An Efficient Biometric-Based Secure Access Mechanism for Cloud Services

A Vijay[1], B Srinivasulu[2]
[1]Dept of CSE
[2]Associate Professor and HOD, Dept of CSE
[1, 2] SIT, PUTTUR

Abstract- *The demand for remote data storage and computation services is increasing exponentially in our data-driven society; thus, the need for secure access to such data and services. In this paper, we design a new biometric-based authentication protocol to provide secure access to a remote (cloud) server. In the proposed approach, we consider biometric data of a user as a secret credential. We then derive a unique identity from the user's biometric data, which is further used to generate the user's private key. In addition, we propose an efficient approach to generate a session key between two communicating parties using two biometric templates for a secure message transmission. In other words, there is no need to store the user's private key anywhere and the session key is generated without sharing any prior information. A detailed Real-Or- Random (ROR) model based formal security analysis, informal (non-mathematical) security analysis and also formal security verification using the broadly-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool reveal that the proposed approach can resist several known attacks against (passive/active) adversary. Finally, extensive experiments and a comparative study demonstrate the efficiency and utility of the proposed approach.*

Keywords- Authentication, biometric-based security, cloud service access, session key.

I. INTRODUCTION

Loud services are a norm in our society. However, providing secure access to cloud services is not a trivial task, and designing robust authentication, authorization and ac- counting for access is an ongoing challenge, both operationally and research-wise. A number of authentication mechanisms have been proposed in the literature, such as those based on Kerberos [1], OAuth [2] and OpenID [3] (see [1], [4]– [12]). Generally, these protocols seek to establish a secure delegated access mechanism among two communicating en- tities connected in a distributed system. These protocols are based on the underlying assumption that the remote server responsible for authentication is a trusted entity in the network. Specifically, a user first registers with a remote server. This is needed to ensure the authorization of the owner. When a user wishes to access a server, the remote server authenticates the user and the user also authenticates the server. Once both verifications are successfully carried out, the user obtains access to the services from some remote server.

One key limitation in existing authentication mechanisms is that the user's credentials are stored in the authentication server, which can be stolen and (mis)used to gain unauthorized access to various services. Also, to ensure secure and fast communication, existing mechanisms generally use symmetric key cryptography, which requires a number of cryptographic keys to be shared during the authentication process. This strategy results in an overhead to the authentication protocols. Designing secure and efficient authentication protocols is challenging, as evidenced by the weaknesses revealed in the published protocols of Jiang et al. [13], Althobaiti et al. [14], Xue et al. [15], Turkanovic et al. [16], Park et al. [17], Dhillon and Kalra [18], Kaul and Awasthi [19] and Kang et al. [20] – see also Section II. Therefore, in this paper we seek to design a secure and efficient authentication protocol. Specifically, we will first provide an alternative to conventional password-based authentication mechanism. Then, we demonstrate how one can build a secure communication between communicating parties involved in the authentication protocol, without having any secret pre-loaded (i.e., shared) information.

In the proposed approach, we consider a fingerprint image of a user as a secret credential. From the fingerprint image, we generate a private key that is used to enroll the user's credential secretly in the database of an authentication server. In the authentication phase, we capture a new biometric fingerprint image of the user, and subsequently generate the private key and encrypt the biometric data as a query. This queried biometric data is then transmitted to the authentication server for matching with the stored data. Once the user is authenticated successfully, he/she is ready to access his/her service from the desired server. To obtain secure access to the service server, mutual authentication between the user and authentication server, and also between the user and service server have been proposed using a short-term session key. Using two fingerprint data, we present a fast and robust approach to generate the session key. In addition, a biometric-based message authenticator is also generated for message authenticity purpose.

We summarize the key contributions/benefits related to the proposed approach as below.

1) An effective way to transmit the user's biometric data through the unsecured network channels to an authentication server is presented.
2) We propose an approach to generate a revocable private key directly from an irrevocable fingerprint image. There is no need to store the private key or a direct form of the user's biometric data anywhere.
3) We mitigate the limitation in traditional mechanisms that require the user's credentials to be stored in the authentication server.
4) We introduce a novel way to generate session keys.
5) In traditional authentication protocol, each entity requires some preloaded information; thus, incurring some overhead. We introduce a new mechanism to avoid the need for secret pre-loaded information.
6) A message authentication mechanism, as an alternative to the existing message authentication protocols (i.e., Message Authentication Code (MAC)), is introduced.

In the next section, we will review existing biometric- based authentication schemes, prior to presenting the proposed biometric-based authentication approach in Section III. We then evaluate the performance and security of the proposed protocol in Sections IV and V, respectively. Specifically, we demonstrate that the protocol is secure in the presence of a Dolev-Yao (DY) adversary [21]. Then, a comparative study is presented in Section VI. Finally, Section VII concludes the paper.

II. RELATED WORK

In this section, we mainly discuss existing biometric-based user authentication schemes that have been presented in the literature.

Based on the authentication types and factors being used, the user authentication protocols can be classified into three categories: 1) single-factor, 2) two-factor and 3) three-factor. In a single-factor authentication protocol, only one factor can be used (for example, user's smart card/mobile device or pass- word or personal biometrics). In a two-factor authentication scheme, the user's smart card or mobile device and password can be used. On the other hand, in a three-factor authentication scheme, the user's smart card/mobile device, password and biometrics can be used.

Jiang et al. [13] designed a password based user authenti- cation scheme for wireless sensor networks (WSNs). This is a two-factor authentication scheme as it relies on both a smart card and some password. During the user registration process, an authorized user registers or re-registers with the trusted gateway node (GWN). The GWN then issues a smart card having the relevant credentials that are stored on the smart card. In addition, all the deployed sensor nodes are registered through a secure channel with the GWN and obtain their respective secret credentials. Using the pre-loaded credentials, a legitimate user authenticates with a designated sensor node with the help of the GWN during the login and authentication phases. However, Das [22] later showed that this particular scheme is vulnerable to privileged insider attacks, where an internal user of the trusted authority (i.e., an insider attacker) having the registration information of a registered user can mount other attacks in the system, such as user impersonation attacks. Moreover, it was also shown that this scheme does not provide proper authentication, and fails to support new sensor node deployment in a target field. As a countermeasure, Das [22] presented an improved and efficient three factor authentication scheme, where the three factors are a smart card, the user's password and the user's personal biometrics. However, the scheme proposed by Das [22] does not preserve sensor node anonymity.

Althobaiti et al. [14] proposed a biometric-based user au- thentication mechanism for WSNs. However, their scheme is insecure against impersonation attacks and man-in-the-middle attacks [23]. Das [23] then proposed a new biometric-based user authentication approach. Xue et al. [15] also designed a temporal-credential-based mutual authenticated key agreement mechanism for WSNs. In their scheme, the remote authorized users are permitted to access authorized sensor nodes in order to obtain information and also to send some important commands to the sensor nodes in WSN. In this scheme, the GWN issues temporal credentials to each user and sensor node deployed in WSN with the help of the password-based authentication mechanism. Later, Li et al. [24] demonstrated that Xue et al.'s scheme fails to resist stolen-verifier, off- line password guessing, insider, many logged-in users, and smart card lost attacks. He et al. [25] also demonstrated that Xue et al.'s scheme is insecure against user impersonation, off-line password guessing, modification and sensor node impersonation attacks.

Turkanovic and Holbl [26], and Turkanovic et al. [16] proposed other user authenticated key agreement approaches. However, Turkanovic et al.'s scheme [16] is insecure against smart card theft, offline password guessing, user imperson- ation, offline identity guessing, and sensor node impersonation attacks [27]. Park et al. [17] designed a privacy-preserving biometric-based user authentication mechanism using smart card, which uses hashing operation for biometric verification. However, the scheme is insecure against denial-of-service (DoS) attacks [28].

Dhillon and Kalra [18] designed a biometric based user authenticated key agreement mechanism for secure access to services provided by Internet of Things (IoT) devices. Though this scheme uses lightweight operations, it does not protect against DoS attacks as it uses the perceptual hashing (biohashing) operation instead of fuzzy extractor [28]. This is primarily because the biohashing technique hardly creates a unique value BH(BIOi) from the biometric data BIOi of a legitimate user Ui at different input times though it may reduce output error [28], where BH( ) is the biohashing function. Kaul and Awasthi [19] designed an authenticated key agreement scheme, but it was later revealed to be insecure against user impersonation and off-line password guessing attacks [20]. In addition, the scheme of Kaul and Awasthi [19] does not preserve user anonymity. Therefore, Kang et al. [20] proposed an enhanced bioemtric-based user authentication scheme. However, this scheme is insecure against DoS attacks and also impersonation attacks where a privileged-insider attacker can easily mount such an attack.

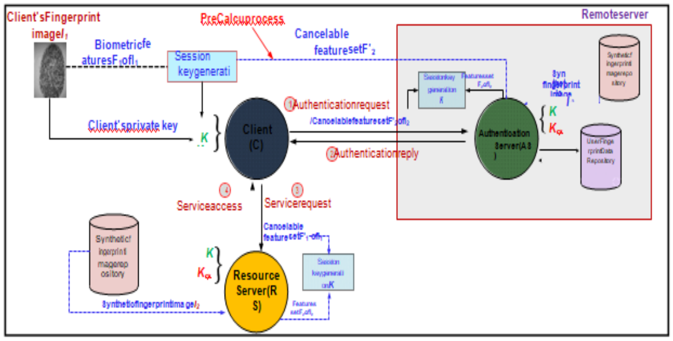
Client'sFingerprint imageI_1
PreCalcuprocess
Cancelable featuresetF'$_2$
Remoteserver
Biometricfe aturesF$_1$ofI$_1$
Session keygenerati
Synthetic fingerprint imagerepository
Sessionkey generation K
Featureset F_2ofI_2
Syn fingerprint image
Authenticationrequest
/CancelablefeaturesetF'$_2$ofI$_2$
Client'sprivate key
K
Client (C)
Authentication Server(AS)
K
K_{α}
UserFingerprintData Repository
Authenticationreply
Serviceaccess
Servicerequest
Synthetic fingerprint imagerepository
Cancelable featuresetF'$_1$ofI$_1$
K
K_{α}
Resource Server(RS)
Session keygeneration K
SyntheticfingerprintimageI$_2$
Features setF$_2$ofI$_2$

Fig.1:The proposed BioCAP: An overview

Xia et al. [29] designed a local descriptor, called the Weber local binary, to facilitate fingerprint liveness detection. Their mechanism is based on Support Vector Machine (SVM). In another work, Yuan et al. [30] introduced a binary pattern (BP) neural network, which replies on fingerprint liveness detection. In their approach, the Laplacian operator is applied to obtain the image gradient values. After that, different parameters for the BP neural network are tested in order to attain superior detection precision. We refer the interested reader to [31] for a comprehensive literature review of fingerprint-based biometric authentication methods.

Huang et al. [32] introduced two different specific security threats based on the smart-card-based password authentication mechanisms for distributed system. In their system, a user needs valid smart card and corresponding password to have a successful authentication. They also considered two different adversaries: first one is an adversary having pre-computed data stored in smart card and second one is an adversary having with different data stored in smart card.

Wang and Wang [33] introduced different property of user privacy perversion in two-factor authentication schemes for wireless sensor networks (WSNs). They designed two different representative schemes to reveal the challenges and subtleties in designing two-facto authentication for privacy preserving for WSNs. They also introduced a game-based security model for two-factor authentication.

Wang et al. [34] proposed three different identity-based user authentication schemes to reveal the challenges in authentica- tion schemes for mobile devices. They also considered session- specific temporary information attack, impersonation attack and also poor usability. Several other authentication protocols [35], [36], [37], [38] have been also proposed in the literature to provide the security in wireless sensor networks and mass storage devices.

III. THE PROPOSED PROTOCOL

In this section, we first discuss about the system model and threat model used in the proposed biometric-based authentica- tion protocol (BioCAP), prior to presenting the various phases in BioCAP.

A. System Model

An overview of BioCAP is shown in Fig. 1, which comprises three entities. These entities are client(s) (C), authentication server(s) (AS) and some resource server (RS). AS contains a database of users' registered data, while AS generates RS's private key during the deployment phase and it is shared between AS and RS. In addition, both AS and RS include a large repository of a similar set of synthetic fingerprint images. Some synthetic fingerprint databases, such as some publicly available databases, are used in the proposed approach.

When C wishes to access a service from RS, C first sends an authentication request to AS. AS verifies C's request and sends a reply message to C upon successful verification. Once C obtains the authentication reply message, C sends a service request to RS for getting the access. RS then verifies the service request. If the service request is verified

successfully, RS sends a reply to C. C and RS mutually authenticate each other. A session key between C and AS, and C and RS are used for subsequent secure message communications. Further, the message authenticity is controlled by a message authenticator. BioCAP has two key processes, namely: user registration and user authentication. The user registration requires private key generation, whereas user authentication requires genera- tion of the session key and the message authenticator. BioCAP provides a provision to rollover the private key of a user. In addition, BioCAP is secure, computationally less expensive, and overcomes the inherent weaknesses of biometric verifi- cation. Moreover, BioCAP does not need pre-shared keys, and provides smooth mutual authentication mechanism and demands less number of keys to be managed from application
and user point of view.

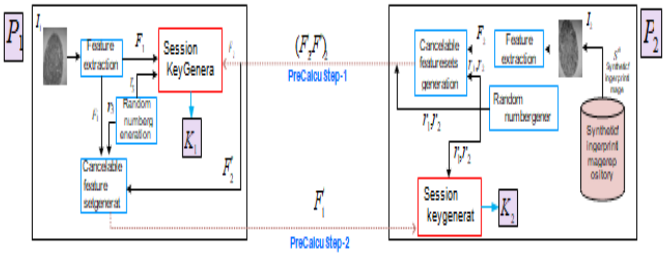

Fig.2:PreCalcu process

V. SECURITY ANALYSIS

We will now demonstrate the robustness of BioCAP with respect to different known attacks using both formal and infor- mal security analysis. In addition, we use the widely-accepted a"Automated Validation of Internet Security Protocols and Applications (AVISPA)" tool [46] to show that BioCAP is secure against replay and man-in-the-middle attacks.

A. Formal Security Analysis Using Real-Or-Random (ROR) Model

In recent years, the Real-Or-Random (ROR) model [47], [48] based formal security analysis has become very popular word and token-based security system, as evidenced by its increased adoption (e.g., on Android and iOS devices).
In this paper, we introduced a biometric-based mechanism to authenticate a user seeking to access services and com- putational resources from a remote location. Our proposed approach allows one to generate a private key from a finger- print biometric reveals, as it is possible to generate the same key from a fingerprint of a user with 95.12% accuracy. Our proposed session key generation approach using two biometric data does not require any prior information to be shared. A comparison of our approach with other similar authentication protocols reveals that our protocol is more resilient to several known attacks.

Future research includes exploring other biometric traits and also multi-modal biometrics for other sensitive applications (e.g., in national security matters).

ACKNOWLEDGMENTS

The authors are grateful to the reviewers and the Associate Editor for their invaluable feedback. The corresponding author was supported in part by the National Science Foundation (NSF) Centers of Research Excellence in Science and Tech- nology (CREST) under Grant HRD-1736209.

REFERENCES

[1] C. Neuman, S. Hartman, K. Raeburn, "The kerberos network authenti- cation service (v5)," RFC 4120, 2005.
[2] "OAuth Protocol." [Online]. Available: http://www.oauth.net/
[3] "OpenID Protocol." [Online]. Available: http://openid.net/
[4] G. Wettstein, J. Grosen, and E. Rodriguez, "IDFusion: An open archi- tecture for Kerberos based authorization," Proc. AFS and Kerberos Best Practices Workshop, June 2006.
[5] A. Kehne, J. Schonwalder, and H. Langendorfer, "A nonce-based pro- tocol for multiple authentications," ACM SIGOPS Operating System Review, vol. 26, no. 4, pp. 84–89, 1992.
[6] B. Neuman and S. Stubblebine, "A note on the use of timestamps as nonces," Oper. Syst. Rev., vol. 27, no. 2, pp. 10–14, 1993.
[7] J. Astorga, E. Jacob, M. Huarte, and M. Higuero, "Ladon : end- to-end authorisation support for resource-deprived environments," IET Infomration Security, vol. 6, no. 2, pp. 93–101, 2012.
[8] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," Washington D.C., USA, October 2003, pp. 62–72.
[9] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks," ACM Wireless Networking, vol. 8, no. 5, pp. 521–534, 2002.
[10] P. Kaijser, T. Parker, and D. Pinkas, "SESAME: The solution to security for open distributed systems," Computer Communications, vol. 17, no. 7, pp. 501–518, 1994.

[11] G. Wettstein, J. Grosen, and E. Rodriguez, “IDFusion: An open archi- tecture for Kerberos based authorization,” Proc. AFS and Kerberos Best Practices Workshop, June 2006.

[12] M. Walla, “Kerberos explained,” Windows 2000 Advantage Magazine, 2000.

[13] Q. Jiang, J. Ma, X. Lu, and Y. Tian, “An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks,” Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1070–1081, 2015.

[14] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, “An efficient biomet- ric authentication protocol for wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 2013, pp. 1–13, 2013, Article ID 407971, http://dx.doi.org/ 10.1155/2013/407971.

[15] K. Xue, C. Ma, P. Hong, and R. Ding, “A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 316 – 323, 2013.

[16] M. Turkanovic, B. Brumen, and M. Holbl, “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion,” Ad Hoc Networks, vol. 20, pp. 96 – 112, 2014.

[17] M. Park, H. Kim, and S. Lee, “Privacy Preserving Biometric-Based User Authentication Protocol Using Smart Cards,” in 17th International Con- ference on Computational Science and Engineering, Chengdu, China, 2014, pp. 1541–1544.

[18] P. K. Dhillon and S. Kalra, “A lightweight biometrics based remote user authentication scheme for IoT services,” Journal of Information Security and Applications, vol. 34, pp. 255 – 270, 2017.

[19] S. D. Kaul and A. K. Awasthi, “Security Enhancement of an Improved Remote User Authentication Scheme with Key Agreement,” Wireless Personal Communications, vol. 89, no. 2, pp. 621–637, 2016.

[20] D. Kang, J. Jung, H. Kim, Y. Lee, and D. Won, “Efficient and Secure Biometric-Based User Authenticated Key Agreement Scheme with Anonymity,” Security and Communication Networks, vol. 2018, pp. 1–14, 2018, Article ID 9046064, https://doi.org/10.1155/2018/9046064.

[21] 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.

[22] 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.

[23] “A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor,” International Journal of Communication Systems, vol. 30, no. 1, pp. 1–25, 2017.

[24] C. T. Li, C. Y. Weng, and C. C. Lee, “An advanced temporal credential- based security scheme with mutual authentication and key agreement for wireless sensor networks,” Sensors, vol. 13, no. 8, pp. 9589–9603, 2013.

[25] D. He, N. Kumar, and N. Chilamkurti, “A secure temporal-credential- based mutual authentication and key agreement scheme for wireless sensor networks,” in International Symposium on Wireless and pervasive Computing (ISWPC), Taipei, Taiwan, 2013, pp. 1–6.

[26] M. Turkanovic and M. Holbl, “An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks,” ELEKTRONIKA IR ELEKTROTECHNIKA, vol. 19, no. 6, pp. 109 – 116, 2013.

[27] R. Amin and G. P. Biswas, “A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks,” Ad Hoc Networks, vol. 36, pp. 58–80, 2016.

[28] C.-C. Chang and N.-T. Nguyen, “An Untraceable Biometric-Based Multi-server Authenticated Key Agreement Protocol with Revocation,” Wireless Personal Communications, vol. 90, no. 4, pp. 1695–1715, 2016.

[29] Z. Xia, C. Yuan, R. Lv, X. Sun, N. N. Xiong, and Y. Shi, “A Novel Weber Local Binary Descriptor for Fingerprint Liveness Detection,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, doi: 10.1109/TSMC.2018.2874281.

[30] C. Yuan, X. Sun, and Q. M. J. Wu, “Difference co-occurrence matrix using BP neural network for fingerprint liveness detection,” Soft Com- puting, vol. 23, no. 13, pp. 5157–5169, 2019.

[31] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, “Security and Accuracy of Fingerprint-Based Biometrics: A Review,” Symmetry, vol. 11, no. 2, 2019. [Online]. Available: https://www.mdpi.com/2073-8994/11/2/141

[32] X. Huang, X. Chen, J. Li, Y. Xiang, and L. Xu, “Further Observa- tions on Smart-Card-Based Password-Authenticated Key Agreement in Distributed Systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, pp. 1767–1775, 2014.

[33] D. Wang and P. Wang, “On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions,” Computer Networks, vol. 73, pp. 41 – 57, 2014.

[34] D. Wang, H. Cheng, D. He, and P. Wang, “On the Challenges in Designing Identity-Based Privacy-Preserving Authentication Schemes for Mobile Devices,” IEEE Systems Journal, vol. 12, no. 1, pp. 916–925, 2018.

[35] D. He, S. Zeadally, N. Kumar, and J. Lee, “Anonymous Authentication for Wireless Body Area Networks With Provable Security,” IEEE Systems Journal, vol. 11, no. 4, pp. 2590–2601, 2017.

[36] D. He, N. Kumar, J. Lee, and R. S. Sherratt, “Enhanced three-factor security protocol for consumer USB mass storage devices,” IEEE Transactions on Consumer Electronics, vol. 60, no. 1, pp. 30–37, 2014.

[37] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, “Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks,” Multimedia Systems, vol. 21, no. 1, pp. 49–60, 2015.

[38] D. He, N. Kumar, and N. Chilamkurti, “A secure temporal-credential- based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks,” Information Sciences, vol. 321, pp. 263 – 277, 2015.

[39] R. Johannesson and K. S. Zigangirov, Fundamentals of Convolutional Coding, 2nd ed. Wiley-IEEE Press, 2015.

[40] G. Panchal and D. Samanta, “A novel approach to fingerprint biometric- based cryptographic key generation and its applications to storage security,” Computers & Electrical Engineering, vol. 69, pp. 461–478, 2018.

[41] “Secure Hash Standard,” FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. Accessed on January 2019.

[42] J. Katz and Y. Lindell, Introduction to Modern Cryptography, Chapter 6. New York, USA: CRC Press, Taylor & Francis Group.

[43] FVC2004 Fingerprint Databases. [Online]. Available: http://bias.csr. unibo.it/fvc2004/Downloads

[44] “NIST Special Database 4 (Fingerprint),” Dec. 2013. [Online]. Available: http://www.nist.gov/srd/nistsd4.cfm

[45] R. Brown, “Dieharder: A random number test suite,” August 2019. [Online]. Available: https://webhome.phy.duke.edu/∼rgb/General/ dieharder.php

[46] AVISPA, “Automated Validation of Internet Security Protocols and Ap- plications,” 2019, http://www.avispa-project.org/. Accessed on February 2019.

[47] R. Canetti and H. Krawczyk, “Analysis of key-exchange protocols and their use for building secure channels,” in International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT’01). Innsbruck (Tyrol), Austria: Springer, 2001, pp. 453–474.

[48] “Universally Composable Notions of Key Exchange and Secure Channels,” in International Conference on the Theory and Applica- tions of Cryptographic Techniques– Advances in Cryptology (EURO- CRYPT’02), Amsterdam, The Netherlands, 2002, pp. 337–351.

[49] J. Srinivas, A. K. Das, N. Kumar, and J. Rodrigues, “Cloud Centric Authentication for Wearable Healthcare Monitoring System,” IEEE Transactions on Dependable and Secure Computing, 2018, DOI: 10.1109/TDSC.2018.2828306.

[50] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, “Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things,” IEEE Transactions on Dependable and Secure Computing, 2018, DOI: 10.1109/TDSC.2018.2857811.

[51] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, “Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks,” IEEE Internet of Things Journal, vol. 5, no. 1, pp. 269–282, Feb 2018.

[52] C. Chang and H. Le, “A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks,” IEEE Transactions on Wireless Communications, vol. 15, no. 1, pp. 357–366, 2016.

[53] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo, “Chaotic Map-Based Anonymous User Authentication Scheme With User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2884–2895, Aug 2018.

[54] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, “Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment,” IEEE Transactions on Dependable and Secure Computing, 2017, doi: 10.1109/TDSC.2017.2764083.

[55] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, “Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment,” IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4900–4913, 2018.

[56] V. Odelu, A. K. Das, and A. Goswami, “A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards,” IEEE Trans- actions on Information Forensics and Security, vol. 10, no. 9, pp. 1953– 1966, Sep. 2015.

[57] G. Panchal, D. Samanta, and S. Barman, “Biometric-based cryptography for digital content protection without any key storage,” Multimedia Tools and Applications, pp. 1–22, 2017. [Online]. Available: https://doi.org/10.1007/s11042-017-4528-x

[58] AVISPA, “SPAN, the Security Protocol ANimator for AVISPA,” 2019, http://www.avispa-project.org/. Accessed on February 2019.

[59] S. Sun and K. Beznosov, “The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems,” in 19th ACM Con- ference on Computer and Communications Security (CCS’12), Raleigh, North Carolina, USA, October 2012.

[60] C. Bansal, K. Bhargavan, A. Delignat-Lavaud, and S. Maffeis, “Discov- ering Concrete Attacks on Website Authorization by Formal Analysis,” The open archive HAL (HAL Id: hal-00815834), pp. 1–50, 2013.

[61] D. Wang and P. Wang, “Two Birds with One Stone: Two-Factor Authen- tication with Security Beyond Conventional Bound,” IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 708–722, 2018.

[62] D. Wang, W. Li, and P. Wang, “Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks,” IEEE Transactions on Industrial Informatics, vol. 14, no. 9, pp. 4081–4092, 2018.

[63] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes,” in IEEE Symposium on Security and Privacy (S&P), San Francisco, CA, USA, 2012, pp. 553–567.

[64] E. Erdem and M. T. Sandıkkaya, “OTPaaS–One Time Password as a Service,” IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 743–756, 2019.

[65] H. Luo, G. Wen, and J. Su, “Lightweight three factor scheme for real- time data access in wireless sensor networks,” Wireless Networks, 2018.

[66] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. P. C. Rodrigues, “Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications,” IEEE Transactions on Industrial Informatics, vol. 15, no. 1, pp. 457–468, 2019.

[67] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” in Proceedings of 19th Annual International Cryptology Conference (CRYPTO’99), LNCS, vol. 1666, Santa Barbara, California, USA, 1999, pp. 388–397.

[68] Y. An, “Security improvements of dynamic ID-based remote user authentication scheme with session key agreement,” 15th International Conference on Advanced Communications Technology (ICACT’13), pp. 1072–1076, 2013.

[69] J. Chou, C. Huang, Y. Huang, and Y. Chen, “Efficient two- pass anonymous identity authentication using smart card,” IACR Cryptology ePrint Archive, pp. 402–410, 2013. [Online]. Available: https://eprint.iacr.org/2013/402

[70] Y. Chang, W. Tai, and H. Chang, “Untraceable dynamic-identity-based remote user authentication scheme with verifiable password update,” International Journal of Communication Systems, vol. 27, no. 11, pp. 3430–3440, 2014.

[71] S. Kumari, M. K. Khan, and X. Li, “An improved remote user authentication scheme with key agreement,” Computers & Electrical Engineering, vol. 40, no. 6, pp. 1997–2012, 2014.

[72] S. Kaul and A. Awasthi, “Security enhancement of an improved remote user authentication scheme with key agreement,” Wireless Personal Communications, vol. 89, no. 2, pp. 621–637, 2016.

[73] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, “NIST Special Publication 800- 63-2: Electronic Authentication Guideline,” 2013, National Institute of Standards and Technology (NIST), U.S. Department of Commerce. Accessed on July 2019.

Gaurang Panchal (M’13) received the Ph.D de- gree in Computer Science and Engineering from IIT Kharagpur, India, in 2017, the M.Tech. degree in Computer Engineering from Dharmsinh Desai University, in 2007 and the B.Tech. degree in In- formation Technology from the Saurashtra Univer- sity, India, in 2003. He is presently working as a Lead Security Analyst in Siemens Technology and Services Pvt. Ltd., Bangalore, India and working on Cyber Security, IoT Trustworthy, Biometric, Threat and Risk Analysis, Vulnerability Management.

Neeraj Kumar (M’16, SM’17) received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra (J&K), India, in 2009. He was a Post-

Doctoral Research Fellow at Coventry University, Coventry, U.K. He is currently a full Professor with the Department of Computer Science and Engineering, Thapar Uni- versity, Patiala, India. He has authored more than 350 technical research papers published in leading journals and conferences from the IEEE, Elsevier, Springer, etc. He is in the editorial board of ACM Computing Survey, IEEE Transactions on Sustainable Computing, IEEE Network Magazine, IEEE Communication Magazine, Journal of Network and Computer Applications (Elsevier), Computer Communications (Elsevier) and International Journal of Communication Systems (Wiley).

Debasis Samanta (M'05, SM'10) received the B.Tech. degree in Computer Science and Engineer- ing from Calcutta University, the M. Tech. degree in Computer Science and Engineering from Jadavpur University, and Ph.D. degree in Computer Science and Engineering from IIT Kharagpur. He is actively working in the field of Human Computer Interaction. He has developed multi-modal interaction technique, text entry mechanisms in Indian languages, which are new of their kinds to bridge the digital divide.

In addition to this his research interest includes crypto biometric system, information security and Cloud security. He is an author of 3 books and more than 70 journals and 110 conference papers of international repute. He is currently Honorary Member of editorial Board of the International Journal of Biosciences and Technology, USA and member of Editorial Board of the International Journal of Communication Networks and Distributed Systems, U.K. He is the recipient of Best Author of the Year Award by Computer Society of India, Best Paper award by 8th ADCOM Conference, Microsoft Valued Professional award by Microsoft, USA and Author of the Best Selling Book by Prentice Hall of India, New Delhi.

Ashok Kumar Das (M'17–SM'18) received the Ph.D. degree in computer science and engineering, the M.Tech. degree in computer science and data processing, and the M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently an Asso- ciate Professor with the Center for Security, Theory and Algorithmic Research, IIIT Hyderabad, India. His current research interests include cryptography, network security and blockchain. He has authored over 210 papers in international journals and confer- ences in the above areas, including more than 180 reputed journal papers. Some of his research findings are published in top cited journals, such as the IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Smart Grid, IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, IEEE Transactions on Vehicular Technology, IEEE Transactions on Consumer Electronics, IEEE Journal of Biomedical and Health Informatics, IEEE Consumer Electronics Magazine, IEEE Access and IEEE Communications Magazine. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is on the editorial board of KSII Transactions on Internet and Information Systems, International Journal of Internet Technology and Secured Transactions (Inderscience), and IET Communications, is a Guest Editor for Computers & Electrical Engineering (Elsevier) for the special issue on Big data and IoT in e-healthcare and for ICT Express (Elsevier) for the special issue on Blockchain Technologies and Applications for 5G Enabled IoT, and has served as a Program Committee Member in many international conferences. He also severed as one of the Technical Program Committee Chairs of the International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019.

Kim-Kwang Raymond Choo (SM'15) received the Ph.D. in Information Security in 2006 from Queens- land University of Technology, Australia. He current holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio. In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of

Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Com- mittee on Scalable Computing (TCSC) Award for Excellence in Scalable Computing (Middle Career Researcher), 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, Outstanding Associate Editor of 2018 for IEEE Access, British Computer Society's 2019 Wilkes Award Runner-up, 2019 EURASIP Journal on Wireless Communications and Networking (JWCN) Best Paper Award, Korea Information Processing Society's Journal of Information Pro- cessing Systems (JIPS) Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, International Conference on Information Security and Cryptology (Inscrypt 2019) Best Student Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, and Co- Chair of IEEE Multimedia Communications Technical Committee's Digital Rights Management for Multimedia Interest Group.