INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND APPLICATIONS
VOLUME XVI, ISSUE VIII, AUGUST 22, WWW.IJCEA.COM, ISSN 2321-3469

BIOMETRIC-BASED SECURE ACCESS MECHANISM FOR CLOUD SERVICES: DESIGNING A SECURE AND EFFICIENT MECHANISM

P. Pullaiah[1], T.Haritha[2], K.Jayanth[3] ,D.Akhilandeswari[4] , SK. Abdul Mohasin[5]
[1] *Asst. Professor, Krishna Chaitanya Institute of Technology & Sciences , Markapur, A.P, India*
[2,3,4,5] *Scholar, Krishna Chaitanya Institute of Technology &Sciences , Markapur, India*

ABSTRACT:

In our data-driven culture, there is an exponential growth in the need for distant data storage and compute services, necessitating the requirement for safe access to such data and services. In order to enable safe access to a distant (cloud) server, we build a new biometric-based authentication system in this article. In the suggested method, we treat a user's biometric information as a secure credential. From the user's biometric information, we then create a unique identity that is utilized to produce the user's private key. Additionally, we offer a practical method for creating a session key for secure message transmission between two conversing participants utilizing two biometric templates. In other words, the user's private key does not need to be stored anywhere, and the session key is produced secretly. The proposed approach can withstand several well-known attacks against (passive/active) adversaries, according to a thorough formal security analysis using the Real-Or-Random (ROR) model, an informal (non-mathematical) security analysis, and formal security verification using the widely-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Finally, thorough tests and a comparison show how effective and practical the suggested strategy is.

Keywords : Bio-metric, Cloud server, Real-or-Random, informal security analysis.

1. INTRODUCTION

In current world, cloud services are typical. It is not simple to provide safe access to cloud services, and creating strong authentication, authorization, and accounting for access is a never-ending problem from both an operational and research standpoint. In the literature, a variety of authentication methods have been put forth, including ones based on Kerberos [1], OAuth [2], and OpenID [3] (see [1], [4]- [12]). These

protocols often aim to create a secure assigned access mechanism between two communicating entities linked through a distributed system.

Based on the underlying presumption that the distant server in charge of authentication is a reliable entity on the network, several protocols are used. In particular, a user must first register with a distant server. To guarantee the owner's consent, this is required. When a user requests access to a server, both the user and the server must be authenticated by the distant server. The user receives access to the services from a remote server when both verifications are completed successfully.

The fact that the user's credentials are kept on the authentication server, where they can be stolen and (mis)used to obtain unauthorised access to numerous services, is a major drawback of the current authentication techniques. Additionally, present techniques often employ symmetric key cryptography, which necessitates the sharing of a number of cryptographic keys throughout the authentication process, to ensure safe and quick communication.The authentication protocols are burdened by this tactic. The flaws found 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] show how difficult it is to design safe and effective authentication procedures. We thus aim to provide a reliable and effective authentication technique in this work. We'll start out by offering an alternative to the typical password-based authentication method. Then, without using any shared or pre-loaded information, we show how to construct a secure connection between the parties engaged in the authentication protocol.

According to the suggested method, a user's fingerprint image serves as a secret credential. We create a private key from the fingerprint picture, which is then used to covertly store the user's credentials in an authentication server database. In the authentication step, we take a fresh picture of the user's biometric fingerprint, create the private key, and then encrypt the biometric information as a query. The authentication server receives the biometric data that has been queried and compares it to the data that has been stored there. The user is now prepared to access his or her service from the chosen server after successfully completing the authentication process.Mutual authentication utilising a short-term session key has been suggested between the user and authentication server as well as between the user and service server in order to achieve secure access to the service server. We describe an efficient and reliable method to create the session key using two fingerprint data. For message authenticity purposes, a biometric-based message authenticator is also created.

The essential contributions and advantages of the suggested strategy are outlined below.

1) It is demonstrated how to send the user's biometric information to an authentication server via secure network channels.
2) We provide a method to instantly create a revocable private key from an irreversible fingerprint image. The private key and a direct representation of the user's biometric information don't need to be kept anywhere.
3) By eliminating the need for the user's credentials to be kept on the authentication server, we overcome the drawback of conventional techniques.
4) We present a fresh method for creating session keys.
5) Each object has to have some preloaded information in a standard authentication system, which adds overhead. To obviate the requirement for hidden pre-loaded information, we present a novel approach.
6) As an alternative to the current message authentication methods (i.e., Message Authentication Code (MAC)), a message authentication mechanism is presented.

[2] LITERATURE SURVEY

We focus on current biometric-based user authentication systems that have been presented in the literature in this area. The user authentication techniques may be divided into three groups based on the types and elements utilised for authentication: three factors: one factor, two factors, and three factors. A single factor (such as the user's smart card, mobile device, password, or personal biometrics) may be utilised in a single-factor authentication process. A user's smart card, mobile device, and password can be utilised in a two-factor authentication system.

In contrast, a three-factor authentication system allows the user to utilise their smart card/mobile device, password, and biometrics. A password-based user authentication system for wireless sensor

networks was created by Jiang et al (WSNs). This kind of authentication uses both a smart card and a password, making it a two-factor method. An authorised user registers or reregisters with the trusted gateway node during the user registration procedure (GWN).

The appropriate credentials are subsequently saved on a smart card that the GWN then provides. Additionally, all of the deployed sensor nodes register with the GWN through a secure connection and receive their corresponding secret credentials. During the login and authentication phases, the GWN assists a genuine user in authenticating with a specified sensor node using the pre-loaded credentials.

However, Das [22] later demonstrated that this specific scheme is susceptible to privileged insider attacks, in which a trusted authority internal user (i.e., an insider attacker) who has access to a registered user's registration information can mount additional attacks against the system, such as user impersonation attacks.

Additionally, it was demonstrated that this technique does not offer sufficient authentication and cannot allow the deployment of new sensor nodes in a target field. Das [22] provided a better and effective three factor authentication technique as a countermeasure, with the three elements being a smart card, the user's password, and their unique biometrics. The Das [22] approach, however, does not protect the anonymity of sensor nodes. A biometric-based user authentication approach for WSNs was suggested by Althobaiti et al. [14]. Their plan, however, is vulnerable to man-in-the-middle and impersonation assaults [23]. Then Das [23] suggested a brand-new biometric-based user authentication strategy. A temporal-credential-based mutual authenticated key agreement technique for WSNs was also created by Xue et al. [15].[In their plan, distant authorised users are allowed to visit approved sensor nodes to acquire information and to transmit some crucial instructions to the WSN sensor nodes. With the aid of the password-based authentication method, the GWN in this scheme gives temporal credentials to each user and sensor node installed in the WSN. Later, Li et al. [24] showed that Xue et altechnique .'s is susceptible to attacks such as smart card loss, insider, numerous logged-in users, offline password guessing, stolen-verifier, and insider. Additionally, He et al. [25] showed that Xue et almethod .'s is vulnerable to attacks such as user impersonation, off-line password guessing, modification, and impersonation of sensor nodes. Other user authenticated key agreement strategies were put out by Turkanovic and Holbl [26] and Turkanovic et al. [16].Turkanovic et al[16] .'s method is vulnerable to assaults such as smart card theft, offline password guessing, user impersonation, offline identity guessing, and sensor node impersonation [27]. A smart card-based user identification system that protects user privacy and employs hashing operations for biometric verification was created by Park et al. [17]. The plan, however, is vulnerable to denial-of-service (DoS) assaults [28]. A biometric-based user verified key agreement system was created by Dhillon and Kalra [18] for safe access to services offered by Internet of Things (IoT) devices.

Despite using lightweight operations, this technique is not immune to DoS assaults since it employs the perceptual hashing (bio hashing) procedure rather than the fuzzy extractor [28]. This is largely due to the fact that the bio hashing approach seldom ever generates a unique value BH(BIOi) from the biometric data BIOi of an authorised user Ui at various input times, despite the fact that it may minimise output error [28]. An authenticated key agreement system created by Kaul and Awasthi [19] was subsequently shown to be vulnerable to user impersonation and offline password guessing attacks [20].

The Kaul and Awasthi [19] approach also does not protect user anonymity. Kang et al. [20] suggested an improved bioemtric-based user authentication technique as a result.This method is vulnerable to DoS and impersonation attacks, both of which may be readily launched by attackers with insider privileges. A local descriptor known as the Weber local binary was created by Xia et al. [29] to aid in the liveness identification of fingerprints. Support Vector Machine is the foundation of their mechanism (SVM). A binary pattern (BP) neural network was established by Yuan et al. [30] in a different study that responds to the liveness detection of fingerprints. Their method uses the Laplacian operation to calculate the values for the picture gradient. The BP neural network's various parameters are then evaluated in order to achieve higher detection precision. We direct the curious reader to provides an extensive overview of the literature on fingerprint-based biometric identification techniques. On the basis of the distributed system's smart-card-based password authentication techniques, Huang et al. presented two distinct unique security vulnerabilities.

A user must have a working smart card and the appropriate password in their system to successfully authenticate. They also took into account two separate opponents, the first of which had pre-computed data placed on a smart card and the second of which had different data stored on a smart card. Different user privacy perversion properties were introduced by Wang and Wang in two-factor authentication methods

for wireless sensor networks (WSNs).To show the difficulties and nuances in creating two-facto authentication for ensuring privacy for WSNs, they created two distinct sample schemes. A game-based security mechanism for two-factor authentication was also introduced. To highlight the difficulties with mobile device authentication techniques, Wang et al. suggested three distinct identity-based user authentication schemes. They also took into account attacks on session-specific transitory information, attacks on false identities, and poor usability. In the literature, a number of other authentication techniques [31], [32], [33],[34], [35] and [36] have also been put out to offer security for wireless sensor networks and mass storage devices and also E-Commerce Security Issues[37] and [38] are discussed and studied.

[3] SYSTEM ARCHITECTURE

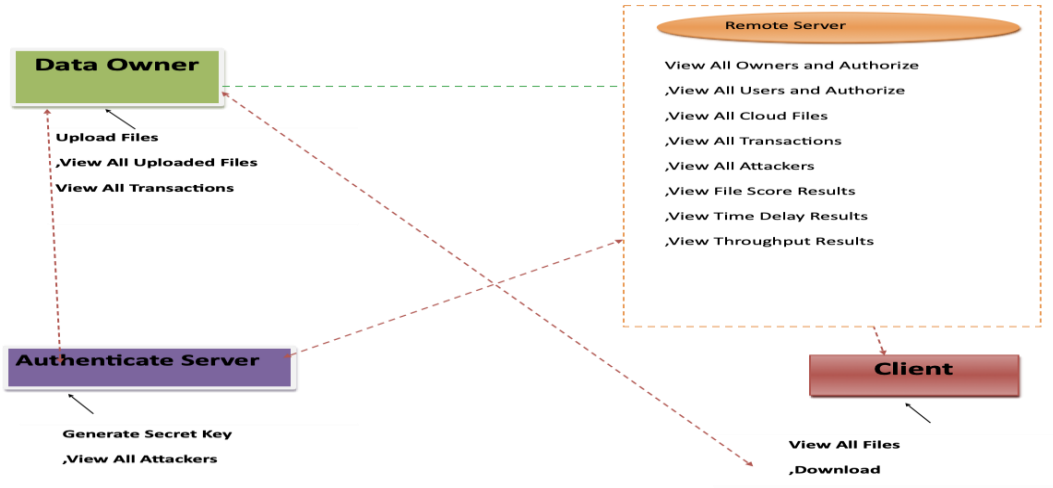


Fig. 1 System Architecture

[4] IMPLEMENTATION

4.1 Modules Description

i) Data Owner: The data owner must first register with the cloud server and get authorization before using this module. After receiving permission from the cloud data owner, the file will be encrypted and added to the cloud server, where it will be stored after the file has been added. View All Transactions and All Files Uploaded.

ii) Remote Server: In order to provide a service for data storage, the distant server runs a cloud. Data owners encrypt their data files before storing them in the cloud to share with cloud end users. They also carry out the following tasks, including Authorize and View All Owners Authorize, View All Users View All Attackers, All Transactions, and All Cloud Files See the results of the File Score, Time Delay, and Throughput tests.

iii) Authenticate Server: The secret key and content key that the end user has requested are generated by CA together with View All Attackers.

iv) Client: For access to files stored in the cloud, the user must register and log in. The cloud has given the user permission to confirm the registration. User must see and download all files.

4.2 Screenshots

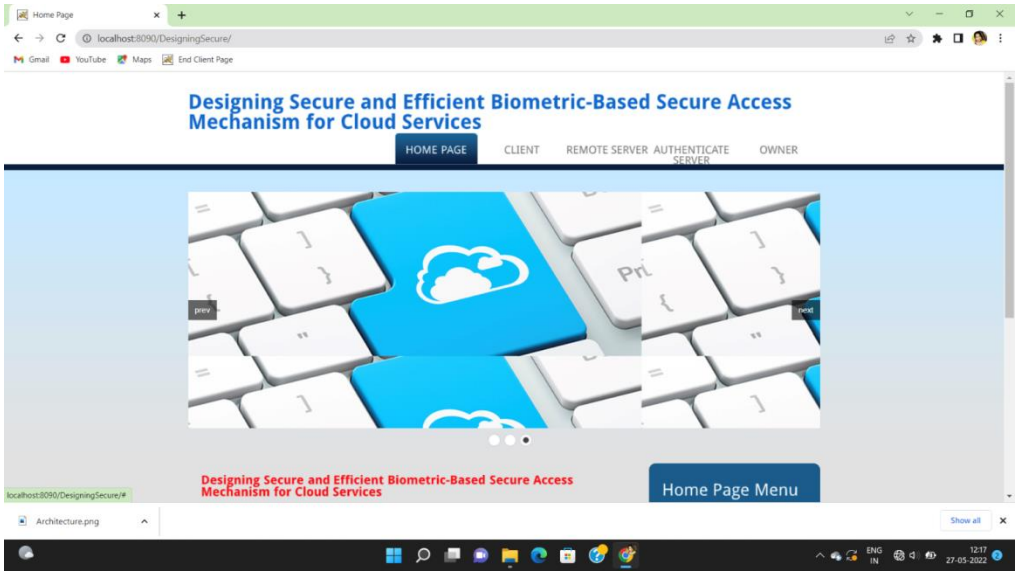
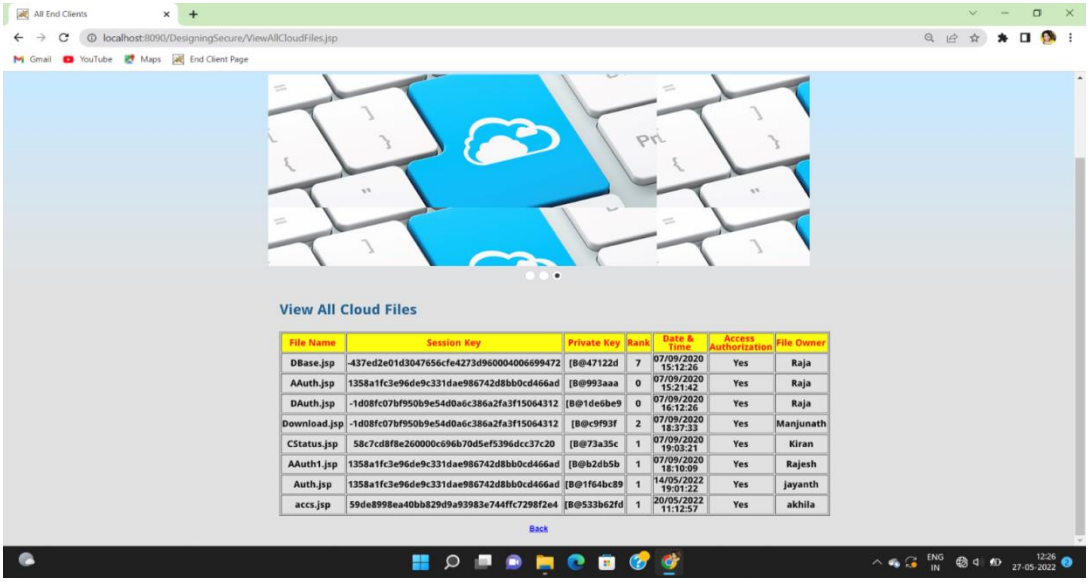


Fig. 2 Home Page



File Name	Session Key	Private Key	Rank	Date & Time	Access Authorization	File Owner
DBase.jsp	-437ed2e01d3047656cfe4273d960004006699472	[B@47122d	7	07/09/2020 15:12:26	Yes	Raja
AAuth.jsp	1358a1fc3e96de9c331dae986742d8bb0cd466ad	[B@993aaa	0	07/09/2020 15:21:42	Yes	Raja
DAuth.jsp	-1d08fc07bf950b9e54d0a6c386a2fa3f15064312	[B@1de6be9	0	07/09/2020 16:12:26	Yes	Raja
Download.jsp	-1d08fc07bf950b9e54d0a6c386a2fa3f15064312	[B@c9f93f	2	07/09/2020 18:37:33	Yes	Manjunath
CStatus.jsp	58c7cd8f8e260000c696b70d5ef5396dcc37c20	[B@73a35c	1	07/09/2020 19:03:21	Yes	Kiran
AAuth1.jsp	1358a1fc3e96de9c331dae986742d8bb0cd466ad	[B@b2db5b	1	07/09/2020 18:10:09	Yes	Rajesh
Auth.jsp	1358a1fc3e96de9c331dae986742d8bb0cd466ad	[B@1f64bc89	1	14/05/2022 19:01:22	Yes	jayanth
accs.jsp	59de8998ea40bb829d9a93983e744ffc7298f2e4	[B@533b62fd	1	20/05/2022 11:12:57	Yes	akhila

Fig. 3 View All Cloud Files

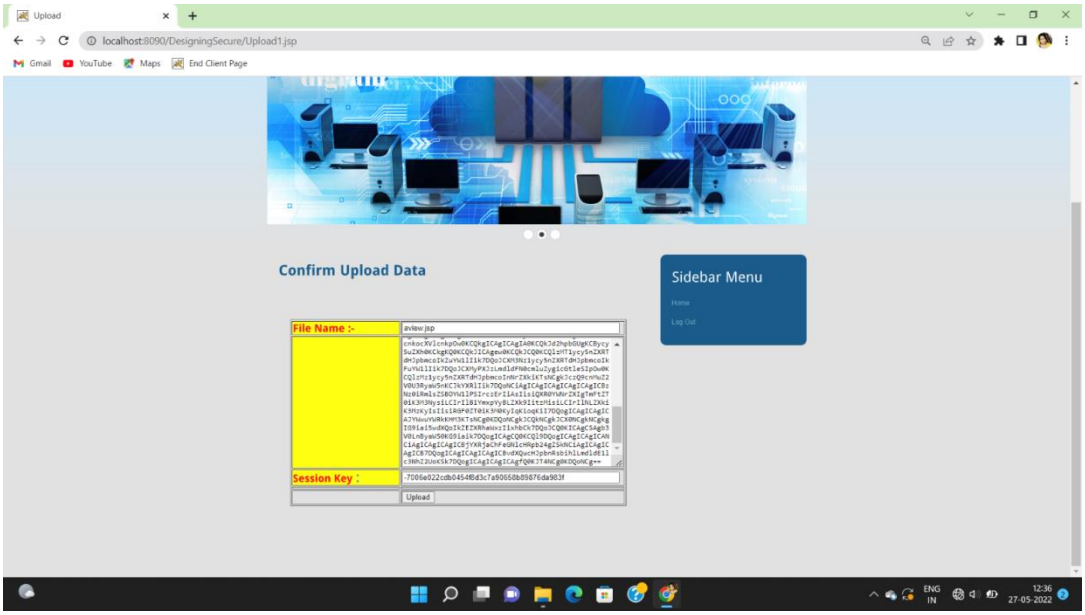


Fig. 4 Confirm Upload Data

[5] CONCLUSION

The growing use of biometrics demonstrates that it offers distinct benefits over traditional passcode and token-based security systems (e.g., on Android and iOS devices). In this research, we present an authentication method based on biometrics for users attempting to access services and computing resources from a distance. Given that a user's fingerprint may be used to produce the same key with an accuracy of 95.12%, our suggested method enables the generation of a private key using biometric fingerprint reveals. There is no need to communicate any prior information when utilising the session key creation method we suggest using two biometric data. Comparing our strategy to other authentication methods of a similar kind demonstrates that our protocol is more resistant to a number of known attacks.

• Future study will examine additional biometric characteristics and multi-modal biometrics for further delicate applications (e.g., in national security matters).

• Biometrics will be used by many sectors in the future to regulate identity and access management (IAM) for important systems, data, and applications.

• The biometric maximises security and convenience for all parties involved and aids businesses in putting their identity and access management infrastructure in place for upcoming changes in security and privacy regulations.

REFERENCES

[1] C. Neuman, S. Hartman, K. Raeburn, “The kerberos network authenticationservice (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 architecturefor Kerberos based authorization,” Proc. AFS and Kerberos BestPractices Workshop, June 2006.

[5] A. Kehne, J. Schonwalder, and H. Langendorfer, “A nonce-based protocolfor multiple authentications,” ACM SIGOPS Operating SystemReview, vol. 26, no. 4, pp. 84–89, 1992.

[6] B. Neuman and S. Stubblebine, “A note on the use of timestamps asnonces,” 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,” IETInfomration Security, vol. 6, no. 2, pp. 93–101, 2012.

[8] S. Zhu, S. Setia, and S. Jajodia, “LEAP: efficient security mechanismsfor 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 securityfor open distributed systems," Computer Communications, vol. 17, no. 7,pp. 501–518, 1994.
[11] G. Wettstein, J. Grosen, and E. Rodriguez, "IDFusion: An open architecturefor Kerberos based authorization," Proc. AFS and Kerberos BestPractices 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 userauthentication 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 biometricauthentication protocol for wireless sensor networks," InternationalJournal 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-basedmutual authentication and key agreement scheme for wireless sensornetworks," 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 authenticationand 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.
[17] M. Park, H. Kim, and S. Lee, "Privacy Preserving Biometric-Based UserAuthentication Protocol Using Smart Cards," in 17th International Conferenceon Computational Science and Engineering, Chengdu, China,2014, pp. 1541–1544.
[18] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote userauthentication scheme for IoT services," Journal of Information Securityand Applications, vol. 34, pp. 255 – 270, 2017.
[19] S. D. Kaul and A. K. Awasthi, "Security Enhancement of an ImprovedRemote User Authentication Scheme with Key Agreement," WirelessPersonal Communications, vol. 89, no. 2, pp. 621–637, 2016.
[20] D. Kang, J. Jung, H. Kim, Y. Lee, and D. Won, "Efficient andSecure Biometric-Based User Authenticated Key Agreement Schemewith 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-factoruser authentication scheme for wireless sensor networks," Peer-to-PeerNetworking and Applications, vol. 9, no. 1, pp. 223–244, 2016.
[23] "A secure and effective biometric-based user authenticationscheme for wireless sensor networks using smart card and fuzzyextractor," 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 credentialbasedsecurity scheme with mutual authentication and key agreementfor wireless sensor networks," Sensors, vol. 13, no. 8, pp. 9589–9603,2013.
[25] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credentialbasedmutual authentication and key agreement scheme for wirelesssensor networks," in International Symposium on Wireless and pervasiveComputing (ISWPC), Taipei, Taiwan, 2013, pp. 1–6.
[26] M. Turkanovic and M. Holbl, "An improved dynamic password-baseduser 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 userauthentication and key agreement in multi-gateway based wireless sensornetworks," Ad Hoc Networks, vol. 36, pp. 58–80, 2016.
[28] C.-C. Chang and N.-T. Nguyen, "An Untraceable Biometric-BasedMulti-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 NovelWeber 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 matrixusing BP neural network for fingerprint liveness detection," Soft Computing,vol. 23, no. 13, pp. 5157–5169, 2019.
[31] Mogili BVK Chaitanya Kumar, Sk. Althaf Hussain Basha , S VenkataPavan Kumar,

"Distributed Anomaly Feature Detection Over Financial Frauds", International Journal For Recent Development In Science And Technology(IJRDST), Volume 4, Issue 1, Jan 2020, pp. 135-141, ISSN 2581 –4575

[32] M. Harish Babu, Sk. Althaf Hussain Basha , S. Lakshmana Kumar, "An Advanced DES Based Dynamic Encryption Scheme Over Distributed Computing Across Moving Target Defence", International Journal For Recent Development In Science And Technology(IJRDST), Volume 03, Issue 12, Dec 2019, pp. 277-285,ISSN 2581 –4575

[33] SkNikhath, SK. Althaf Husain Basha,, P YejdaniKhan . "Safety Fear/Attacks Current in Cloud Environment", Volume 4, Issue 2, November 2019, pp. 324-330, International Journal of Recent Issues on Computer Science & Electronics(IJRICSE)

[34] Ch. Sowmya, SK Althaf Hussain Basha, P Yasdhani Khan, "Primary Set and Protection Service IS Transform Data Distribution in Cloud Techniques", Volume 5, Issue 1, Jan-Jun 2019, pp.9-12, International Journal of Recent Issues on Computer Science and Electronics(IJRICSE).

[35] Shaik Yasmin Sulthana , SK Althaf Hussain Basha, "IOT Based Shutter Alarm Security System" Journal of Engineering Sciences (JES), Vol.11, Issue 7,July/2020, pp.1035-1045, ISSN No:0377-9254.

[36] Sd.Muneer, SK Althaf Hussain Basha,, E.Srinivasa Reddy, I Ramesh Babu," Robust Watermarking Method For Any Images Based On Noise Density" International Journal of Advanced Computing(IJAC), Volume 4,Issue 3&4,2012,pp.114-121,ISSN: 0975-7686.

[37] SK Althaf Hussain Basha, B Sasidhar, "A Review on the Challenges of E-Commerce Security Issues, Privacy, Trust and Solutions", International Conference on Consumer Dynamic and Marketing Strategies in Globalized Economic Era-Perspectives and Challenges, GRIET, Hyderabad, 2013.

[38] B Sasidhar, SK Althaf Hussain Basha, , " The Effect of E-Commerce Applications on Marketers and Consumers: A Case Study ", International Conference on Consumer Dynamic and Marketing Strategies in Globalized Economic Era-Perspectives and Challenges, GRIET, Hyderabad,2013.