ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

ISSN2454-9940

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

Vol 13, Issue.4 Dec 2019

A CUTTING-EDGE APPROACH TO RFID-BASED KEY ARRANGEMENT: DYNAMIC, EFFICIENT, AND SECURE

M.NIRMALA[1],SRIMATHI KESHETTI[2]
[12]Assistant Professor
Department Of CSE
Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT

In the current digital era, security and privacy are vital. The user and server should decide on a common key in advance so that the sensitive user data can only be read by a legitimate server. In order to achieve this, several dynamic ID-based authenticated key agreement (DIDAKA) protocols have been proposed in the last ten years. These protocols can ensure that users and servers will communicate securely in the future. However, a review of related publications reveals that the current DIDAKA methods have one or more security flaws. In an attempt to address the security flaws in earlier systems, Xie et al. recently proposed an intriguing anonymous DIDAKA protocol; nonetheless, we discovered that their scheme is vulnerable to three assaults. Thus, in order to address the security shortcomings, we present in this study an anonymous DIDAKA protocol that is both more secure and has a faster execution time than the one suggested by Xie et al. While maintaining all of the benefits of their original scheme. We provide formal security evidence and automatic formal verification of security to prove the security of the suggested scheme, and we provide a thorough comparative performance study to illustrate its effectiveness. In summary, the outcomes show how important the suggested plan is.

I. INTRODUCTION

SECURITY is an indispensable part of every digital communication. Evidently, without employing proper security measures, the integrity, confidentiality, and privacy of communicating parties cannot be fulfilled. As a result, overlooking the security concerns will affect the wide adoption and acceptance of many new advanced technologies that are based on digital communications. To provide a secure communication channel between two entities, both symmetric and asymmetric encryption methods can be used. However, for the symmetric encryption algorithms, like the advanced encryption standard (AES), the two parties need to have a shared key in advance. Further, since in comparison to the symmetric encryption methods, the asymmetric encryption algorithms are costly, they cannot be employed frequently for each message transmission [1]. Hence, what is normally used is that the two parties, through an authenticated key agreement (AKA) protocol, first agree upon a common key and then, by utilization of a well-known symmetric encryption mechanism and the generated shared key, they are able to communicate securely and efficiently. In the last decade, a considerable number of AKA protocols have been presented for different applications, such as telecare medical information systems [2], internet of things [3], wireless sensor networks [4] [5], wireless body area networks [6] [7], vehicle to grid networks [8], smart grids [1] [9] [10]], multi server environments [11] [12], global mobility networks [13], and so on. Because of the simplicity and portability of the two-factor smart card based AKA protocols, they have grasped noticeable attention among the other AKA schemes [14].

However, investigating the literature indicates that most of these protocols suffer from one or more security threats. Thus, quite recently, to overcome the security limitations of the previous schemes, Xie et al. [14] have put forward an interesting anonymous two-factor dynamic ID-based AKA (DIDAKA) protocol with an extended security model. Nonetheless, as we will show in section II, their scheme is vulnerable to three attacks. The goal of the current paper is to propose an efficient anonymous DIDAKA protocol, which not only is free from the security limitations of Xie et al.'s and other related schemes, but also provides better computational performance than [14]. To be more specific, in this paper, since Xie et al.'s [14] and all other previous schemes cannot resist the key compromise impersonation attack, we will cover this important security challenge with an acceptable level of performance.

II. SYSTEM ANALYSIS

EXISTING SYSTEM

Despite the many research efforts done for the DIDAKA protocols, designing a protocol that can fulfil both desired efficiency and security features is still a challenging task. In 2004, Das et al. [15] proposed a dynamic ID-based remote user authentication scheme using smart card. In 2009, Wang et al. [16] indicated that [15] does not provide mutual authentication and is susceptible to the impersonation attack. Accordingly, they proposed an enhanced scheme. However, in 2011, Khurram Khan et al. [17] showed that [16] does not provide anonymity and session key agreement and does not support smart card revocation. Another DIDAKA scheme presented by Liao and Wang [18] in 2009 for multiserver environments.

However, at the same year, Hsiang and Shih [19] indicated that [18] suffers from the insider and masquerade attacks and fails to provide mutual authentication. Afterwards, they proposed an improved protocol; nonetheless, in 2011, Lee et al. [20] demonstrated that [19] cannot resist the masquerade attack and cannot provide mutual authentication. In 2012, Wen and Li [21] presented another ID-based AKA protocol. However, Tang and Liu [22] demonstrated the susceptibility of [21] against the offline password guessing and impersonation attacks. In 2013, Li et al. [23] showed that [20] still cannot provide mutual authentication and is susceptible to some attacks. Further, in 2013, Qu and Zou [24] indicated that [21] does not provide anonymity and perfect forward secrecy. In 2014, Islam and Biswas [25] presented another ID-based AKA protocol. Nevertheless, in 2015, Sarvabhatla and Vorugunti [26] indicated that [25] cannot resist the impersonation and offline password guessing attacks. Additionally, an efficient DIDAKA scheme presented by Lin [27] in 2014; nevertheless, their scheme fails to provide the desired security features, such as perfect forward secrecy.

In 2015, Shunmuganathan et al. [28] showed that [23] is vulnerable to both the offline password guessing and stolen smart card attacks and accordingly, they presented an enhanced protocol. However, recently, Jangirala et al. [29] have indicated that [28] also fails to withstand the offline password guessing, impersonation, and stolen smart card attacks and cannot provide perfect forward secrecy. Furthermore,

ISSN2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

www.ijasem.org

Vol 13, Issue.4 Dec 2019

Chaturvedi et al. [30] proposed an enhanced DIDAKA protocol; nonetheless, careful consideration of their work indicates that it cannot totally provide the desired security properties. Recently, Xie et al. [14] have presented a novel DIDAKA protocol with an extended security model. Nonetheless, we found that their scheme cannot resist the known session-specific temporary information, denial of service, and key compromise impersonation attacks.

Disadvantages

- ❖ An existing methodology doesn't implement Authenticating server and checking message integrity method.
- ❖ The system not implemented Key Compromise Impersonation Attack (KCIA).

Proposed System

In order to double check the resistance of the proposed DIDAKA protocol against the various attacks, such as impersonation, key compromise impersonation (KCI), known session-specific temporary information (KSSTI), modification, injection, replay, and offline password guessing attacks and further, to verify the provision of the strong anonymity and perfect forward security (PFS), in this section, we take the advantage of a powerful tool called ProVerif [40]. This tool not only is able to check the "reachability properties," but also can validate the "correspondence assertions" or "observational equivalences."

As a result, it has grasped noticeable attention from the academia. Nonetheless, most scholars just use its very basic capabilities. Fig. 4 illustrates the implementation of the proposed protocol in the ProVerif input language besides the obtained results. As can be seen in the proposed system, unlike the previous works that have just employed the basic capabilities of ProVerif, we have utilized its advanced features.

In the proposed system, the first result is the result of a reachability query, which proves the secrecy of the generated session key; the second one is the result of an observational equivalence query, which corroborates the strong anonymity of user; the third one indicates the resistance against the offline password guessing attack; and eventually, the fourth and fifth ones are the results of two injective correspondence assertions that prove the replay, impersonation, and modification attacks resistance of the proposed protocol. Moreover, to demonstrate that the proposed protocol can provide the PFS and resist the KSSTI attack, respectively, we have made the long-term and ephemeral secrets available to attacker. Following, for the both cases, we have reran the model and checked the result of the first query, i.e.,
query attacker.SK• :

The results were again true that show the secrecy of session key will be still preserved in case of long-term or ephemeral secrets leakage. Finally yet significantly, in order to ensure the resistance against the KCI attack, we have disclosed the secrets of server to attacker. Since the fourth result was again true for this case, we become sure that in case of server secret keys leakage, an attacker cannot still impersonate user and hence, our scheme is resilient to the KCI attack.

Advantages

- ❖ The proposed system implements DYNAMIC ID-BASED AUTHENTICATED KEY AGREEMENT SCHEME method.
- ❖ The system implemented authenticating server and checking message integrity method.

ISSN2454-9940

www.ijasem.org

Vol 13, Issue.4 Dec 2019

III. SYSTEM SPECIFICATION

Hardware Requirements:

- System : Pentium IV 3.5 GHz.
- Hard Disk : 40 GB.
- Monitor : 14' Colour Monitor.
- Mouse : Optical Mouse.
- Ram : 1 GB.

Software Requirements:

- Operating system : Windows XP or Windows 7, Windows 8.
- Coding Language : Java – AWT,Swings,Networking
- Data Base : My Sql / MS Access.
- Documentation : MS Office
- IDE : Eclipse Galileo
- Development Kit : JDK 1.6

IV. SYSTEM STUDY

FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY

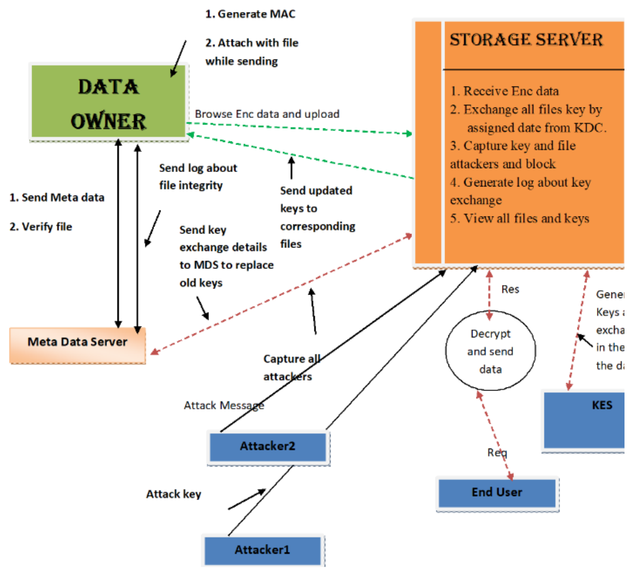
This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

V. SYSTEM DESIGN

SYSTEM ARCHITECTURE



VI. IMPLEMENTATION MODULES

Data Owner

In this module, client browse a file encrypt and upload to the router. Generates a mac address for the particular file while uploading and Sends meta data to meta data server

Storage Server

Receive encrypted data from client. Exchange all files key by assigned date from KES and Send updated keys to corresponding files, Send key exchange details to meta data server to replace old keys. Capture key and file attackers and block. Generate log about key exchange and View all files and keys, Decrypts the data and sends to the receiver

KES

Generate New Keys and exchange keys in the server on the date period

Meta Data Server

Data owner send meta data to keep copy of the file and Send log about file integrity and Capture all attackers

Receivers—End User

Request secret key and available files in the router, Request and receive decrypted files

Attacker

Type-1 attacks secret key

Type-2 injects malicious data and corrupts original file.

VII. CONCLUSION

A secure channel for user and server interactions has been established through a number of ID-based authenticated key agreement methods that have been presented thus far. A thorough examination of these protocols, however, shows that they fall short of meeting all security requirements. In order to address the current issues, we have first demonstrated the shortcomings of a recently published dynamic ID-based authenticated key agreement protocol in this study. Next, we have proposed an effective scheme that includes an increased security provision. We have performed an automated formal verification of security and a rigorous formal security proof using two widely used and potent methods to show that the suggested scheme is robust to several types of assaults. Additionally, we have evaluated our scheme's communication efficiency against a wide range of relevant ones.

REFERENCES

[1] D. Abbasinezhad-Mood and M. Nikooghadam, "An Anonymous ECC-based Self-certified Key Distribution Scheme for the Smart Grid," IEEE Transactions on Industrial Electronics, vol. 65, no. 10, pp. 7996–8004, 2018.

[2] M. Masdari and S. Ahmadzadeh, "A Survey and Taxonomy of the Authentication Schemes in Telecare Medicine Information Systems," Journal of Network and Computer Applications, vol. 87, pp. 1–19, 2017.

[3] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication Protocols for

Internet of Things: A Comprehensive Survey," Security and Communication Networks, vol. 2017, 2017.

[4] D. Alrababah, E. Al-Shammari, and A. Alsuht, "A Survey: Authentication Protocols for Wireless Sensor Network in the Internet of Things; Keys and Attacks," pp. 270–276, 2017.

[5] K.-A. Shim, "Basis: A Practical Multi-user Broadcast Authentication Scheme in Wireless Sensor Networks," IEEE Transactions on Information Forensics and Security, vol. 12, no. 7, pp. 1545–1554, 2017.

[6] H. Xiong and Z. Qin, "Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1442–1455, 2015.

[7] M. Masdari and S. Ahmadzadeh, "Comprehensive Analysis of the Authentication Methods in Wireless Body Area Networks," Security and Communication Networks, vol. 9, no. 17, pp. 4777–4803, 2016.

[8] N. Saxena and B. J. Choi, "Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks," IEEE Transactions on Information Forensics and Security, vol. 11, no. 7, pp. 1438–1452, 2016.

[9] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and Hardware Implementation of a Security-enhanced Elliptic Curve Cryptography Based Lightweight Authentication Scheme for Smart Grid Communications," Future Generation Computer Systems, vol. 84, pp. 47–57, 2018.

[10] N. Saxena, B. J. Choi, and R. Lu, "Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid," IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 907–921, 2016.

[11] V. Odelu, A. K. Das, and A. Goswami, "A Secure Biometrics-based Multi-server Authentication Protocol Using Smart Cards," IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1953–1966, 2015.

[12] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and Anonymous Mobile User Authentication Protocol Using Self-certified Public Key Cryptography for Multi-server Architectures," IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2052–2064, 2016.

[13] F. Wei, P. Vijayakumar, Q. Jiang, and R. Zhang, "A Mobile Intelligent Terminal Based Anonymous Authenticated Key Exchange Protocol for Roaming Service in Global Mobility Networks," IEEE Transactions on Sustainable Computing, vol. 99, pp. 1–1, 2018.

[14] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, "Provably Secure Dynamic ID-based Anonymous Two-factor Authenticated Key Exchange Protocol with Extended Security Model." IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, pp. 1382–1392, 2017.

[15] M. L. Das, A. Saxena, and V. P. Gulati, "A Dynamic ID-based Remote User Authentication Scheme," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, pp. 629–631, 2004.

[16] Y.-Y. Wang, J.-Y. Liu, F.-X. Xiao, and J. Dan, "A More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme," Computer Communications, vol. 32, no. 4, pp. 583–585, 2009.

[17] M. K. Khan, S.-K. Kim, and K. Alghathbar, "Cryptanalysis and Security Enhancement of a 'More Efficient & Secure Dynamic IDbased Remote User Authentication Scheme'," Computer Communications, vol. 34, no. 3, pp. 305–309, 2011.

[18] Y.-P. Liao and S.-S. Wang, “A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment,” Computer Standards & Interfaces, vol. 31, no. 1, pp. 24–29, 2009.

[19] H.-C. Hsiang and W.-K. Shih, “Improvement of the Secure Dynamic ID Based Remote User Authentication Scheme for Multiserver Environment,” Computer Standards & Interfaces, vol. 31, no. 6, pp. 1118–1123, 2009.

[20] C.-C. Lee, T.-H. Lin, and R.-X. Chang, “A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-server Environment Using Smart Cards,” Expert Systems with Applications, vol. 38, no. 11, pp. 13 863–13 870, 2011.

[21] F. Wen and X. Li, “An Improved Dynamic ID-based Remote User Authentication with Key Agreement Scheme,” Computers & Electrical Engineering, vol. 38, no. 2, pp. 381–387, 2012.

[22] H.-B. Tang and X.-S. Liu, “Cryptanalysis of a Dynamic ID-based Remote User Authentication with Key Agreement Scheme,” International Journal of Communication Systems, vol. 25, no. 12, pp. 1639–1644, 2012.

[23] X. Li, J. Ma,W.Wang, Y. Xiong, and J. Zhang, “A Novel Smart Card and Dynamic ID Based Remote User Authentication Scheme for Multi-server Environments,” Mathematical and Computer Modelling, vol. 58, no. 1-2, pp. 85–95, 2013.

[24] J. Qu and L.-M. Zou, “An Improved Dynamic ID-based Remote User Authentication with Key Agreement Scheme,” Journal of Electrical and Computer Engineering, vol. 2013, p. 17, 2013.

[25] S. H. Islam and G. Biswas, “Dynamic ID-based Remote User Mutual Authentication Scheme with Smartcard Using Elliptic Curve SSCryptography,” Journal of Electronics (China), vol. 31, no. 5, pp. 473–488, 2014.

[26] M. Sarvabhatla and C. S. Vorugunti, “A Secure and Robust Dynamic ID-based Mutual Authentication Scheme with Smart Card Using Elliptic Curve Cryptography,” in Signal Design and its Applications in Communications (IWSDA), 2015 Seventh International Workshop on. IEEE, 2015, pp. 75–79.

[27] H.-Y. Lin, “Efficient Mobile Dynamic ID Authentication and Key Agreement Scheme Without Trusted Servers,” International Journal of Communication Systems, vol. 30, no. 1, p. e2818, 2017.

[28] S. Shunmuganathan, R. D. Saravanan, and Y. Palanichamy, “Secure and Efficient Smart-card-based Remote User Authentication Scheme for Multiserver Environment,” Canadian Journal of Electrical and Computer Engineering, vol. 38, no. 1, pp. 20–30, 2015.