CSCI 530 Security Systems
Research Proposal

Laxmi Garde

Title: A study of different techniques of Key Management and Authentication for IoT systems with a focus on Blockchain.

Introduction

With an increase in the number of connected devices and their proximity to humans on a day-to-day basis, the security of these connected devices must be ensured. To assure the safety of these systems and apply the relevant cryptographic strategy, key management and authentication processes become vital to use encryption techniques and manage access to these systems. As the devices in an IoT system network are mainly distributed and have a limited computational capacity, it becomes even more challenging to apply today's complex encryption strategies that require large storage, large key sizes, and high computational power to ensure that the security of these devices is managed. The key management in terms of key creation and distribution with other key life-cycle phases is challenging for IoT devices. Therefore, it is of great importance to understand the basics of key management and authentication, and further understand and analyze the different techniques that can be leveraged for IoT devices and systems to ensure their security.

The research paper highlights the explorations of different key management techniques and authentication methods that ensure the security of IoT devices, with a focus on Blockchain. Blockchain is a distributed ledger technology that ensures transactions node-to-node without the need for a centrally located authority, and its fast, accurate, and efficient traits make it suitable as a key management platform for IoT devices. Along with a focus on Blockchain, the paper also showcases other existing key management and authentication techniques, like (but not limited to), a lightweight authentication and key management mechanism for edge-based IoT devices, dual authentication mechanisms for VANETs (Vehicular Ad-Hoc networks), link-layer oriented key management systems, hybrid key management, and mutual authentication protocol, and analyzing multiple authentication mechanisms and schemes including certificate-based schemes, raw public key schemes, identity-based schemes, etc. and provide a detailed view and comparison of these techniques and approaches, finding meaningful insights.

The paper showcases a basic conceptual understanding of key management and authentication, its types, methods, advantages, and usages. The paper then evolves by highlighting the techniques in key management and authentication in IoT devices. The research examines the existing research in different techniques and the associated challenges, limitations, and advantages. The paper concludes with a comparison of all the approaches discussed in the paper.

Objective

The objective of the research paper is to gain enough expertise in the key management and authentication mechanisms in security systems. Further, the scope of research is to investigate and understand how these mechanisms are applied in distributed systems and networks, like IoT systems. The main goal of this research is to study the nuances, methods, and challenges faced while thinking about the security of IoT systems that are at higher risk and are vulnerable to malicious attacks, and the impact this can have on the end users.

Methodologies to be included in the Research Paper

The methodologies planned to be covered in the research paper include a brief understanding of the different types of keys and the usage of these keys in different cryptographic techniques. Research on key management includes key creation, exchanges, key distribution, key usage, storage, replacement, and destruction which are the basic steps in key management. The research paper involves a detailed view of key lifecycle management processes and standards. The paper discusses the KMIP (Key Management Interoperability Protocol), risk, and mitigation strategies around key management. The paper includes authentication types, factors, and techniques like password-based, token-based, single-factor, multi-factor, and single-sign-on authentication.

The paper gives an overview of IoT systems, the associated vulnerabilities, and the need for security of these systems. The paper briefly investigates the methods used for key management and authentication in IoT devices. The research mainly revolves around the mechanisms included in WSNs (Wireless sensor networks) that are an application of IoT devices. The mechanisms include a Hybrid Key Management Scheme based on Elliptic Curve Cryptography (ECC) and a hash function to generate pre-distribution keys, which are required for mutual authentication between sensor nodes [4], studying link-layer oriented key management systems processes in IoT devices. The Blockchain infrastructure uses public key infrastructure (PKI) for authentication and Bitcoin-based key management approaches, as mentioned in the paper, a key management scheme for distributed sensor networks, dual authentication, and key management in Vehicular ad-hoc networks. The limitations associated with the discussed techniques would be covered in the paper to provide a complete analysis and overview.

Literature Survey

The research papers studied to arrive at the topic and to apprehend the techniques used for Key management and authentication in IoT devices are as follows: (mentioning only a few papers from the survey)

The research paper [4] establishes a technique of Hybrid key management and mutual authentication method between the sensor nodes in an IoT (distributed WSN) network. The paper proposes the above design and provides a detailed comparison of techniques and limitations of other similar methods based on computational advantages and better security. The research paper [1] provides another approach to key management in WSN systems using a link-layer-based strategy for key management.

Paper [3] proposes a key management scheme for Distributed sensor networks that includes a selective distribution and revocation of keys and node re-keying without substantial computation and communication capabilities.

Paper [9] provides a blockchain-based solution that uses hash chains for secure key management and exploits primary characteristics of blockchain technology (open, immutable, traceability, and fault-tolerance) to ensure data security in IoT systems.

References

[1] Roman, R., Alcaraz, C., Lopez, J., & Sklavos, N., ‘Key management systems for sensor networks in the context of the Internet of Things’, Computers & Electrical Engineering, 37(2), 147–159, 2011. https://doi.org/10.1016/j.compeleceng.2011.01.009

[2] Panda, S. S., Jena, D., Mohanta, B. K., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H., ‘Authentication and Key Management in Distributed IoT Using Blockchain Technology’, IEEE Internet of Things Journal, 8(16), 12947–12954, 2021.
https://doi.org/10.1109/jiot.2021.3063806

[3] Eschenauer, L., & Gligor, V. D., ‘A Key-Management Scheme for Distributed Sensor Networks’, citeseer.ist.psu.edu, Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002
https://citeseer.ist.psu.edu/viewdoc/citations?doi=10.1.1.19.9193

[4] Sharmila, Pramod Kumar, Shashi Bhushan, Manoj Kumar, Mamoun Alazab, ‘Secure Key Management and Mutual Authentication Protocol for Wireless Sensor Network using Hybrid Approach’, 2021, https://www.researchgate.net/publication/350207785_Secure_Key_Management_and_Mutual_Authentication_Protocol_for_Wireless_Sensor_Network_using_Hybrid_Approach

[5] Tan, H., & Chung, I, ‘Secure Authentication and Key Management With Blockchain in VANETs’, IEEE Access, 8, 2482–2498, 2020. https://doi.org/10.1109/access.2019.2962387

[6] Deebak, B. D., Memon, F. H., Khowaja, S. A., Dev, K., Wang, W., Qureshi, N. M. F., & Su, C.,‘Lightweight Blockchain Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems’, IEEE Internet of Things Journal, 1–1, 2022, https://doi.org/10.1109/JIOT.2022.3152546

[7] Vijayakumar, P., Azees, M., Kannan, A., & Jegatha Deborah, L., ‘Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks’, IEEE Transactions on Intelligent Transportation Systems, 17(4), 1015–1028, 2016, https://doi.org/10.1109/tits.2015.2492981

[8] Wazid, M., Das, A. K., Shetty, S., J. P. C. Rodrigues, J., & Park, Y. ‘LDAKM-EIoT: Lightweight Device Authentication and Key Management Mechanism for Edge-Based IoT Deployment’. Sensors, 19(24), 5539, 2019, https://doi.org/10.3390/s19245539

[9] Pal, O., Alam, B., Thakur, V., & Singh, S., ‘Key management for blockchain technology’, ICT Express, 2019, https://doi.org/10.1016/j.icte.2019.08.002

[10] Tabassum, T., Hossain, S. A., Rahman, Md. A., Alhamid, M. F., & Hossain, M. A., ‘An Efficient Key Management Technique for the Internet of Things’, Sensors, 20(7), 2049, 2020, https://doi.org/10.3390/s20072049

[11] Ievgeniia Kuzminykh, Bogdan Ghita, Stavros Shiaeles, ‘Comparative Analysis of Cryptographic Key Management Systems’, October 3, 2022, from https://arxiv.org/pdf/2109.09905.pdf

[12] Attkan, A., & Ranga, V, ‘Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security’, Complex & Intelligent Systems volume 8, pages3559–3591, 2022. https://doi.org/10.1007/s40747-022-00667-z

[13] Kim, K.-W., Han, Y.-H., & Min, S.-G., ‘An Authentication and Key Management Mechanism for Resource Constrained Devices in IEEE 802.11-based IoT Access Networks’, Sensors, 17(10), 2170, 2017. https://doi.org/10.3390/s17102170

[14] Fang, H., Qi, A., & Wang, X., ‘Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement’, IEEE Network, 34(3), 24–29, 2020. https://doi.org/10.1109/mnet.011.1900276