INTERNATIONAL JOURNAL OF NETWORKS AND SECURITY (ISSN: 2693-387X)
Volume 03, Issue 01, 2023
Published Date: - 07-07-2023 Page no:- 1-5

GUARDING MOBILITY: A COMPOSABLE AUTHENTICATION PROTOCOL FOR SECURE ROAMING IN CLOUD-ASSISTED BODY SENSOR NETWORKS

Shun-Chen Wang
Department of Information Engineering and Computer Science, Feng Chia University, Wenhwa Rd., Seatwen, Taichung, Taiwan

Abstract

The proliferation of Body Sensor Networks (BSNs) has revolutionized healthcare monitoring, but it also introduces security challenges, particularly in roaming scenarios. This article presents a novel Composable Authentication Protocol (CAP) designed to ensure secure roaming in Cloud-assisted Body Sensor Networks. CAP leverages a dynamic, context-aware approach to authentication, adapting to diverse environments and scenarios while guaranteeing data privacy and integrity. We explore CAP's architecture and demonstrate its effectiveness in safeguarding BSNs during roaming, thereby enhancing the security and reliability of healthcare monitoring.

Key Words

Body Sensor Networks (BSNs); Secure roaming; Authentication protocol; Cloud-assisted BSNs; Healthcare monitoring; Data privacy; Data integrity.

INTRODUCTION

The advent of Body Sensor Networks (BSNs) has brought about a transformative paradigm in healthcare monitoring, enabling continuous and real-time tracking of vital physiological parameters. BSNs, composed of wearable and implantable sensors, have the potential to revolutionize patient care, disease management, and wellness monitoring. However, this remarkable innovation is not without its challenges, particularly in scenarios where mobility and seamless data transmission are essential.

Roaming scenarios in BSNs, such as a patient moving between different areas of a hospital or between home and a healthcare facility, present unique security challenges. Ensuring the privacy and integrity of sensitive healthcare data during these transitions is paramount. To address this concern, we introduce a novel Composable Authentication Protocol (CAP) tailored explicitly for secure roaming in Cloud-assisted Body Sensor Networks.

CAP is designed to provide robust security while accommodating the inherent mobility of BSNs. It takes a dynamic, context-aware approach to authentication, adapting to the changing environments and scenarios that characterize healthcare monitoring. This authentication protocol not only guarantees data privacy and integrity but also enhances the overall security and reliability of BSNs during roaming, contributing significantly to the advancement of healthcare monitoring systems.

In the following sections, we delve into the architecture and workings of CAP, exploring how this innovative approach to authentication can safeguard the mobility of BSNs, maintain data confidentiality, and ensure the trustworthiness of healthcare data in an increasingly interconnected

healthcare ecosystem. As healthcare monitoring evolves, CAP stands as a steadfast guardian, committed to preserving the privacy and security of patients' health data, ultimately empowering the promise of seamless and secure healthcare delivery.

METHOD

In the realm of modern healthcare, Body Sensor Networks (BSNs) have emerged as a transformative force, heralding a new era of patient care and health monitoring. BSNs, comprised of wearable and implantable sensors, offer unparalleled insights into patients' physiological data, enabling real-time monitoring and timely interventions. However, the mobility inherent to healthcare scenarios, where patients move between various environments and healthcare facilities, introduces a complex challenge—how to maintain the security and privacy of sensitive health data during these transitions.

Roaming scenarios in BSNs require robust security mechanisms to ensure the confidentiality and integrity of healthcare data as it traverses diverse network environments. To address this critical concern, we present the Composable Authentication Protocol (CAP), a pioneering solution tailored explicitly for secure roaming in Cloud-assisted Body Sensor Networks. CAP is designed to provide not only strong security safeguards but also the flexibility to adapt to the dynamic nature of healthcare monitoring scenarios.

What sets CAP apart is its dynamic, context-aware approach to authentication. It takes into account the shifting landscapes of healthcare, where patients move seamlessly between different areas of a hospital, their homes, or even different healthcare facilities. CAP not only guarantees the privacy and integrity of healthcare data but also enhances the overall security and reliability of BSNs during roaming. This innovative authentication protocol aims to be a cornerstone in the foundation of secure healthcare monitoring systems, where patient data remains confidential, unaltered, and secure, no matter where they are within the healthcare ecosystem.

As we delve deeper into the architecture and functionality of CAP, we will explore how this protocol can empower healthcare providers and institutions to embrace the promise of interconnected healthcare delivery. CAP stands as a guardian of mobility, ensuring that patients' health data remains protected as they move through the intricate web of healthcare environments. In an era where health monitoring is increasingly intertwined with technology and connectivity, CAP is poised to play a pivotal role in securing the future of healthcare.

Protocol Architecture Design: The development of the Composable Authentication Protocol (CAP) began with the meticulous design of its architecture. CAP's architecture was crafted to accommodate the dynamic and context-aware authentication requirements of Cloud-assisted Body Sensor Networks (BSNs) during roaming scenarios. It incorporates layers of security measures to ensure the privacy and integrity of healthcare data.

Context-aware Authentication Logic: CAP's core authentication logic is inherently context-aware. It takes into consideration various parameters and contextual information, such as the patient's location, the healthcare facility's network infrastructure, and the type of data being transmitted. This context-awareness enables CAP to adapt its authentication mechanisms dynamically, ensuring that the appropriate level of security is applied in different scenarios.

Dynamic Key Management: One of CAP's key features is its dynamic key management system. It generates and manages encryption keys in real-time, which are used to secure data transmission during roaming. These keys are dynamically adjusted based on the context, ensuring that only authorized entities can access and decrypt healthcare data.

Multi-factor Authentication: CAP incorporates multi-factor authentication mechanisms to bolster security during roaming. This includes a combination of factors such as user credentials, device authentication, and contextual information. These multiple layers of authentication add resilience to the protocol, making it more challenging for unauthorized entities to breach the security perimeter.

Data Encryption and Secure Channels: CAP employs state-of-the-art encryption techniques to secure healthcare data during transmission. It establishes secure communication channels between BSN devices and cloud servers, ensuring that data remains confidential and protected against eavesdropping or tampering.

Continuous Monitoring and Adaptation: CAP continually monitors the network environment and the context in which healthcare data is transmitted. If it detects anomalies or deviations from the expected context, it can trigger adaptive security measures, such as re-authentication or increased encryption strength, to mitigate potential security risks.

In the subsequent sections, we will explore how CAP's innovative approach to authentication enhances the security of Cloud-assisted Body Sensor Networks during roaming scenarios. By combining context-awareness, dynamic key management, and multi-factor authentication, CAP stands as a robust guardian of mobility in healthcare, ensuring that sensitive health data remains confidential and secure in an increasingly interconnected healthcare landscape.

RESULTS

The implementation of the Composable Authentication Protocol (CAP) in Cloud-assisted Body Sensor Networks (BSNs) has yielded promising results in enhancing the security and privacy of healthcare data during roaming scenarios:

Enhanced Security: CAP's dynamic, context-aware authentication logic has significantly bolstered the security of data transmissions within BSNs. By adapting authentication mechanisms to the specific context of roaming scenarios, CAP effectively mitigates potential security vulnerabilities that could arise during transitions between different network environments.

Robust Data Privacy: CAP's dynamic key management and encryption mechanisms have ensured the confidentiality and integrity of healthcare data during transmission. These security measures have been instrumental in safeguarding patient privacy and protecting sensitive health information from unauthorized access or tampering.

Adaptive Security: CAP's ability to continuously monitor the network environment and adapt security measures in real-time has proven invaluable. It responds swiftly to anomalies or deviations from expected context, ensuring that security remains uncompromised even in dynamic healthcare scenarios.

DISCUSSION

The deployment of CAP in Cloud-assisted BSNs marks a significant step forward in addressing the security challenges posed by roaming scenarios. The protocol's context-aware

authentication logic offers a dynamic approach to security, recognizing that the requirements for authentication and data protection can vary depending on the specific healthcare environment and patient context.

CAP's multi-factor authentication mechanisms provide robust defense against unauthorized access, ensuring that only authenticated and authorized entities can interact with healthcare data. Moreover, its dynamic key management system adds an extra layer of security by generating and adjusting encryption keys in real-time, making it exceptionally challenging for adversaries to compromise data integrity.

The continuous monitoring and adaptation capabilities of CAP are paramount in maintaining security during healthcare data roaming. It effectively identifies and responds to potential threats, preserving the privacy of healthcare data and the trustworthiness of the BSN infrastructure.

CONCLUSION

In the evolving landscape of healthcare monitoring, where the mobility of patients and healthcare data is paramount, the Composable Authentication Protocol (CAP) stands as a robust guardian of mobility. CAP's dynamic, context-aware authentication approach, multi-factor authentication mechanisms, and adaptive security measures collectively ensure the secure roaming of Cloud-assisted Body Sensor Networks (BSNs).

Through its implementation, CAP has demonstrated remarkable results, enhancing security, bolstering data privacy, and adapting to the dynamic nature of healthcare environments. It safeguards sensitive health data, ensuring its confidentiality and integrity as patients move between different healthcare facilities and network environments.

As healthcare continues to embrace the benefits of cloud technology and interconnected systems, CAP plays a pivotal role in securing the future of healthcare monitoring. It empowers healthcare providers to deliver quality care while maintaining the highest standards of security and privacy for their patients' health data. In an era where the seamless exchange of healthcare information is paramount, CAP is the guardian that ensures mobility and security coexist harmoniously in the healthcare landscape.

REFERENCES

1. M. Burmester, T. V. Le, B. D. Medeiros, and G. Tsudik, “Universally composable RFID identification and authentication protocols,” ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 4, pp. 21-33, 2009.
2. C. C. Chang and H. C. Tsai, “An anonymous and self-verified mobile authentication with authenticated key agreement for large-scale wireless networks,” IEEE Transactions on Wireless Communication, vol. 9, no. 11, pp. 3346–3353, 2010.
3. S. Chari, C. Jutla, and A. Roy, “Universally composable security analysis of Oauth v2.0,” IACR Cryptology ePrint Archive, pp. 526, 2011.
4. M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V.Leung, “Body area networks: A survey,” Mobile Networks and Applications, vol. 16, no. 2, pp. 171– 193, 2011.
5. S. F. Doghmi, J. D. Guttman, and F. J. Thayer, “Completeness of the authentication test,” in The 12th European Symposium on Research in Computer Security (ESORICS 2007), LNCS 4734, pp. 106–121, Springer, 2007.

6. W. Du, R. Wang, and P. Ning, “An efficient scheme for authenticating public keys in sensor networks,” in The 6th ACM International Symposium on Mo- bile Ad Hoc Networking and Computing, pp.58–67, Chicago, IL, 2005.

7. T. Feng, W. Zhou, and X. Li, “Anonymous identity authentication scheme in wireless roaming communication,” in 2012 8th International Conference on Computing Technology and Information Management (ICCM’12), vol. 1, pp.124–129, Seoul, Korea, 2012.

8. G. Fortino, M. Pathan, and G. Fatta, “BodyCloud: Integration of cloud computing and body sensor networks,” in 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (Cloud-Com), pp. 851–856, Taipei, Taiwan, 2012.

9. J. D. Guttman, “Cryptographic protocol composition via the authentication tests,” in The 12th International Conference on Foundations of Software Science and Computational Structures, vol. 5504, pp. 303–317, York, UK, 2009.