_D$$

$$\text{by (DB.9), (AB.7), BA}$$

$$(DB.11) D \models D \triangleleft \{P \xleftrightarrow{CID_{J,K}} D\}_K$$

$$\text{by Modusponens using (CB.3), (PB.3)}$$

$$(DB.12) D \models P \sim P \xleftrightarrow{CID_{J,K}} D$$

$$\text{by (DB.11), (DB.5), SAA, BA}$$

$$(DB.13) D \models P \approx P \xleftrightarrow{CID_{J,K}} D$$

$$\text{by (DB.12), (HB.3), FA, NV}$$

Appendix C. Formal Verification Result for Lo et al. [46]

Annotation

$$(RC.1) SP \triangleleft \{NID_D, PW_D, BIO_D\}_{PU_{SP}}$$

$$(RC.2) SP \triangleleft \{NID_P\}_{PU_{SP}}$$

$$(RC.3) D \triangleleft \{SData\}_{PU_D}$$

Comprehension

$$(CC.1) SP \models SP \triangleleft \{NID_D, PW_D, BIO_D\}_{PU_{SP}}$$

$$(CC.2) SP \models SP \triangleleft \{NID_P\}_{PU_{SP}}$$

$$(CC.3) D \models D \triangleleft \{SData\}_{PU_D}$$

Interpretation

$$(PC.1) SP \models SP \triangleleft \{NID_D, PW_D, BIO_D\}_{PU_{SP}}$$

$$\rightarrow SP \models SP \triangleleft \{NID_D, PW_D, D \xleftrightarrow{BIO_D} SP\}_{PU_{SP}}$$

$$(PC.2) SP \models SP \triangleleft \{NID_P\}_{PU_{SP}}$$

$$\rightarrow SP \models SP \triangleleft \{NID_P\}_{PU_{SP}}$$

$$(PC.3) D \models D \triangleleft \{SData\}_{PU_D}$$

$$\rightarrow D \models D \triangleleft \{D \xleftrightarrow{SData} SP\}_{PU_D}$$

Assumption

$$(AC.1) SP \xleftrightarrow{PU_{SP}} SP$$

$$(AC.2) D \xleftrightarrow{PU_D} D$$

$$(AC.3) D \models \#(SData)$$

$$(HC.1) SP \models \#(NID_D, PW_D, BID_D)$$

$$(HC.2) SP \models \#(NID_P)$$

Goal

$$(GC.1) SP \models D \approx D \xleftrightarrow{BIO_D} SP$$

$$(GC.2) SP \models D \approx SP \xleftrightarrow{NID_P} D$$

$$(GC.3) SP \models D \approx D \xleftrightarrow{SData} SP$$

Derivation

$$(DC.1) SP \models SP \triangleleft \{NID_D, PW_D, D \xleftrightarrow{BIO_D} SP\}_{PU_{SP}} \quad \text{by Modusponens using (CC.1), (PC.1)}$$

$$(DC.2) SP \models D \sim (NID_D, PW_D, D \xleftrightarrow{BIO_D} SP) \quad \text{by (DC.1), (AC.1), SAA, BA}$$

$$(DC.3) SP \models D \approx (NID_D, PW_D, D \xleftrightarrow{BIO_D} SP) \quad \text{by (DC.2), (HC.1), FA, NV, BA}$$

$$(DC.4) SP \models D \approx D \xleftrightarrow{BIO_D} SP \quad \text{by (DC.3), BA}$$

$$(DC.5) SP \models SP \triangleleft \{NID_P\}_{PU_{SP}} \quad \text{by Modusponens using (CC.2), (PC.2)}$$

$$(DC.6) SP \models D \sim SP \xleftrightarrow{NID_P} D \quad \text{by (DC.5), (AC.1), SAA}$$

$$(DC.7) SP \models D \approx SP \xleftrightarrow{NID_P} D \quad \text{by (DC.6), (HC.2), FA, NV}$$

$$(DC.8) D \models D \triangleleft \{SData\}_{PU_D} \quad \text{by Modusponens using (CC.3), (PC.3)}$$

$$(DC.9) D \models SP \sim D \xleftrightarrow{SData} SP \quad \text{by (DC.8), (AC.2), SAA, BA}$$

$$(DC.10) D \models SP \approx D \xleftrightarrow{SData} SP \quad \text{by (DC.9), (AC.3), FA, NV}$$

Appendix D. Formal Verification Result for Masud et al. [47]

Annotation

$$(RD.1) D \triangleleft \{G_1, G_2, G_3\}_{\langle D_{ID}^H, D_{LN}^{MCC} \rangle}$$

$$(RD.2) G \triangleleft \{U_2, U_3, SN_{IEI}^*\}_{\langle D_{ID}^H, D_{LN}^{MCC} \rangle}$$

$$(RD.3) S \triangleleft \{G_5, G_6, G_7, SK_{SN}^*, \mu, C_{SN}\}_{\langle SN_{IEI}, TID_{SN} \rangle}$$

$$(RD.4) G \triangleleft \{SN_2, SN_3\}_{TID_{SN}^0}$$

$$(RD.5) D \triangleleft \{G_9, SK_U^*, G_{10}, C_U^{1*}\}_{D_{ID}^H}$$

Comprehension

$$(CD.1) D \models D \triangleleft \{G_1, G_2, G_3\}_{\langle D_{ID}^H, D_{LN}^{MCC} \rangle}$$

$$(CD.2) G \models G \triangleleft \{U_2, U_3, SN_{IEI}^*\}_{D_{LN}^{MCC}}$$

$$(CD.3) S \models S \triangleleft \{G_5, G_6, G_7, SK_{SN}^*, \mu, C_{SN}'\}_{\langle SN_{IEI}, TID_{SN} \rangle}$$

$$(CD.4) G \models G \triangleleft \{SN_2, SN_3\}_{TID_{SN}^0}$$

$$(CD.5) D \models D \triangleleft \{G_9, SK_U^*, G_{10}, C_U^{1*}\}_{D_{ID}^H}$$

Interpretation

$$(PD.1) D \models D \triangleleft \{G_1, G_2, G_3\}_{\langle D_{ID}^H, D_{LN}^{MCC} \rangle}$$

$$\rightarrow D \models D \triangleleft \{C_U^0, N_G^1, R_U^0, D_{ID}^H, D_{LN}^{MCC}\}_{\langle D_{ID}^H, D_{LN}^{MCC} \rangle}$$

$$(PD.2) G \models G \triangleleft \{U_2, U_3, SN_{IEI}^*\}_{\langle D_{ID}^H, D_{LN}^{MCC} \rangle}$$

$$\rightarrow G \models G \triangleleft \{C_U^0, N_G^1, R_U^0, D_{ID}^H, D_{LN}^{MCC}, N_U^2\}_{D_{LN}^{MCC}}$$

$$(PD.3) S \models S \triangleleft \{G_5, G_6, G_7, SK_{SN}^*, \mu, C_{SN}'\}_{\langle SN_{IEI}, TID_{SN} \rangle}$$

$$\rightarrow S \models S \triangleleft \{C_{SN}^0, N_G^2, R_{SN}^0, G \xleftrightarrow{SK} SN, C_{SN}^1\}_{\langle SN_{IEI}, TID_{SN} \rangle}$$

$$(PD.4) G \models G \triangleleft \{SN_2, SN_3\}_{TID_{SN}^0}$$

$$\rightarrow G \models G \triangleleft \{C_{SN}^0, N_G^2, R_{SN}^0, G \xleftrightarrow{SK} SN, N_{SN}^1\}_{TID_{SN}^0}$$

$$(PD.5) D \models D \triangleleft \{G_9, SK_U^*, G_{10}, C_U^{1*}\}_{D_{ID}^H}$$

$$\rightarrow D \models D \triangleleft \{N_G^3, TID_U^0, D_{ID}^H, D_{LN}^{MCC}, D \xleftrightarrow{SK} G\}_{D_{ID}^H}$$

Assumption

$$(AD.1) D \blacktriangleleft D \xleftrightarrow{D_{ID}^H, D_{LN}^{MCC}} G$$

$$(AD.2) G \blacktriangleleft D \xleftrightarrow{D_{ID}^H, D_{LN}^{MCC}} G$$

$$(AD.3) G \models \#(N_G^1)$$

$$(AD.4) S \blacktriangleleft G \xleftrightarrow{SN_{IEI}, TID_{SN}^0} S$$

$$(AD.5) S \models G \Rightarrow G \xleftrightarrow{SK} S$$

$$(AD.6) G \blacktriangleleft G \xleftrightarrow{TID_{SN}^0} S$$

$$(AD.7) G \models \#(N_G^2)$$

$$(AD.8) D \models G \Rightarrow D \xleftrightarrow{SK} G$$

$$(HD.1) D \models \#(N_G^1)$$

$$(HD.2) S \models \#(N_G^2)$$

$$(HD.3) D \models \#(N_G^3)$$

Goal

$$(GD.1) D \models G \approx (D_{ID}^H, D_{LN}^{MCC})$$

$$(GD.2) G \models D \approx (D_{ID}^H, D_{LN}^{MCC})$$

$$(GD.3) S \models G \approx G \xleftrightarrow{SK} SN$$

$$(GD.4) S \models G \xleftrightarrow{SK} SN$$

$$(GD.5) S \models G \approx C_{SN}^1$$

$$(GD.6) G \models S \approx G \xleftrightarrow{SK} SN$$

$$(GD.7) D \models G \approx D \xleftrightarrow{SK} G$$

$$(GD.8) D \models D \xleftrightarrow{SK} G$$

Derivation

(DD.1) $D \models D \triangleleft \{C_U^0, N_G^1, R_U^0, D_{ID}^H, D_{LN}^{MCC}\}_{<D_{ID}^H, D_{LN}^{MCC}>}$	by Modusponens using (CD.1), (PD.1)
(DD.2) $D \models G \sim (C_U^0, N_G^1, R_U^0, D_{ID}^H, D_{LN}^{MCC})$	by (DD.1), (AD.1), SAA, BA
(DD.3) $D \models G \approx (C_U^0, N_G^1, R_U^0, D_{ID}^H, D_{LN}^{MCC})$	by (DD.2), (HD.1), FA, NV, BA
(DD.4) $D \models G \approx (D_{ID}^H, D_{LN}^{MCC})$	by (DD.3), BA
(DD.5) $G \models G \triangleleft \{C_U^0, N_G^1, R_U^0, D_{ID}^H, D_{LN}^{MCC}, N_U^2\}_{D_{LN}^{MCC}}$	by Modusponens using (CD.2), (PD.2)
(DD.6) $G \models D \sim (C_U^0, N_G^1, R_U^0, D_{ID}^H, D_{LN}^{MCC}, N_U^2)$	by (DD.5), (AD.2), SAA, BA
(DD.7) $G \models D \approx (C_U^0, N_G^1, R_U^0, D_{ID}^H, D_{LN}^{MCC}, N_U^2)$	(DD.6), (AD.3), FA, NV, BA
(DD.8) $G \models D \approx D_{ID}^H, D_{LN}^{MCC}$	by (DD.7) BA
(DD.9) $S \models S \triangleleft \{C_{SN}^0, N_G^2, R_{SN}^0, G \xleftrightarrow{SK} SN, C_{SN}^1\}_{<SN_{IEI}, TID_{SN}>}$	by Modusponens, (CD.3), (PD.3)
(DD.10) $S \models G \sim (C_{SN}^0, N_G^2, R_{SN}^0, G \xleftrightarrow{SK} SN, C_{SN}^1)$	by (DD.9), (AD.4), SAA, BA
(DD.11) $S \models G \approx (C_{SN}^0, N_G^2, R_{SN}^0, G \xleftrightarrow{SK} SN, C_{SN}^1)$	by (DD.10), (HD.2), FA, NV, BA
(DD.12) $S \models G \approx G \xleftrightarrow{SK} SN$	by (DD.11), BA
(DD.13) $S \models G \xleftrightarrow{SK} SN$	by (DD.12), (AD.5), JR
(DD.14) $S \models G \approx C_{SN}^1$	by (DD.11), BA
(DD.15) $G \models G \triangleleft \{C_{SN}^0, N_G^2, R_{SN}^0, G \xleftrightarrow{SK} SN, N_{SN}^1\}_{TID_{SN}^0}$	by Modusponens using (CD.4), (PD.4)
(DD.16) $G \models S \sim (C_{SN}^0, N_G^2, R_{SN}^0, G \xleftrightarrow{SK} SN, N_{SN}^1)$	by (DD.15), (AD.6), SAA, BA
(DD.17) $G \models S \approx (C_{SN}^0, N_G^2, R_{SN}^0, G \xleftrightarrow{SK} SN, N_{SN}^1)$	by (DD.16), (AD.7), FA, NV, BA
(DD.18) $G \models S \approx G \xleftrightarrow{SK} SN$	by (DD.17), BA
(DD.19) $D \models D \triangleleft \{N_G^3, TID_U^0, D_{ID}^H, D_{LN}^{MCC}, D \xleftrightarrow{SK} G\}_{D_{ID}^H}$	by Modusponens using (CD.5), (PD.5)
(DD.20) $D \models G \sim (N_G^3, TID_U^0, D_{ID}^H, D_{LN}^{MCC}, D \xleftrightarrow{SK} G)$	by (DD.19), (AD.1), SAA, BA
(DD.21) $D \models G \approx (N_G^3, TID_U^0, D_{ID}^H, D_{LN}^{MCC}, D \xleftrightarrow{SK} G)$	by (DD.20), (HD.3), FA, NVV, BA
(DD.22) $D \models G \approx D \xleftrightarrow{SK} G$	by (DD.21) BA
(DD.23) $D \models D \xleftrightarrow{SK} G$	by (DD.22) JR

Appendix E. Formal Verification Result for Miao et al. [48]

Annotation

- (RE.1) $GN \triangleleft \{D_1, D_3, D_4, D_5, T_1\}_{D_2}$
 (RE.2) $MSN \triangleleft \{D_1, D_6, D_7, D_8, T_2\}_{SD}$
 (RE.3) $UE \triangleleft \{D_9, D_{11}, T_3\}_{D_{10}}$

Comprehension

- (CE.1) $GN \models GN \triangleleft \{D_1, D_3, D_4, D_5, T_1\}_{D_2}$
 (CE.2) $MSN \models MSN \triangleleft \{D_1, D_6, D_7, D_8, T_2\}_{SD}$
 (CE.3) $UE \models UE \triangleleft \{D_9, D_{11}, T_3\}_{D_{10}}$

Interpretation

- (PE.1) $GN \models GN \triangleleft \{D_1, D_3, D_4, D_5, T_1\}_{D_2}$
 $\rightarrow GN \models GN \triangleleft \{SID_j, ID_i, U_B, U_A, T_1\}_{D_2}$
 (PE.2) $MSN \models MSN \triangleleft \{D_1, D_6, D_7, D_8, T_2\}_{SD}$
 $\rightarrow MSN \models MSN \triangleleft \{D_1, SID_j, ID_i, T_2\}_{SD}$
 (PE.3) $UE \models UE \triangleleft \{D_9, D_{11}, T_3\}_{D_{10}}$
 $\rightarrow UE \models UE \triangleleft \{D_9, UE \xleftrightarrow{K} GN, T_3\}_{D_{10}}$

Assumption

- (AE.1) $GN \blacktriangleleft UE \xleftrightarrow{D_2} GN$
 (AE.2) $GN \models \#(T_1)$
 (AE.3) $GN \models UE \Rightarrow ID_i$
 (AE.4) $MSN \blacktriangleleft GN \xleftrightarrow{SD_j} MSN$
 (AE.5) $MSN \models \#(T_2)$

- (AE.6) $MSN \models GN \Rightarrow SID_j$
 (AE.7) $MSN \blacktriangleleft D_{10}$
 (AE.8) $UE \models UE \xleftrightarrow{D_{10}} MSN$
 (AE.9) $UE \models \#(T_3)$
 (AE.10) $UE \models MSN \Rightarrow D_9$
 (AE.11) $UE \blacktriangleleft ID_i$
 (AE.12) $UE \blacktriangleleft SID_i$
 (AE.13) $UE \blacktriangleleft D_1$
 (AE.14) $MSN \models UE \xleftrightarrow{K} GN$

Goal

- (GE.1) $GN \models U_A$
 (GE.2) $GN \models U_B$
 (GE.3) $MSN \models K$
 (GE.4) $MSN \models UE \xleftrightarrow{K} MSN$
 (GE.5) $UE \models K$
 (GE.6) $UE \models UE \xleftrightarrow{K} MSN$

Derivation

- (DE.1) $GN \models GN \triangleleft \{SID_j, ID_i, U_B, U_A, T_1\}_{D_2}$ *by Modusponens using (CE.1), (PE.1)*
 (DE.2) $GN \models UE \mid \sim (SID_j, ID_i, U_B, U_A, T_1)$ *by (DE.1), (AE.1), SAA, BA*
 (DE.3) $GN \models UE \mid \approx (SID_j, ID_i, U_B, U_A, T_1)$ *by (DE.2), (AE.2), FA, NV, BA*
 (DE.4) $GN \models (SID_j, ID_i, U_B, U_A, T_1)$ *by (DE.3), (AE.3), JR, BA*
 (DE.5) $GN \models U_A$ *by (DE.4), BA*
 (DE.6) $GN \models U_B$ *by (DE.4), BA*
 (DE.7) $MSN \models MSN \triangleleft \{D_1, SID_j, ID_i, T_2\}_{SD}$ *by Modusponens using (CE.2), (PE.2)*
 (DE.8) $MSN \models GN \mid \sim (D_1, SID_j, ID_i, T_2)$ *by (DE.7), (AE.4), SAA, BA*
 (DE.9) $MSN \models GN \mid \approx (D_1, SID_j, ID_i, T_2)$ *by (DE.8), (AE.5), FA, NV, BA*
 (DE.10) $MSN \models (D_1, SID_j, ID_i, T_2)$ *by (DE.9), (AE.6), JR, BA*
 (DE.11) $MSN \models K$
 where $K = H(H(ID_i \parallel SID_j \parallel D_1) \parallel D_{10})$ *by (DE.10), (AE.7), BA*
 (DE.12) $UE \models UE \triangleleft \{D_9, UE \xleftrightarrow{K} GN, T_3\}_{D_{10}}$ *by Modusponens using (CE.3), (PE.3)*
 (DE.13) $UE \models MSN \mid \sim (D_9, UE \xleftrightarrow{K} GN, T_3)$ *by (DE.12), (AE.8), SAA, BA*
 (DE.14) $UE \models MSN \mid \approx (D_9, UE \xleftrightarrow{K} GN, T_3)$ *by (DE.13), (AE.9), FA, NV, BA*
 (DE.15) $UE \models (D_9, UE \xleftrightarrow{K} GN, T_3)$ *by (DE.14), (AE.10), JR, BA*
 (DE.16) $UE \models K$
 where $K = H(H(ID_i \parallel SID_j \parallel D_1) \parallel D_{10})$ *by (AE.8), (AE.11), (AE.12), (AE.13), BA*
 (DE.17) $UE \models UE \xleftrightarrow{K} GN$ *by (DE.15), BA*

Appendix F. Formal Verification Result for Garg et al. [49]

Annotation

- (RF.1) $PS \triangleleft \{\$1, T_1\}_{RID_{IMD}}$
 (RF.2) $IMD \triangleleft \{\$2, \$3, T_2\}_{RID_{PS}}$
 (RF.3) $CS \triangleleft \{\$4, \$5, T_3\}_{RID_{TA}}$
 (RF.4) $PS \triangleleft (\$6, \$7, T_4)$
 (RF.5) $CS \triangleleft (\$8, T_5)$

Comprehension

- (CF.1) $PS \models PS \triangleleft \{\$1, T_1\}_{RID_{IMD}}$

$$(CF.2) \text{ } IMD \models IMD \triangleleft \{\$2, \$3, T_2\}_{RID_{PS}}$$

$$(CF.3) \text{ } CS \models CS \triangleleft \{\$4, \$5, T_3\}_{RID_{TA}}$$

$$(CF.4) \text{ } PS \models PS \triangleleft \{\$6, \$7, T_4\}_{RID_{TA}}$$

$$(CF.5) \text{ } CS \models CS \triangleleft \{\$8, T_5\}_{SK_2}$$

Interpretation

$$(PF.1) \text{ } PS \models PS \triangleleft \{\$1, T_1\}_{RID_{IMD}}$$

$$\rightarrow PS \models PS \triangleleft \{RID_{IMD}, T_1\}_{RID_{IMD}}$$

$$(PF.2) \text{ } IMD \models IMD \triangleleft \{\$2, \$3, T_2\}_{RID_{PS}}$$

$$\rightarrow IMD \models IMD \triangleleft \{RID_{PS}, H(SK||T_2), T_2\}_{RID_{PS}}$$

$$(PF.3) \text{ } CS \models CS \triangleleft \{\$4, \$5, T_3\}_{RID_{TA}}$$

$$\rightarrow CS \models CS \triangleleft \{H(r_1||TC_1) \oplus RID_{TA}, H(H(r_1||TC_1)||RID_{TA}||T_3), T_3\}_{RID_{TA}}$$

$$(PF.4) \text{ } PS \models PS \triangleleft \{\$6, \$7, T_4\}_{RID_{TA}}$$

$$\rightarrow PS \models PS \triangleleft \{H(r_2||RID_{CS}) \oplus RID_{TA}, H(SK_2||T_4), T_4\}_{RID_{TA}}$$

$$(PF.5) \text{ } CS \models CS \triangleleft \{\$8, T_5\}_{SK_2}$$

$$\rightarrow CS \models CS \triangleleft \{H(SK_2||T_5), T_5\}_{SK_2}$$

Assumption

$$(AF.1) \text{ } PS \blacktriangleleft PS \xleftrightarrow{RID_{IMD}} IMD$$

$$(AF.2) \text{ } PS \models \#(T_1)$$

$$(AF.3) \text{ } PS \models IMD \Rightarrow H(ID_{IMD}||N)$$

$$(AF.4) \text{ } PS \blacktriangleleft RID_{PS}$$

$$(AF.5) \text{ } IMD \blacktriangleleft IMD \xleftrightarrow{RID_{PS}} PS$$

$$(AF.6) \text{ } IMD \models \#(T_2)$$

$$(AF.7) \text{ } IMD \models PS \Rightarrow H(SK||T_2)$$

$$(AF.8) \text{ } IMD \blacktriangleleft T_1$$

$$(AF.9) \text{ } IMD \blacktriangleleft RID_{IMD}$$

$$(AF.10) \text{ } CS \models PS \xleftrightarrow{RID_{TA}} CS$$

$$(AF.11) \text{ } CS \models \#(T_3)$$

$$(AF.12) \text{ } CS \models PS \Rightarrow H(r_1||TC_1)$$

$$(AF.13) \text{ } CS \blacktriangleleft T_4$$

$$(AF.14) \text{ } CS \blacktriangleleft H(r_2||RID_{CS})$$

$$(AF.15) \text{ } PS \models PS \xleftrightarrow{RID_{TA}} CS$$

$$(AF.16) \text{ } PS \models \#(T_4)$$

$$(AF.17) \text{ } PS \models CS \Rightarrow H(SK_2||T_4)$$

$$(AF.18) \text{ } PS \blacktriangleleft RID_{TA}$$

$$(AF.19) \text{ } PS \blacktriangleleft T_3$$

$$(AF.20) \text{ } PS \blacktriangleleft H(r_1||TC_1)$$

$$(AF.21) \text{ } CS \models \#(T_5)$$

Goal

$$(GF.1) \text{ } PS \models SK$$

$$(GF.2) \text{ } IMD \models SK$$

$$(GF.3) \text{ } CS \models SK_2$$

$$(GF.4) \text{ } PS \models SK_2$$

$$(GF.6) \text{ } PS \models PS| \approx CS \xleftrightarrow{SK_2} PS$$

$$(GF.6) \text{ } CS \models PS| \approx CS \xleftrightarrow{SK_2} PS$$

Derivation

(DF.1) $PS \equiv PS \triangleleft \{RID_{IMD}, T_1\}_{RID_{IMD}}$	by Modusponens, (CF.1), (PF.1)
(DF.2) $PS \equiv IMD \mid \sim (RID_{IMD}, T_1)$	by (DF.1), (AF.1), SAA, BA
(DF.3) $PS \equiv IMD \mid \approx (RID_{IMD}, T_1)$	by (DF.2), (AF.2), FA, NV, BA
(DF.4) $PS \equiv (RID_{IMD}, T_1)$	by (DF.3), (AF.3), JR, BA
(DF.5) $PS \equiv SK$ where $SK = (H(RID_{PS}, RID_{IMD}), T_1)$	by (DF.4), (AF.1), (AF.4), BA
(DF.6) $IMD \equiv IMD \triangleleft \{RID_{PS}, H(SK \mid T_2), T_2\}_{RID_{PS}}$	by Modusponens using (CF.2), (PF.2)
(DF.7) $IMD \equiv PS \mid \sim (RID_{PS}, H(SK \mid T_2), T_2)$	by (DF.6), (AF.5), SAA, BA
(DF.8) $IMD \equiv PS \mid \approx (RID_{PS}, H(SK \mid T_2), T_2)$	by (DF.7), (AF.6), FA, NV, BA
(DF.9) $IMD \equiv (RID_{PS})$	by (DF.8), (AF.7), JR
(DF.10) $IMD \equiv SK$ where $SK = (H(RID_{PS}, RID_{IMD}), T_1)$	by (DF.9), (AF.8), (AF.9)
(DF.11) $CS \equiv CS \triangleleft \{H(r_1 \mid TC_1) \oplus RID_{TA}, H(H(r_1 \mid TC_1) \mid RID_{TA} \mid T_3), T_3\}_{RID_{TA}}$	by Modusponens using (CF.3), (PF.3)
(DF.12) $CS \equiv PS \mid \sim (H(r_1 \mid TC_1) \oplus RID_{TA}, H(H(r_1 \mid TC_1) \mid RID_{TA} \mid T_3), T_3)$	by (DF.11), (AF.10), SAA, BA
(DF.13) $CS \equiv PS \mid \approx (H(r_1 \mid TC_1) \oplus RID_{TA}, H(H(r_1 \mid TC_1) \mid RID_{TA} \mid T_3), T_3)$	by (DF.12), (AF.11), FA, NV, BA
(DF.14) $CS \equiv (H(r_1 \mid TC_1) \oplus RID_{TA}, H(H(r_1 \mid TC_1) \mid RID_{TA} \mid T_3), T_3)$	by (DF.13), (AF.12), JR, BA
(DF.15) $CS \equiv SK_2$ where $SK_2 = H(H(r_2 \mid RID_{CS}) \mid RID_{TA} \mid H(r_1 \mid TC_1) \mid T_3 \mid T_4)$	by (DF.14), (AF.13), (AF.14), BA
(DF.16) $PS \equiv PS \triangleleft \{H(r_2 \mid RID_{CS}) \oplus RID_{TA}, H(SK_2 \mid T_4), T_4\}_{RID_{TA}}$	by Modusponens using (CF.5), (PF.5)
(DF.17) $PS \equiv CS \mid \sim (H(r_2 \mid RID_{CS}) \oplus RID_{TA}, H(SK_2 \mid T_4), T_4)$	by (DF.16), (AF.15), SAA, BA
(DF.18) $PS \equiv CS \mid \approx (H(r_2 \mid RID_{CS}) \oplus RID_{TA}, H(SK_2 \mid T_4), T_4)$	by (DF.17), (AF.16), FA, NV, BA
(DF.19) $PS \equiv (H(r_2 \mid RID_{CS}) \oplus RID_{TA}, H(SK_2 \mid T_4), T_4)$	(DF.18), (AF.17), JR, BA
(DF.20) $PS \equiv SK_2$ where $SK_2 = H(H(r_2 \mid RID_{CS}) \mid RID_{TA} \mid H(r_1 \mid TC_1) \mid T_3 \mid T_4)$	by (DF.19), (AF.18), (AF.19), (AF.20), BA
(DF.21) $PS \equiv CS \xleftrightarrow{SK_2} PS$	
(DF.22) $CS \equiv CS \triangleleft \{H(SK_2 \mid T_5), T_5\}_{SK_2}$	by Modusponens using (CF.5), (PF.5)
(DF.23) $CS \equiv PS \mid \sim (CS \xleftrightarrow{SK_2} PS, T_5)$	by (DF.22), (DF.15), SAA, FA
(DF.24) $CS \equiv PS \mid \approx (CS \xleftrightarrow{SK_2} PS, T_5)$	by (DF.23), (AF.21), FA, NV, BA
(DF.25) $CS \equiv PS \mid \approx CS \xleftrightarrow{SK_2} PS$	by (DF.24), BA

Appendix G. Formal Verification Result for Pradhan et al. [50]

Annotation

- (RG.1) $FN \triangleleft \{U_{ID}, T_1, \{token_i\}_{PU_{FN}}\}_{PSK}$
 (RG.2) $U \triangleleft \{Y_6, T_2\}_{PSK}$
 (RG.3) $FN \triangleleft \{Y_5, X_3, T_1, T_1\}_{PSK}$

Comprehension

- (CG.1) $FN \equiv FN \triangleleft \{U_{ID}, T_1, \{token_i\}_{PU_{FN}}\}_{PSK}$
 (CG.2) $U \equiv U \triangleleft \{Y_6, T_2\}_{PSK}$
 (CG.3) $FN \equiv FN \triangleleft \{Y_5, X_3, T_1, T_1\}_{PSK}$

Interpretation

- (PG.1) $FN \equiv FN \triangleleft \{U_{ID}, T_1, Y_4\}_{PSK}$
 $\rightarrow FN \equiv FN \triangleleft \{U_{ID}, T_1, \{token_i\}_{PU_{FN}}\}_{PSK}$
 (PG.2) $U \equiv U \triangleleft \{Y_6, T_2\}_{PSK}$

$$\begin{aligned}
&\rightarrow U \models U \triangleleft \{U \xleftrightarrow{SK} FN, T_2\}_{PSK} \\
&(PG.3) FN \models FN \triangleleft \{Y_5, X_3, T_1\}_{PSK} \\
&\rightarrow FN \models FN \triangleleft \{ID_i, U \xleftrightarrow{SK} FN, T_1\}_{PSK}
\end{aligned}$$

Assumption

$$\begin{aligned}
&(AG.1) FN \blacktriangleleft U \xleftrightarrow{PSK} FN \\
&(AG.2) FN \models \#(T_1) \\
&(AG.3) FN \models U \Rightarrow U_{ID} \\
&(AG.4) FN \blacktriangleleft Y_3 \\
&(AG.5) FN \blacktriangleleft T_2 \\
&(AG.6) FN \blacktriangleleft \xrightarrow{PU_{FN}} FN \\
&(AG.7) U \blacktriangleleft U \xleftrightarrow{PSK} FN \\
&(AG.8) U \models \#(T_2) \\
&(AG.9) UE \blacktriangleleft Y_3
\end{aligned}$$

Goal

$$\begin{aligned}
&(GG.1) FN \models SK \\
&(GG.2) FN \models U \approx token_i \\
&(GG.3) U \models FN \approx U \xleftrightarrow{SK} FN \\
&(GG.4) UE \models SK \\
&(GG.5) FN \models U \approx U \xleftrightarrow{SK} FN
\end{aligned}$$

Derivation

(DG.1) $FN \models FN \triangleleft \{U_{ID}, T_1, \{token_i\}_{PU_{FN}}\}_{PSK}$	by Modusponens using (CG.1), (PG.1)
(DG.2) $FN \models U \sim (U_{ID}, T_1, \{token_i\}_{PU_{FN}})$	by (DG.1), (AG.1), SAA, BA
(DG.3) $FN \models U \approx (U_{ID}, T_1, \{token_i\}_{PU_{FN}})$	by (DG.2), (AG.2), FA, NV, BA
(DG.4) $FN \models U \approx (U_{ID}, T_1)$	by (DG.3) BA
(DG.5) $FN \models SK$	
where $SK = Y_3 T_2$	by (AG.4), (AG.5)
(DG.6) $FN \models U \approx \{token_i\}_{PU_{FN}}$	by (DG.3), BA
(DG.7) $FN \models U \approx token_i$	by (DG.6), (AG.6), SAA
(DG.8) $U \models U \triangleleft \{U \xleftrightarrow{SK} FN, T_2\}_{PSK}$	by Modusponens using (CG.2), (PG.2)
(DG.9) $U \models FN \sim (U \xleftrightarrow{SK} FN, T_2)$	by (DG.8) (AG.7), SAA, BA
(DG.10) $U \models FN \approx (U \xleftrightarrow{SK} FN, T_2)$	by (DG.9) (AG.8), FA, NV, BA
(DG.11) $U \models FN \approx U \xleftrightarrow{SK} FN$	by (DG.10) BA
(DG.12) $UE \models SK$	
where $SK = Y_3 T_2$	by (DG.10), (AG.9), BA
(DG.13) $FN \models FN \triangleleft \{ID_i, U \xleftrightarrow{SK} FN, T_1\}_{PSK}$	by Modusponens using (CG.3), (PG.3)
(DG.14) $FN \models FN \sim (ID_i, U \xleftrightarrow{SK} FN, T_1)$	by (DG.13), (AG.1), SAA, BA
(DG.15) $FN \models U \approx (ID_i, U \xleftrightarrow{SK} FN, T_1)$	by (DG.14), (AG.2), FA, NV, BA
(DG.16) $FN \models U \approx U \xleftrightarrow{SK} FN$	by (DG.15), BA

Appendix H. Formal Verification Result for Gautam et al. [51]

Annotation

$$\begin{aligned}
&(RH.1) GW \triangleleft \{B_2, R_a, T_1\}_{K_1} \\
&(RH.2) SN \triangleleft \{B_5, T_2\}_{SGK_{BC}} \\
&(RH.3) GW \triangleleft \{B_7, R_c, T_3\}_{K_2}
\end{aligned}$$

$$(RH.4) U \triangleleft \{B_8, T_4\}_{K_1}$$

Comprehension

$$(CH.1) GW \models GW \triangleleft \{B_2, R_a, T_1\}_{K_1}$$

$$(CH.2) SN \models SN \triangleleft \{B_5, T_2\}_{SGK_{BC}}$$

$$(CH.3) GW \models GW \triangleleft \{B_7, R_c, T_3\}_{K_2}$$

$$(CH.4) U \models U \triangleleft \{B_8, T_4\}_{K_1}$$

Interpretation

$$(PH.1) GW \models GW \triangleleft \{B_2, R_a, T_1\}_{K_1}$$

$$\rightarrow GW \models GW \triangleleft \{GW \xrightarrow{K_1} U, SID_a, SID_c, R_a, T_1\}_{K_1}$$

$$(PH.2) SN \models SN \triangleleft \{B_5, T_2\}_{SGK_{BC}}$$

$$\rightarrow SN \models SN \triangleleft \{GW \xrightarrow{SGK_{BC}} SN, B_3, R_b, T_2\}_{SGK_{BC}}$$

$$(PH.3) GW \models GW \triangleleft \{B_7, R_c, T_3\}_{K_2}$$

$$\rightarrow GW \models GW \triangleleft \{GW \xrightarrow{K_2} SN, r_c, SID_c, R_c, T_3\}_{K_2}$$

$$(PH.4) U \models U \triangleleft \{B_8, T_4\}_{K_1}$$

$$\rightarrow U \models U \triangleleft \{GW \xrightarrow{K_1} U, B_3, T_3, r_c, T_4\}_{K_1}$$

Assumption

$$(AH.1) GW \blacktriangleleft GW \xrightarrow{K_1} U$$

$$(AH.2) GW \models \#(T_1)$$

$$(AH.3) SN \blacktriangleleft GW \xrightarrow{SGK_{BC}} SN$$

$$(AH.4) SN \models \#(T_2)$$

$$(AH.5) SN \models GW \Rightarrow B_3$$

$$(AH.6) SN \blacktriangleleft GID_g$$

$$(AH.7) SN \blacktriangleleft SID_c$$

$$(AH.8) SN \blacktriangleleft K_2$$

$$(AH.9) SN \blacktriangleleft T_3$$

$$(AH.10) GW \blacktriangleleft GW \xrightarrow{K_2} SN$$

$$(AH.11) GW \models \#(T_3)$$

$$(AH.12) GW \blacktriangleleft GID_g$$

$$(AH.13) GW \blacktriangleleft B_3$$

$$(AH.14) U \blacktriangleleft GW \xrightarrow{K_1} U$$

$$(AH.15) U \models \#(T_4)$$

$$(AH.16) U \blacktriangleleft \xrightarrow{PU_{GW}} U$$

$$(AH.17) U \blacktriangleleft GID_g$$

$$(AH.18) U \blacktriangleleft SID_c$$

Goal

$$(GH.1) GW \models U \approx GW \xrightarrow{K_1} U$$

$$(GH.2) SN \models GN \approx GW \xrightarrow{SGK_{BC}} SN$$

$$(GH.3) SN \models SK$$

$$(GH.4) SN \models GW \approx GW \xrightarrow{SK} U$$

$$(GH.5) GW \models SN \approx GW \xrightarrow{K_2} SN$$

$$(GH.6) GW \models SK$$

$$(GH.7) U \models GW \approx GW \xrightarrow{K_1} U$$

$$(GH.8) U \models SK$$

$$(GH.9) U \models GW \approx GW \xrightarrow{SK} U$$

Derivation

(DH.1) $GW \models GW \triangleleft \{GW \xleftrightarrow{K_1} U, SID_a, SID_c, R_a, T_1\}_{K_1}$	by Modusponens using (CH.1), (PH.1)
(DH.2) $GW \models U \triangleleft (GW \xleftrightarrow{K_1} U, SID_a, SID_c, R_a, T_1)$	by (DH.1), (AH.1), SAA, BA
(DH.3) $GW \models U \approx (GW \xleftrightarrow{K_1} U, SID_a, SID_c, R_a, T_1)$	by (DH.2), (AH.2), FA, NV, BA
(DH.4) $GW \models U \approx GW \xleftrightarrow{K_1} U$	by (DH.3), BA
(DH.5) $SN \models SN \triangleleft \{GW \xleftrightarrow{SGK_{RC}} SN, B_3, R_b, T_2\}_{SGK_{BC}}$	by Modusponens using (CH.2), (PH.2)
(DH.6) $SN \models GN \sim (GW \xleftrightarrow{SGK_{RC}} SN, B_3, R_b, T_2)$	by (DH.5), (AH.3), SAA, BA
(DH.7) $SN \models GN \approx (GW \xleftrightarrow{SGK_{RC}} SN, B_3, R_b, T_2)$	by (DH.6), (AH.4), FA, NV, BA
(DH.8) $SN \models GN \approx GW \xleftrightarrow{SGK_{RC}} SN$	by (DH.7), BA
(DH.9) $SN \models B_3$	
(DH.10) $SN \models SK$	
where $SK = H(GID_g SID_c K_2 B_3 T_3)$	by (DH.9), (AH.6), (AH.7), (AH.8)
(DH.11) $GW \models GW \triangleleft \{GW \xleftrightarrow{K_2} SN, r_c, SID_c, R_c, T_3\}_{K_2}$	by Modusponens using (DH.3), (PH.3)
(DH.12) $GW \models SN \sim (GW \xleftrightarrow{K_2} SN, r_c, SID_c, R_c, T_3)$	by (DH.11), (AH.10), SAA, BA
(DH.13) $GW \models SN \approx (GW \xleftrightarrow{K_2} SN, r_c, SID_c, R_c, T_3)$	by (DH.12), (AH.11), FA, NV, BA
(DH.14) $GW \models SN \approx GW \xleftrightarrow{K_2} SN$	by (DH.13), BA
(DH.15) $GW \models SK$	
where $SK = H(GID_g SID_c K_2 B_3 T_3)$	by (DH.13), (AH.12), (AH.13), BA
(DH.16) $U \models U \triangleleft \{GW \xleftrightarrow{K_1} U, B_3, T_3, r_c, T_4\}_{K_1}$	by Modusponens using (CH.4), (PH.4)
(DH.17) $U \models GW \sim (GW \xleftrightarrow{K_1} U, B_3, T_3, r_c, T_4)$	by (DH.16), (AH.14), SAA, BA
(DH.18) $U \models GW \approx (GW \xleftrightarrow{K_1} U, B_3, T_3, r_c, T_4)$	by (DH.17), (AH.15), FA, NV, BA
(DH.19) $U \models GW \approx GW \xleftrightarrow{K_1} U$	by (DH.19), BA
(DH.20) $U \models K_2$	
where $K_2 = R_c \cdot PU_{GW}$	by (DH.18), (AH.16), BA
(DH.21) $U \models SK$	
where $SK = H(GID_g SID_c K_2 B_3 T_3)$	by (DH.18), (DH.20), (AH.17), (AH.18), BA

Appendix I. Formal Verification Result for Su et al. [53]**Annotation**

- (RI.1) $GW \triangleleft \{RID_i, n_1, T_1\}_{K_1}$
 (RI.2) $SD \triangleleft \{B, n_1, T_2\}_{K_2}$
 (RI.3) $U \triangleleft \{C, n_2, RSID_j, T_3\}_{K_3}$

Comprehension

- (CI.1) $GW \models GW \triangleleft \{RID_i, n_1, T_1\}_{K_1}$
 (CI.2) $SD \models SD \triangleleft \{B, n_1, T_2\}_{K_2}$
 (CI.3) $U \models U \triangleleft \{C, n_2, RSID_j, T_3\}_{K_3}$

Interpretation

- (PI.1) $GW \models GW \triangleleft \{RID_i, n_1, T_1\}_{K_1}$
 $\rightarrow GW \models GW \triangleleft \{U \xleftrightarrow{RID_i} GW, n_1, T_1\}_{K_1}$
 (PI.2) $SD \models SD \triangleleft \{B, n_1, T_2\}_{K_2}$
 $\rightarrow SD \models SD \triangleleft \{GW \xleftrightarrow{b} SD, n_1, T_2\}_{K_2}$
 (PI.3) $U \models U \triangleleft \{C, n_2, RSID_j, T_3\}_{K_3}$
 $\rightarrow U \models U \triangleleft \{U \xleftrightarrow{C} SD, n_2, RSID_j, T_3\}_{K_3}$

Assumption

- (AI.1) $GW \blacktriangleleft U \xleftrightarrow{K_1} GW$
 (AI.2) $GW \models \#(T_1)$
 (AI.3) $GW \models U \Rightarrow U \xleftrightarrow{RID_i} GW$
 (AI.4) $SD \blacktriangleleft GW \xleftrightarrow{K_{GW}} SD$
 (AI.5) $SD \models \#(T_2)$
 (AI.6) $SD \models GW \Rightarrow GW \xleftrightarrow{B} SD$
 (AI.7) $SD \blacktriangleleft n_2$
 (AI.8) $SD \blacktriangleleft C$
 (AI.9) $SD \blacktriangleleft RSID_j$
 (AI.10) $SD \blacktriangleleft T_3$
 (AI.12) $U \blacktriangleleft U \xleftrightarrow{K_2} SD$
 (AI.13) $U \models \#(T_3)$
 (AI.14) $U \models USD \Rightarrow U \xleftrightarrow{C} SD$
 (AI.15) $U \blacktriangleleft n_1$

Goal

- (GI.1) $GW \models U \xleftrightarrow{RID_i} GW$
 (GI.1) $SD \models SK$
 (GI.2) $SD \models SK \xleftrightarrow{SK} U$
 (GI.3) $U \models SK$
 (GI.4) $U \models SK \xleftrightarrow{SK} U$

Derivation

- | | |
|--|--|
| (DI.1) $GW \models GW \triangleleft \{U \xleftrightarrow{RID_i} GW, n_1, T_1\}_{K_1}$ | by Modusponens using (CI.1), (PI.1) |
| (DI.2) $GW \models U \sim (U \xleftrightarrow{RID_i} GW, n_1, T_1)$ | by (DI.1), (AI.1), SAA, BA |
| (DI.3) $GW \models U \approx (U \xleftrightarrow{RID_i} GW, n_1, T_1)$ | by (DI.2), (AI.2), FA, NV, BA |
| (DI.4) $GW \models U \approx U \xleftrightarrow{RID_i} GW$ | by (DI.3), BA |
| (DI.5) $GW \models U \xleftrightarrow{RID_i} GW$ | by (DI.4), (AI.3), JR |
| (DI.6) $SD \models SD \triangleleft \{GW \xleftrightarrow{b} SD, n_1, T_2\}_{K_2}$ | by Modusponens using (CI.2), (PI.2) |
| (DI.7) $SD \models GW \sim (GW \xleftrightarrow{b} SD, n_1, T_2)$ | by (DI.6), (AI.4), SAA, BA |
| (DI.8) $SD \models GW \approx (GW \xleftrightarrow{b} SD, n_1, T_2)$ | by (DI.7), (AI.5), FA, NV, BA |
| (DI.9) $SD \models (GW \xleftrightarrow{b} SD, n_1, T_2)$ | by (DI.8), (AI.6), JR, BA |
| (DI.10) $SD \models SK$ | |
| where $SK = H(n_1 n_2 RISD_j C T_3)$ | by (DI.9), (AI.7), (AI.8), (AI.9), (AI.10), BA |
| (DI.11) $U \models U \triangleleft \{U \xleftrightarrow{C} SD, n_2, RSID_j, T_3\}_{K_3}$ | by Modusponens using (CI.3), (PI.3) |
| (DI.12) $U \models SD \sim (U \xleftrightarrow{C} SD, n_2, RSID_j, T_3)$ | by (DI.11), (AI.12), SAA, BA |
| (DI.13) $U \models SD \approx (U \xleftrightarrow{C} SD, n_2, RSID_j, T_3)$ | by (DI.12), (AI.13), FA, NV, BA |
| (DI.14) $U \models (U \xleftrightarrow{C} SD, n_2, RSID_j, T_3)$ | by (DI.13), (AI.14), JR, BA |
| (DI.15) $U \models SK$ | |
| where $SK = H(n_1 n_2 RISD_j C T_3)$ | by (DI.14), (AI.15), BA |

Appendix J. Formal Verification Result for Deebak et al. [54]

Annotation

- (RJ.1) $AG \triangleleft \{n_1, M_s, PID, S_{KEY}\}_K$
 (RJ.2) $ME \triangleleft \{n_2, n_3, TP_1^{NEW}, TID_i^{mew}, S_{KEY}\}_K$

Comprehension

$$(CJ.1) AG \models AG \triangleleft \{n_1, M_s, PID, S_{KEY}\}_K$$

$$(CJ.2) ME \models ME \triangleleft \{n_2, n_3, TP_1^{NEW}, TID_i^{NEW}, S_{KEY}\}_K$$

Interpretation

$$(PJ.1) AG \models AG \triangleleft \{n_1, M_s, PID, S_{KEY}\}_K$$

$$\rightarrow AG \models AG \triangleleft \{n_1, M_s, PID, ME \xleftrightarrow{S_{KEY}} AG\}_K$$

$$(PJ.2) ME \models ME \triangleleft \{n_2, n_3, TP_1^{NEW}, TID_i^{NEW}, S_{KEY}\}_K$$

$$\rightarrow ME \models ME \triangleleft \{n_2, n_3, TP_1^{NEW}, TID_i^{NEW}, ME \xleftrightarrow{S_{KEY}} AG\}_K$$

Assumption

$$(AJ.1) AG \models AG \xleftrightarrow{K} ME$$

$$(AJ.2) AG \models ME \Rightarrow n_1$$

$$(AJ.3) AG \blacktriangleleft (n_2)$$

$$(AJ.4) AG \blacktriangleleft (n_3)$$

$$(AJ.5) ME \models AG \xleftrightarrow{K} ME$$

$$(AJ.6) ME \models \#(TID_i^{NEW})$$

$$(AJ.7) ME \models AG \Rightarrow TP_1^{NEW}$$

$$(AJ.8) ME \blacktriangleleft n_1$$

$$(AJ.9) ME \blacktriangleleft M_s$$

$$(HJ.1) AG \models \#(n_1)$$

Goal

$$(GJ.1) AG \models ME \xleftrightarrow{S_{KEY}} AG$$

$$(GJ.2) AG \models SK$$

$$(GJ.3) AG \models ME \xleftrightarrow{SK} AG$$

$$(GJ.4) ME \models ME \xleftrightarrow{S_{KEY}} AG$$

$$(GJ.5) ME \models SK$$

$$(GJ.6) ME \models ME \xleftrightarrow{SK} AG$$

Derivation

$$(DJ.1) AG \models AG \triangleleft \{n_1, M_s, PID, ME \xleftrightarrow{S_{KEY}} AG\}_K$$

by Modusponens using (CJ.1), (PJ.1)

$$(DJ.2) AG \models ME \mid \sim (n_1, M_s, PID, ME \xleftrightarrow{S_{KEY}} AG)$$

by (DJ.1), (AJ.1), SAA, BA

$$(DJ.3) AG \models ME \mid \approx (n_1, M_s, PID, ME \xleftrightarrow{S_{KEY}} AG)$$

by (DJ.2), (HJ.1), FA, NV, BA

$$(DJ.4) AG \models (n_1, M_s, PID, ME \xleftrightarrow{S_{KEY}} AG)$$

by (DJ.3), (AJ.2), JR, BA

$$(DJ.5) AG \models ME \xleftrightarrow{S_{KEY}} AG$$

by (DJ.4), BA

$$(DJ.6) AG \models SK$$

$$\text{where } SK = H(M_s \parallel n_1 \parallel n_2 \parallel n_3 \parallel S_{KEY})$$

by (DJ.4), (DJ.5), (AJ.3), (AJ.4), BA

$$(DJ.7) ME \models ME \triangleleft \{n_2, n_3, TP_1^{NEW}, TID_i^{NEW}, ME \xleftrightarrow{S_{KEY}} AG\}_K$$

by Modusponens using (CJ.2), (PJ.2)

$$(DJ.8) ME \models AG \mid \sim (n_2, n_3, TP_1^{NEW}, TID_i^{NEW}, ME \xleftrightarrow{S_{KEY}} AG)$$

by (DJ.7), (AJ.5), SAA, BA

$$(DJ.9) ME \models AG \mid \approx (n_2, n_3, TP_1^{NEW}, TID_i^{NEW}, ME \xleftrightarrow{S_{KEY}} AG)$$

by (DJ.8), (AJ.6), FA, NV, BA

$$(DJ.10) ME \models (n_2, n_3, TP_1^{NEW}, TID_i^{NEW}, ME \xleftrightarrow{S_{KEY}} AG)$$

by (DJ.9), (AJ.7), JR, BA

$$(DJ.11) ME \models ME \xleftrightarrow{S_{KEY}} AG$$

by (DJ.10), BA

$$(DJ.12) ME \models SK$$

$$\text{where } SK = H(M_s \parallel n_1 \parallel n_2 \parallel n_3 \parallel S_{KEY})$$

by (DJ.12), (AJ.8), (AJ.9), BA

References

- Jain, S.; Nehra, M.; Kumar, R.; Dilbaghi, N.; Hu, T.; Kumar, S.; Kaushik, A.; Li, C.Z. Internet of medical things (IoMT)-integrated biosensors for point-of-care testing of infectious diseases. *Biosens. Bioelectron.* **2021**, *179*, 113074. [[CrossRef](#)] [[PubMed](#)]
- Xenofontos, C.; Zografopoulos, I.; Konstantinou, C.; Jolfaei, A.; Khan, M.K.; Choo, K.K.R. Consumer, commercial, and industrial iot (in) security: Attack taxonomy and case studies. *IEEE Internet Things J.* **2021**, *9*, 199–221. [[CrossRef](#)]
- Mejía-Granda, C.M.; Fernández-Alemán, J.L.; Carrillo-de Gea, J.M.; García-Berná, J.A. Security vulnerabilities in healthcare: An analysis of medical devices and software. *Med Biol. Eng. Comput.* **2024**, *62*, 257–273. [[CrossRef](#)]
- He, P.; Huang, D.; Wu, D.; He, H.; Wei, Y.; Cui, Y.; Wang, R.; Peng, L. A survey of internet of medical things: Technology, application and future directions. *Digit. Commun. Netw.* **2024**, *in press*. [[CrossRef](#)]
- Shivagangatharani, B.; Rabiya, M.S. Enabling Technologies in IoMT Smart Healthcare: A Survey. In Proceedings of the 2024 10th International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 12–14 April 2024; pp. 665–670.
- Gkonis, P.; Giannopoulos, A.; Trakadas, P.; Masip-Bruin, X.; D’Andria, F. A survey on IoT-edge-cloud continuum systems: Status, challenges, use cases, and open issues. *Future Internet* **2023**, *15*, 383. [[CrossRef](#)]
- Osama, M.; Ateya, A.A.; Sayed, M.S.; Hammad, M.; Pławiak, P.; Abd El-Latif, A.A.; Elsayed, R.A. Internet of medical things and healthcare 4.0: Trends, requirements, challenges, and research directions. *Sensors* **2023**, *23*, 7435. [[CrossRef](#)]
- Abbas, T.; Khan, A.H.; Kanwal, K.; Daud, A.; Irfan, M.; Bukhari, A.; Alharbey, R. IoMT-Based Healthcare Systems: A Review. *Comput. Syst. Sci. Eng.* **2024**, *48*, 871–895. [[CrossRef](#)]
- Sindhuja, R. A survey of Internet of Medical Things (IoMT) applications, architectures and challenges in smart healthcare systems. In Proceedings of the 1st ITM Web of Conferences, Coimbatore, India, 23–24 June 2023; EDP Sciences: Les Ulis, France, 2023; Volume 56, p. 05013.
- Lu, T.; Ji, S.; Jin, W.; Yang, Q.; Luo, Q.; Ren, T.L. Biocompatible and long-term monitoring strategies of wearable, ingestible and implantable biosensors: Reform the next generation healthcare. *Sensors* **2023**, *23*, 2991. [[CrossRef](#)]
- Guo, Y.; Liu, X.; Peng, S.; Jiang, X.; Xu, K.; Chen, C.; Wang, Z.; Dai, C.; Chen, W. A review of wearable and unobtrusive sensing technologies for chronic disease management. *Comput. Biol. Med.* **2021**, *129*, 104163. [[CrossRef](#)] [[PubMed](#)]
- Özkartal, T.; Demarchi, A.; Caputo, M.L.; Baldi, E.; Conte, G.; Auricchio, A. Perioperative management of patients with cardiac implantable electronic devices and utility of magnet application. *J. Clin. Med.* **2022**, *11*, 691. [[CrossRef](#)] [[PubMed](#)]
- Varshney, A.S.; DeFilippis, E.M.; Cowger, J.A.; Netuka, I.; Pinney, S.P.; Givertz, M.M. Trends and outcomes of left ventricular assist device therapy: JACC focus seminar. *J. Am. Coll. Cardiol.* **2022**, *79*, 1092–1107. [[CrossRef](#)] [[PubMed](#)]
- Wu, Y.C.; Liao, Y.S.; Yeh, W.H.; Liang, S.F.; Shaw, F.Z. Directions of deep brain stimulation for epilepsy and Parkinson’s disease. *Front. Neurosci.* **2021**, *15*, 680938. [[CrossRef](#)] [[PubMed](#)]
- Lam, C.M.; Latif, U.; Sack, A.; Govindan, S.; Sanderson, M.; Vu, D.T.; Smith, G.; Sayed, D.; Khan, T. Advances in spinal cord stimulation. *Bioengineering* **2023**, *10*, 185. [[CrossRef](#)] [[PubMed](#)]
- Wang, C.; Wu, B.; Lin, R.; Cheng, Y.; Huang, J.; Chen, Y.; Bai, J. Vagus nerve stimulation: A physical therapy with promising potential for central nervous system disorders. *Front. Neurol.* **2024**, *15*, 1516242. [[CrossRef](#)]
- Ahmed, A.; Taj, I.; Farhan, K.; Tariq, B.; Raufi, N. Revolutionizing diabetes care: New insulin pump and algorithm-based software for automatic insulin delivery. *IJS Glob. Health* **2024**, *7*, e0431. [[CrossRef](#)]
- Schaepelynck, P.; Renard, E.; Jeandidier, N.; Hanaire, H.; Fermon, C.; Rudoni, S.; Catargi, B.; Riveline, J.P.; Guerci, B.; Millot, L.; et al. A recent survey confirms the efficacy and the safety of implanted insulin pumps during long-term use in poorly controlled type 1 diabetes patients. *Diabetes Technol. Ther.* **2011**, *13*, 657–660. [[CrossRef](#)]
- Tchoe, H.J.; Shin, H.W.; Shin, C.M.; Lim, C.M. Assisted breathing with a diaphragm pacing system: A systematic review. *Yonsei Med. J.* **2020**, *61*, 1024.
- Islam, A.S.; Pingree, G.; Chafin, A.; Fitzpatrick IV, T.H.; Nord, R.S. Respiratory sensing lead malfunction in upper airway stimulation: A single institution report. *Laryngoscope* **2024**, *134*, 1479–1484. [[CrossRef](#)]
- Kim, H.; Ahn, J.; Rhee, J.; Ahn, S. Application of wireless power transfer technology to implantable medical devices. In Proceedings of the 2022 IEEE MTT-S International Microwave Biomedical Conference (IMBioC), Suzhou, China, 16–18 May 2022; pp. 299–301.
- Catuogno, L.; Galdi, C. Implantable Medical Device Security. *Cryptography* **2024**, *8*, 53. [[CrossRef](#)]
- Köhler, C.; Bartschke, A.; Fürstenau, D.; Schaaf, T.; Salgado-Baez, E. The Value of Smartwatches in the Health Care Sector for Monitoring, Nudging, and Predicting: Viewpoint on 25 Years of Research. *J. Med. Internet Res.* **2024**, *26*, e58936. [[CrossRef](#)]
- Perez-Guzman, M.C.; Shang, T.; Zhang, J.Y.; Jornsay, D.; Klonoff, D.C. Continuous glucose monitoring in the hospital. *Endocrinol. Metab.* **2021**, *36*, 240–255. [[CrossRef](#)]
- Liu, W.; Zhang, J.; Li, C. Design of intelligent wearable equipment based on real-time dynamic ECG-monitoring system. *Am. J. Transl. Res.* **2023**, *15*, 6413.

26. Wong, S.H.D.; Deen, G.R.; Bates, J.S.; Maiti, C.; Lam, C.Y.K.; Pachauri, A.; AlAnsari, R.; Bělský, P.; Yoon, J.; Dodda, J.M. Smart skin-adhesive patches: From design to biomedical applications. *Adv. Funct. Mater.* **2023**, *33*, 2213560. [\[CrossRef\]](#)
27. Zhang, J.; Li, J.; Huang, Z.; Huang, D.; Yu, H.; Li, Z. Recent progress in wearable brain-computer interface (BCI) devices based on electroencephalogram (EEG) for medical applications: A review. *Health Data Sci.* **2023**, *3*, 0096. [\[CrossRef\]](#)
28. Huang, M.; Peng, Q.; Zhu, X.; Deng, T.; Cao, R.; Liu, W. Ensuring Trustworthy and Secure IoT: Fundamentals, Threats, Solutions, and Future Hotspots. *Comput. Netw.* **2025**, *263*, 111218. [\[CrossRef\]](#)
29. Lombardi, M.; Pascale, F.; Santaniello, D. Internet of things: A general overview between architectures, protocols and applications. *Information* **2021**, *12*, 87. [\[CrossRef\]](#)
30. Mrabet, H.; Belguith, S.; Alhomoud, A.; Jemai, A. A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors* **2020**, *20*, 3625. [\[CrossRef\]](#) [\[PubMed\]](#)
31. Calderón, D.; Folgado, F.J.; González, I.; Calderón, A.J. Implementation and experimental application of industrial IoT architecture using automation and IoT Hardware/Software. *Sensors* **2024**, *24*, 8074. [\[CrossRef\]](#)
32. Koulouras, G.; Katsoulis, S.; Zantalis, F. Evolution of Bluetooth Technology: BLE in the IoT Ecosystem. *Sensors* **2025**, *25*, 996. [\[CrossRef\]](#)
33. Zohourian, A.; Dadkhah, S.; Neto, E.C.P.; Mahdikhani, H.; Danso, P.K.; Molyneaux, H.; Ghorbani, A.A. IoT Zigbee device security: A comprehensive review. *Internet Things* **2023**, *22*, 100791. [\[CrossRef\]](#)
34. Devi, D.H.; Duraisamy, K.; Armghan, A.; Alsharari, M.; Aliqab, K.; Sorathiya, V.; Das, S.; Rashid, N. 5G technology in healthcare and wearable devices: A review. *Sensors* **2023**, *23*, 2519. [\[CrossRef\]](#) [\[PubMed\]](#)
35. Alshammari, H.H. The internet of things healthcare monitoring system based on MQTT protocol. *Alex. Eng. J.* **2023**, *69*, 275–287. [\[CrossRef\]](#)
36. Bormann, C.; Castellani, A.P.; Shelby, Z. Coap: An application protocol for billions of tiny internet nodes. *IEEE Internet Comput.* **2012**, *16*, 62–67. [\[CrossRef\]](#)
37. Saripalle, R.; Runyan, C.; Russell, M. Using HL7 FHIR to achieve interoperability in patient health record. *J. Biomed. Inform.* **2019**, *94*, 103188. [\[CrossRef\]](#)
38. Askar, N.A.; Habbal, A.; Mohammed, A.H.; Sajat, M.S.; Yusupov, Z.; Kodirov, D. Architecture, protocols, and applications of the internet of medical things (IoMT). *J. Commun.* **2022**, *17*, 900–918. [\[CrossRef\]](#)
39. Razdan, S.; Sharma, S. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE Tech. Rev.* **2022**, *39*, 775–788. [\[CrossRef\]](#)
40. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of medical things security assessment framework. *Internet Things* **2019**, *8*, 100123. [\[CrossRef\]](#)
41. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet Things J.* **2020**, *8*, 8707–8718. [\[CrossRef\]](#)
42. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of security and privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 457–464.
43. Bhushan, B.; Kumar, A.; Agarwal, A.K.; Kumar, A.; Bhattacharya, P.; Kumar, A. Towards a secure and sustainable internet of medical things (iomt): Requirements, design challenges, security techniques, and future trends. *Sustainability* **2023**, *15*, 6177. [\[CrossRef\]](#)
44. Abdussami, M.; Amin, R.; Vollala, S. Provably secured lightweight authenticated key agreement protocol for modern health industry. *Ad Hoc Netw.* **2023**, *141*, 103094. [\[CrossRef\]](#)
45. Qiu, S.; Li, J.; Di, X.; Li, X.; Wu, Y.; Ibrahim, M. Lightweight mutual authentication scheme based on blockchain for the Internet of Medical Things. *IEEE Internet Things J.* **2024**, *12*, 8848–8861. [\[CrossRef\]](#)
46. Lo, C.K.M.; Tan, S.F.; Chung, G.C. Enhanced Authentication Protocol for Securing Internet of Medical Things with Lightweight Post-Quantum Cryptography. In Proceedings of the 2024 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAET), Kota Kinabalu, Malaysia, 26–28 August 2024; pp. 625–630.
47. Masud, M.; Gaba, G.S.; Alqahtani, S.; Muhammad, G.; Gupta, B.B.; Kumar, P.; Ghoneim, A. A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care. *IEEE Internet Things J.* **2020**, *8*, 15694–15703. [\[CrossRef\]](#) [\[PubMed\]](#)
48. Miao, J.; Wang, Z.; Wu, Z.; Ning, X.; Tiwari, P. A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. *Expert Syst. Appl.* **2024**, *237*, 121329. [\[CrossRef\]](#)
49. Garg, N.; Wazid, M.; Das, A.K.; Singh, D.P.; Rodrigues, J.J.; Park, Y. BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment. *IEEE Access* **2020**, *8*, 95956–95977. [\[CrossRef\]](#)
50. Pradhan, M.; Mohanty, S. A blockchain-assisted multifactor authentication protocol for enhancing IoMT security. *IEEE Internet Things J.* **2024**, *11*, 39323–39332. [\[CrossRef\]](#)

51. Gautam, D.; Thakur, G.; Obaidat, M.S.; Hsiao, K.F.; Kumar, P. Security Analysis and Improvement of Authenticated Key Agreement Protocol for Remote Patient Monitoring IoMT. In Proceedings of the 2024 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), Beijing, China, 16–18 October 2024; pp. 1–8.
52. Chen, C.M.; Liu, S.; Li, X.; Islam, S.H.; Das, A.K. A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT. *J. Syst. Archit.* **2023**, *136*, 102831. [[CrossRef](#)]
53. Su, X.; Xu, Y. Secure and Lightweight Cluster-Based User Authentication Protocol for IoMT Deployment. *Sensors* **2024**, *24*, 7119. [[CrossRef](#)]
54. Deebak, B.; Hwang, S.O. Federated learning-based lightweight two-factor authentication framework with privacy preservation for mobile sink in the social IOMT. *Electronics* **2023**, *12*, 1250. [[CrossRef](#)]
55. ISO/IEC 29128-1:2023; Information Security, Cybersecurity and Privacy Protection—Verification of Cryptographic Protocols—Part 1: Framework. International standard; International Organization for Standardization: Geneva, Switzerland, 2023.
56. Syverson, P.F.; Van Oorschot, P.C. On unifying some cryptographic protocol logics. In Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, CA, USA, 16–18 May 1994; pp. 14–28.
57. Cremers, C.J. The scyther tool: Verification, falsification, and analysis of security protocols: Tool paper. In *Computer Aided Verification, Proceedings of the 20th International Conference on Computer Aided Verification, Princeton, NJ, USA, 7–14 July 2008*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 414–418.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.