International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Iris Authentication For Taas on Cloud

S.Karthik, K.Priyadarsini

Abstract: Security in cloud has become an important issue in day to day life. As consumers store all their important data in the cloud there should be a proper security available in cloud. The small sized and medium sized industries need a testing tool which is of high cost for testing their product. These companies utilize the cloud testing tools (Testing as a Service) by saving their product in the cloud which needs to be tested. The level of security is not much higher in cloud since the product information can be easily hacked by the third parties. In this paper, to overcome the issues in authentication and Data protection in Testing as a service –Taas, iris based authentication using cryptography has been proposed.

Keywords : Authentication, Biometrics, Cryptography, Data protection, Iris, Public key, Secret key

I. INTRODUCTION

Advancement in testing ensures the organization to guarantee higher quality products with extensively lesser funds. Subsequently the requirement for moving to the solution of the cloud developed to protect the organization for concentrate their centre business than suffering over the finance and support of their framework of IT. In any case, the agreement has a few issues looked regarding reliability, strengthen and support which the organization should concentrate on exact testing. Validating applications which is related to functional and non-functional aspects requires a selection of testing tools and due to this testing has become more complex and costly. Cloud service providers-CSP is the one who issues Cloud computing services. CSPs offer the services as to pay for what the user has been used. Cloud computing deal with various security types that concerns with Security in technology based on virtualization, Processing Vast distributed Data, accessibility, attack on massive traffic, Security on application, control over access, and verification. Procedure for physical protection has not provided by Cloud computing platform. Physical protection depends only on the user authentication. User authentication calls for a particularly assured security [12][13].

When the consumer tests their data in the cloud using the testing tools available in the cloud the consumer product information is not much safe being security is the main concern.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author

S.Karthik*, Department of ECE, SRMIST, Vadapalani, Chennai India. Email:skarthikvit@gmail.com

K.Priyadarsini, Department of CSE, VISTAS, Pallavaram, Chennai India. Email:priyadarsinikk@gmail.com

Security issues are solved in cloud computing by different techniques. One of the most accepted authentication mechanism is password authentication. Normally people pick phone numbers and names as their passwords. These passwords are very easy to remember but unprotected. Thus, the adversary can easily accumulate a chart of significant names or numbers to intervene the security. This procedure is known as the dictionary attack [14][15][16].

The security method of Biometric authentication depends on the distinguish characteristics of an human in biologically aspects being to confirm that who is he who says he is. The systems of Biometric authentication evaluate a capture of biometric data to store; confirm the data which is authentic in a database. Biometrics is generally focused on the face, fingerprint, iris authentication, and identification method. At the time of detection the face, iris, fingerprint will be checked for the available data with the reading procedure. If we use the cloud service, detection procedure is pursued by the verification process. The procedure data is detected by the system and it is similar with the existing data. If there is a match then the corresponding user will be authorized to use the service available in the cloud otherwise they will not be able to access. Biometrics is about character checking or distinguishing proof on physiological or behavioral qualities. The four levels of a Biometric system are level of sensor, feature extraction, matching module and the decision module [8].

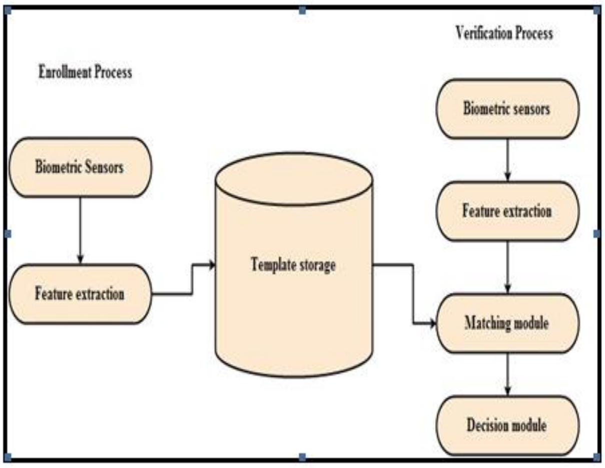

Fig. 1. Biometric authentication Process

Retrieval Number: L30231081219/2019©BEIESP
DOI: 10.35940/ijitee.L3023.1081219
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

II. EXISTING WORK

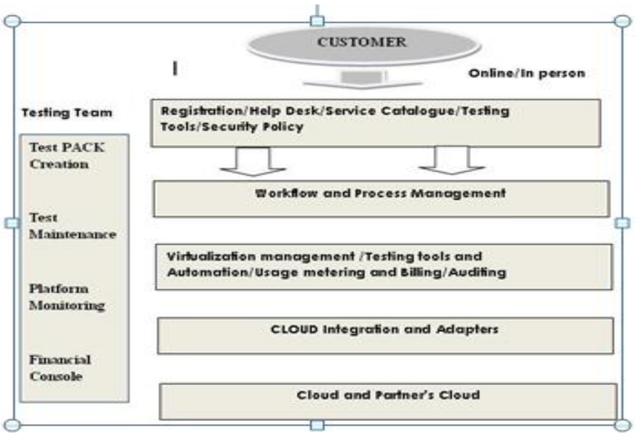
CUSTOMER
Online/In person
Testing Team
Registration/Help Desk/Service Catalogue/Testing Tools/Security Policy
Test PACK Creation
Test Maintenance
Platform Monitoring
Financial Console
Workflow and Process Management
Virtualization management /Testing tools and Automation/Usage metering and Billing/Auditing
CLOUD Integration and Adapters
Cloud and Partner's Cloud

Fig. 2. TaaS Architecture

The Existing architecture consists of four main Layers. Clients can avail the platform using online, or in person. This platform gives out a way for testing the application. The companies can use by uploading the application that needs to be tested or they can avail the other testing company to test their application by paying for the usage of testing tools.

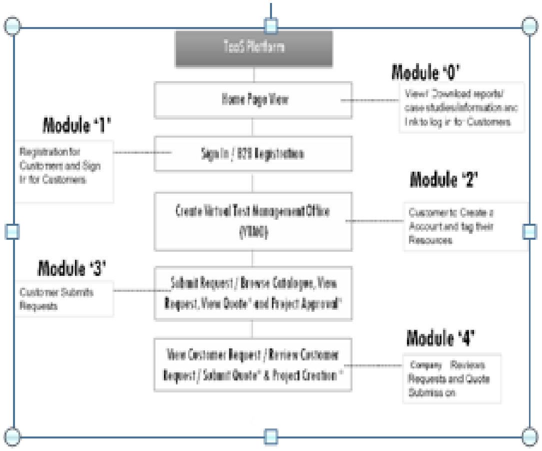
TaaS Platform
Module '0'
Home Page View
View/ Download reports/ case studies/information and link to log in for Customers
Module '1'
Sign In / B2B Registration
Registration for Customers and Sign in for Customers
Create Virtual Test Management Office (VTMO)
Module '2'
Customer to Create a Account and tag their Resources
Module '3'
Submit Request / Browse Catalogues, View Request, View Quote" and Project Approval"
Customer Submits Requests
View Customer Request / Review Customer Request / Submit Quote" & Project Creation "
Module '4'
Company Reviews Requests and Quote Submission

Fig. 3. The module*(0-4)* description

In the module 1 During the Registration process the companies register themselves and start using their application. They request for quoting of tools that they are going to use for the application. Once they got there quoting they upload their application and start using the testing tools. But the application that has been uploaded in the cloud will not be secured. Any third parties can hack the application and all the private information's will be hacked.

III. PROPOSED WORK

Iris biometrics combined with cryptography to provide a proper authentication. When the encryption on biometric verification is successful the data protection will be handled. During Registration end users iris image will be subjected to scanning and it will be transformed as x and y coordinates values using digital template format. Then the cloud consumer will ask for a public key from the cloud provider. Once the key received the consumer encrypt the iris digital template with the key using El Gamal public key crypto system. The encrypted key with the preset format is given to the cloud provider. There is decryption is taken place on encrypted digital template and the that is once again gets encrypted by the procedure of Blowfish encryption and it will be stored in the database of cloud providers.

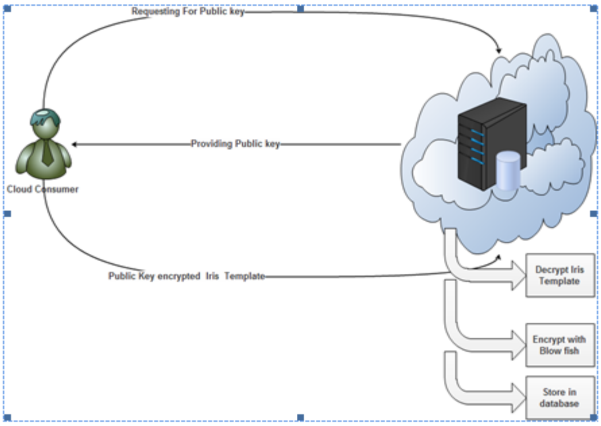

Fig. 4. Enrollment Phase

During Verification/authentication, the same procedure of encrypting the users IRIS image will be carried as out. So the ElGamal encryption of the template and forwarding the encrypted digital template to end of cloud provider will be done. At the end of cloud provider the iris digital template will be decrypted and customers enrolled iris template will be fetched from the database and decryption of that will be done by blowfish algorithm and that should l be matched with the digital template. is reduces The dilemma between security and privacy and security of stored template is reduced with the comparison of plain templates

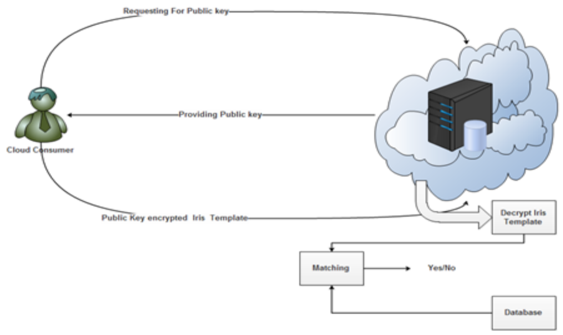

Fig. 5. Authentication Phase

IV. ALGORITHMS USED

A. Algorithms used

- *El Gamal Public key cryptosystem:*

Diffie-Hellman key exchange works of El Gamal encryption [11], Alice and Bob have a (publicly known) 'pr' as a prime number and a 'gr' as a generator

Alice chooses a random number ar and computes 'Ar' = gr^{ar}.

Bob choose a random number br and generates 'Br' = gr^{br}.

'Ar' is a Alice's public key and 'ar' is a private key. Like this 'Br' is a Bob's public key and 'br' is a private key.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

If Bob send a message 'mr' to Alice, then he picks a number 'kr' which is smaller than 'pr' then computes cr1,cr2 and sends cr_1 and cr_2 to Alice

$$cr_1 = g^{kr} \bmod pr$$
$$cr_2 = A^{kr} * mr \bmod pr$$

. Alice computing the recreate message m by

$$cr_1^{-ar} * cr_2 \bmod pr = mr$$
$$\begin{aligned} cr_1^{-ar} * cr_2 \bmod pr &= (gr^{kr})^{-ar} * Ar^{kr} * mr \\ &= gr^{-ar * kr} * Ar^{kr} * mr \\ &= (gr^{ar})^{-kr} * Ar^{kr} * mr \\ &= Ar^{-kr} * Ar^{kr} * mr \end{aligned}$$

$$= 1 * MR = MR$$

- ***Blowfish Algorithm:***

Feistel Network is followed by Blow fish Algorithm, iterating an encryption function 16 times. The size of block is 64 bits, and the key length can be up to a maximum of 448 bits. Each round has a key dependent permutation, and a substitution of key and data dependent. All operations are XORs and additions on 32-bit words. Four indexed array data lookups per round are only additional processes [10].

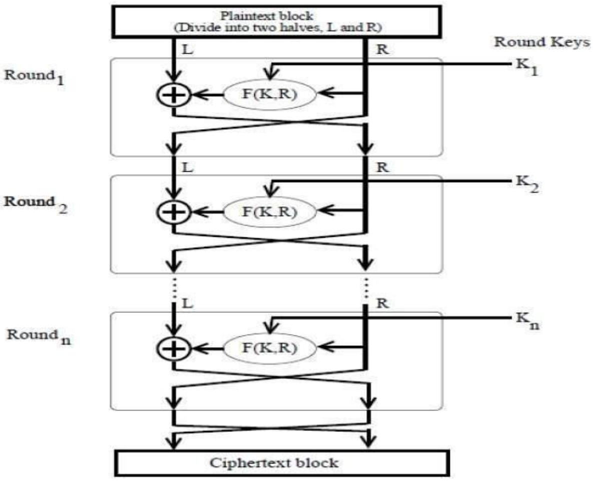

Fig 6: Sub key Generation

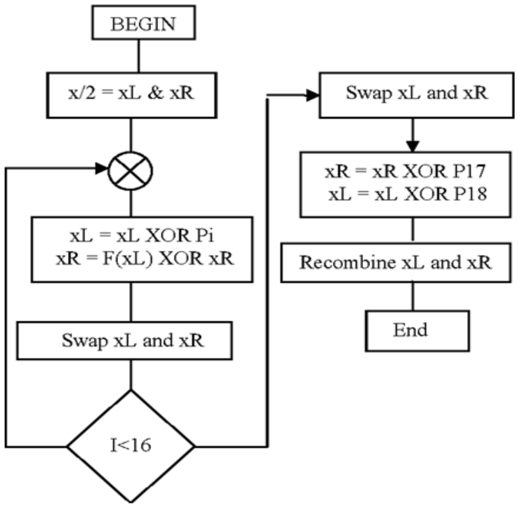

Fig 7: Flow Chart

The continuously changing Blowfish algorithm output will replacing all p entries array and then all four S-boxes in continue process. All required sub keys are generated by totally 521 iterations. Applications can supply the sub keys rather than execute this derivation process multiple times.

V. RESULT ANALYSIS

This implementation is tested with various attacks and that was tested for two different metrics .They are FAR- False Acceptance Rate and FRR -False Rejection Rate of eighty different user's Iris patterns. And the results are just about zero false acceptance rates. There is some higher level of FRR since I have used 90% threshold value. The threshold Value is reduced with the reduction of FRR but with the increment of FAR. Higher security FAR should be almost reduced. Threshold is directly proportional relation with FRR, and threshold is inversely proportional relation with FAR.

Table - I: FAR vs FRR

S.NO	ITERATIONS	USERS	FAR	FRR
1	1	25	0	2
2	2	35	0	2
3	3	55	1	3
4	4	65	1	4
5	5	75	1	6

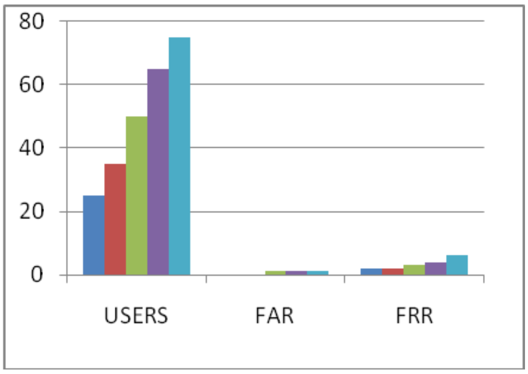

Fig 8: FAR vs FRR Representation in Graphical

VI. CONCLUSIONS

This Cloud based biometric validation has a frightening total addressable market worth and also there is a way for development of research work. In this paper, discussion on how the application saved in cloud can be secured till the testing has been done by the companies. And also discussion was made on existing issues which needs to be considered when designing biometric services. This biometric authentication which is based on Iris is presented for an required system that uses web applications and data management over the Cloud. The system approves the user's identity and access the data in easy and secure manner by providing strong authentication. Thus the biometrics adoption with cryptography ensures proposed template protection

REFERENCES

1. Bowyer, K.W., Hollingsworth, K. and Flynn, P.J., 2008. Image understanding for iris biometrics: A survey. Computer vision and image understanding, 110(2), pp.281-307.

2. Chong, S.C., Jin, A.T.B. and Ling, D.N.C., 2005, December. Iris authentication using privatized advanced correlation filter. In Proceedings of 1st International Conference on Biometrics. LNCS (Vol. 3832, pp. 382-388).
3. Daugman, J., 2004. How iris recognition works. IEEE Transactions on circuits and systems for video technology, 14(1), pp.21-30.
4. He, Z., Tan, T., Sun, Z. and Qiu, X., 2009. Toward accurate and fast iris segmentation for iris biometrics. IEEE transactions on pattern analysis and machine intelligence, 31(9), pp.1670-1684.
5. Hogan, M., Liu, F., Sokol, A. and Tong, J., 2011. Nist cloud computing standards roadmap. NIST Special Publication, 35.
6. Jain, A., Bolle, R. and Pankanti, S. eds., 2006. Biometrics: personal identification in networked society (Vol. 479). Springer Science & Business Media.
7. Lian Yu, Wei-Tek Tsai1, Xiangji Chen, Linqing Liu, Yan Zhao, Liangjie Tang, Wei Zhao2, “Testing as a service over cloud”, Proceedings of Fifth IEEE International Symposium on Service Oriented System Engineering.
8. Lian Yu, Le Zhang, Huiru Xiang, Yu Su, Wei Zhao, Jun Zhu, "A Framework of Testing as a Service", Proceedings of the Conference of Information System Management 2009.
9. Ratha, N.K., Connell, J.H. and Bolle, R.M., 2001. Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal, 40(3), pp.614-634.
10. Schneier, B., 1994. The Blowfish encryption algorithm. Dr Dobb's Journal-Software Tools for the Professional Programmer, 19(4), pp.38-43.
11. Schnorr, C.P. and Jakobsson, M., 2000, December. Security of signed ElGamal encryption In ASIACRYPT (Vol. 1976, pp. 73-89).
12. Cloud Test by SOASTA: http://www.soasta.com/
13. Lenk, M. Klems, J. Nimis, S. Tai, and T. Sandholm, What’s in the Cloud: An Architectural Map of the Cloud Landscape,” 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing
14. Sudhan, S.K.H.H. and Kumar, S.S., 2016. Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9(44).
15. Vielhauer, C., 2005. Biometric user authentication for IT security: from fundamentals to handwriting (Vol. 18). Springer Science & Business Media.
16. Zissis, D. and Lekkas, D., 2012. Addressing cloud computing security issues. Future Generation computer systems, 28(3), pp.583-592.

AUTHORS PROFILE

S.Karthik has completed his PhD in the area of VLSI.He has published more than 20 international journals.His research area includes High Performance computing, Reconfigurable architecture,VLSI Testing,DFT,Low power VLSI techniques. He has attended many conference and workshops throughout the world.He is well versed in HDLs like Verilog,VHDL.He has worked in many development board like PI,PYCOM,ZED.He was actively involved in projects such as low power pattern generation for BIST architecture, fault-tolerant architectures, dynamic partial reconfiguration in FPGAs, and low power adders. He believes in life-long learning. To update his skill set he has attended numerous training programs/workshops such as the Cadence training program, workshop in FPGA Based System Design using ALTERA EDA Tools and in Advanced Engineering Optimization and Modeling using MATLAB & SCILAB, just to name a few.

K.Priyadarsini has completed her M.Tech from VIT University. She was an Intern at CTS. She has worked in many IT companies has developer. She started her career at SRM University. She did her PhD from VISTAS. Her area of research includes High performance cloud computing, security aspects at Multicloud, data science. Data mining,Big data analytics. She has completed many online MOOC courses. She is interested in Object Oriented Programming and carrying out workin building software models . She has published more than 10 international journals and she has presented many papers in conferences.