IMPLEMENTATION OF SECURE HEALTH CARE DATA IN IOMT USING BLOCKCHAIN TECHNOLOGY

[a] Dr. P. Sivakumar, [b]S. Aiswariya, [b]S. Keerthana, [b]N,Ezhilaraci
[a] Professor, [a ,b]Department of Information Technology, Manakula Vinayagar Institute of Technology, Puducherry, India.

Abstract-The Internet of Medical Things (IoMT) has emerged as a promising technology in the healthcare industry, enabling the seamless integration of medical devices and systems for improved patient care. However, ensuring the security and privacy of sensitive medical data transmitted and stored by these interconnected devices poses significant challenges. In particular, the management of authentication keys for secure communication becomes critical to protect against unauthorized access and data breaches. This paper proposes a novel blockchain-enabled securing the health care data using key management protocol designed specifically for IoMT deployment. The protocol leverages the inherent security features of blockchain technology to establish a decentralized and tamper-resistant infrastructure for key management. By utilizing distributed ledger technology, the protocol ensures the integrity, availability, and confidentiality of authentication keys, while providing transparency and auditability in key management operations. The protocol employs a hybrid cryptographic approach combining symmetric and asymmetric encryption algorithms to secure the transmission and storage of authentication keys. Furthermore, it incorporates a robust mechanism for key generation, distribution, revocation, and renewal, ensuring that only authorized entities have access to encrypted medical data. The protocol also incorporates mechanisms to handle key compromises and key revocation in case of security incidents. To evaluate the effectiveness of the proposed protocol, extensive simulations, and performance analysis are conducted. The results demonstrate that the protocol achieves high security, scalability, and efficiency, making it suitable for large-scale IoMT deployments in healthcare environments. The proposed blockchain-enabled securing the healthcare data using key management protocol for IoMT deployment addresses the critical security challenges in managing authentication keys for interconnected medical devices. By leveraging the security and transparency of blockchain technology, the protocol enhances the overall security posture of IoMT systems, enabling healthcare providers to confidently adopt this technology for improved patient care while ensuring the privacy and confidentiality of sensitive medical data.

Keywords: Blockchain,Hybrid cryptographic approach, Security, Confidentiality.

I. INTRODUCTION

The rapid advancement of technology has led to the emergence of the Internet of Things (IoT), which has revolutionised various industries, including healthcare. One significant subset of the IoT in the healthcare sector is the Internet of Medical Things (IoMT), where interconnected medical devices and sensors are used to gather and transmit valuable patient data for monitoring, diagnosis, and treatment. However, the proliferation of IoMT devices has introduced numerous security and privacy challenges, highlighting the need for robust key management protocols. In this context, this paper presents the design of the blockchain-enabled security of healthcare data using the Key Management Protocol for IoMT deployment. It leverages the decentralised nature of blockchain technology to enhance the security, privacy, and integrity of key management in IoMT systems. This protocol addresses the limitations of traditional key management approaches by providing a reliable and tamper-resistant framework for generating, distributing, and revoking cryptographic keys within the IoMT ecosystem.The IoMT, stressing the expansion of the usage of medical technology as well as the challenges in guaranteeing its secure functioning and communication. It emphasises the critical role key management plays in protecting the confidentiality, precision, and accessibility of sensitive medical data. It explains how to generate keys, perform authentication, distribute keys securely, and use blockchain technology to store and retrieve keys efficiently. Security Analysis and Performance Evaluation, including a thorough assessment of its resistance to typical assaults such as key compromise, man-in-the-middle assaults, and replay assaults Additionally, a performance evaluation is carried out, with particular attention paid to key management latency, resource usage, and scalability.

II. LITERATURE SURVEY

B.Bera,D.Chattaraj and A.K.Das[1]-In recent times, the Internet of Drones(IoD) has surfaced as an important exploration content in the academe and assiduity because it has several implicit operations ranging from mercenary to service. All the drones and the GSS are registered with a central trusted authority, Control Room(CR), before deployment. Once the blocks are added to the blockchain, the deals contained in the blocks can not be altered, modified, or indeed removed. We give all feathers of security analysis including formal security under the arbitrary mystic model, informal security, and simulation- grounded formal security verification to assure that the proposed scheme can repel colorful implicit attacks.M.Wazid, A.K.Das, V.Odeln [2]-In recent years, the research in generic Internet of Things (IoT) attracts a lot of practical applications including smart home, smart cityetc.., The hierarchical IoT network (HIoTN) is aspecial kind of the generic IoT network. In HIoTN, there is a need, where a user can directly access the real-time data from the sensing nodes for a particular application. This paper emphasizes on the designofanew secure light weight three-factor remote user authentication scheme for HIoTNs, called the user authenticated key management protocol (UAKMP). The three factors used in UAKMP are the user smart card, password, and personal biometrics. The security of the scheme is thoroughly analyzed under the formal security in the widely accepted real-or-random model, the informal security as well as the formal security verification using the widely accepted automated validation of Internet security protocols and applications tool. UAKMP offers several functionality features including off line sensing node registration, freely password and biometric update facility, user anonymity, and sensing node anonymity compared to other related existing schemes.AminandBiswas [4]- A new provably secure and efficient three-factor remote user authentication scheme for TMIS is proposed in this paper. The proposed scheme overcomes all drawbacks of their scheme and also provides additional features such as user unlink ability, user anonymity, efficient password, and biometric update. The rigorous in formal and formal security analysis using random oracle models and the mostly acceptable Automated Validation of Internet Security Protocols and Applications tool is also performed. During the experimentation, it has been observed that the proposed scheme is secure against various known attacks that include replay and man-in-the- middle attacks. Furthermore, the analysis of computation and communication cost estimation of the proposed scheme depicts that our scheme is efficient as compared with other related exiting schemes.

III. EXISTING WORK

The existing system for key management in the context of Internet of Medical Things (IoMT) deployments faces significant challenges in ensuring secure and authenticated communication between interconnected medical devices. Traditional approaches often rely on centralized key management systems, which are vulnerable to single points of failure and potential security breaches. Additionally, these systems may lack transparency and auditability, making it difficult to verify the integrity and confidentiality of authentication keys. Moreover, conventional cryptographic protocols used in key management may not be designed to handle the unique characteristics and requirements of IoMT environments. The scale, heterogeneity, and mobility of medical devices in IoMT necessitate robust and efficient key management mechanisms to ensure secure communication.

Furthermore, the growing concern for privacy and data protection in the healthcare industry demands more sophisticated approaches to safeguard sensitive medical data. Existing systems may not adequately address these concerns, leaving medical devices and patient data vulnerable to unauthorized access and potential misuse. Overall, the limitations of the existing system for key management in IoMT deployments include: Centralized architecture: Reliance on centralized key management systems that can be susceptible to single points of failure and security breaches. Lack of transparency and auditability: Inadequate mechanisms to verify the integrity and confidentiality of authentication keys, making it challenging to track and audit key management operations. Inefficient cryptographic protocols: Traditional cryptographic protocols may not be optimized for the unique requirements of IoMT environments, leading to performance bottlenecks and scalability issues. Insufficient privacy and data protection: The existing system may not provide adequate measures to protect sensitive medical data, leaving it vulnerable to unauthorized access and potential misuse. Limited resilience to security incidents: Inadequate mechanisms to handle key compromises and key revocation in the event of security incidents, potentially resulting in prolonged exposure to vulnerabilities. Addressing these limitations is crucial to establish a robust and secure key management system for IoMT deployments. The proposed blockchain-enabled authenticated key management protocol aims to overcome these challenges by leveraging the security, transparency, and decentralized nature of blockchain technology, thereby enhancing the overall security posture of IoMT systems and ensuring the privacy and confidentiality of sensitive medical data.

IV. PROPOSED METHOD

The proposed system is a blockchain-enabled securing healthcare data using key management protocol specifically designed for Internet of Medical Things (IoMT) deployments. This protocol addresses the limitations of the existing system by leveraging the security features of blockchain technology to establish a decentralized and tamper-resistant infrastructure for key management in IoMT environments.

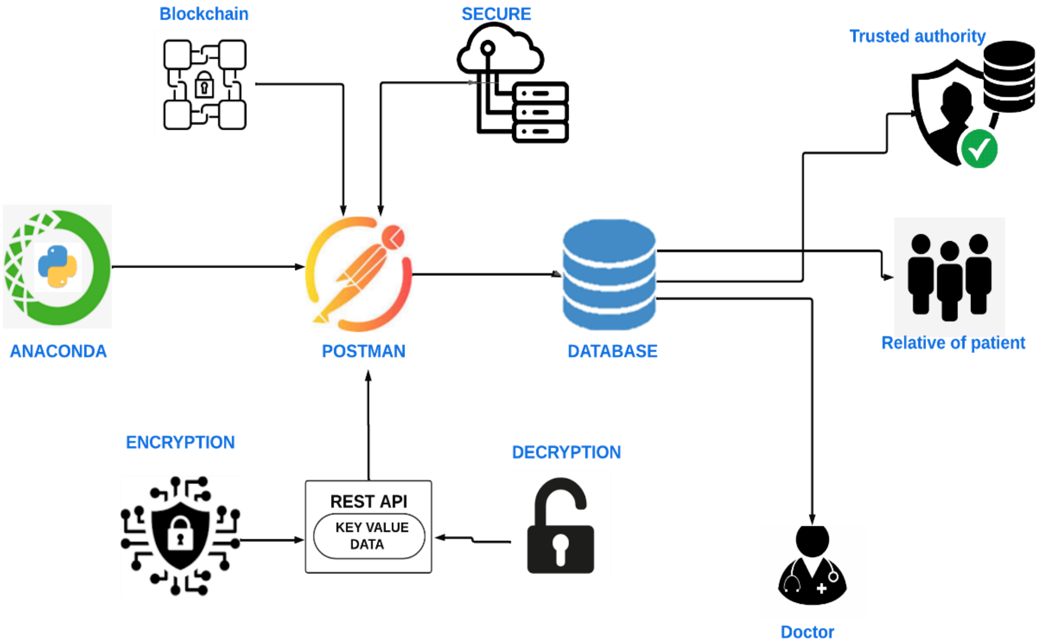

Fig.1 Architectural Diagram for Proposed Work

A.Blockchain-based Decentralization

The protocol utilizes a distributed ledger technology, such as blockchain, to decentralize the key management infrastructure. This eliminates the reliance on a centralized authority and reduces the risk of single points of failure or security breaches. The distributed nature of the Blockchain ensures the integrity and availability of authentication keys.

B.Hybrid Cryptographic Approach

The protocol employs a hybrid cryptographic approach that combines symmetric and asymmetric encryption algorithms. Symmetric encryption is used for efficient and secure communication between devices, while asymmetric encryption is used for secure key exchange and distribution. This combination ensures both the efficiency and security of key management operations.

C.Key Generation and Distribution

The protocol incorporates a robust mechanism for key generation, ensuring the generation of strong and unique authentication keys. It also includes secure key distribution mechanisms to ensure that only authorized entities have access to the encrypted medical data. This enhances
The overall security of the system and prevents unauthorized access.

D.Key Revocation and Renewal

The proposed system includes mechanisms for key revocation and renewal. In case of a compromised key or security incident, the protocol allows for the revocation of compromised keys and the generation of new keys, ensuring continued security of the system. This helps to mitigate the impact of security breaches and ensures the integrity of the communication.

E.Transparency and Auditability

The use of blockchain technology provides transparency and auditability in key management operations. Every key management transaction is recorded on the blockchain, creating an immutable and transparent log of all key-related activities. This enables efficient auditing and verification of key management operations, ensuring the integrity and confidentiality of authentication keys. By incorporating these features, the proposed system enhances the security, privacy, and efficiency of key management in IoMT deployments. It ensures secure and authenticated communication between medical devices, protects sensitive medical data from unauthorized access, and provides transparency and auditability in key management operations. The use of blockchain technology establishes a robust and resilient infrastructure for key management, making the proposed system suitable for large-scale IoMT deployments in healthcare environments.

V.CONCLUSION

In conclusion, the design of the BAKMP-IoMT protocol presents a novel and efficient solution for authenticated key management in the context of the Internet of Medical Things (IoMT) deployment. By incorporating blockchain technology, the protocol ensures the security and integrity of key management operations, addressing the vulnerabilities and privacy concerns associated with traditional centralized systems. The BAKMP-IoMT protocol provides a decentralized and tamper-proof ledger for storing and managing cryptographic keys used in IoMT devices, such as medical sensors and wearable devices. Through the use of smart contracts and consensus mechanisms, the protocol establishes a trustless environment where key management transactions are transparent, auditable, and resistant to unauthorized modifications. One of the key advantages of BAKMP-IoMT is its ability to enhance the security and privacy of sensitive medical data. By leveraging blockchain's immutability and transparency, the protocol reduces the risk of data breaches, unauthorized access, and tampering. Additionally, the use of cryptographic techniques ensures the confidentiality and integrity of the keys, safeguarding the communication and authentication processes within the IoMT ecosystem. Furthermore, the BAKMP-IoMT protocol addresses the scalability challenges of traditional key management systems by leveraging the distributed nature of blockchain technology. Through its decentralized architecture, the protocol enables efficient key generation, distribution, and revocation processes, accommodating the growing number of IoMT devices and ensuring smooth and reliable operation. In summary, the BAKMP-IoMT protocol demonstrates the potential of blockchain-enabled authenticated key management in securing the Internet of Medical Things deployment. By leveraging the benefits of blockchain technology, the protocol enhances security, privacy, and scalability, providing a robust foundation for the widespread adoption of IoMT applications in the healthcare industry.

VI. REFERENCES

[1] B. Bera, D. Chattaraj, and A. K. Das, ``Designing secure blockchain-based access control scheme inIoT-enabled Internet of drones deployment," Comput. Commun., vol. 153,pp.229249, Mar. 2020.

[2] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, ``Design of secure user authenticated key management protocolfor generic IoT networks," IEEE Internet Things J., vol. 5, no. 1, pp. 269282, Feb. 2018.

[3] A. K. Das, A. K. Sutrala, S. Kumari, V. Odelu, M. Wazid, and X. Li, ``An efcient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks," Secur. Commun. Netw., vol. 9, no. 13, pp. 20702092, 2016.

[4] M.Wazid, A.K.Das,S.Kumari,X.Li,andF.Wu,``Design of an efcient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS," Secur. Commun. Netw., vol. 9, no. 13, pp. 19832001, Sep. 2016.

[5] S. Chatterjee, A. K. Das, and J. K. Sing, ``A secure user anonymity preserving three-factor remote user authentication scheme for the telecare medicine information systems," Adhoc Sensor Wireless Netw., vol. 21, no. 1, pp. 121149, 2014.

[6] A. K. Das, ``A secure user anonymity-preserving three-factor remote user authentication scheme for the telecare medicine information systems," J. Med. Syst., vol. 39, no. 3, p. 30, Mar. 2015.

[7] V. Odelu, A. K. Das, M. Khurram Khan, K.-K.-R. Choo, and M. Jo, ``Expressive CP-ABE schemeformobiledevicesinIoTsatisfyingconstant-sizekeysandciphertexts,"IEEEAccess,vol. 5, pp. 32733283, 2017.

[8] S.Challa,M.Wazid,A.K.Das,N.Kumar,A.GouthamReddy,E.-J.Yoon,andK.-Y.Yoo, ``Secure signature-based authenticated key establishment scheme for future IoT applications," IEEE Access, vol. 5, pp. 30283043, 2017.