ISSN 2394-739X

IJRSET

International Journal for Research in Science Engineering and Technology

PRIVACY AWARE SECURE AUTHENTICATION SCHEME FOR IOT NETWORKS BASED ON DIGITAL SIGNATURES

[1] D. Priyanka, [2] P. Nisha Priya,
[1] PG Scholar, CSI College of Engineering, Ketti,
[2] Dept of Computer Science & Engineering, CSI College of Engineering, Ketti.

ABSTRACT: Internet of Things (IoT) is a network of all devices that can be accessed through the internet. These devices can be remotely accessed and controlled using existing network infrastructure, thus allowing a direct integration of computing systems with the physical world. This also reduces human involvement along with improving accuracy, efficiency and resulting in economic benefit. In this proposed framework, we present a Hybrid Mechanism as Three Factor, Cryptography digital signature with Double encryption (TF_CDS-DE) for Secure Authentication in IoT Networks. Our Hybrid Mechanism consists of different frameworks. First, we used a new scheme three-factor authentication scheme because it applies the user smart card, password and personal biometrics as three factors. Second, we used Cryptographic key generation from fused features, here a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. Finally, utilize Double encryption Scheme. This encryption provides image data security using cryptographic technique and Confidentiality of data is ensured by use of strong encryption.

Key terms: [Internet of Things, Three-factor authentication, Cryptographic key generation, Double encryption]

1. INTRODUCTION

The Internet of Things (IoT) is an important topic in technology industry, policy, and engineering circles and has become headline news in both the specialty press and the popular media. This technology is embodied in a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible.

An abundance of conferences, reports, and news articles discuss and debate the prospective impact of the "IoT revolution" from new market opportunities and business models to concerns about security, privacy, and technical interoperability.

The smart devices can be remotely accessed and controlled using existing network infrastructure which allows a direct integration of computing systems with the physical world. This facility further reduces human involvement, and also improves accuracy and efficiency that result in economic benefit. Thus, the smart devices in IoT facilitate the day-to-day life of people.

A generic IoT network architecture given in Fig. 1 has four different scenarios (i.e., smart home, transport, and national applications) in which several smart devices, such as sensors and actuators, are installed. In all these scenarios, the smart devices are connected to the Internet through their nearby gateway node (GWN). Several users (i.e., smart home users and doctors) can access the real-time data from some IoT devices.

In this techniques, we present a Hybrid Mechanism as Three Factor, Cryptography digital signature with Double encryption (TF_CDS-DE) for Secure Authentication in IoT Networks. Our Hybrid Mechanism consists of different frameworks. First, we used a new scheme three-factor authentication scheme because it applies the user smart card, password and personal biometrics as three factors. Second, we used Cryptographic key generation from fused features, here a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. Finally, utilize Double encryption Scheme. This encryption provides image data security using cryptographic technique and Confidentiality of data is ensured by use of strong encryption.

2. LITERATURE REVIEW

This section provides the basic significance of security in IoT. It also provides thenumerous methodology to efficiency and privacy aware techniques. This web development has resulted in huge usage of many applications and other service-oriented applications.

Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications -. A new signature-based authenticated key establishment scheme for IoT environment. The proposed scheme is tested for security with the help of the widely-used Burrows-Abadi-Needham logic (BAN logic), informal security analysis, and also the formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The proposed scheme is also implemented using the widely-accepted NS2 simulator, and the simulation results demonstrate the practicability of the scheme.

Flexible data access control in D2D communications -.The important role of trust in securing D2D communications, in this paper, we propose a scheme using either a General Trust (GT) level issued by a core network or a Local Trust (LT) level evaluated by a device or both to control D2D communication data access by applying Attribute-Based Encryption (ABE). This scheme realizes secure data communications among mobile devices under the legacy system model of Long-Term Evolution (LTE). Performance analysis and evaluation demonstrate that the proposed scheme is effective with regard to security, computation complexity, communication cost, flexibility and scalability.

A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes- an improved energy-efficient, secure, and privacy-preserving communication protocol for the smart home systems. In our proposed scheme, data transmissions within the smart home system are secured by a symmetric encryption scheme with secret keys being generated by chaotic systems. Meanwhile, we incorporate Message Authentication Codes (MAC) to our scheme to guarantee data integrity and authenticity. We also provide detailed security analysis and performance evaluation in comparison with our previous work in terms of computational complexity, memory cost, and communication overhead.

A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. -The real-time data can be given access directly to the external users (parties) those who are authorized to access data as and when they demand. The user authentication plays a vital role for this purpose. In this paper, we propose a new password-based user authentication scheme in hierarchical wireless sensor networks. Our proposed scheme achieves better security and efficiency as compared to other existing password-based approaches. In addition, our scheme has merit to change dynamically the user’s password locally without the help of the base station or gateway node.

End-to-End Authentication in Under-Water Sensor Networks - Under-Water Wireless Sensor Networks (UWSNs) are a particular class of Wireless Sensor Networks (WSNs) in which sensors are located, as the name suggests, underwater.Applications of UWSNs range from oceanographic data collection to disaster prevention. UWSNs are vulnerable to attacks and because of their idiosyncrasies; security solutions for ground WSNs might not be applicable underwater. As a result, there is a need for mechanisms exclusively tailored to underwater environments.

In this work we address the problem of authentication in UWSNs. We evaluate energy costs for different digital signature schemes for end-to-end authentication and discuss the trade-off involved in a number of scenarios. Our results show that schemes that perform well in ground WSN do not necessarily do well in UWSNs; and shed light on characteristics of a digital signature scheme that make them particularly suited to underwater networks.

3. METHODOLOGIES

We present a Hybrid Mechanism as Three Factor, Cryptography digital signature with Double encryption (TF_CDS-DE) for Secure Authentication in IoT Networks. Our Hybrid Mechanism consists of different frameworks. First, we used a new scheme three-factor authentication scheme because it applies the user smart card, password and personal biometrics as three factors. Second, we used Cryptographic key generation from fused features, here a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. Finally, utilize Double encryption Scheme. This encryption provides image data security using cryptographic technique and Confidentiality of data is ensured by use of strong encryption.

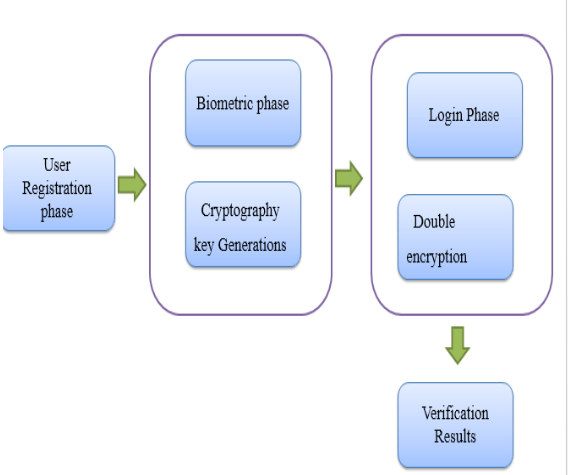


Figure 3.1 Block Diagram of Proposed work

3.1 User Registration Phase

To access the real-time information from the sensing nodes SNk , the registration process of a user Ui is required at the GWN . This phase requires the following steps:

Step REG1. - Ui picks a unique identity ID I and also a password P Wi on his/her choice. Ui then generates a 128-bit random secret r a , computes the masked password RP Wi = h(P Wi ||r a).

Step REG2. -After receiving hIDi , RP W i i from Ui , GWN calculates temporary identity of Ui as RIDi = h(ID I ||Ks) and temporal credential of Ui as T C Ui = h(ID I ||IDGWN ||Ks) using the 160-bit long random secret key Ks already chosen by the GWN in Section III-A

Step REG3. - After receiving SCi from GWN , once Ui imprints his/her personal biometrics , SCi is ready to compute secret signature i and public parameter τ i with the help of the fuzzy extractor probabilistic generation function as Gen(BIOi) = (σ I , τ i).

3.2 Password and Biometric Update Phase

A legitimate user Ui can update password as well as biometric information at any time completely locally without involving the GWN as and when it is required. The required steps are discussed below:

Step PB1. After inserting SCi into the card reader, Ui supplies ID I and old password P old I . Ui also imprints old biometric information BIO old I at the sensor of the same terminal.

Step PB2. After receiving the instruction from SCi ,Ui inputs a new password P W new I and also imprints new biometrics BIO new I .

On the other hand, both the back ends verify if any man-in-the middle attack possible by the intruder for the Dolev-Yao model checking. In UAKMP, all the three verifications, such as excitability checking on non-trivial HLPSL specifications.

Replay attack checking and Dolev-Yao model checking are satisfied. Hence, the replay & man-in-the-middle attacks are protected in UAKMP.

3.3 Cryptography Digital signatures

A digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party. Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

Cryptographic key generation from fused features

In key generation consider two prime numbers (i.e.) p and q. it consists of public key and a private key. The public key will be known to everyone. Calculate the value of n. select a random encryption key e calculates the GCD and it should be equal to 1. In key generation consider two prime numbers (i.e.) p and q. it consists of public key and a private key. The public key will be known to everyone. Then find the decryption key d. finally calculate the public key and private key.

The key generation steps are

1. Generate two different primary keys P and Q
2. Calculate the module n=p*q
3. Calculate the $(n)=(p-1)\times(q-1)$
4. Select the public exponent an integer e such that $1<e<(n)$ and $GCD(\varphi(n),e)=1$
5. Calculate the private exponent a value of d such that $d=e$^$(-1)\ mod \varphi(n)$
6. Public key =[e, n]
7. Private key =[d, n]

3.4 Double encryption

Double encryption provides image data security using cryptographic technique. Confidentiality of data is ensured by use of strong encryption. Image is divided into blocks than permuted and at last gets encrypted then saved to the disk or send onto the network. By using Public-Key cryptographic technique, it is used to control the access of the file.

In this section, double encryption provides image data security using cryptographic technique. Confidentiality of data is ensured by use of strong encryption.

Image is divided into blocks than permuted and at last gets encrypted then saved to the disk or send onto the network. By using Public-Key cryptographic technique, it is used to control the access of the file. This approach enhances the security of file by avoiding unwarranted access.

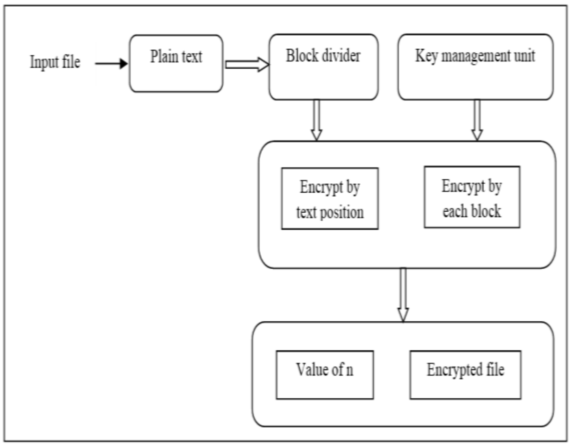


Figure 2.2 Double encryption

3.5 Login Phase

Once the registration process is completed, a user Ui is now ready to login in the system using the supplied smart card SCi with the following steps:

Step L1. - After the identity ID I , password P Wi are entered and biometric information BIO ∗ I a the sensor of the card reader are imprinted by Ui , SCi proceeds to recover secret biometric key as σ ∗ I = Rep(BIO ∗ I , τ i) provided that the Hamming distance between the current entered BIO ∗ I & the original biometrics BIOi at registration time is less than or equal to the threshold value t.

Step L2. - SCi further calculates r ∗ a = BIi⊕h(ID I ||σ ∗ I), RP W ∗ I = h(P Wi || r ∗

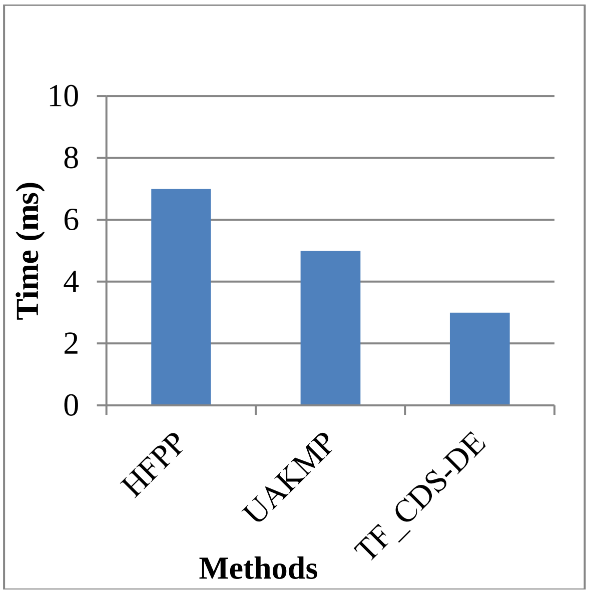
a), CI ∗ I = h(ID I ‖RP W ∗ I ‖σ ∗ I), ID ∗ GWN = ID 0 GWN ⊕h(ID I ‖σ ∗ I), T C ∗Ui = Bi ⊕ h(RP W ∗ ‖ID ∗ GWN), RID ∗ I = RID 0 I ⊕ h(ID ∗ GWN ‖σ ∗ I), RID ∗∗ = h(RID ∗ I ‖T 1), C ∗ I = h(T C ∗Ui ‖RP W ∗ I ‖ID i) and D ∗ I = h(CI ∗ I ‖C ∗ I) and checks whether D ∗ I = Di .

Step L3. -. Using secrete signature to steps are performed login and access the data. This formation is determined at the time of user registration.

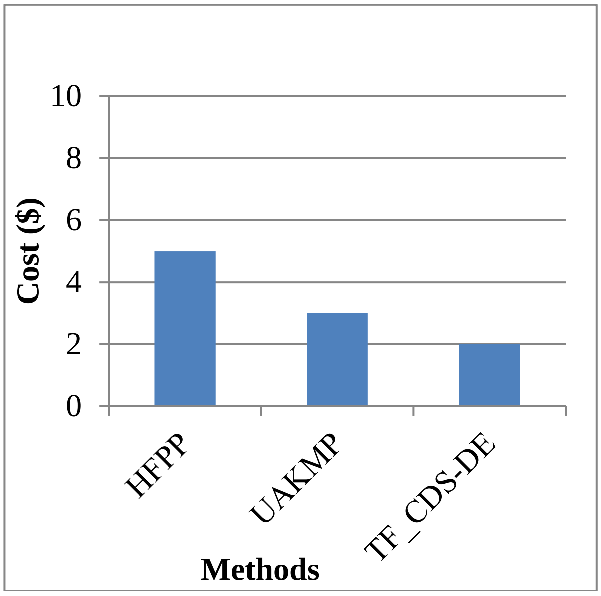
4. RESULTS

In this section, the overall setup of our experiment and the results obtained from it is described to validate the proposed Hybrid Mechanism as Three Factor, Cryptography digital signature with Double encryption (TF_CDS-DE). In our experiment, two well-known workflow applications, user authenticated key management protocol (UAKMP)and Hash Function based Privacy Preserving (HFPP), are chosen as test cases.

4.1 Communication Time



4.2 Communication Cost



CONCLUSION

In this chapter, we present a Hybrid Mechanism as Three Factor, Cryptography digital signature with Double encryption (TF_CDS-DE) for Secure Authentication in IoT Networks. Our Hybrid Mechanism consists of different frameworks. First, we used a new scheme three-factor authentication scheme. Second, we used Cryptographic key generation from fused features,this binding can be independently verified by receiver as well as any third party. Finally, utilize Double encryption Scheme. This encryption provides image data security using cryptographic technique and Confidentiality of data is ensured by use of strong encryption.

The proposed Hybrid Mechanism TF_CDS-DEcan find out better non-dominated secure and privacy solutions effectively, which has been proved by experiences. The experimental results show that the algorithm can achieve better solutions than other ones.

Future, investigate privacy aware efficient communication of intermediate data sets in IoT by taking privacy preserving as a metric together with other metrics such as storage and computation. Optimized balanced communication strategies are expected to be developed toward overall highly efficient privacy aware data set communication in IoT.

REFERENCES

[1] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," IEEE Access, vol. 5, pp. 3028– 3043, 2017.

[2] Z. Yan, H. Xie, P. Zhang, and B. B. Gupta, "Flexible data access control in D2D communications," Future Generation Computer Systems, 2017, DOI: 10.1016/j.future.2017.08.052.

[3] M. Wang, Z. Yan, and V. Niemi, "UAKA-D2D: Universal Authentication and Key Agreement Protocol in D2D Communications," Mobile Networks and Applications, vol. 22, no. 3, pp. 510–525, 2017.

[4] N. Khalil, M. R. Abid, D. Benhaddou, and M. Gerndt, "Wireless sensors networks for Internet of Things," in IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, 2014, pp. 1–6.

[5] I. M. Khalil, Y. Gadallah, M. Hayajneh, and A. Khreishah, "An adaptive OFDMA-based MAC protocol for underwater acoustic wireless sensor networks," Sensors, vol. 12, no. 7, pp. 8782–8805, 2012.

[6] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," Ad Hoc Networks, vol. 3, no. 3, pp. 257–279, 2005.

[7] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes," IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2707489.

[8] A. Stefanov and M. Stojanovic, "Hierarchical underwater acoustic sensor networks," in Proceedings of the Fifth ACM International Workshop on Under Water Networks. Woods Hole, USA: ACM, 2010, pp. 10:1–10:4.

[9] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," Journal of Network and Computer Applications, vol. 35, no. 5, pp. 1646 – 1656, 2012.

[10] E. Souza, H. C. Wong, I. Cunha, A. A. F. Loureiro, L. F. M. Vieira,and L. B. Oliveira, "End-to-end authentication in Under-Water Sensor Networks," in IEEE Symposium on Computers and Communications (ISCC), Split, Croatia, 2013, pp. 000 299–000 304.

[11] C. Lal, R. Petroccia, M. Conti, and J. Alves, "Secure Underwater Acoustic Networks: Current and Future Research Directions," in Proceedings of IEEE/NATO Underwater Communications and Networking (UComm2016), La Spezia, Italy, 2016.

[12] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 9, no. 1, pp. 223–244, 2016.

[13] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," Future Generation Computer Systems, vol. 63, pp. 56 – 75, 2016.

[14] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credentialbased mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," Information Sciences, vol. 321, 2015.

[15] C. T. Li, C. Y. Weng, and C. C. Lee, "An Advanced Temporal CredentialBased Security Scheme with Mutual Authentication and Key Agreement for Wireless Sensor Networks," Sensors, vol. 13, no. 8, pp. 9589–9603, 2013.

[16] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Twophase authentication protocol for wireless sensor networks in distributed IoT applications," in IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, Turkey, 2014, pp. 2728–2733.

[17] M. Turkanovic, B. Brumen, and M. Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensornetworks, based on the

Internet of Things notion," Ad Hoc Networks,vol. 20, pp. 96 – 112, 2014.

[18] C. C. Chang and H. D. Le, "A Provably Secure, Efficient and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks," IEEE Transactions on Wireless Communications, vol. 15, no. 1, 2016.

[19] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," Security and Communication Networks, vol. 9, no. 16, pp. 3670–3687, 2016.

[20] D. Dolev and A. C. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.

[21] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 51, no. 5, pp. 541–552, 2002.

[22] P. Sarkar, "A simple and generic construction of authenticated encryption with associated data," ACM Transactions on Information and System Security, 2010.

[23] S. Wu and K. Chen, "An Efficient Key-Management Scheme for Hierarchical Access Control in E-Medicine System," Journal of Medical Systems, vol. 36, no. 4, 2012.

[24] "Advanced Encryption Standard (AES)," FIPS PUB 197, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Accessed on April 2016.

[25] 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.