Preservation Of Iris Biometrics In Cloud With Cloud Id Screen Algorithm

A.Arulprakash, R.Viswanathan

Abstract: Biometric has a vital significant role in identity or authentication. Since designing a secure and efficient authentication system in cloud is still a challenging one. Biometrics is more valuable assert which is security parameters for many secure environments. Biometrics with Cloud-ID-Screen uses less cloud space and quit large computation and produces comparably increased security, in the same time speed is quite high as compare to the iris cloud Id Screen. Increased security is done by dividing the iris features into several units and stored under the different clouds. Therefore, no individual cloud storage has the complete set of iris features while at the time of matching operation all the units of iris features has been retrieved from the clouds and perform the matching operation. Here parallel processing techniques has been used for to reduce the time consumption. The experimental results here are compared with the existing fingerprint algorithm to find the efficiency of our IRIS based algorithm. This comparison clarifies that the proposed has greater values as compared to the existing finger print algorithm. Proposed IRIS algorithm produces excellent results in 4 and 8 groups. But the 16 and 32 groups it has quit less genuine acceptance rate because of smaller amount of templates. As compared to the finger prints iris has little amount of templates for matching. When divide these smaller templates to the larger amount the originality has reduced so the genuine acceptance rate will little reduce with the group of 4 and 8. Results clears that when the number of group is increased then the genuine acceptance rate is reduced.

Index Terms: Cloud security, Matching Process, Cloud – ID-Screen, Biometric.

1 INTRODUCTION

Cloud storage is more generously useful in for individual and as well the organiza-tion in terms of availability, scalability, usage of unbounded resources and processing of large data like biometrics. Because of these behavior of the cloud, biometric system utilizes the cloud computing or storage for the authentication not only for the processing it improves the performance, reduction of computation cast of identification, matching and decryption of template from the cloud, and security over the cloud environment. And also, it takes the advantages of secure data sharing data among the multiple personals and entity or the organization. Although, teem for the computation [5]. In India, the government of India collecting every citizen's iris, fingerprint and personal data (contact details) for the purpose of identification in the name of AADHAR. Cloud provides a many advantage but still the privacy and security is the major concern on data while storing and transmission [19] [20]. Even though, biometric information itself more sensitive information. And it has been under attack by many attacks like adversary attacks and intrinsic failures and [10] [13]. Furthermore, bio-metric dilemma attacks and doppelganger attacks are as well measured dangerous to the privacy and security of a biometric based system [10] [18]. Nevertheless, More Techniques are available to secure the biometric data from those attacks. For exam-ple, Template protection schemes have been implemented to resolve the security problem which has four classifications [16]. But unfortunately, the security problems still exist and it became more challenging. Few of these methods keep the biometric data as it is which means storing the data without encryption. This leads the data insecurity for the many attacks [13].

- *A.Arulprakash*, School of Computing Science and Engineering, Galgotias University, Uttra Pradesh, India. Email: arulprakash@galgotiasuniversity.edu.in*
- *Dr.R.Viswanathan, School of Computing Science and Engineering, Galgotias University, Uttra Pradesh, India. Email: rvnathan06@gmail.com*

To avoid this few techniques, store the information in encrypted type [6] however it makes the method time intense and wish the information to be decrypted throughout matching process that represents the biometric system to unconstitutional try [19]. Additionally, man biometric systems get affected by accuracy and performance problem [8] [20]. To lecture to the privacy and security drawback of biometric information like iris, fingerprint, we have a tendency to introduce a way referred to as Cloud-ID-Screen plot. Cloud ID screen is the platform where expected to store and compare iris information in different clouds or systems though keeping exactness, refuge, assurance, growing the rate of getting ready. In the center of the selection assignment, Cloud-ID-Screen parts interesting iris structures (i.e. consolidate table) into little groups subject to detachments, by then passes on these groups of match tables into different cloud simultaneously. In the center of the organizing action, Cloud-ID-Screen compares test groups of the one of a kind iris impression features against all showcase groups of all iris impression incorporates into parallel, by then reestablishes the planning score. Cloud-ID-Screen make use of negligible exertion cloud processing or accumulating and Hadoop, Map Reduce, to pass on and process one of a kind check textures while improving security and assurance while quickening the methodology of the biometric data and undertakingsThe remaining paper has been illustrated like: under section II, gives the detailed work of the previous system. Section III deals Objective of the proposed system. Cloud ID screen algorithm has been described in the section IV. Experimental meth-ods and results and conclusion have been illustrated in the sections V, VI, VII respectively.

2 RELATED WORK

The biometrics based applications are increasing in recent times and it requires large processing storages also the separate processing unit. Rapid growth of this bio-metrics is not because of its multidimensionality, also for its responses against the application. Biometric performs well in de-duplication of among the n entities, Identi-fication of one among the n entities and verification of one with one entity. It is fine the growth is healthy to the environment but the problem is storage for the computa-tion which is managed by cloud. Sussman A et. al.[13] introduced the concept cloud to the

biometrics processing. Which has the advantages of large storage, parallelism, business processing's, flexibility, Robustness of data, supports biometric applications. Later they discussed about how to integrate advanced techniques of cloud to biomet-rics environment. Advance techniques are like Hadoop Map reduces, HDFS, Hadoop distributed file system, MangoDB, HBase, etc. Shelly et al. [16] developed iris based recognition system with parallel processing and sequential processing. They produced 67% of enhanced result for parallel processing over the sequential processing. All the above approaches are takes about speed up the process not about the security of the system. In 2018, F. Alsolami et al [17] found the solutions for the security problem that divides the biometrics into smallest units and stored in different clouds which produces the gentle response in security. He experiments the system with fingerprint but we have different types of biometrics. As in AADHAR we are maintaining both fingerprint and iris. It is important to increase the security of this biometrics. They are not discuss about the iris biometrics over the cloud in terms of security.

3 PROPOSED WORK

In this section, we tend to show the architecture of Cloud-ID-Screen for the both enrollment and matching operations. First, we tend to show however we tend to split gallery iris options into small groups and save them as gallery pair-table. Second, we split the probe iris features into small groups and save them as a probe pair-table. Finally, we tend to show the way to match the probe pair-table against all gallery pair-tables and return the matching score.

3.1 Enrollment Operation of Cloud-ID-Screen

Among the term of enlistment task, Cloud-ID-Screen takes a display unique mark picture and makes the details indicates all at once build the combine table dependent on the NIST Bozorth iris matcher [26] and Forest-Finger coordinating calculation [9]. At that point, Cloud-ID-Screen parts display the match table of every iris highlight into littler groups dependent on separation where the separations are diverse in every group. Cloud-ID-Screen parts the exhibition match table without cover between groups to keep up security and protection. When these little groups of the display match table are made, Cloud-ID-Screen circulates those exhibition groups of the combine table into various mists/machine stores one exhibition group of the combine table of every iris feature. Cloud-ID-Screen conspire bolsters three methods of group-part sizes for part each match table into littler groups: 8 Groups, 16 Groups, and 32 Groups. Figure 1 demon-strates the Cloud-ID-Screen enlistment operation. In the enlistment activity of 8-Groups mode, Cloud-ID-Screen parts the exhibition combines table (unique mark highlights) into 8 little match tables dependent on separation. The display match table comprises of relative separation between two particulars focuses and three relative points [9] [20].

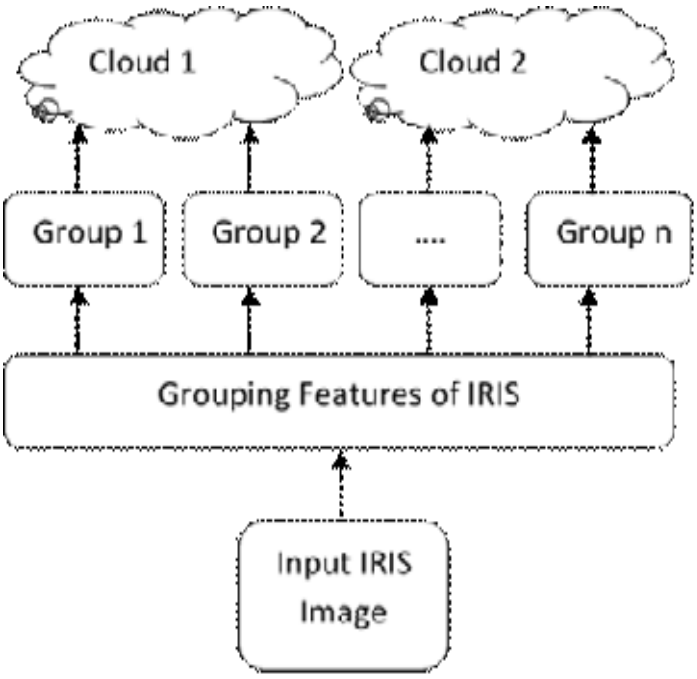

***Fig.1**. Cloud-ID-Screen Enrollment operation*

***TABLE 1.** CLOUD-ID-SCREEN DIVIDES THE PAIR-TABLE SUPPORTED DISTANCE INTO SMALLER GROUPS: 8 GROUPS, 16 GROUPS AND 32 GROUPS.*

Cloud-Id-Screen mode	*Groups*	*Distances*	*Machines*	*Clouds*
8 Groups	*Group-1*	*Between 0 and 2000*	*Machine-1*	*Cloud-1*
	Group-2	*Between 2000-4000*	*Machine-1*	*Cloud-2*
	Group-8	*Above 14000*	*Machine-1*	*Cloud-8*
16 Groups	*Group-1*	*Between 0-800*	*Machine-1*	*Cloud-1*
	Group-2	*Between 800-1600*	*Machine-2*	*Cloud-1*
	Group-16	*Above 12000*	*Machine-2*	*Cloud-8*
32 Groups	*Group-1*	*Between 0-400*	*Machine-1*	*Cloud-1*
	Group-2	*Between 400-800*	*Machine-2*	*Cloud-1*

	Group-32	*Above 12400*	*Machine-4*	*Cloud-8*

The information is put away in the exhibition match table dependent on the relative distance requested from the littlest to biggest separation. As appeared in Table 1, Cloud-ID-Screen parts the exhibition combine table into 8groups, where display group-1 stores the little separation of the display match table while display group-8 stores the biggest separation of the exhibition match table. In alternate words, display combine tables store sets with in-wrinkling separation. When each one of the 8groups of the match tables are created, Cloud-ID-Screen transfers those very little 8 sub-sets into the distributed storage wherever every cloud/machine store simply a single group of the combine tables to preserve up secu-rity and privacy. Additionally, Cloud-ID-Screen follows an equivalent technique as in 8-Groups Mode except for 16 and 32Groups.

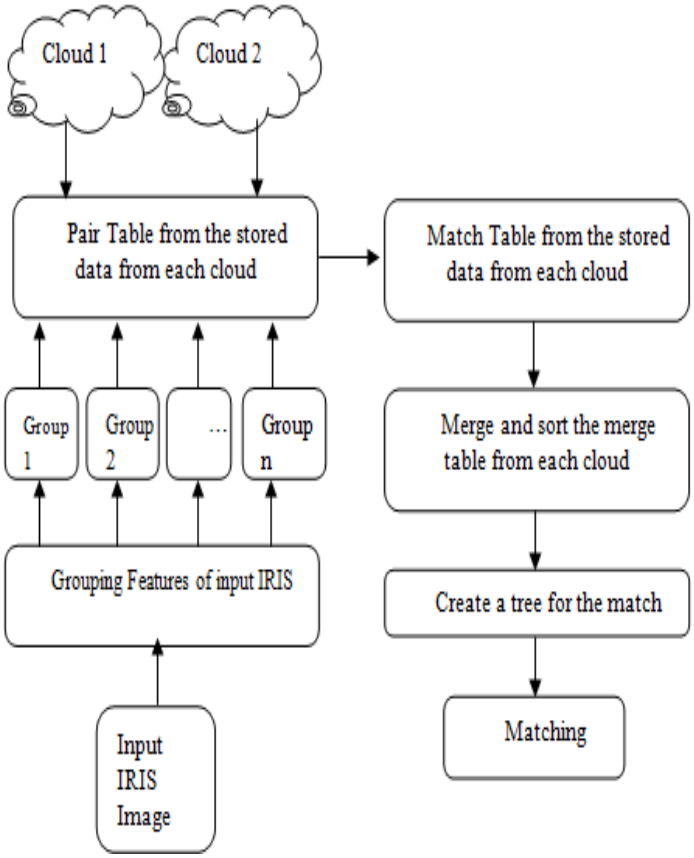

***Fig.2**. Cloud ID Screen Matching Process*

In 8-Groups, the group-1 begins from 0 to 2000, group-2 begins from 2000 to 4000 and so on and so forth until the last group where group-8 more noteworthy than 14000. While in 16-Groups mode, group-1 begins from 0 to 800, group-2 begins from 800 to 1600 and so on and so forth until the last sub-set where group-16 more note-worthy than 12000. Same as, in 32-Groups mode, the group-1 begins from 0 to 400, group-2 begins from 400 to 800 and so on and so forth until the last group where group-32 more prominent than 12400. Figure 2 illustrate the detailed architecture of the proposed system. Which accept the input of iris and features of iris are grouped for retrieval of template from the cloud. Once the all the templates are ready then all are merged into a single unit because templates are stored as smallest units and kept in different clouds. After the complete packaging of templates matching has been done with any of the standard matching approach.

3.2 Matching Process

Among the coordinative activity, Cloud-ID-Screen follows indistinguishable strides from within the enlistment task with the end goal to create the test combine tables. Once each single little group of the test combine tables are created, Cloud-ID-Screen coordinates these test groups of the match table against display groups of the combine tables that as of currently place away in the mists. Figure 2 and Algorithm 1 demonstrates the coordinative activity of Cloud-ID-Screen. In the coordinative activity of 8-Groups mode, Cloud-ID-Screen elements the combine table into 8 little sub-sets with the end goal to create the test match tables for 8-Groups mode. Once each one of the 8groups of the test match tables are created, Cloud-ID-Screen performs coordinative procedure (delineate and diminishing) between test groups against show groups with the end goal to process the coordinative score. In the phase of mapping, Cloud-ID-Screen organizes these test groups of the consolidate tables against exhibition groups of the match tables that are starting at now secured in mists. Cloud-ID-Screen matches test groups against exhibition groups where separations are comparative. In cloud-1 and machine-1, test group-1 matches against all display group-1, et cetera for all groups in all mists/machines. All postulations match occurs in parallel with the end goal to develop the match-table for all primary mark includes in each cloud/machine. At that point, in Cloud-1 or machine-1, Cloud-ID-Screen construct organize table-1, where arrange table-1 is a consequence of coordinating between test group-1 against display group-1 et cetera for other test/exhibition groups in all mists/machines. In the fading stage, the mappers give the reducers most of the match-tables that were by taken worked in guide different mists/machines. By then, Cloud-ID-Screen combines facilitate tables from related characters across over neighboring mists/machines. Along these lines, Cloud-ID-Screen constructs steady details combine aggregate tables (CMPG) from the given match tables with the end goal to make associate between columns to create trees and frame woodland. Finally, Cloud-ID-Screen enrolls the match score and returns only the greatest coordinating score alongside its ID. Similarly, Cloud-ID-Screen seeks after in distinguish capable method from in 8-Groups Mode yet for 16 and 32Groups.

4 EXPERIMENTAL DESIGN

Upgrading the accuracy and enhancing the speed of Cloud Screen is the ultimate aim of this experiment. The procedure compares two architectures, one is Iris matching algorithm and another one is cloud ID Screen.

Input: input image I_j where j=1,2,3,. . . n
Output: matching score
for (all input image j = 1 to n)
    Extract the minutiae point $m_{j,}$ Each point has location, angle and quality
    Create a minutiae file (fm_j) for each K_j
    Build a Pair Table(t_j) for minutiae file

Cluster the Pair Table(t_j) into group g_j based on the relative distance and angle of the pairs in fm_j.
for(all group g_j)
Compare the input group with stored group of the templates which stored in various cloud.
for (Each matching in each cloud)
Build a match table(mt_j) for different cloud
Each match table(mt_j) contains two minutiae point of both input image and store template image, distance of the points and angle between the points
Combine all the match table(mt_j)
for(from each mt_j)
Find the consistent points and form a consistent group
Where minutiae point of input image is not matched with many points of stored template image
From the consistent point group construct a tree using the points

Calculate the forest matching score for all the input images with the stored template image Return the maximum score among all the matching score. Algorithm 1: Minutiae matching algorithm (MMA) for Cloud-ID-Screen. We designed the work on utilizing Hadoop MapReduce algorithm [2].In the experiment, we built the pair-tables from iris images and saved them in text files (Cloud-ID-Screen ((8-Groups) pair-tables, Cloud-ID-Screen (16-Groups) match tables, and Cloud-ID-Screen (32-Groups) consolidate tables), for both display and test unique iris pictures. Among the enlistment activity, we exchanged the display match tables to Amazon S3. We utilized 8 conveyed storage focal points of Amazon S3 open cloud storage (N. Virginia, Oregon, N. California, Ireland, Singapore, Tokyo, Sydney, and Sao Paulo). In the midst of coordinating operation, we used Amazon Elastic MapReduce (EMR) [1] to synchronize the test combine table of exclusive mark highlights against all display match table in parallel. By then, EMR lessens the eventual outcomes of planning and reestablished the coordinating score with the balance Iris ID. We associated our coordinating calculation to a generally known dataset (F V C2002Db2 a) [15]. This dataset has 8 impressions for 100 subjects, which suggests there are 800 novel iris impression pictures. The consequences of these investigations are the typical of something like twenty runs. We executed the experiment in C and Python. We created the mapper and reducer in C and ran it on Amazon EMR. For Internet affiliation, we utilized Comcast home Internet, with an intentional exchange band-width of 11.65 Mbps and a download data transmission of 37.12 Mbps.

4.1 Baseline Setup Process

We used Forest-Finger organizing calculation [9] as our standard. Amid the enlistment activity, we have a tendency to build the details focuses from distinctive iris impression pictures with the end goal to construct the match tables. At that point, we have a tendency to spared these displays combine tables in records. Amid the coordinating activity, we developed the particulars focuses from unique mark pictures with the end goal to construct the test match tables. At that point, we spared these tests combine tables in documents. We at that point utilized the Linux pipe direction line to coordinate the test and exhibition unique finger impression pictures alongside the score of coordinating. At long last, we got the aftereffect of coordinating as the ID of test and exhibition unique finger impression images alongside the score of coordinating.

4.2 Setup of Cloud-ID-Screen

In the midst of the enlistment task, we split each exhibition match table (unique iris impression highlights) into littler consolidated tables dependent on separation begin from group-1 to group-n (where n=8 in 8-Group mode, n=16, n=32). At that point, we made exhibition of n groups of together table where each group is spared in document arrangement to be consistent with Hadoop record framework. At that point, we transferred these exhibition n-groups of coordinative tables into Amazon S3 where every cloud/machine store one group. Among the coordinating task, we split every test combine tables (unique mark highlights) into n-groups of match tables dependent on a separation. We used the Amazon EMR [1] for coordinating. The mapper composed test group-1 in contrast to exhibition group-1 in cloud-1 and machine-1 et cetera for all the groups in all the cloud/machines. At that point, the mapper gave the reducer the most of the match-table that was by then gathered from the most of the mists/machines, one match-table for each ID. The reducer accumulated most of the match-tables together to create one match-table per ID. Finally, the reducer build the reliable coordinating table, trees, and backwoods of trees (we pursue Forest-Finger coordinating calculation [9]) with the end goal to process the coordinating score alongside the matching display ID.

5 RESULT AND DISCUSSION

In this trial, we try to demonstrate that in the event that we split the combine table of the unique finger impression highlights into little groups and disperse them over different mists/machines, we can in-wrinkle the coordinating velocity while keeping up practically identical exactness. We will assess to decide whether the Cloud-ID-Screen achieves its objective in quicker preparing as well as security. Right off the bat, we dismember if the Cloud-ID-Screen accomplishes their objective in precision by testing GAR and FAR, by then contrasting it with best in class gauge [9]. Besides, we break down if Cloud-ID-Screen accomplishes its objective in expanded speed by estimating the aggregate time, including mapping, diminishing time, for the coordinative activity and standing out it with best in class benchmark [9]. At long last, we make our inference if our experiment results bolster our speculation guarantee by utilizing formal insights (T-Test P-Value).

5.1 Evaluation of Accuracy

In the precision assessment, we assessed Cloud-ID-Screen in contrast to the cutting-edge standard (Forest-Finger coordinating calculation [9]). We pursued our examination split-ting the combine table, at that point we assessed the False Accept Rate (FAR) and Genuine Accept Rate (GAR) on the information previously we measure the execution, to guarantee that we have a for all intents and purposes indistinguishable exactness with benchmark [9]. In this investigation, we found that the Cloud-ID-Screen got promising results in 8-Groups and 16-Groups while it got equivalent outcomes in 32-Groups, Table 2 and Figure 3 demonstrate the subtle elements of these outcomes.

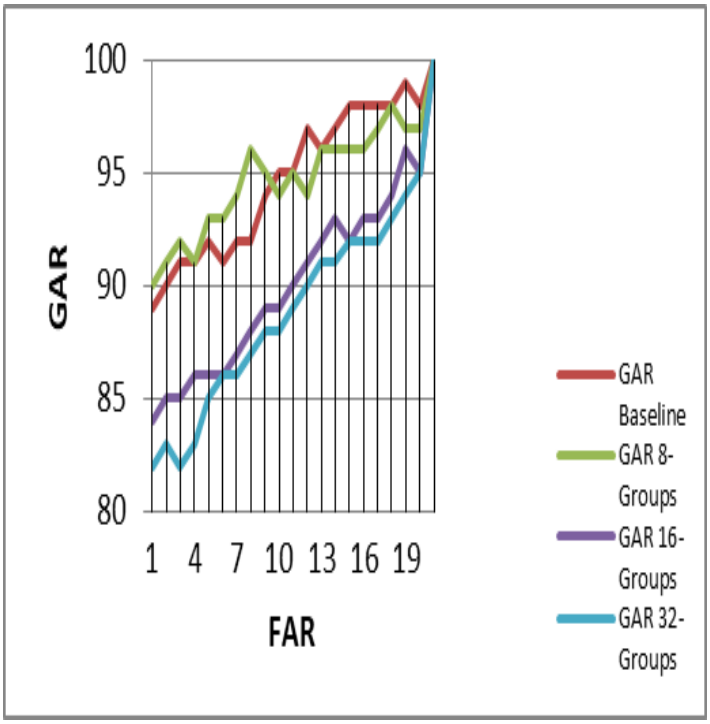

***Fig 3**. ROC curve comparing between Forest-Fingers algorithm and Cloud-ID Screen algorithm (group-8, group-16, and group-32).*

These promising results for Cloud-ID-Screen demonstrate that part the match table of the unique mark highlights into little combine tables would give a promising precision in 8-Group and 16-Group contrasting with the pattern [9]. Regardless, Cloud-ID-Screen has low precision in 32-Groups and this since we fragmented the combine table into 32 tables, which decreases the match includes that rely upon the limit in match calculation. In alternate words.

***TABLE 2**. THE COMPARISON BETWEEN FOREST-FINGERS ALGORITHM AND CLOUD-ID-SCREEN IRIS ALGORITHM IN TERMS OF GENUINE ACCEPT RATE AND FALSE ACCEPT RATE.*

Approach	*Metrics*	*Baseline*	*8-Groups*	*16-Groups*	*32-Groups*
Proposed IRIS Approach	*GAR*	*94%*	*93%*	*91%*	*91%*
	FAR	*0%*	*0%*	*1%*	*1%*
Forest Fingers Algorithm	*GAR*	*93%*	*93%*	*91%*	*89%*
	FAR	*0%*	*0%*	*0%*	*0%*

5.2 Evaluations of Security and Privacy

In the security and protection assessment, we assessed Cloud-ID-Screen against the cutting-edge benchmark [9]. We watch the parallel test in the enlistment and coordinating activities. In the enlistment activity, we see Cloud-ID-Screen does not store all gatherings of a couple table in one cloud/machine. Besides, Cloud-ID-Screen does not store unique mark pictures or particulars focuses, which can be imperiled. Nonetheless, Cloud-ID-Screen stores parts of a couple table in each cloud/machine. This circulation gives extra security to unique finger impression information in the cloud amid the enrollment activity. In addition, the security level in-wrinkles with the quantity of gatherings. At the end of the day, on the off chance that we increment the quantity of gatherings, the security level wills in-wrinkle. Thus, the 32-Group has the most noteworthy security level since the individual gathering just stores a little snippet of data. Along these lines, the individual gathering has an insignificant information about the special imprint features. In the midst of the coordinating activity, Cloud-ID-Screen could not gather all groups of a couple tables from all mists/machines with the end goal to perform coordinating. Cloud-ID-Screen coordinates each group of a couple table autonomously and in parallel at each cloud/machine, at that point gathers the outcomes (coordinate tables) with the end goal to figure the coordinating score. Cloud-ID-Screen gave security and protection to the unique mark includes in the cloud. Moreover, Cloud-ID-Screen gives more protection/security when utilizing the Forest-Finger coordinating calculation that matches slap unique finger impression pictures. Consequently, the Forest-Finger coordinating calculation is intended for unsegmented slap unique finger impression to give protection/security to the unique mark information while avoiding seeking with an idle print [9].

5.3 Availability of Cloud-ID-Screen

Cloud-ID-Screen gives adaptability to the coordinating procedure. Cloud-ID-Screen can coordinate 10,000 * N individuals in parallel and afterward blend the last most extreme coordinating score. This coordinating in parallel for different individuals up to N, gives the Cloud-ID-Screen greater versatility by including more mama chines and coordinating more individuals in parallel, at that point combining the last most extreme coordinating score.

6 CONCLUSION AND FEATURE WORK

From the experiment we can see the accuracy of the different group 8-Group, 16-Group and 32- Group. It clearly says that the accuracy has been increased in group 8 and baseline. Besides in other groups also has good accuracy which is little low with 8-Group and baseline. Therefore, if the number of groups increases the accuracy is also reduced. In other word number of groups is indirectly probation to accuracy. In terms of accuracy cloud Id Screen for iris is producing promising result. In future, we can extend the system with different matching algorithm to improve the accuracy and speed of the system.

7 REFERENCES

[1] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. DonidaLabati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva. Privacy-preserving fingercode authentication. In Proceedings of the 12th ACM Workshop

on Multimedia and Security, MM&Sec '10, pages 231–240, New York, NY, USA, 2010. ACM.
[2] Fahad Alsolami, Bayan Alzahrani, and Terrance Boult, Cloud-ID-Screen: Secure Fingerprint Data in the Cloud, IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA), 2018
[3] Bendale and T. E. Boult. id-privacy in large scale biometric systems. In 2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010, Seattle, WA,USA, December 12-15, 2010, pages 1–6, 2010.
[4] Y.-J. Chang, W. Zhang, and T. Chen. Biometrics-based cryptographic key generation. In 2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat.No.04TH8763), volume 3, pages 2203–2206 Vol.3, June2004.
[5] T. E. Boult, W. J. Scheirer, and R. Woodworth. Revocable fingerprint biotokens: Accuracy and security analysis. In The IEEE Conference on Computer Vision and Pattern Recognition(CVPR), June 2007.
[6] K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. EURASIP J. Adv. Signal Process, 2008:113:1–113:17, Jan. 2008.
[7] Y.-J. Chang, W. Zhang, and T. Chen. Biometrics-based cryptographic key generation. In 2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat.No.04TH8763), volume 3, pages 2203–2206 Vol.3, June2004.
[8] J. Dean and S. Ghemawat. Mapreduce: Simplified data processing on large clusters. In Proceedings of the 6th Conference on Symposium on Opearting Systems Design & Implementation-Volume 6, OSDI'04, pages 10–10, Berkeley, CA,USA, 2004. USENIX Association.
[9] Apache zookeeper. Zookeeper.apache.org, [Online]. Available:http://zookeeper.apache.org/.
[10] New biometric technology improves security and facilitatesus entry process for international travelers. Homeland Security, https://www.dhs.gov.[Available Online].
[11] Apache hadoop. Hadoop.apache.org, [Available Online] http://hadoop.apache.org/.
[12] Data catalog. Unique Identification Authority of India, [Available Online]: https://data.uidai.gov.
[13] Sussman, J. Trost, A. Maurer, and E. Kohlwey. Leveraging the cloud for big data biometrics: Meeting the performance requirements of the next generation biometric systems. 2011 IEEE World Congress on Services (SERVICES 2011), 00:597–601, 2011.
[14] Apache hbase. Hbase.apache.org, [Available Online].:http://hbase.apache.org/.
[15] Amazon emr amazon web services. Amazon Web Services, Inc., [Available Online] http://aws.amazon.com/elasticmapreduce/.
[16] Shelly and N. S. Raghava. Iris recognition on hadoop: A biometrics system implementation on cloud computing. In 2011 IEEE International Conference on Cloud Computing and Intelligence Systems, pages 482–485, Sept 2011.
[17] F. Alsolami, B. Alzahrani and T. Boult, "Cloud-ID-Screen: Secure fingerprint data in the cloud," 2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA), Singapore, 2018, pp. 1-8.
[18] Gokul Rajan V, Vijayalakshmi S, "A Novel Approach for Human Identification using Sclera Recognition" , International Journal of Computer Sciences and Engineering, Vol. 6, Issue 4,May 2018, 228 – 235.
[19] H. Takabi, J. B. D. Joshi, and G. J. Ahn. Security and privacy challenges in cloud computing environments. IEEE SecurityPrivacy, 8(6):24–31, Nov 2010.
[20] W. J. Scheirer, B. Bishop, and T. E. Boult. Beyond pki: The biocryptographic key infrastructure. In The IEEE International Workshop on Information Forensics and Security(WIFS), December 2010.
[21] K. Nandakumar, A. Nagar, and A. K. Jain. Hardening Fingerprint Fuzzy Vault Using Password, pages 927–937.Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.
[22] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. Journal ofNetwork and Computer Applications, 34(1):1 – 11, 2011.
[23] Watson, M. D. Garris, E. Tabassi, C. L. Wilson, R. M. McCabe, S. Janet, and K. Ko. User's guide to nonexport controlled distribution of nist biometric image software.Technical report, NIST, 2004.