Integrating Biometric Mechanism to Protect User Data in Cloud Computing

B Naga Raju #1, A Mallikharjuna Rao #2, S Venkata Siva Naga Raju #3, V Sevanth Kumar #4

#1 Asst.Professor, Dept of Computer Science and Engineering, Qis College of Engineering and Technology, Ongole
#2 Student, Dept of Computer Science and Engineering, Qis College of Engineering and Technology, Ongole
#3 Student, Dept of Computer Science and Engineering, Qis College of Engineering and Technology, Ongole
#4 Student, Dept of Computer Science and Engineering, Qis College of Engineering and Technology, Ongole

Abstract:

In the course of recent years, numerous organizations have acquired advantages from the execution of cloud solutions inside the organization. Because of the benefits like adaptability, portability, and costs saving, the quantity of cloud clients is required to develop quickly. Therefore, organizations need a safe method to authenticate its clients to guarantee the usefulness of their administrations and information put away in the cloud storages are overseen in a private climate. In the current methodologies, the client verification in cloud computing depends on the qualifications presented by the client like secret word, token and computerized authentication. Lamentably, these accreditations can frequently be taken, inadvertently uncovered or difficult to recollect. Taking into account this, we propose a biometric-based validation convention to help the client verification for the cloud climate. Our answer can be utilized as the second factor for the cloud clients to send their verification demands. In our plan, we join a few players (customer, administration specialist and specialist co-op) to work together to play out the coordinating with activity between the inquiry include vector and the biometric layout of the client. Specifically, we consider an appropriated situation where the biometric layouts are put away in the cloud storage while the client validation is performed without the spillage of any sensitive data.

1 Introduction

Cloud Computing is a model for on-request network access of configurable computing assets Network, Server, Storage, Application, Services. Cloud computing can be seen as a high level form of the information preparing administration authorities accessible in the educated present reality. NIST characterizes cloud as follows, "Cloud Computing is a model for empowering omnipresent, Convenient, on-request network access to shared Pool of configurable computing assets that can be violently Provisional and delivered with insignificant administration. Cloud is utilized to bring down forthright expense and decreased foundation cost." Cloud computing is by and large considered as an administrations dividing among various clients in a huge scope. In this manner, the client just as the assistance must be authenticated to guarantee the protection and the trust of the cloud administration that is being given. The significant components of cloud computing privacy, Integrity, accessibility. Privacy protecting information since information is put away on conveyed

data set. Honesty alludes to the part of two contextual investigation concentrates of the assaults on information put away on

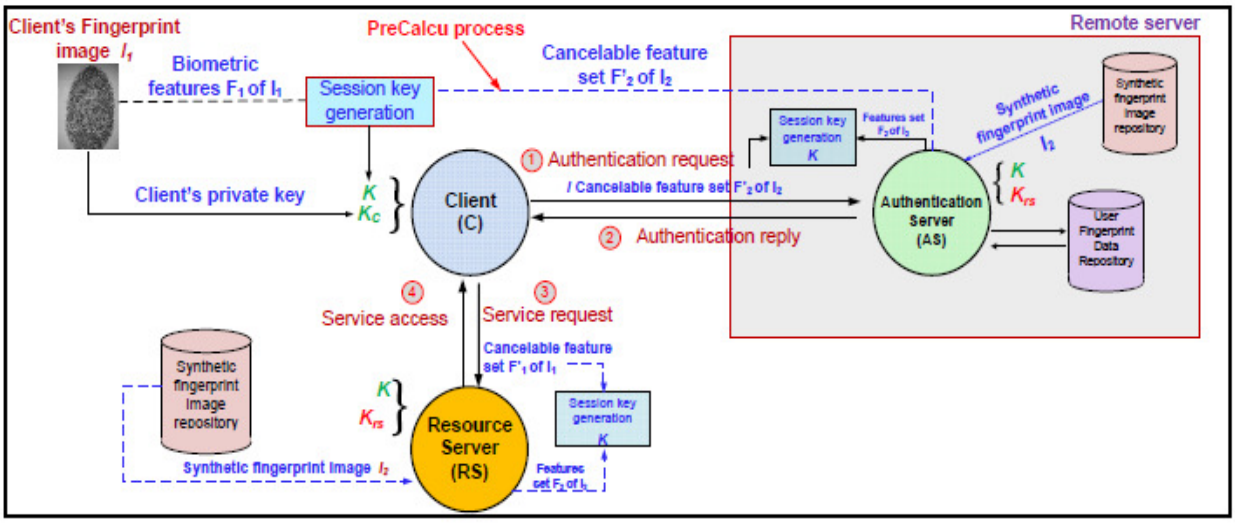

Fig. 1: The proposed BioCAP: An overview

confining an individual who isn't approved

from getting to the information. Accessibility alludes to the information being accessible for access at some random time. Client confirmation is a need to have the option to limit the entrance of the cloud administration to just the individuals who are bound to admittance to the information put away as a feature of the Cloud administration. The client must be recognized utilizing either distinguishing proof component to authenticate him towards getting to the cloud computing services.(Li et al., 2009) The client verification can be worked with by an ID confirmation about the client through strategies like a secret word, biometric characteristics and so on Our work is an endeavor in having a wide outline of the current verification methods. The examination at first spotlights on the information security and protection worries in cloud computing with the assistance of cloud administrations. The paper then, at that point steadily proceeds onward to the kinds of confirmation and a short examination of each sort. The embodiment of this paper is to have a thorough foundation investigation of the biometric based verification methods in cloud computing administrations. We have addressed all the current biometric validation methods comprehensively in two kinds to be specific physical biometric and social biometric qualities. The paper indicates the greater part of the major existing verification procedures which have either been executed or have been proposed by giving a brief about that biometric attribute is utilized to authenticate, its variables of ID, its benefits and bad marks.

2 Related Work

In this segment, we predominantly talk about existing biometric-based client

validation plots that have been introduced in the writing.

Jiang et al. [13] planned a secret key based client verification conspire for remote sensor networks (WSNs). This is a two-factor validation plot as it depends on both a keen card and some secret key. During the client enlistment measure, an approved client registers or re-registers with the trusted passage hub (GWN). The GWN then, at that point gives a brilliant card having the applicable qualifications that are put away on the savvy card. Also, all the conveyed sensor hubs are enrolled through a safe channel with the GWN and acquire their individual mystery qualifications. Utilizing the pre-stacked certifications, a real client authenticates with an assigned sensor hub with the assistance of the GWN during the login and verification stages. Nonetheless, Das [22] later showed that this specific plot is powerless against advantaged insider assaults, where an interior client of the confided in power (i.e., an insider aggressor) having the enlistment data of an enrolled client can mount different assaults in the framework, like client pantomime assaults. Additionally, it was likewise shown that this plan does not give appropriate validation, and neglects to help new sensor hub arrangement in an objective field. As a countermeasure, Das [22] introduced an improved and effective three factor verification conspire, where the three variables are a brilliant card, the client's secret phrase and the client's very own biometrics. Notwithstanding, the plan proposed by Das [22] doesn't save sensor hub obscurity.

Althobaiti et al. [14] proposed a biometric-based client verification component for WSNs. Be that as it may, their plan is uncertain against pantomime assaults and man-in-the-center assaults [23]. Das [23] then proposed another biometric-based client validation approach.

Xue et al. [15] likewise planned a transient accreditation based shared authenticated key arrangement system for WSNs. In their plan, the far off approved clients are allowed to get to approved sensor hubs in request to acquire data and furthermore to send some significant orders to the sensor hubs in WSN. In this plan, the GWN issues fleeting accreditations to every client and sensor hub sent in WSN with the assistance of the secret phrase based validation instrument. Afterward, Li et al. [24] illustrated that Xue et al's. conspire neglects to oppose taken verifier, disconnected secret key speculating, insider, many signed in clients, and keen card lost assaults. He et al. [25] likewise showed that Xue et al's. conspire is unreliable against client pantomime, disconnected secret key speculating, adjustment and sensor hub pantomime assaults.

Turkanovic and Holbl [26], and Turkanovic et al. [16] proposed other client authenticated key understanding methodologies. Be that as it may, Turkanovic et al's. conspire [16] is uncertain against brilliant card robbery, disconnected secret phrase speculating, client pantomime, disconnected personality speculating, and sensor hub pantomime assaults [27]. Park et al. [17] planned a protection saving biometric-based client verification

instrument utilizing savvy card, which uses hashing activity for biometric check. Nonetheless, the plan is uncertain against forswearing of-administration (DoS) assaults [28].

Dhillon and Kalra [18] planned a biometric based client authenticated key arrangement component for secure access to administrations given by Internet of Things (IoT) gadgets. In spite of the fact that this plan utilizes lightweight tasks, it doesn't secure against DoS assaults as it utilizes the perceptual hashing (biohashing) activity rather than fluffy extractor [28]. This is basically in light of the fact that the biohashing procedure scarcely makes a special worth BH(BIOi) from the biometric information BIOi of a genuine client Ui at various information times however it might diminish yield blunder [28], where BH() is the biohashing capacity.

Kaul and Awasthi [19] planned an authenticated key understanding plot, however it was subsequently uncovered to be uncertain against client pantomime and disconnected secret word speculating assaults [20]. Also, the plan of Kaul and Awasthi [19] does not safeguard client secrecy.

In this way, Kang et al. [20] proposed an improved bioemtric-based client validation plot. Nonetheless, this plan is uncertain against DoS assaults and furthermore pantomime assaults where a favored insider aggressor can undoubtedly mount such an assault.

Xia et al. [29] planned a neighborhood descriptor, called the Weber nearby paired, to work with finger impression liveness location. Their instrument depends on Support Vector Machine (SVM). In another work, Yuan et al. [30] presented a paired example (BP) neural network, which answers on finger impression liveness recognition. In their methodology, the Laplacian administrator is applied to acquire the picture inclination esteems. From that point onward, various boundaries for the BP neural network are tried to achieve predominant recognition exactness. We allude the intrigued peruser to [31] for a extensive writing survey of unique finger impression based biometric verification strategies.

Wang and Wang [33] presented distinctive property of client security depravity in two-factor confirmation plans for remote sensor networks (WSNs). They planned two unique delegate plans to uncover the difficulties and nuances in planning two-facto validation for security saving for WSNs. They likewise presented a game-based security model for two-factor verification.

3 Authentication Methods

The fundamental undertaking of authentication is to approve the client's identity when he attempts to get to a substance put away in the Cloud service.(Babaeizadeh et al., 2015) The main rule of authentication centers around the proof of information, for example, conventional password based authentication method which has a great deal of burdens with regards to distinguishing the user.(Yassin et al., 2012)

Firstly, a password based authentication doesn't confirm the identity of the client in essence. It simply requests a certain mix of characters to be entered. Besides, most clients will in general utilize a typical password on various sites. As on account of the Dropbox examined before, the significant explanation for the break-in was password recovered from comparative outsider sites. Thirdly, there is an absence of system to follow the client identity throughout some stretch of time. Accordingly, password is definitely not a strong methodology and besides different angles like a PIN or OTP based two-factor procedures are additionally not secure. This is obvious from the example of Cloudfare where the two factor authentication was by-passed.(Ahmad and Ehsan, 2013, Babaeizadeh et al., 2015)

The next authentication rule centers around confirming identity through the proof-of-possession. This likewise doesn't seem to be a powerful innovation as there is still degree for control into the cloud administration. There are conceivable outcomes of burglary or loss of the brilliant cards, tokens and so forth and it presents a gigantic danger to information dwelling in the distributed computing administrations. Albeit a couple of these components include biometric highlights for example, palm veins likewise, it can't be grouped either as proofof-possession or proof-of-identity totally (Ziyad and Kannammal, 2014)

The third authentication guideline centers around confirming the identity of the client through his attributes. The framework checks for the proof-of-qualities that is intrinsic in a client or that the client shows over the span of his connection with the framework. These are profoundly identified with the physical or the behavioral parts of the individual client and are bound to be a superior methods for authentication than the strategies referenced previously. The lone significant disadvantage of this authentication is that in numerous cases, there is a requirement for an outer equipment gadget to work with the authentication process.(Singh and Singh, 2012) Our concentrate further spotlights on just the current Biometric based authentication strategies that have been discovered to be more productive than other conventional methods.

4 Biometric Authentication

Biometric authentication alludes to the recognizable proof of human by their Physical qualities or conduct characteristics. Biometric authentication for the most part upholds three fundamental elements which are recognizable proof, authentication and non-disavowal which is utilized for distinguishing the physical and the behavioral properties of the people. This authentication has supplanted the customary structure which utilizes the cryptographic methods based on keys. Biometric authentication are static authentication framework where the individual will be checked at the beginning of the actual interaction. The biometric authentication in itself has been arranged comprehensively into the Physical Biometric method and the behavioral biometric method.

4.1 Physical Biometric Method

Unique finger impression The finger impression is a profoundly unmistakable component in people as no two people share a similar finger prints. Henceforth it is a strong proof-of-trademark for the identity of individual client while performing authentication. The finger impression designs are distinguished utilizing sub-qualities such as hybrid, center, bifurcation, edge finishing, island, delta, pores and so on The significant disadvantages of unique mark as an authentication is that the parts of skin surface like dryness, wetness can altogether influence the nature of the unique mark authentication. Likewise, this authentication isn't proficient in situations where the fingerprints of the clients like concentrated workers, elderly folks individuals and so on are blurred. (Araújo et al., 2005, Manasa et al., 2014) Like a few other physical based biometric authentication methods, there is a requirement for extra equipment to help the utilization of this authentication.(Singh and Singh, 2012)

Palm print-The confirmation done utilizing palm prints close by is a new turn of events and is being utilized in a more extensive space of biometric based authentications. Like a finger impression, the palm prints are additionally viewed as interesting and are discovered to be better compared to fingerprints in perceiving prints with consumes, oil stains, cuts and so on The sub-attributes used to verify a client through a palm print authentication incorporate chief lines, wrinkles, edges, distal cross over wrinkle, proximal cross over wrinkle, pores, particulars etc.(Manasa et al., 2014) Iris recognizable proof The authentication in this procedure includes check done by coordinating with the sub-attributes around the student of eye. An example of the eye's iris is developed utilizing peculiar highlights like angling tendons, fiber, spots, wrinkles, edges rings, crown, fractures Its total example is developed through peculiar highlights, for example, curving tendons, fiber, spots, wrinkles, edges, rings, breaks, crown and so on The sub-attributes that are focused on incorporate student, sclera, pupillary region, collarette, outspread wrinkles, sepulchers, shade spots and concentric wrinkles. Iris ID is for the most part utilized for high security Application. Iris Patterns arise in eighth month and stays same all through the lifetime. The significant disadvantage is that Iris ID can't be applied all around and isn't feasible for individuals experiencing extreme eye sickness and outwardly tested people.(Manasa et al., 2014)

Retinal Scanning-This authentication method includes confirmation of the client identity through the pictures of blood vessels toward the rear of eye by the utilization of infrared brightening. The sub attributes centered during the retinal checking are external iris, student edge, veins. The significant disadvantage is that, like Iris checking, it can't be perceived for individuals languishing from serious eye ailment and outwardly tested people.(Darve furthermore, Theng, 2015)

Hand Geometry-This authentication system includes the investigation of hand mathematical highlights like thickness,

width of palm, length and width of fingers in minute level to work with check. The hand calculation is definitely not an exceptional element however also, consequently can't be utilized as all around strong authentication strategy. In this way, it very well may be utilized as a strategy to confirm a client be that as it may, not recognize him. Yet, research has shown that it has huge achievement when utilized in mix with different highlights for authentication. Complex eye development In this authentication strategy, check is finished by consolidating with oculomotor plant attributes where numerical model for an eye and its related muscle development is set up when eyes react to boosts. In spite of the fact that, it is not difficult to secure and utilize, the defense of this method is as yet void. Hand vascular Movement-The authentication procedure includes check done by infrared light to deliver picture of individual's vein design in the face, wrist, hand and so on The essential ID sub-attributes are development in the lower arms also, the fingers. The method includes no physical contact with sensor and the example can recorded by any gadget like a video camera. The method is far reaching as in there is no exhibition debasement even within the sight of scars or hand pollution.

Face acknowledgment The facial acknowledgment authentication is done through the check of coordinating with the human face. It has not been discovered to be vigorous as human face is dynamic in nature. The pieces of ID used to work with the confirmation are eyes, eyebrows, nose, jaw, mouth highlights, hair and so forth The disadvantages, for example, changes in hairdo, facial hair and Aging making acknowledgment troublesome are solid. (Khan et al., 2015) Step This is an altogether different authentication method that includes check done by planning cyclic blend of development that will bring about human headway. It is by and large a strolling or running style of a person. This is a cutting edge authentication method and a portion of the recognizable proof attributes are running, running, getting objects, skipping and so on The significant disadvantage of this method is that the check is perplexed by maturing, foot wear, wounds and so on

4.2 Behavioral Biometric

DNA Recognition-99.7% of human DNA is shared where as 0.3% of the human DNA is variable and special. DNA isn't done continuously. A physical example, for example, hair strand, blood or then again spit of the individual client should be taken. DNA results can't be approved and confirmed promptly as the other biometric methods and this is a significant disadvantage. DNA based biometric framework can't be effortlessly animated however is obtrusive. Voice acknowledgment The biometric authentication utilizing the voice acknowledgment is finished by confirmation of voice recurrence, nasal tone, rhythm, Inflection and so forth to perceive the speaker. The voice is for the most part remarkable as far as the vocal recurrence. Voice based software can dissect and isolate voice dependent on a large number of boundaries that can even forestall impersonating of the one's voice by someone else. The significant benefit of a

voice acknowledgment authentication is that it doesn't need any exorbitant gadgets. The downside is that the voice of individual can change with age, disease, mental state. Also, Recorded voice can additionally played to sidestep the framework.

Personal stench In this strategy, confirmation is finished by dissecting the olfactory properties of the human body aroma. The authentication sensor will accumulate human scent from non-nosy regions like the rear of a human hand. Investigates bring up the certainty that smell.

5 Cloud Authentication Mechanism

This segment unequivocally centers around setting up how the biometric layout is installed in the cloud processing structure to guarantee authentication. The whole authentication mechanism utilizing bio-metric in Cloud can be comprehensively grouped into 3 phases – the Registration phase, Log-in phase and the Verification phase.(Sudhan and Kumar, 2015) The registration phase is the introductory phase wherein a client who likes to utilize the Cloud administration registers his biometric subtleties with the cloud figuring worker. The login phase quickly succeeds the registration phase furthermore, is the phase wherein the biometric highlight to work with admittance to Cloud is caught and verification for authentication is started. The real authentication happens in the verification phase.

5.1 Registration Phase

Capture the essential subtleties and afterward the biometric information to be utilized for authentication. Biometric information is checked for quality. Feature of the biometric information is separated. Generate a novel name for separated component for ID. Encrypt the element utilizing the public key acquired from cloud worker. Send it to the cloud worker after encryption. Cloud Sever then, at that point decodes the element and encodes once more (preparing) before store in the Cloud information base.

5.2 Login Phase

Capture the biometric information from the client for authentication. Extract the element that will be looked at. Calculate the name id for recognizable proof. Encrypt the concentrate layout utilizing the public key of the cloud worker. Send the concentrate format to the worker side post encryption. Cloud worker decodes the element format. Retrieve the scrambled format from the

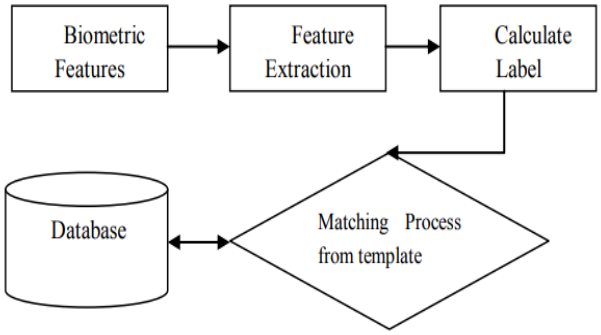

Figure 2: *Login Phase*

information base.

5.3 Verification Phase (sub phase inside the Login Phase)

Web API helps in the recovery of the format put away in the cloud and goes about as a connection between the UI and the cloud worker. Decrypt the store biometric format utilizing the pertinent decoding method. Compare the biometric format with the removed component contingent on rules set. If the layouts match, validate the client to get to the cloud administration. Else, end the client login meeting with suitable message.

6 Conlcusion

The paper is a push to play out a fastidious writing study on the current Biometric authentication methods utilized to get the information in cloud figuring administrations. We have examined the actual attributes based just as the conduct characteristics based authentication strategies as a piece of the biometric authentication. In view of our writing review study, we have discovered that regardless of the requirement for extra highlights to help execution biometric authentication, it is as yet a superior authentication procedure than the ordinary strategies as far as verification and ID of the client. Among the biometric attributes, every procedure has various benefits and burdens. Additionally, the social biometric attributes are more inclined to be influenced by mental differences of the individual client rather than the actual characteristics. The actual qualities likewise have certain disadvantages as talked about in before in this paper. What's to come course of our work will zero in on building a far reaching authentication model with a mix of the current physicalbehavioral biometric qualities just as thought of new angles of biometric attribute examination to diminish the disadvantages and increment the power of the cloud administration authentication set up. Besides, we additionally plan to deal with fresher parts of biometric characteristics and authentication calculations in our next phase of research. The primary targets of things to come research work to build the degree of safety gave to information in cloud administrations what's more, diminish the disadvantages related with the biometric authentication strategies that exist.

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 : endto-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 cheme 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. W. Yang, S.Wang, J. Hu, G. Zheng, and C. Valli, “Security and Accuracyof 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 Observationson Smart-Card-Based Password-Authenticated Key Agreement inDistributed Systems,” IEEE Transactions on Parallel and DistributedSystems, vol. 25, no. 7, pp. 1767–1775, 2014.