International Journal of Scientific & Engineering Research Volume 11, Issue 6, June-2020
ISSN 2229-5518

Role-Based Access Control (RBAC) in Cloud Computing Security

Sukesh Bhardwaj, Dr. Surendra Yadav

Abstract— Many Organizations look for consistent control and an exact diagram of clients and access over their frameworks. Overseeing access rights for many clients over an association, while holding consistency over the different frameworks are complicated and tedious. Having full control of access rights, which clients are continually changing in an intricate blend, IT frameworks and hierarchical structures and add to that nearby international guidelines and enactments, persistently suggesting changes. Your experience issues keeping these access rights are continually updated. RBAC sees the framework of clients being through the allocated roles, and from these roles, consents expected to perform specific capacities. RBAC implies that clients are not doled out from the authorizations legitimately, but instead secure them through their relegated activity capacity or roles, which means on the off chance that somebody joins the organization, moves offices, goes on leave, or leaves the association, and it is anything but difficult to oversee and stay in control of their access rights. This paper reviews the implementation of Role-based access controls also explores and examines the work done by other authors.

Keywords: Cloud computing, Cryptographic, Role-Based Access Control, Role-Based Encryption, Role-Based Security.

1 Introduction

The world of cloud computing is continually extending with more undertaking associations sending more applications to the cloud than any other time in recent memory. A 2019 study of about 800 IT experts found that the cloud computing innovation had almost arrived at full market infiltration with a reception pace of 91% for public cloud and 72% for private cloud arrangements. What's more, 84% of big business IT associations are overseeing more than one cloud foundation arrangement (multi-cloud) with the standard association running applications in five separate cloud situations. [1],[5] As big business cloud foundations keep on developing, IT experts become liable for making sure about a developing number of uses in progressively complex cloud situations. Controlling client access to applications and assets inside the cloud is an essential advance towards keeping up the security of the association's data resources and proactively ensuring against digital assaults.[1] RBAC is an essential ability for associations that convey applications into the cloud. With RBAC, IT security and tasks, experts increase the total perceivability and oversight into application authorizations. The capacity to effortlessly oversee who approaches cloud-based assets, what clients can access zones of the system and what kinds of activities clients can perform with the assets, they are allowed to use.[2]

2 Role-Based Security Concept

The philosophy of RBAC awards access to a cloud computing asset (or set of assets) based on a client's role inside the association. With people in every position allowed only enough adaptability and consents to play out the assignments required for their activity, the association diminishes general assault surface and level of weakness for digital attacks.[2],[4]

The RBAC philosophy based on three essential guidelines that oversee access to made sure about frameworks: [2], [3], [9]

- ***Role Assignment*:** If the client has expected a suitable role, each exchange or activity must be done. An activity is characterized taken regarding a framework or system object that is ensured by RBAC. Roles may be allocated by different gathering or chose by the client endeavouring to play out the activity.
- ***Role Authorization***: The motivation behind role approval is to guarantee that clients can just accept a role for which they have assigned appropriate permission. At the point when a client expects a role, they should do as such with approval from an administrator.
- *Exchange Authorization*: An activity must be finished if the client endeavouring to finish the exchange has a proper role.

In RBAC, every IT association is allowed to build up its attributes for every role. Roles on the system can relate straightforwardly to work roles inside the association, or they may primarily speak to sets of consents that might be doled out or approved for people based on other rules.

With these three principles as essential supporting for all RBAC frameworks, things can get very mind-boggling. A subject can have various role approvals, exchanging openly between roles relying upon the authorizations they require to play out a particular errand. [1], [3] This is normal in significant business security activities focuses where IT security and activities investigators work next to each other and may require various arrangements of authorizations for security or operational assignments. [6]

3 Prototypes of Role-Based Security

The National Institute of Standards and Technology (NIST), in proposing a brought together standard for RBAC portrays four distinctive execution prototypes for RBAC. These are not independent prototypes, be that as it may - they are levels of a similar prototype, with everyone based on the prerequisites of the past while including new useful capacities that

upgrade security and usability. [4] The prototypes of role-based security divided into four parts:

- ***Flat RBAC*:** Flat RBAC is based on the three essential principles of RBAC. What's more, Flat RBAC frameworks should bolster many-to-numerous client role assignments, many-to-numerous authorization role assignments, and ought to permit clients to utilize consents of different roles simultaneously. [4]
- ***Hierarchical RBAC*:** Hierarchical RBAC consolidates the entirety of the guidelines and capacities of Flat RBAC alongside help for pecking orders. A pecking order characterizes connections of rank between roles where senior roles relegated the whole of the consents of roles that are junior to them. Chains of command can be designed based on the requirements of the IT association and the capacities of the software instrument used to execute RBAC. A few devices force hierarchical structures like trees or modified trees, while others permit the IT association greater adaptability in planning an altered hierarchical prototype for doling out consents. [2]
- ***Constrained RBAC*:** A constrained RBAC consolidates the entirety of the highlights of the hierarchical RBAC, alongside help for separation of obligations (SoD). Separation of obligations alludes to the idea of requiring more than one individual to finish an errand. RBAC implies if workers of the association endeavour to submit a fake demonstration, they should include another person at the association with correlative authorizations - altogether expanding the all-out danger of getting captured.

  Also, a digital assault that accesses a solitary record - even one with elevated level consents - may at present come up short on the capacity to do significant damage as a result of SoD. [4]
- ***Symmetric RBAC*:** The most elevated level of RBAC usage, symmetric RBAC has the entirety of similar prerequisites of constrained RBAC alongside one new element: support for consent role survey with execution like client role audit. The thought here is that venture IT associations that desire to keep up consent assignments must have the option to survey and change the authorizations related to every role occasionally. While this procedure can demonstrate critical work and hard to oversee, it empowers associations to adequately respond to change and alter authorization role connections as needs are. [4]

4 Literature Survey

In the literature review, we have combined the various studies in the Role-Based Security in cloud computing and based on ways and concepts which the authors have taken the implementation-related issues of Role-Based Security. Some of the few important RBAC related studies have cited in this review paper:

4.1 Role-Based Security with Attribute-Based Access

A proper particular methodology of the attribute-based access control (ABAC) proposes utilizing the Event-B technique is described by **Gadouche et al., 2019** [5]. Authors apply the earlier proper confirmation to manufacture the right prototype in a stepwise way. The prototype demonstrates deliberation levels that are created through refinement tasks. A lot of ABAC properties is characterized in each degree of refinement beginning from the most elevated unique level to the most solid one. Proofs save these properties with the conduct particular. The methodology is delineated in social insurance web administrations. The authors **Chakraborty et al. (2019)** [6] recommended that ABAC arrangement mining issue expect that attribute esteems for different substances, for example, clients and items in the framework are given, notwithstanding the approval state, from which the ABAC approach should be found. Creators formalize the ABAC RuleSet Existence issue in this exceptional circumstance and develop a computation and unusualness assessment for its answer. Authors further present the idea of ABAC RuleSet Infeasibility Correction alongside a calculation for its solution. In another study, **Majid Afshar et al. (2018)** [7] suggested an ABAC structure for human services framework. They utilized the motor of ABAC for rendering and upholding social insurance strategies. Also, we handle crisis circumstances in this system. **Yingjie Xue et al.** (2019) [8] investigated an extraordinary attribute-based access control situation where various clients having distinctive attribute sets can work together to get entrance authorization if the information proprietor permits their joint effort in the access approach. They suggested an attribute-based controlled synergistic access control scheme through appointing understanding center points in the access structure. Security assessment shows that their suggested plan can guarantee data privacy and has various other essential security properties. Expansive execution assessment shows that our suggested plot is productive to the extent for storage and count overhead.

Additionally, **Yang Xu et al. (2018)** [9] suggested a doable fluffy expanded ABAC (FBAC) method to improve the adaptability in excellent critical approvals and in this way improving the asset ease of use and business practicality. We utilize the fluffy appraisal mechanism to assess the strategy coordinating degrees of the solicitations that don't agree to strategy, with the goal that the framework can settle on different endorsement choices in like manner to accomplish unattended extraordinary approvals. We likewise planned an assistant credit mechanism joined by occasional credit modification inspecting to direct expediential approvals for alleviating dangers. Hypothetical examinations and trial assessments show that the FBAC approach upgrades asset promptness and ease of use with controllable hazard. In another study, **Qasim Mahmood Rajpoot et al.** (2015) [10] suggested an access control prototype that consolidates the two prototypes in a novel manner to bind together their advantages. Their methodology gives fine-grained access control mechanism that not just considers logical data while settling on the access control choices but at the same time is

appropriate for applications where access to assets is controlled by misusing substance of the assets in the arrangement.

Muhammad Umar Aftab et al. (2015) [11] presented an access control prototype that amasses the qualities of RBAC and ABAC and evacuate a portion of the inadequacies of above-expressed prototypes. The suggested prototype actualizes and adventures the attributes of items, authorizations, roles, and clients as an establishment. Besides, the suggested prototype utilizes the role organizing capacity of ABAC and tight security conduct of RBAC. They likewise actualized the suggested prototype and examined a contextual investigation. Ultimately, in this portion, in another study, **N. Geetha et al. (2017)** [12] suggested a methodology which centres around the SaaS prototype of cloud. The two fundamental issues in Software as an assistance conveyance prototype are Access Control and piece of strategies when administrations are made. A legitimate protection safeguarding access control prototype is required for secure help provisioning and piece. In the suggested system, a safe help piece is made conceivable by positioning the potential chains of composite administrations as indicated by the client's role and the affectability of their information. As indicated by the role of a client, administrations are picked for arrangement, and the strategies are created. Additionally, the protection of the client post is looked after here.

4.2 ROLE-Based Security with Encryption

Lan Zhou et al. (2014) [13] presents a cryptographic legitimate prototype administration of cryptographic-RBAC for directing and actualizing access approaches for cryptographic RBAC plans. Administration of cryptographic-RBAC prototype uses cryptographic systems to ensure that the regulatory assignments are performed unmistakably by endorsed managerial jobs. By then, Creators suggested a RBE plan and show how the administration of cryptographic-RBAC prototype decentralizes the definitive assignments in the RBE plot as such creation it feasible for security approach the board in colossal extension cloud systems. In another study by the creator, **L. Zhou et al. (2011)** [14] depicts such a RBE plot using an impart encryption count. This paper portrays the security assessment of the suggested plan and gives proofs showing that the suggested plot is secure against attacks. Authors additionally investigate the proficiency and execution of our scheme and show that it has unrivalled qualities contrasted and other recently distributed schemes. **Yong Wang et al. (2018)** [15] arranged and executed a RBAC framework dependent on property encryption. The Client job task and the job assent task process are realized through attribute based encryption, with the objective that the entrance decision isn't, now dependent upon unequivocal methodology decision centers, ensuring the trustworthy usage of access techniques. In the meantime, their approach add ascribes to the RBAC prototype, executes attribute-based customer job assignments and role authorization assignments, which makes the access control process logically versatile. The endorsement affirmation and execution testing of a prototype exhibit the reachability of our plan. In one more paper by **Lan Zhou et al. (2013)** [16] suggested a RBE scheme that facilitates cryptographic procedures with RBAC. Our RBE scheme licenses RBAC procedures to be maintained for the mixed data set aside in public cloud. In view of the suggested conspire, they present an ensured RBE-based hybrid cloud storage engineering that allows a relationship to store information securely in a public cloud while keeping up the delicate information related to the affiliation's structure in a private cloud. They delineated a convenient execution of the suggested RBE-based plan and discussed the presentation results. They in like manner show that customers simply need to spare a singular key for unscrambling, and structure assignments are effective paying little regard to the multifaceted idea of the role progressive system and customer anticipation in the system.

Role-Based Encryption Scheme may be utilized for putting away the information safely in a cloud framework which is transferred by the proprietor of information. However, this encryption technique accepts that there will be the presence of a trusted administrator who will deal with all the client and role of association which don't occur in genuine condition. **Gajanan Ganorkar et al. (2015)** [17] suggested a prototype that gives versatile controls and the administrators by having two mappings, User to Role and Role to Privileges on the data. This prominent prototype which can be used for guaranteeing the data in the distributed storage. In this paper, Creators have executed the RBE plot, which can be completed with the RBAC prototype for taking care of data securely in the cloud system. In this framework client of any role who has been included by the administrator of association should remind just his decoding key which will be given by the administrator to the client when he may be added to a specific role. **G. V. Bandewar et al. (2015)** [18] means to diminish the issue of information access from the cloud numerous schemes are utilized to forestall this issue. RBE (Role Based Encryption) is exceptionally valuable to lessen organization among different clients of the cloud. They suggested a viable RBAC prototype to hold different security highlights like encryption, role the board, role chain of command, and so on. RBAC is the strategy for organizing access to PC as indicated by singular roles of the client in an undertaking.

4.3 ROLE-Based Security with Trust Management

The security objectives that ought to be considered in a proficient trust-based framework. At that point, **Mahdi Ghafoorian et al. (2018)** [19], suggested a novel trust and reputation based RBAC prototype that not solely can suitably withstand the security perils of trust-based RBAC prototypes, yet moreover is versatile as it has sensible execution time. From that point onward, they evaluate the suggested prototype using the famous trust arrangement of Advogato dataset. Over the long haul, they differentiate the suggested prototype and starting late circulated ones to the extent to mean an incomparable error, the execution time of convoluted trust figuring, and gave features. The cultivated results shows the suggested prototype to be used in certified cloud conditions. In another study, **Huang Lanying et al.**

(2016) [20] suggested a trusted RBAC prototype (T-RBAC), by the blend of confided in instrument and job. The prototype cases self-ruling trust the board place, which could as an issue of first significance judge customer credibility before role mapping and consent allowing. On the off chance that the customer's trustworthiness doesn't show up at the breaking point regard, the customer won't get the authorization for resource get to. This would satisfactorily keep potential damage from unlawful ambush impelled by such customer. As claims moderately, minor believability, viably arrange blockage, upgrade the capacity to oppose impedance and throughput of the access control prototype. T-RBAC would organize, postpone and improve the framework proficiency to somewhat. The similar scheme used in another study **Yue-Qin & Yong-Sheng (2015)** suggested propels trusted access control prototype dependent on job task in distributed computing. It can hinder the unlawful customers getting to cloud data even more suitably. Uniting advantages of the Role Access and the Assignment Access control prototype, the possibility of reputation worth will be introduced, and a particular edge will be given. It can control the customer's gathering times by choosing the amount of reputation [21]. A flexible access figuring by carrying the trust into Cloud computing to pick the access control to the assets using an improved RBAC strategy to deal with dynamically eccentric and inconvenient issues in the cloud computing condition. **Wenhui Wang et al. (2011)** [22] suggested a ground-breaking security level and access control for ordinary resources. As such, it should give legitimate security organizations according to the dynamic changes of the standard resources. This access control prototype dependent on trust chooses if the customer has the alternative to pick up induction to the advantage by intensely affirming. Likewise, this mechanism can control the customer's noxious direct suitably.

Troubles of cloud access control, perceive appealing properties of access control prototypes, and present the novel outline theoretical semantics of the entrance control prototype is depicted by **Ray et al. (2014).** They determine how approval happens in the suggested prototype, and present how to consolidate highlights, for example, separation of duty (SoD) [23]. In another study, **Muthunagai and Anitha (2019)** [24] In another study, investigated that keeping up the client information on an exclusive close by storage gadget becomes a testing task. The cloud-based storage tends to this issue potentially by putting them away in a remote database through which the client can access the records from anyplace. In this study, the above security issues are tended to by dividing the client transferred information and wrapping of divided information with the suggested improved Attribute-Based Encryption strategy to amass at different areas. Protection of figure content at different focuses forestalls the client transferred information not been mediated by any interlopers. At last, the information situated at a particular point recovered with a decoding procedure. Subsequently, it downsizes the system traffic happened during the recovery of the client transferred information from a different location.

4.4 ROLE-Based Security with the use of Biometrics

Nagaraju et al. (2013) [25] suggested a Role-Based Access Control (RBAC) utilizing unique mark biometrics for cloud administration, which makes the administration in cloud increasingly helpful and secure to the purchasers. Suggested cloud administration means to convey dependable, subjective, straightforward and progressively conservative administrations to clients. Another study **Changhee Hahn** and **Junbeom Hur (2016)** [26], distinguished that to embrace biometric recognizable proof frameworks in reasonable applications, two fundamental snags as far as effectiveness and customer security must be settled all the while. That is, recognizable proof ought to be performed at an adequate time, and just a customer ought to approach his/her biometric qualities, which are not revocable whenever spilt. As of recently, different investigations have exhibited adequate insurance of customer biometric information; in any case, such frameworks need effectiveness that prompts excessive time use for recognizable proof. The most starting late investigated plot shows viability redesigns; anyway reveals client biometric characteristics to various substances, for instance, biometric database server. This dismisses client security. In this paper, [26] Creators suggested a powerful and assurance protecting novel imprint unmistakable evidence conspire by using cloud systems. The suggested plot extensively abuses the figuring power of a cloud, so most by far of the exhausting estimations are performed by the cloud authority center. According to our test results on an Amazon EC2 cloud, the suggested plot is speedier than the present plans and guarantees client security by abusing symmetric homomorphic encryption. Their security examination shows that during the distinctive confirmation, the customer unique mark information isn't unveiled to the cloud specialist co-op or finger impression database server. **Zuo et al. (2016)** [27] have planned a high-security two-way constant validation framework utilizing dynamic secret phrase and multi-biometric to understand the deficiencies of conventional data framework. To ensure the security of unique mark eigen worth and facial element esteem, they encode them with a dynamic secret phrase. By the technique for two-way validation, it not exclusively can guarantee confirmation server to perceive the clients, yet additionally ensure the clients to check verification server, viably keep data from spillage brought about by fake servers and altering. Right when they use the structure, the server gets face feature extraction information from the client at ordinary stretches, to make sure about the basic thought of the customer. The innovation of RBAC improves grant administrators. The advancements of MPEG-4 and close by directional mode LDP are used to deal with the information of human face, to assess the properties of the possible worth. **Wójtowicz A. and Joachimiak K. (2016)** [28] suggested setting based biometric confirmation prototype for cell phones suggested. It empowers deciding the most precise confirmation technique right now alongside the most exact type of communicating with a client w.r.t. Confirmation process. The nonexclusive prototype planned and checked with proof-of-idea execution establishes an establishment for building further versatile and

extensible multifaceted setting subordinate frameworks for portable validation.

5 Conclusion and Future Work

Cloud security is critical for both business and individual customers. Everyone needs to understand that their information is shielded and secure, and associations have genuine responsibilities to keep client data secure, with explicit fragments having progressively severe rules about data stockpiling. Along these lines, RBAC gives access to clients as indicated by their role. For role, the executive's role chain of importance is being utilized. The role-based progressive system gives just allowed information access to a unique role individually. Consequently, keeps up information security inside the association itself.

In future work, we also like to work in the role-based security following the dynamic approach of Biometrics and some sort of graphical passwords to make it more secure.

References

[1] R. Bose, X. R. Luo and Y. Liu, "The roles of security and trust: Comparing cloud computing and banking," *Proc-Soc Behavioral Sci.*, vol. 73, pp. 30-34, 2013.

[2] Y. A. Younis, K. Kifayat and M. Merabti, "An access control model for cloud computing," *J Inf. Security Applications*, vol. 19, pp. 45-60, 2014.

[3] A. Chatterjee, Y. Pitroda and M. Parmar, "Dynamic Role-Based Access Control for Decentralized Applications," *arXiv preprint arXiv: 2002.05547,* 2020.

[4] R. Vidhate and V. D. Shinde, "Secure Role-Based Access Control on Encrypted Data in Cloud Storage using Raspberry PI," *Int. J. Multidisciplinary Res Develop.*, vol. 2, pp. 20-27, 2015.

[5] H. Gadouche, Z. Farah and A. Tari, "A correct-by-construction model for attribute-based access control," *Clust. Comp.*, pp. 1-12, 2019.

[6] S. Chakraborty, R. Sandhu and R. Krishnan, "On the feasibility of attribute-based access control policy mining," in IEEE *20th Int. Conf. Inf. Reuse Integrat. Data Sci. (IRI),* July 2019, pp. 245-252.

[7] M. Afshar, S. Samet and T. Hu, "An attribute based access control framework for healthcare system," *J. Phy. Conf. Ser.* vol. 933, 2018, p. 012020.

[8] Y. Xue, K. Xue, N. Gai, J. Hong, D. S. Wei and P. Hong, "An attribute-based controlled collaborative access control scheme for public cloud storage," *IEEE Tran. Inf. Forens. Security*, vol. 14, pp. 2927-2942, 2019.

[9] Y. Xu, W. Gao, Q. Zeng, G. Wang, J. Ren and Y. Zhang, "A feasible fuzzy-extended attribute-based access control technique," *Sec. Comm. Net.*, 2018.

[10] Q. M. Rajpoot, C. D. Jensen, and R. Krishnan, "Attributes enhanced role-based access control model," *Int. Conf. Trust Priv. Dig. Bus.,* Sept. 2015, pp. 3-17.

[11] M. U. Aftab, M. A. Habib, N. Mehmood, M. Aslam, and M. Irfan, "Attributed role based access control model," in *IEEE Conf. Inf. Assur. Cyber Sec. (CIACS),* Dec. 2015, pp. 83-89.

[12] N. Geetha and M. S. Anbarasi, "Role and attribute based access control model for web service composition in cloud environment," in *IEEE Int. Conf. Computat. Intelligenc. Data Sci. (ICCIDS)* June 2017, pp. 1-4.

[13] L. Zhou, V. Varadharajan and M. Hitchens, "Secure administration of cryptographic role-based access control for large-scale cloud storage systems," *J. Comp. Sys. Sci.*, vol. 80, pp. 1518-1533, 2014.

[14] L. Zhou, V. Varadharajan and M. Hitchens, "Enforcing role-based access control for secure data storage in the cloud," *Computer J.*, vol. 54, pp. 1675-1687, 2011.

[15] Y. Wang, Y. Ma, K. Xiang, Z. Liu and M. Li, "A Role-Based Access Control System Using Attribute-Based Encryption," in *IEEE Int. Conf. Big Data Artific. Intellig. (BDAI),* June 2018, pp. 128-133.

[16] L. Zhou, V. Varadharajan and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," *IEEE Tran. Inf. Foren. Sec.*, vol. 8, pp. 1947-1960, 2013.

[17] G. Ganorkar, A. Deshmukh and M. D. Tambhakhe, "Implementation of role based access control on encrypted data in hybrid cloud," *Int. J. Comp. Sci. Mobile Comput.*, vol. 3, pp. 384-390, 2015.

[18] G. V. Bandewar and R. H. Borhade, "Role Based Encryption with Efficient Access Control in Cloud Storage," *Int. J. Sci. Res.* (IJSR), 2016.

[19] M. Ghafoorian, D. Abbasinezhad-Mood and H. Shakeri, "A thorough trust and reputation based RBAC model for secure data storage in the cloud," *IEEE Tran. Paral. Distribut. Sys.*, vol. 30, pp.778-788, 2018.

[20] L. Huang, Z. Xiong and G. Wang, "A trust-role access control model facing cloud computing," in *35th Chinese Cont. Conf. (CCC),* July 2016, pp. 5239-5242.

[21] F. Yue-Qin and Z. Yong-Sheng, "Trusted Access Control Model Based on Role and Task in Cloud Computing," in *7th Int Conf. Inf. Tech. Med. Educ. (ITME),* Nov. 2015, pp. 710-713.

[22] W. Wang, J. Han, M. Song and X. Wang, "The design of a trust and role based access control model in cloud computing," in *6th IEEE Int. Conf. Pervas. Comput. Applicat.,* Oct. 2011, pp. 330-334.

[23] I., Ray and I. Ray, "Trust-based access control for secure cloud computing," in *High Perform. Cloud Audit. Applicat.,* Springer, NY, pp. 189-213, 2014.

[24] S. U. Muthunagai and R. Anitha, "Secure Access Control Method in Cloud Environment Using Improved Attribute Based Encryption Technique," *Int. J. Engineer. Adv. Tech. (IJEAT)*, 2019.

[25] S., Nagaraju, L., Parthiban and B. Santhosh Kumar, "An enhanced symmetric Role-Based Access Control using fingerprint biometrics for cloud governance," *PCCR*, vol. 1, pp. 12-18, 2013.

[26] C. Hahn and J. Hur, "Efficient and privacy-preserving biometric identification in cloud," *ICT Express*, vol. 2, pp. 135-139, 2016.

[27] H. Zuo, Y. Shen, S. Li and H. Shen, "Two-Way Real-Time Authentication System Based on Dynamic Password and Multi-biometric," *Int. Conf. Comp. Sci. Ser. Sys.,* Aug. 2012, pp. 1254-1257.

[28] A. Wójtowicz and K. Joachimiak, "Model for adaptable context-based biometric authentication for mobile devices," *Per. Ubiquit. Comput.*, vol. 20, pp. 195-207, 2016.