Asian Journal of Convergence in Technology **Volume V, Issue II**
ISSN No.:2350-1146, I.F-5.11

A study on Dynamic ID based user authentication system using smart card

Ankur Biswas
Research Scholar, Dept. of Comp. Sc. &Engg,
Adamas University, Kolkata 700126, INDIA
ankur2u@gmail.com

Abhishek Roy
Associate Professor, Dept. of Comp. Sc. &Engg,
Adamas University, Kolkata 700126, INDIA
dr.aroy@yahoo.com

Abstract—Advancement of Information and Communication Technology (ICT) have enabled electronic communication among its users through Internet. As a virtual communication medium, Internet transmit messages faster than its conventional counterpart, which encounter multiple constraints of physical medium that slows down the rate of message communication. As electronic message communication is conducted among its virtually connected users, their identity should be verified properly before initiating the electronic communication. Strict cryptographic security protocols should be designed to prevent intruders so as to establish Privacy, Integrity, Authentication and Non Repudiation (PINA) over the electronic transaction. The application of dynamic identification will help to achieve this objective during transmission of sensitive information over public communication channel like Internet. Considering the gravity of situation, researchers have already proposed several dynamic identification techniques for authentication of user. In this paper authors have thoroughly studied those applications of dynamic authentication techniques over smart card based electronic transaction to explore future scope of work.

Keywords—Dynamic ID, Authentication,Smart Card

I. INTRODUCTION

Advancement of Information and Communication Technology (ICT) have enabled electronic communication among its users through Internet. As a virtual communication medium, Internet transmit messages faster than its conventional counterpart, which encounter multiple constraints of physical medium that slows down the rate of message communication. As this mode of communication is purely technology dependent, there are limited scope of man power engagement, which helps to deliver electronic messages even to remote locations at budget friendly manner. For this reason, this mode of communication is more preferable for delivery of electronic services to its users within affordable budget. As messages are communicated to its user who are virtually connected to each other, it is highly susceptible to infringement attempts, and hence their identity should be verified properly before initiating the electronic communication. Strict cryptographic security protocols should be designed to prevent intruders so as to establish Privacy, Integrity, Authentication and Non Repudiation (PINA) over the electronic transaction. To achieve this objective, dynamic identification may be used during electronic communication through Internet. Considering the gravity of situation, researchers have already proposed several dynamic identification techniques for authentication of user. In this paper authors have thoroughly studied those applications of dynamic authentication techniques over smart card based electronic transactions to explore future scope of work.

Section – II discuss the fundamentals of dynamic identification of digital user during electronic message communication. Section – III states the literature survey on authentication of user during electronic message communication using dynamic identification. Section – IV explore future scope of work using identification of user during delivery of multifaceted electronic services to its user.

2. FUNDAMENTALS OF DYNAMIC IDENTIFICATION

User ID and password are very important, convenient and mostly used in authenticating the user to gain access to the content of the system or server. While measuring the security in terms of authentication process, Dynamic ID was introduced over Static ID to prevent some attacks likes replay attack, forgery attack, guessing attack and insider attack [19]. In case of Dynamic ID, it allows an user to change its ID and Password, for which system does not need to maintain password table and verification table.

In the process of Dynamic ID based user authentication system,user sends a message to the server containing login information and the secret key of the server which returns a message with an authentication session key. After completion of authentication, the session key is generated, which is used for exchange of sensitive information.

Mostly Dynamic ID based user authentication system using smart card consist of several phases [2], which are described below:

STEP I: Registration Phase

In this phase, the user needs to register themselves in the remote server of service provider. The user puts the password to register on this remote server. After receiving the registration request from the user,the remote server performs the desired operation [2] and generates a secret key. This secret key is stored in the user's smart card for further use.

STEP II: Authentication Phase

While the user needs to get access to the remoteserver of service provider, the user sends login information to the remote server. This login information contains Dynamic ID and the secret key which is generated during the registration phase. Upon getting the details remote server goes through its operations [2] and gives access if satisfies.

STEP III: Password Change Phase

When the user wants to change their password, they can change it without connecting to the remote server. In this phase, the user needs to plug in the smart card into the local system and enter the old password as well as a new password to change the existing password [2]. The Smart card stores the new password and it can be used for the next authenticating process.

3. LITERATURE SURVEY

Application of dynamic ID based userauthentication using smart card for secure transmission of sensitive information over multivariate applications are further described below in table no 1.

Sl	**Paper title, Year**	**Author**	**Description**
1	"Cloud-Based Electronic Signature Authentication Issues"[31], 2019.	Vera Andrianova and Dmitry Efanov	This paper deals with the authentication issue of electronic signature in the cloud based system. It describes various drawbacks of user authentication system.
2	"An Improved Lightweight Two-Factor Authentication and Key Agreement Protocol with Dynamic Identity Based on Elliptic Curve Cryptography" [32], 2019.	ShumingQiu, GuoshengXu, Haseeb Ahmad, GuoaiXu, XinpingQiu and Hong Xu	In this article author did analysis of Nikooghadam et al. [28] and Kumari et al.'s [29]paper and finds that some security issuesare present in it. They proposed a new scheme to overcome those vulnerabilities. Also they used AVISPA software simulation to validate their scheme.
3	"User Define Time Based Change Pattern Dynamic Password Authentication Scheme" [33], 2018.	Salisu Ibrahim Yusuf, MoussaMahamatBoukar, AminuMukhtar, Ahmed Dalhatu Yusuf	It proposed a dynamic password algorithm that changes dependent on a client characterized design which is dynamic password without the utilization of outsider frameworks. It changes the password powerfully utilizing a calculation which is relies upon current time and interval. Creator investigation the calculation and demonstrated it's simple to learn and utilize.
4	"An Improved and Secure Two-factor Dynamic ID Based Authenticated Key Agreement Scheme for Multiserver Environment" [34], 2018.	ShreeyaSwagatikaSahoo, SujataMohanty and BanshidharMajhi	In this paper author cryptanalysis Jangirala et al.'s scheme [27] and pointed some vulnerabilities includes "forgery attack, replay attack, user impersonation attack and lack of proper mutual authentication. He also proposed a new scheme to prevent the attack from the attacker. Author also used AVISPA tool to validate his scheme.
5	"Comments on "Provably secure dynamic id-based anonymous two-factorauthenticated key exchange protocol with extended security model" [35], 2018.	Xiaowei Li, Dengqi Yang, Xing Zeng, Benhui Chen, Yuqing Zhang	The Author finds some vulnerabilities in "Password-based authenticated key exchange (PAKE) protocol" and suggests a solutions to overcome the attack.
6	"An Improvement on Remote User	Chin-Ling Chen, Yong-	Author analyzed and finds security drawback in Yeh et al.'s [30] scheme

	Authentication Schemes Using Smart Cards" [36], 2018.	Yuan Deng, Yung-Wen Tang, Jung-Hsuan Chen and Yu-Fan Lin	and proposed a robust scheme to conquer the vulnerabilities like "ID- theft attacks, off-line password guessing attacks, undetectable on-line password, guessing attacks and user impersonation attacks".
7	"An Improved Remote User Authentication Scheme for MultiserverEnvironment Using Smart Cards"[37], 2018.	ShreeyaSwagatikaSahoo, SujataMohanty, Saurabh Kumar Sunny and BanshidharMajhi.	In this paper author analyzed and described the security flaws like "online and offline password guessing attack" of Lee et al.'s [23] scheme. He Also proposed a strong algorithm to overcome the issues.
8	"Security analysis of password authenticated key retrieval" [38], 2017.	SeonghanShinand and KazukuniKobara	In this paper author security analysis of "PAKR (Password-Authenticated Key Retrieval)" protocol and its multi-server system and identifies that passive / active attack can happen.
9	"Remote User Authentication Schemes: A Review" [1], 2017	Narendra Singh Panwar, Dr. Manmohan Singh Rauthan, Dr. Amit Agarwal	Remote user authentication is a procedure to validate remote user securely over insecure network.in this paper author describe the various proposed scheme of remote user authentication.
10	"Comment on 'Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards'" [39], 2017.	AlavalapatiGoutham Reddy, Eun-Jun Yoon, Kee-Young Yoo	This is a review paper of Leu et al.'s [22] scheme. In this paper Author describe the analysis details of its scheme and finds some structural drawback on system design of "user registration phase" and "password changing phase".
11	"Cryptanalysis of three dynamic ID-based remote user authentication schemes using smart cards" [40], 2016.	ZhengxianGao, ShouHsuan Stephen Huang, Wei Ding	In this paper author cryptanalysis of three paper based on dynamic ID-based remote user authentication and reported some fact that in those technics some attack can happen by the attacker like "smart card forge attack, impersonation attack, message forge attack, and resembling account attack". They also proposed a solution to prevent the security issues.
12	"Cryptanalysis and Improvement of Remote User Authentication Scheme Using Smart Card" [41], 2016.	R. Madhusudhan and ManjunathHegde	This paper is a cryptanalysis report of Wen and Li's [26] scheme. In this author's discoveries are the plan defenseless against insider and smart card stolen attack. The creator proposed another plan to beat the security issues.
13	"Dynamic Id Based Remote User Authentication In Multi Server Environment Using Smart Cards: A Review" [18], 2015.	ShanuGaharana and DarpanAnand	In this Paper author cryptanalysis four dynamic id based remote user authentication schemes for multi-server environment using smart card. The author puts some mandate of user authentication scheme. They also shown that future research scopes is present in user authentication scheme using smart card.
14	"Comments on a Dynamic-ID-based Remote User Authentication Scheme for Multiserver Environment Using Smart Cards" [13], 2012.	Ya-Fen Chang and Pei-Yu Chang	Lee et al. [17] proposed a dynamic-ID based remote user authentication scheme for multi-server environment using smart cards. They used dynamic ID to use the service by the user anonymously. In this Paper authors find some security loopholes in which three are possible attacks and two are flaws. Which are as follows "1. Insider and smart card forgery attack. 2. Off-line password guessing attack. 3. Identity disclosure attack. 4. Inappropriate password change. 5. Failed mutual authentication "
15	"A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments" [42], 2012.	Xiong Li , Jian Ma, Wendong Wang, YongpingXiong, Junsong Zhang	In this paper author cryptanalysis Lee et al. [17] scheme and finds some security drawbacks includes "Improper authentication, Forgery attack, server spoofing attack" in it. Author also proposed a new secure scheme over "registration phase, login phase, verification phase and password change phase".
16	"Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards" [22], 2011.	JenqShiouLeu, Wen-Bin Hsieh	In this paper author analysis and finds some vulnerabilities Lee et al.'s [23] scheme which are password guessing attack, server spoofing attack and masquerade attack. Author proposed an enhanced scheme for distributed system which is improvised scheme of Lee et al.'s [23] scheme.
17	"A novel user authentication scheme using smart cards" [4], 2008.	Qi Xie, Ji-Lin Wang, De-Ren Chen, Xiu-Yuan Yu	In their paper author proposed a new scheme ofLiao et al. [3] modified scheme in which secret number is not required in smart card and it can prevent all types of attack.

18	"Security Enhancement for a Dynamic ID-based Remote User Authentication" [3], 2005.	I-En Liao, Cheng-Chi Lee, Min-Shiang Hwang	Static Id based remote user authentication system is vulnerable in terms of a partial leak of user information. In this paper, the author finds loopholes in Das et al. [2] paper of dynamic id based remote user authentication and they proposed an enhanced scheme of it.
19	"A Dynamic ID-based Remote User Authentication Scheme" [2], 2004.	ManikLal Das, AshutoshSaxena, and Ved P. Gulati	Secret phrase based verification plans are the most prominent utilized strategy for remote client confirmation. There are lots of static-ID based remote user authentication schemes have been proposed in which they are with and without a smart card. In some schemes, a user can't change their password and it verifies the user login from the verifier table. In this paper author proposed a dynamic ID-based remote user authentication in which user can change their password and verifier table is not required and it can withstand reply attacks, forgery attacks, guessing attack, insider attack, and stolen verifier attack.
20	"An enhanced remote user authentication scheme using smart cards" [12], 2004.	Amit K. Awasthi and Sunder Lal	In this paper, the authors proposed a slightly modified version of Hwang and Li's [5] scheme. The proposed scheme overcomes the Leung et al. [15] proposed schemes vulnerabilities.
21	"A user friendly remote authentication scheme with smart cards" [7], 2003.	Shyi-Tsong Wu and Bin-Chang Chieu	Sun et al. [6] proposed a remote authenticate system in which password table was not required and it was very cost effective. The password is system generated. In this paper, the author modified the system and proposed a new scheme.
22	"A modified remote user authentication scheme using smart cards" [8], 2003.	Jau-JiShen, Chih-Wei Lin, and Min-Shiang Hwang	Hwang and li [5] proposed another remote confirmation conspire utilizing brilliant card dependent on Elgamal's [25] public key cryptosystem. In this paper author elaborate an attack on Hwang and Li [5] scheme and the author enhanced the scheme to prevent such king of attack.
23	"Some forgery attacks on a remote user authentication scheme using smart cards" [10], 2003.	C. H. Chang and K. F. Hwang	In Hwang and li [5] proposed scheme Chan and Cheng [9] finds some weakness in remote user authentication and they modified the scheme. In this paper Author finds Chang and Cheng's [9] proposed scheme also does not work properly, and author proposed some different scheme to solve the Chan and Cheng's [9] attack.
24	"Cryptanalysis of a modified remote user authentication scheme using smart cards" [11], 2003.	Kai-Chi Leung, L.M. Cheng, Anthony S. Fong, and Chi-Kwong Chan	In this paper, the author analyzes the scheme of Shen, Lin, and Hwang [8] They also showed up that the proposed scheme of attack by Chan and Cheng [9] is still vulnerable and the proposed scheme of attack by Chang and Hwang [16] is more secure.
25	"A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards" [17], 2003.	Cheng-Chi Lee , Tsung-Hung Lin, Rui-Xiang Chang	The creator discovers a few escape clauses of Hsiang's [19] conspire which can't anticipate disguise assault, server mocking assault and these assaults can't fix effectively. In this paper author suggest a new improved scheme to overcome the issues.
26	"A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture" [20], 2003.	KaipingXue, P. Hong and C. Ma	The author analysis and finds some vulnerabilities Li's [21] paper and proposed a new protocol which elaborate the vulnerabilities of Li 's [21] paper and also it gives details about traceability and identity protection.
27	"A remote password authentication scheme for multi-server architecture using neural networks" [14], 2001.	Li-Hua Li, Iuon-Chang Lin, and Min-Shiang Hwang	Normally remote password authentication scheme uses to validate the remote user. This scheme is not applicable to a multi-server architecture environment. In this paper, the author proposed a new scheme of remote password scheme for multi-server environment. This scheme is a pattern classification system based on artificial neural networks. In this scheme, the user can change their password and a verification table is not required. This scheme also prevents the reply attack.

28	"A new remote user authentication scheme using smart cards" [5], 2000.	M. S. Hwang and L. H. Li	In early 2000 the author proposed a new remote user authentication scheme using smart card which is based on Elgamal's [25] public key cryptosystem and in it password system is not required. This scheme can protect the massage replaying attack. In this paper, the author analyzes the scheme of Shen, Lin, and Hwang [8]. They also showed up that the proposed scheme by Chan and Cheng [9] is still vulnerable and the proposed attack by Chang and Hwang is more secure.
29	"An efficient remote use authentication scheme using smart cards" [6], 2000.	Hung-Min Sun	In this paper, author proposed an efficient and practical remote user authentication scheme using smart card based onHwang et al. [5] remote user authentication scheme using a smart card which was derived from discrete logarithm problem and it is very novel because it was not required any password table.
30	"Cryptanalysis of a remote user authentication scheme using smart cards" [9], 2000.	Chi-Kwong Chan and L. M. Cheng	Hwang and li [5] proposed another remote affirmation plot using splendid card reliant on Elgamal's [25] open key cryptosystem. In this author cryptanalysis the Hwang et al. [5] paper and finds the schema is breakable.

Table -1: Literature Review on Dynamic ID based user authentication system

4. CONCLUSION

The literature review mentioned above has clearly depicted the global situation of dynamic ID based user authentication system. Several authentication systems has been proposed based on dynamic ID using smart card to ensure the security. To extend its applicationover Cloud Governance [24] transaction for delivery of multifaceted electronic services to the user, its object oriented designing will be considered as the next scope of this work.

REFERENCES

[1] Singh Panwar, N., Singh Rauthan, M. and Agarwal, A. Remote User Authentication Schemes: A Review. *In proceedings International Journal of Engineering Science Invention (IJESI)*, vol. 6, issue 12, pp.09-12,2017. ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726.

[2] Das, M., Saxena, A. and Gulati, V. A dynamic ID-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics*, 50(2), pp.629-631, 2004. DOI: 10.1109/TCE.2004.1309441.

[3] Liao, I., Lee, C. and Hwang, M. Security Enhancement for a Dynamic ID-Based Remote User Authentication Scheme. *In proceedingsInternational Conference on Next Generation Web Services Practices (NWeSP'05)*, 2005. DOI: 10.1109/NWESP.2005.67.

[4] Xie, Q., Wang, J., Chen, D. and Yu, X. A Novel User Authentication Scheme Using Smart Cards. *2008 International Conference on Computer Science and Software Engineering*, 2008. DOI: 10.1109/CSSE.2008.1043

[5] Hwang, M. and Li, L. A new remote user authentication scheme using smart cards. *In proceedings IEEE Transactions on Consumer Electronics*, 46(1), pp.28-30, 2000. DOI: 10.1109/30.826377

[6] Sun, H. An efficient remote use authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(4), pp.958-961, 2000. DOI: 10.1109/30.920446.

[7] Wu, S. and Chieu, B. A user friendly remote authentication scheme with smart cards. *Computers & Security*, 22(6), pp.547-550, 2003. DOI: 10.1016/S0167-4048(03)00616-3.

[8] Shen, J., Lin, C. and Hwang, M. A modified remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 49(2), pp.414-416, 2003. DOI: 10.1109/TCE.2003.1209534

[9] Chan, C. and Cheng, L. Cryptanalysis of a remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(4), pp.992-993, 2000. DOI: 10.1109/30.920451

[10] Chang, H. C. and Hwang, K. F.Some forgery attacks on a remote user authentication scheme using smart cards. Informatics, vol. 14, No. 3, pp. 289 -294, 2003.

[11] Leung, K., Cheng, L., Fong, A. and Chan, C. Cryptanalysis of a modified remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 49(4), pp.1243-1245, 2003. DOI: 10.1109/TCE.2003.1261224.

[12] Awasthi, A. and Lal, S. An enhanced remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 50(2), pp.583-586, 2004. DOI: 10.1109/TCE.2004.1309430.

[13] Chang, Y. and Chang, P. Comments on a Dynamic-ID-Based Remote User Authentication Scheme for Multi-server Environment Using Smart Cards. *2012 Sixth International Conference on Genetic and Evolutionary Computing*, 2012. DOI: 10.1109/ICGEC.2012.73.

[14] Li, L., Lin, L. and Hwang, M. A remote password authentication scheme for multiserver architecture using neural networks. *IEEE Transactions on Neural Networks*, 12(6), pp.1498-1504, 2001. DOI: 10.1109/72.963786.

[15] Leung, K., Cheng, L., Fong, A. and Chan, C. Cryptanalysis of a modified remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 49(4), pp.1243-1245, 2003. DOI: 10.1109/TCE.2003.1261224.

[16] Chang, C. C., and Hwang, K. F.Some forgery attacks on a remote user authentication scheme using smart cards. *Informatics*, vol. 14, no. 3, pp. 289-294, 2003.

[17] Lee, C. C., Lin, T. H. and Chang, R. X. 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. 13863-13870, 2011.DOI: 10.1016/j.eswa.2011.04.190.

[18] Gaharana, S. and Anand, D. Dynamic Id Based Remote User Authentication in Multi Server Environment Using Smart Cards: A Review. *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, 2015. DOI: 10.1109/CICN.2015.212.

[19] Hsiang, H. and Shih, W. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. *Computer Standards & Interfaces*, 31(6), pp.1118-1123, 2009. DOI: 10.1016/j.csi.2008.11.002.

[20] Xue, K., Hong, P. and Ma, C. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture. *Journal of Computer and System Sciences*, 80(1), pp.195-206, 2014. DOI: 10.1016/j.jcss.2013.07.004.

[21] Li, X., Xiong, Y., Ma, J. and Wang, W. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. *Journal of Network and Computer Applications*, 35(2), pp.763-769, 2012. DOI: 10.1016/j.jnca.2011.11.009.

[22] Leu, J. and Hsieh, W. Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards. *IET Information Security*, 8(2), pp.104-113,2014. DOI: 10.1049/iet-ifs.2012.0206.

[23] Lee, W. B., and Chang, C. C. User identification and key distribution maintaining anonymity for distributed computer network. *Computer Systems Science and Engineering*. 15(4), pp.211-214, 2000.

[24] Roy, A. Smart delivery of multifaceted services through connected governance. In: *Proceeding of the Third International Conference on Computing Methodologies and Communication (ICCMC 2019) (IEEE)*. pp.493-499, 2019. ISBN: 978-1-5386-7807-7.

[25] Elgamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4), pp.469-472, 1985. DOI: 10.1109/TIT.1985.1057074.

[26] 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. DOI: 10.1016/j.compeleceng.2011.11.010.

[27] S. Jangirala, S. Mukhopadhyay and A. Das, "A Multi-server Environment with Secure and Efficient Remote User Authentication Scheme Based on Dynamic ID Using Smart Cards", *Wireless Personal Communications*, vol. 95, no. 3, pp. 2735-2767, 2017. DOI: 10.1007/s11277-017-3956-2.

[28] M. Nikooghadam, R. Jahantigh and H. Arshad, "A lightweight authentication and key agreement protocol preserving user anonymity", *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13401-13423, 2016. DOI: 10.1007/s11042-016-3704-8.

[29] S. Kumari, M. Khan and X. Li, "An improved remote user authentication scheme with key agreement", *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1997-2012, 2014. DOI: 10.1016/j.compeleceng.2014.05.007.

[30] K. Yeh, C. Su, N. Lo, Y. Li and Y. Hung, "Two robust remote user authentication protocols using smart cards", *Journal of Systems and Software*, vol. 83, no. 12, pp. 2556-2565, 2010. DOI: 10.1016/j.jss.2010.07.062.

[31] V. Andrianova and D. Efanov, "Cloud-Based Electronic Signature Authentication Issues", *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2019. DOI: 10.1109/eiconrus.2019.8656803.

[32] S. Qiu, G. Xu, H. Ahmad, G. Xu, X. Qiu and H. Xu, "An Improved Lightweight Two-Factor Authentication and Key Agreement Protocol with Dynamic Identity Based on Elliptic Curve Cryptography", *KSII Transactions on Internet and Information Systems*, vol. 13, no. 2, 2019. DOI: 10.3837/tiis.2019.02.027.

[33] S. Yusuf, M. Boukar, A. Mukhtar and A. Yusuf, "User Define Time Based Change Pattern Dynamic Password Authentication Scheme", *2018 14th International Conference on Electronics Computer and Computation (ICECCO)*, 2018. DOI: 10.1109/icecco.2018.8634675.

[34] S. Sahoo, S. Mohanty and B. Majhi, "An Improved and Secure Two-factor Dynamic ID Based Authenticated Key Agreement Scheme for Multiserver Environment", *Wireless Personal Communications*, vol. 101, no. 3, pp. 1307-1333, 2018. DOI: 10.1007/s11277-018-5764-8.

[35] X. Li, D. Yang, i. Zeng, B. Chen and Y. Zhang, "Comments on “Provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model”", *IEEE Transactions on Information Forensics and Security*, pp. 1-1, 2018. DOI: 10.1109/tifs.2018.2866304.

[36] C. Chen, Y. Deng, Y. Tang, J. Chen and Y. Lin, "An Improvement on Remote User Authentication Schemes Using Smart Cards", *Computers*, vol. 7, no. 1, p. 9, 2018. DOI: 10.3390/computers7010009.

[37] S. Sahoo, S. Mohanty, S. Sunny and B. Majhi, "An Improved Remote User Authentication Scheme for Multiserver Environment Using Smart Cards", *Advances in Intelligent Systems and*

Computing, pp. 217-224, 2018. DOI: 10.1007/978-981-10-8639-7_22.

[38] S. Shinand and K. Kobara, "Security Analysis of Password-Authenticated Key Retrieval", *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 5, pp. 573-576, 2017. DOI: 10.1109/tdsc.2015.2490064.

[39] A. Goutham Reddy, E. Yoon and K. Yoo, "Comment on 'Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards'", *IET Information Security*, vol. 11, no. 4, pp. 220-221, 2017. DOI: 10.1049/iet-ifs.2016.0218.

[40] Z. Gao, S. Huang and W. Ding, "Cryptanalysis of three dynamic ID-based remote user authentication schemes using smart cards", *2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS)*, 2016. DOI: 10.1109/icoacs.2016.7563046.

[41] R. Madhusudhan and M. Hegde, "Cryptanalysis and Improvement of Remote User Authentication Scheme Using Smart Card", *2016 International Conference on Computer and Communication Engineering (ICCCE)*, 2016. DOI: 10.1109/iccce.2016.30.

[42] 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. DOI: 10.1016/j.mcm.2012.06.033.

Authors' Profiles

Mr. Ankur Biswas, He iscurrently pursuing his Ph.D. degree fromDept. of CSE, Adamas University, Kolkata, India. He is Founder and Director of SASLAB Technologies Pvt Ltd, Kolkata, India. He is also member of IEEE, life Member of Cryptology Research Society of India. His research interests include: Cryptography, Cyber Security and E-Governance.

Dr.Abhishek Roy, He is an Associate Professorof Dept. of CSE, Adamas University, Kolkata,India.He is also life Member of Cryptology Research Society of India, Indian Statistical Institute, Kolkata. His research interest includes: Cyber Security, E-Governance.