International Research Journal of Advanced Engineering and Science
ISSN: 2455-9024

A Survey on AMUA Protocol Based On Cryptographic Algorithm

Sumeena P S[1], Alpha Vijayan[2]
[1]PG Scholar, Computer Science and Engineering, Mar Baselios Christian College of Engineering & Technology, India
[2]Associate Professor, Computer Science and Engineering, Mar Baselios Christian College of Engineering & Technology, India

***Abstract*—** *Cryptography is the principle and study of techniques for secure communication that is for providing data integrity, authentication, data confidentiality etc….More precisely cryptography is about building and inspecting protocols that provide secure communication between two users. The cryptographic algorithms can be broadly divided into two based on their keys. They are private key cryptographic algorithms which uses the similar secret key for encryption and decryption and public key cryptographic algorithms which uses different keys for encryption and decryption. The mobile devices become rapidly appearing everywhere and popular due to the expeditious advances in wireless communication technologies. Therefore authentication protocol is used between two entities for transfer of authenticated data. One such protocol is the AMUA (Anonymous Mobile User Authentication Protocol) that can provide security of various mobile applications. This paper presents a comprehensive survey of various AMUA protocols based on the cryptographic algorithms used.*

***Keywords*—** *Cryptography, AMUA protocol, authentication, multi-server architectures.*

I. INTRODUCTION

AMUA protocol can resist malicious attacks and it also can reduce the computation and communication costs to a great extend. The traditional single server architecture is inefficient for ensuring the availability of many mobile services. To cope with this issue, there is a need to deploy multi server architectures. So here consider AMUA protocols in the multi server architectures. Based on the cryptographic algorithm used, the AMUA protocols can be divided into public key cryptography based AMUA protocols, private key cryptography based AMUA protocols and Self-Certified Public Key Cryptography (SCPKC) based AMUA protocols.

II. AMUA PROTOCOL CLASSIFICATION

The AMUA Protocols can be classified into three types based on the cryptographic algorithm as shown below.

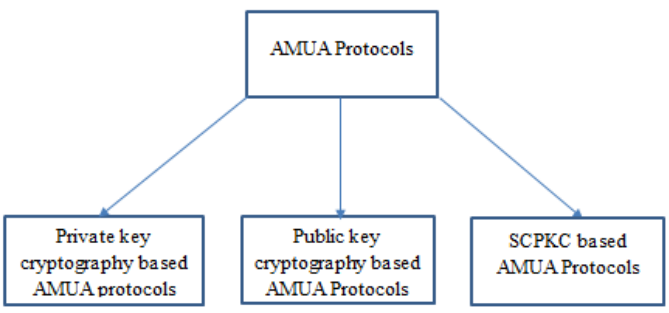

Fig. 1. AMUA Protocol classification.

A. Private Key Cryptography Based AMUA Protocols

The AMUA protocols that uses same key for both encryption and decryption come under this category.

a) Dynamic ID based protocol

An efficient and secure dynamic identity based authentication protocol which uses smart cards is developed here [1]. It is an authentication protocol suitable for multi-server architecture. It can remove the weakness of the previous schemes. It is secure and efficient.

Advantages

- In distributed multi-server architecture it is extremely suitable for use.
- Provide user anonymity and mutual authentication.
- Secure and efficient.

b) Multi-server authentication scheme

A smart card based multi-server authentication scheme which is efficient and secure is introduced by Chuang and Chen [2]. It is used to achieve anonymity and light-weight authentication. It involves a biometric based authentication. The scheme reviews their scheme and find the various attacks on them and introduced in [3]. The scheme can withstand the security weakness found in [2].

Advantages

- Supports mutual authentication.
- Satisfy all desirable security attributes.
- Secure against active and passive attacks.
- Computationally efficient.

Disadvantages

- Energy and communication overhead is high.
- Computation overhead is high.

c) Mining association rules from high utility itemsets

A compressed representation for association rules having maximal consequent and minimal antecedent is introduced in this paper [4]. High Utility Closed Itemsets (HUCI) and their generators are used for the development. With the help of an algorithm, the utility based non redundant methods and association rules for reconstructing all association rules are generated.. There are algorithms such as [5] [6] [7] which generate high utility itemsets. The algorithms are implemented using both real datasets and synthetic datasets.

Advantages

- Efficient and effective.
- Under conditional framework better quality in compressed representation of the entire ruleset.

Disadvantages

Sumeena P S and Alpha Vijayan, "A survey on AMUA protocol based on cryptographic algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 4, pp. 114-116, 2016.

- It does not support negative item utilities.
- It cannot integrate to associative classification model.

d) Password authentication based on biometric scheme

Users register only once and can access arbitrary services using remote authentication for multi-server environment. But security problems arise in most of the solutions. In [8] they combine four technologies such as client puzzle, message authentication code (MAC), fuzzy extractor and Diffie-Hellman key exchange**.**

Advantages

- Preserves user privacy with optimal access mode.
- Work correctly through BAN-logic.
- Secure, robust and practical.

e) Authentication based on robust biometrics

In multi-server environments the biometric authenticated schemes employing smart card is very much important. There are some design flaws in schemes proposed in the past. This paper [9] makes a review of Mishra et al's scheme [10] and analyze the security weakness such as the scheme do not resist replay attack and fails to provide an efficient password change phase.

Advantages

- Strong authentication against several attacks.
- Practical and efficient.
- Robustness of this scheme is more secure.

Disadvantages

- Large scale implementation is little difficult.

B. Public Key Cryptography Based AMUA Protocols

The AMUA protocols that uses different key for both encryption and decryption come under this category.

a) Remote user authentication scheme

To validate the legitimacy of a remote user, a remote user authentication is used. For a single client/server architecture environment privacy and security problems are solved using conventional user authentication schemes. The use of information technology and computer networks is increasing rapidly day by day. This paper presents a new remote user authentication scheme [11]. It is suitable for multi-server environments. In this system there is no need to maintain any verification table, and users registered in server do not need to remember different passwords. The scheme uses Elgamal digital signature scheme.

Advantages

- Can withstand replay and modification attacks.
- Allow users to choose their passwords freely.
- A user can be removed from the system easily.

b) Authentication with key agreement scheme

A new efficient and secure biometric-based multi-server authentication with key agreement scheme suitable for smart cards is presented in [12]. It is done on the elliptic curve cryptosystems without using a verification table. It can fit on to the multi-server communication environments.

Advantages

- Can provide strong user authentication function.
- Provide strong key agreement function.
- Strong security and enhanced computational efficiency.
- Suitable in distributed multi-server network environments.

c) Improvement and cryptanalysis of a biometrics-based scheme

This system [13] reviews the Yoon et al's scheme [14]. The scheme introduced a key agreement scheme using biometrics and elliptic curve cryptosystem for smart cards. Here uses a robust multi-server authentication. The above said scheme is vulnerable to offline password guessing attack. Here introduces a system that can withstand these attacks. Modification are done on the user registration and key agreement phases only.

Advantages

- Can withstand offline password guessing attack.

d) Biometrics based authentication scheme

In an open network environment, the two parties communicating in network should authenticate each other, therefore authentication scheme is an important cryptographic mechanism. Many authentication schemes such as smart cards and using passwords are already available. But they cannot provide high security. There are several biometric based authentication schemes such as remote authentication via biometrics [15], speaker identification [16] etc. This scheme is a three factor authenticated scheme [17].

Advantages

- Satisfy requirements of multi-server environment.
- Overcome the weakness of previous schemes.
- Appropriate for distributed multi-server network environments.

C. SCPKC Based AMUA Protocols

a) Authenticated key agreement which is ID-based

The widely used cryptographic protocols are key agreement protocols. The ID-based authenticated key agreement (AKA) protocol uses bilinear maps. It is sufficient for unstable computing environments. The AKA protocol which is ID-based is for client and server. Here [18] combines two notions that is ID-based authentication and key agreement.

Advantages

- Removes expensive operations: The authentication mechanism allows key sharing and key agreement protocol provides two or more participants to share a key. The AKA protocol achieves these two properties.
- It is possible to simplify key management protocols using ID-based authenticated system.
- Protocol is efficient for low power mobile devices.

b) Novel remote user authentication scheme

It is a novel remote user authentication scheme based on pairing for multi-server environment [19]. Based on SCPKS this scheme first provides a more secure key distribution. The scheme can also achieve session key agreement and mutual authentication with the help of the registration server. The scheme enhances the password change phase to withstand offline dictionary attack.

Advantages

- While maintaining a simple ID table the scheme satisfies all essential requirements.

Sumeena P S and Alpha Vijayan, "A survey on AMUA protocol based on cryptographic algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 4, pp. 114-116, 2016.

- The scheme is well suited for mobile clients.
- Can withstand various possible attacks.

Disadvantages

- The system cannot provide a formal security proof on any cryptographic protocol.

III. CONCLUSION

Depending upon the cryptographic algorithm [20] used AMUA protocols can be classified into three categories. From the survey it is clear that AMUA protocols which uses private key cryptography shows better performance. But they cannot provide perfect forward secrecy and two factor security .Because of this reason public key cryptography based AMUA protocol become popular. But to achieve mutual authentication they need on-line registration center's help. Recently AMUA protocols based on SPCKC is introduced. They need no on-line registration and have lower communication cost. Because of this advantage they are now popular.

REFERENCES

[1] X. Li, Y. Xiong, J. Ma, and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 763–769, 2012.

[2] M. C. Chuang and M. C. Chen, "An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics," *Expert Systems with Applications*, vol. 41, issue 4, pp. 1411–1418, 2014.

[3] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure user anonymity preserving biometric-based multi-server authenticated key agreement scheme using smart cards," *Expert Systems with Applications*, vol. 41, no. 18, pp. 8129–8143, 2014.

[4] J. Sahoo, A. K. Das, and A. Goswami, "An efficient approach for mining association rules from high utility itemsets," *Expert Systems with Applications*, vol. 42, no. 13, pp. 5754–5778, 2015.

[5] Liu, Ying, W. K. Liao, and A. Choudhary, "A two-phase algorithm for fast discovery of high utility itemsets," *Pacific-Asia Conference on Knowledge Discovery and Data Mining*, Springer Berlin Heidelberg, 2005.

[6] Tseng, Vincent S., C.-J. Chu, and T. Liang, "Efficient mining of temporal high utility itemsets from data streams," *Second International Workshop on Utility-Based Data Mining*, vol. 18, 2006.

[7] V. S. Tseng, C.-W. Wu, B.-E. Shie, and P. S. Yu, "UP-Growth: an efficient algorithm for high utility itemset mining," *Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ACM, 2010.

[8] X. Li, Q. Wen, W. Li, H. Zhang, and Z. Jin, "A biometric-based password authentication with key exchange scheme using mobile device for multiserver environment," *Applied Mathematics & Information Sciences*, vol. 9, no. 3, pp. 1123–1137, 2015.

[9] Y. Lu, L. Li, X. Yang, and Y. Yang, "Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards," *PLoS ONE*, vol. 10, no. 5, p. e0126323, 2015.

[10] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards," *Expert Systems with Applications*, 2014.

[11] I.-C. Lin, M.-S. Hwang, and L.-H. Li, "A new remote user authentication scheme for multi-server architecture," *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13–22, 2003.

[12] E.-J. Yoon and K.-Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *The Journal of Supercomputing*, vol. 63, no. 1, pp. 235–255, 2013.

[13] H. Kim, W. Jeon, K. Lee, Y. Lee, and D. Won, "Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme," in *Proc. 12th International Conference Computational Science and Its Applications – ICCSA*, pp. 391–406, 2012.

[14] E. J. Yoon and K. Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *Journal of Supercomputing*, 2010.

[15] K. Ntalianis, and N. Tsapatsoulis, "Remote authentication via biometrics: A robust video-object steganographic mechanism over wireless networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, issue 1, pp. 156-174, 2016.

[16] N. Almaadeed, A. Aggoun, and A. Amira, "Speaker identification using multimodal neural networks and wavelet analysis," *IET Biometrics*, vol. 4, issue 1, pp. 18-28, 2015.

[17] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," *IEEE Systems Journal*, vol. 9, no. 3, pp. 816–823, 2015.

[18] K. Y. Choi, J. Y. Hwang, D. H. Lee, and I. S. Seo, "ID-based authenticated key agreement for low-power mobile devices," in *Proceeding 10th Australasian Conference Information Security Privacy (ACISP)*, pp. 494–505, 2005.

[19] Y.-P. Liao and C.-M. Hsiao, "A novel multi-server remote user authentication scheme using self-certified public keys for mobile clients," *Future Generation Computer Systems*, vol. 29, no. 3, pp. 886–900, 2013.

[20] P. Bali, "Comparative study of private and public key cryptography algorithms: A survey," *International Journal of Research in Engineering and Technology*, vol. 03, issue 09, pp. 191-195, 2014.

Sumeena P S and Alpha Vijayan, "A survey on AMUA protocol based on cryptographic algorithm," *International Research Journal of Advanced Engineering and Science*, Volume 1, Issue 4, pp. 114-116, 2016.