A Powerful Three-Party Identification and Secret Negotiation Mechanism for Portable Computation Offloading IoT Device Security Protection

P.Adi Lakshmi #1, M.Tharak Ram #2, Ch.Saiteja #3, M.Vamsi Krishna #4, S.Pavan Malyadri #5
#1 Asst. Professor, Department of Computer Science and Engineering
#2,3,4,5 Student, Department of Computer Science and Engineering
QIS College of Engineering & Technology

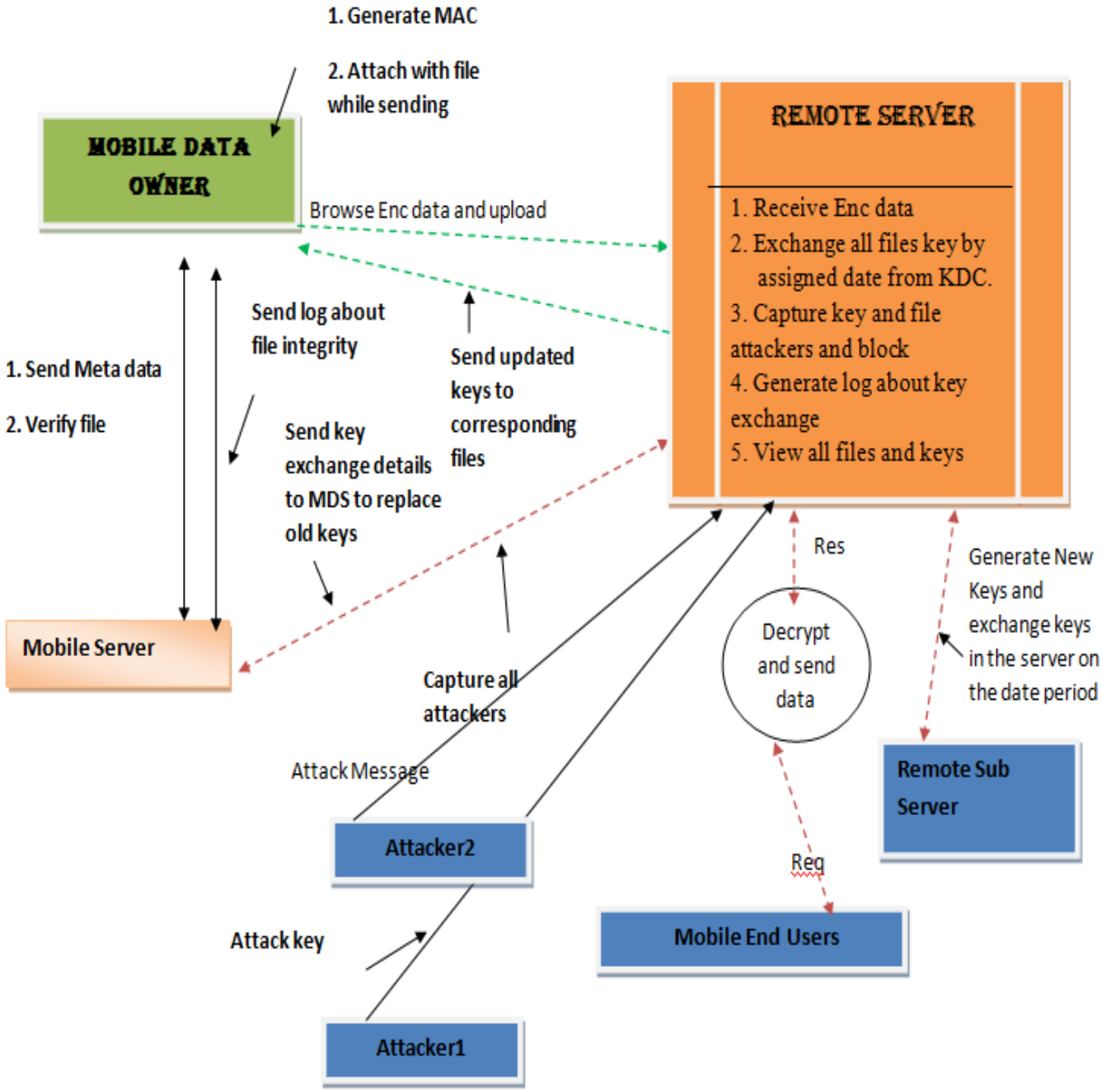
Abstract

Mobile edge computing development (MEC). All Internet of Things devices at mobile edge use wireless networking. Therefore, protecting the sender's data and privacy during transmission is of utmost importance. The current state of user authentication techniques in MEC is crowded with proposals from several researchers. Unfortunately, there is currently no lightweight and efficient method of authenticating between users, edge devices, and the cloud server. In this research, we develop a mechanism for secure authentication and key agreement between three parties that does not rely on bilinear pairings. The suggested protocol enabled authentication between end users, edge devices, and the cloud server, and it also enabled the three parties to perform key agreement in order to establish a shared session key. Our protocol is safe and secure according to the security analysis, since it satisfies security criteria including session-key security and forward secrecy. A little amount of computing is required for this technique, as shown experimentally.

1. Introduction

Security, as we are all well aware, is a major concern in the world of MEC. Since MEC relies on wireless networks for communication, it is susceptible to a wide variety of threats. As an example, malevolent users might potentially intercept the information or even change it, posing a serious threat to the users' privacy. By pretending to be other users or edge devices, unscrupulous individuals might send false messages to unsuspecting users, posing major security risks. Consequently, it is a topic of interest to consider how to safeguard data transfer between iot gadgets, edge gadgets, and the cloud server.

MEC also has a serious challenge when it comes to protecting users' privacy. Protecting a user's privacy when interactions with edge devices or a cloud server is essential (such as real identity). A conditional privacy-preserving has been presented based on this. Legal authentication of cloud servers, edge devices, and users is an area worth exploring to ensure user privacy.


1. Generate MAC
2. Attach with file while sending
MOBILE DATA OWNER
Browse Enc data and upload
REMOTE SERVER
1. Receive Enc data
2. Exchange all files key by assigned date from KDC.
3. Capture key and file attackers and block
4. Generate log about key exchange
5. View all files and keys
Send log about file integrity
1. Send Meta data
2. Verify file
Send updated keys to corresponding files
Send key exchange details to MDS to replace old keys
Mobile Server
Capture all attackers
Res
Decrypt and send data
Generate New Keys and exchange keys in the server on the date period
Remote Sub Server
Attack Message
Attacker2
Req
Attack key
Mobile End Users
Attacker1

2. Related Works

Several other authentication schemes have been proposed by scientists recently.

Using a cuckoo filter, Cui et al. [14] suggested an anonymous authentication method. In this method, the cuckoo filter stores the hash value of the first authenticated signature. The Cuckoo filter only requires a comparison of the signature's hash value when further authentication of the signature is required. Unfortunately, a large data structure is needed in this technique to keep the signature safe. Because it will cut down on the time spent storing unnecessary data and will increase the effectiveness of message filtering. A lightweight multi-key privacy-preserving approach with message filtering was presented by Zhou et al. [15] for use with location-based services. Each user's communication is given a redundancy score by the Road Side Units (rsus), which then uses that score to filter out duplicates before authenticating the information they contain. With this method, we can drastically cut down on the money spent on computation and communication. Additionally, several encryptions using various keys are used to safeguard the message and the user's anonymity.

A Diffie-Hellman key exchange based, three-party mutual authentication and key agreement mechanism was suggested by Lee et al. [16]. The book was created by Lv et al. [17]. Mechanism for authenticated key exchange between three parties, which has lower computational cost and is hence more efficient. Meanwhile, the issue of a missing key may be avoided by using a one-time key.

Unfortunately, none of these options offers a very high degree of security. As such, the three-party mutual authentication mechanism has broad applicability. The three-party mutual authentication protocol was implemented by Chiou et al. [18] in a medical setting, and it met higher security standards than the previous two. Using the three-party mutual authentication mechanism, Jia et al. [19] implemented iot devices in a hospital setting. To reduce computational cost and increase security, Ma et al. [20] adapted and implemented this protocol to vehicular ad hoc networks (vanets), allowing for mutual authentication between automobiles, fog nodes, and the cloud server.

The dynamic addition of cars and rsus was accomplished thanks to the work of Bagga et al. [21], who presented a novel mutual authentication and key agreement protocol that uses two layers of authentication and key agreement. Using formal security verification using the well-known AVISPA tool, Wazid et al. [22] integrated user authentication and key agreement into Internet of Drones Deployment, making it resistant to multiple assaults.

3. Existing System

For e-Health systems, Guo et al. [22] suggested an attribute-based authentication technique that also protected user privacy. Attribute-based encryption uses a lot of power, but it allows for very

granular control over who has access to which resources [23]. For the most part, bilinear pairings are employed in identity-based authentication systems. Unfortunately, the bilinear pairing method is computationally costly and time-consuming on a mobile device. As a result, several different bilinear-pair-free authentication algorithms for mobile users have been proposed. Some protocols were discovered to be unsafe after they were released, much like the history of key establishment and agreement protocols (e.g. The protocol in [30] was found to be vulnerable to impersonate attack mentioned

When it comes to private keys, the current system and protocols seldom take mobile device security into account. Researchers have investigated the use of threshold secret sharing as a means of securing the private keys. For instance, Chandramowliswaran et al. [32] suggested a Chinese reminder theory-based authenticated key distributed protocol to secure group shareholder key information broadcast from a centralised location. Of safeguard the private key to one's bitcoin wallet, Jarecki et al. Presented a password-based secret sharing system with great efficiency.

Cloud storage system by Hu et al. [34] in which the key is kept in three parts by users, cloud storage providers, and a different third trusted party. These protocols protect keys against external attacks, but there is still a risk of compromise during key reconstruction, and mobile devices can't take full use of the secret-sharing mechanism.

Disadvantages

Traditional authentication and key agreement procedures aim to protect messages from prying eyes and to set up a safe key for use during a session.

O No currently available user authentication protocol can both guarantee safe key agreement and private key security while also being sufficiently efficient for the system.

4. Proposed System

A novel identity-based anonymous authentication protocol is proposed in this research to improve security and efficiency in the mobile Internet context by providing both secure keg agreement and key protection for mobile authentication. What follows is a brief summary of the main contribution of the proposed protocol.

First, we present a secure authentication protocol for mobile Internet environments based on the two-party computation, which is both efficient and resistant to the key exposure attack (assuming a mobile device is maliciously controlled by an attacker).

Second, we provide a thorough security analysis to show that the proposed protocol satisfies all current standards for secure authentication over the mobile Internet, especially with regards to keeping sensitive information safe.

Finally, we evaluate the protocol's computational and communication costs to show that it is suitable for a mobile Internet setting.

Advantages

Due to the system's implementation of Two-factor Security and Mutual Authentication, data is more secure than ever before, and the system also incorporates data security so that no one user may claim exclusive control over the system's keys.

5. Conclusion

In this work, we propose a robust and private three-party authentication and key agreement technique for MEC-based Internet of Things (iot) privacy. Users, edge devices, and the cloud server all participated in the scheme's three-way authentication and key agreement. We then study the security features of the protocol and provide a proof of its security.

The results of the security analysis prove that our protocol is safe and that it has desirable security characteristics like session key security and forward secrecy. Finally, we conduct an assessment of the protocol's performance, and the results demonstrate that our protocol is superior in terms of computation cost and communication cost.

References

[1] Z. Lu, G. Qu, Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy

[2] Trust in VANET: A Survey of Current Solutions and Future Research Opportunities R. Hussain, J. Lee, S. Zeadally.

[3] Lightweight Cryptographic Protocols for Iot-Constrained Devices: A Survey, M. N. Khan, A. Rao, S. Camtepe

[4] G. Mei, N. Xu, J. Qin, B. Wang, P. Qi, A Survey of iot for Geohazard Prevention: Applications, Technologies, and Challenges.

[5] Fast and Secure Computational Offloading with Lagrange Coded Mobile Edge Computing,

[6] C. Park and J. Lee, "Mobile Edge Computing-Enabled Heterogeneous Networks."

[7] M. Abdel-Basset, R. Mohamed, M. Elhoseny, A. K. Bashir, A. Jolfaei, N. Kumar, Energy-Aware Marine Predators Algorithm for Task Scheduling in Iot-Based Fog Computing Applications.

[8] Emerging Topics in Device to Device Communications as Enabling Technology for 5g Systems, Transactions on Emerging Telecommunications Technologies, W. Xiang, K. Zheng, D. Niyato, L. Militano, G. Araniti.

[9] Multi-Band All-Digital Transmission for 5G NG-RAN Communication, N. Kumar, K. Rawat, F. M. Ghannouchi.

[10] Future Generation Computer Systems S. Hu and Y. Xiao, Design of Cloud Computing Task Offloading Algorithm Based on Dynamic multiobjective Evolution.

[11] Cooperation Advances on Vehicular Communications: A Survey, by J. A. F. F. Dias, J. J. P. C. Rodrigues, and L. Zhou, Vehicular Communications,

[12] An Effective Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks, D. He, S. Zeadally, B. Xu, and X. Huang,

[13] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, P. Lorenz, Based Authentication Scheme for Internet of Vehicles Deployment."

[14] J. Cui, J. Zhang, H. Zhong, Y. Xu, SPACF: A Secure Privacy-Preserving Authentication Scheme for VANET with Cuckoo Filter.

[15] Lightweight Privacy-Preserving Authentication from Efficient Multi-Key Secure Outsourced Computation for Location-based Services

[16] Computers & Mathematics with Applications,

[17] C. Lv, M. Ma, H. Li, J. Ma, Y. Zhang, An Novel threeparty Authenticated Key Exchange Protocol Using onetime Key.

[18] January 2018 issue of Security and Communication Networks has "An Efficient Three-Party Authentication Scheme for Data Exchange in the Medical Environment" by S. Chiou and C. Lin.

[19] X. Jia, D. He, N. Kumar, K. R. Choo, Authenticated Key Agreement Scheme for Fog-Driven Iot Healthcare System.

[20] M. Ma, D. He, H. Wang, N. Kumar, K. R. Choo, This article presents an efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad hoc networks.

[21] On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System

[22] Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment

[23] S. Mukherjee, D. S. Gupta, G. P. Biswas, The Use of Lattice to Create a Fast and Batch-Verifiable Privacy-Preserving Authentication Scheme for Vanets

[24] Y. Zhou, X. Long, L. Chen, Z. Yan, Conditional Privacy-Preserving Authentication and Key Agreement Scheme for Roaming Services in vanets.

[25] I. Ali and F. Li, "An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicle-to-Infrastructure Communication in vanets

[26] Enhancing Security and Privacy for identitybased Batch Verification Scheme in vanets, S. Tzeng, S. Horng, T. Li, X. Wang, P. Huang, M. K. Khan.

[27] Distributed aggregate privacy-preserving authentication on vanets L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, C. Hu.

[28] Privacy-Preserving Authentication Scheme with Full Aggregation in VANET, H. Zhong, S. Han, J. Cui, J. Zhang, Y. Xu, Information Sciences

[29] Authors: M. Han, L. Hua, S. Ma Preprint at arxiv: 1611.09009, November 2016; title: "A Self-Authentication and Deniable Efficient Group Key Agreement Protocol for VANET."

[30] Y. Jiang, S. Ge, X. Shen, AAAS: An Anonymous Authentication Scheme based on Group Signature in vanets.

[31] Trust Model for Secure Group Leader-Based Communications in VANET, H. Hasrouny, A. E. Samhat, C. Bassil, A. Laouiti, Wireless