Biometric Mobile Data on Secure Public Cloud Vulnerabilities

Venkata Venugopal Rao Gudlur @ Saigopal, Sundresan Perumal

Abstract: Companies who are implementing the cloud solutions have increased numerous advantages in the recent years. Cloud solutions provide a very few preferences, for example, portability, adaptability and costs funds. Alongside the numerous advantages that distributed computing offers the security challenges that it presents are similarly striking. The two essential capacities for secure cloud administration are character administration and access control in distributed computing, the current methodologies for client confirmation depend on accreditation that are put together by the client. These accreditations incorporate passwords, tokens and computerized authentications. Most of the cases unapproved access by outsiders, for example, programmers likewise exist and simple for information control and abuse. In any case, the most serious issue with this methodology is that the presence of such many secret phrase account pairings for each individual client prompts either overlooked passwords or utilizing a similar mix for different locales. Security issue is significant concern, region of research in versatile distributed computing and clients. Shielding the remote information and applications from any ill-conceived get to remain an essential security worry in portable distributed computing. This paper explains about secure bio metric and face recognized based authentication protocol which is best suited for the public cloud environment to improve the safer and secure user authentication process. The above strategy will anchor approved clients as well as keep the cloud suppliers can't get in to the information and data access.

Keywords: Cloud Computing, Forensic Bio Matric, Internet of Things (IoT), Mobile Data.

I. INTRODUCTION

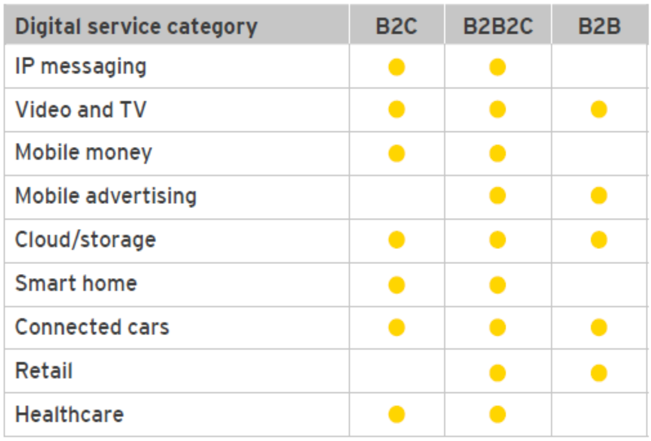
The usage of bio metric technology to cloud means that the cloud services can be used through an electronic interface. This interface can either be an internet browser or a portable application. The fundamental format of any bio metric ID framework stays same regardless of the methodology that is utilized [1] [2]. This methodology includes moving both the bio metric database and the product part to the cloud. This will guarantee fitting innovation versatility and enough measures of capacity. In addition, a cloud-based framework has a few different angles, for example, constant and parallel handling abilities that make it additionally engaging.

The far-reaching accessibility of cell phones makes it open for some applications and administrations that depend on versatile customers [3]. The current age of bio metric frameworks offers numerous new potential outcomes for distributed computing security. Embracing bio metrics in distributed computing and applications will assist customers with ensuring data security and give a financially savvy security answer for the specialist organizations. Along these lines, it is normal that the quantity of cloud clients will develop quickly in the following couple of years.

Cloud computing allows dynamically reliable online resources to be allocate proper internet technology services [4].

II. LITERATURE REVIEW

Relevant business model of cloud decisions by present telco organizations: Cloud based plan of action, choice ought to be bolstered by scope of association situations, Potential accomplices both level and vertical should be deliberately (and regularly quickly) assessed by administration of nation to anchor open information [5].



Digital service category	B2C	B2B2C	B2B
IP messaging	●	●	
Video and TV	●	●	●
Mobile money	●	●	
Mobile advertising		●	●
Cloud/storage	●	●	●
Smart home	●	●	
Connected cars	●	●	●
Retail		●	●
Healthcare	●	●	

● = Telcos currently active

Fig. 1 Global navigation study navigating road to 2020 (Ernst & Young Global Limited

The organization of bio metric innovation to distributed computing offers numerous appealing potential outcomes that incorporate shrewd spaces, get to control applications, encompassing insight conditions and so on. Portable cloud-based bio metrics is a developing business sector incline fueled by components, for example, adaptability and improved cost funds.

This further adds to the quantity of portable cloud clients which is developing quickly.

Revised Manuscript Received on June 22, 2019.

Venkata Venugopal Rao Gudlur@Saigopal, (Phd Aspirant), Limkokwing University of Creative Technology, Malaysia E-mail: saigopal1123@gmail.com

Dr. Sundresan Perumal, Faculty of Science & Technology (FST), Universiti Sains Islam Malaysia (USIM), E-mail: sunderesan.p@usim.edu.my

A Bloomberg review uncovers that distributed computing is relied upon to acquire around $ 270 billion of every 2020.Vulnerability of web applications to security ruptures and programmer assaults is an immense worry as these applications include both and undertaking and private client data. For any web application improvement, ensuring such resources is an essential need. The assurance instrument can include different advances, for example, validation and approval, resource taking care of, action logging and evaluating. Although conventional instruments, for example, secret phrase administration or encryption can be utilized to deal with this reason, their viability can't be ensured.

3.1 Related work: Current public could data access and storage model.

Current internet authentication approaches for most cases Using the username and password combination. The most concerning issue with this methodology is that the presence of an excessive number of secret word account pairings for each individual client prompts either overlooked passwords or utilizing a similar blend for various locales. Shielding the remote information and applications from any ill-conceived get to remain an essential security worry in versatile distributed computing. The principle issue is along with the approved clients, the cloud companies can likewise get to the information. The possibility of unauthorized access by outsiders, for example, programmers additionally exists. Security issue is in this way a noteworthy territory of research in versatile distributed computing [14].

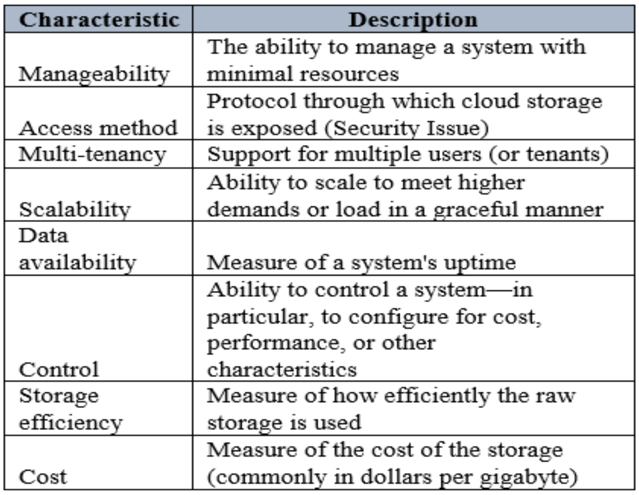
On the other side, be that as it may, we likewise found there are various precedents where high development clients like Apple, The Weather Company, Dropbox, Instagram, General Motors, Target, and HubSpot either exceeded open cloud or utilize a multi-cloud technique to exploit value wars between the best companies around. Reasons we found for leaving AWS were often to accomplish better execution, bring down cost, increment control or abstain from being affected by boisterous neighbors.

III. PUBLIC COULD

Strengths	Weakness
High availability	Compliance with legal regulations
Reliability and access	Isolation issues due to multi-tenancy
High elasticity	Less detailed logging capabilities
Facilitated patch management	Proprietary interfaces
Distribution for failure safety	Security issues
Low costs and easy access	Mobile data redundancy

Ref: (Bernd Zwattendorfer)

3.2 Could Storage Characteristics



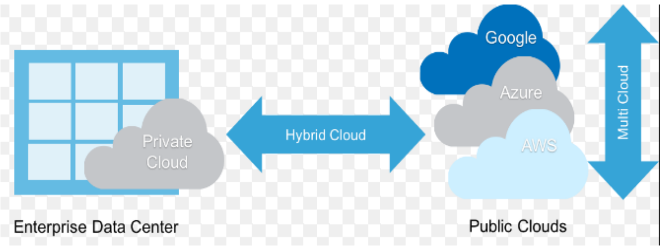
Characteristic	Description
Manageability	The ability to manage a system with minimal resources
Access method	Protocol through which cloud storage is exposed (Security Issue)
Multi-tenancy	Support for multiple users (or tenants)
Scalability	Ability to scale to meet higher demands or load in a graceful manner
Data availability	Measure of a system's uptime
Control	Ability to control a system—in particular, to configure for cost, performance, or other characteristics
Storage efficiency	Measure of how efficiently the raw storage is used
Cost	Measure of the cost of the storage (commonly in dollars per gigabyte)

Ref: (v.spoorthy and mamtha)

3.2.1 Proposed public could Data Storage Model:

The Bio metric impression verification will be used to anchor distributed Cloud computing applications. This approach utilizes the mobile camera to capture and convert the image and upload to the public cloud for authentication. The thought is to change over the fingertip picture captured by the cell phone camera to a unique finger impression will give final edge and secure authentication as conceivable to the user to access the data. Each time the client access to the public cloud, he just sweeps his unique mark and logs in. The entire methodology is facilitated on pubic cloud with safer login identification and verification process.

.



3.2.2 Advantages of implementing Secure public could mobile data storage:

Biometrics framework can be rapidly set up truly inside a matter of couple of minutes. Biometric services can be given as an on-demand service where it is conceivable to include or cancel components promptly. It is a reasonable innovation particularly for the little and medium-sized organizations. In contrast to customary validation frameworks, the costs engaged with a biometric cloud-based infrastructure is for the most part settled. For instance, secret key-based like passwords and frameworks require support costs for resetting of passwords and maintenance of network infrastructure **[6] [7].**

The accessible resources pooling empowers biometric databases to be scaled and can fit any variety of utilizations going from a basic 1:1 to the most mind boggling 1: N check situations. Advantages of secure validation:

One of the most prevalent and powerful biometric approaches is unique mark confirmation conspire with face acknowledgment. The most vital advantage of portable distributed computing is the ability to get to information and applications whenever and from anyplace easily and cost-successfully utilizing basic login techniques. Additionally, the non-refusal necessities of remote client verification approach suggest that it very well may be proficiently accomplished utilizing biometrics and face perceived based technique. The cloud condition depends on abstracting and giving different assets like computing power, network, storage and software and mobile applications remotely as administrations on the web. Current web validation approaches for most cases infer a username and password combination [8] [9].

3.2.3 Technical Process and Flow:

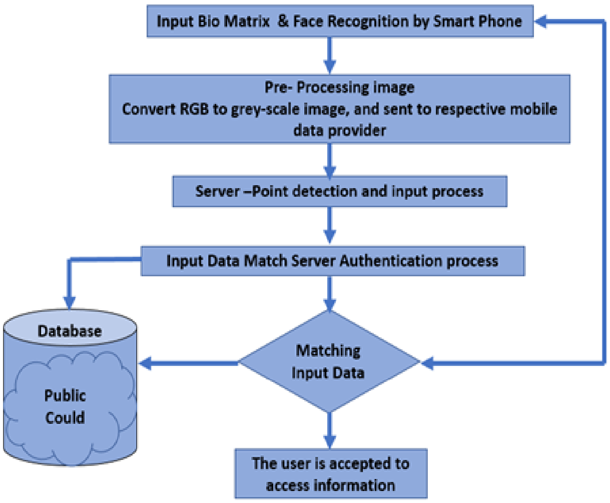

Input Bio Matrix & Face Recognition by Smart Phone
Pre- Processing image
Convert RGB to grey-scale image, and sent to respective mobile data provider
Server –Point detection and input process
Input Data Match Server Authentication process
Database
Public
Could
Matching
Input Data
The user is accepted to access information

Fig. 1 Proposed Research Model

The user will display his finger to the sensor that captures the picture with face recognition and this is known as the enrolment stage. The unique finger impression and face recognition sample are pre-processed to obtain permission to access data from the could database. whereas at the point when a client needs to login to get to applications on public cloud, he gives his unique finger impression and face recognition to the mobile phone or sensor which catches the picture and plays out some pre-handling capacity to remove the highlights sent to the cloud server for validation check or process [13][15] [16].The cloud data base will perform the matching function performs a comparison check and updates the user with access granted or denied. The access process can be set maximum tries depends on public network setting. Proposed face recognition with bio matric solution for public could will have common challenges and security concerns pertaining to public could. Implementation of such secure authentication services may incur cost or must look in other cost-effective measures to the general population. Therefore, it is expected that the number of public cloud user in near future will grow rapidly due to high demand of mobile communications [17] [18] [19].

IV. SECURITY AND PRIVACY RISK IN MOBILE COULD COMPUTING

I. As Mobile Cloud Computing is blend of versatile could computing in distributed environment, security hazard in portable processing is acquired from cloud computing. Mobile public Cloud Computing experiences following risk.

II. In Mobile public could computing, client does not know where his information is stored, so client has next to zero authority over the area of information.

III. Because of physical damage of cloud server, loss of encoding key or because of malignant insider, danger of information lost may emerge.

IV. A client with sick intention may plant virus of phishing attack in to cloud server which may compromise data of other clients and cloud provider will be unable to track it considering security and policy of the organization.

V. A gap in security of applications and interface of cloud administrations can prompt attack like bypass of API assault.

VI. When public cloud provider services and benefits to a few clients, blemish in encryption calculation can prompt unapproved access to one's information. According to administrative consistence cloud provider must keep up required security level. [10] [11] [12].

VII. In IaaS security risks are may arise due to lack of isolation in virtualization when number of virtual machines are hosted on a single server with more data transaction gateway.

VIII. Mobile phone users store and transfers critical personal and corporate information while using mobile applications accessing the public could. (Ref: *Sapna malik and MM Chaturvedi)*

V. CONCLUSION AND FUTURE WORK

Biometric and face recognition innovation can be connected to Mobile public cloud server and applications to battle the security dangers, for example, hacked passwords and information intrusion.[20][21] The favorable circumstances that biometrics and face recognition gives to distributed computing makes it a reasonable and positive answer for all elements associated with the procedure, yet it might cost for open could particular portable administrators and particularly creating nations like Malaysia. The best preferred standpoint of executing biometrics and face recognition security features in broad daylight public cloud would now be able to be made accessible for different types and sorts information techniques for more secure condition and users of Mobile Commerce and future generation to come.

It is normal that with the progression of time the use of the above security future with distributed computing will be more efficiently connected and quickly executed on a bigger scale [22] [23].

There may be questions arise to the administrators on plans of use of this information by police and other law requirement offices. Biometrics, nonetheless, have demonstrated successful in recognizable proof of offenders and fear-based oppressors. The improper use of Biometric and face recognition idea may look simply yet required more most recent mobile phone version with Wi-Fi connectivity features to connect to the public cloud and it might be costly and future research and information may require assessing conceivable outcomes and more secure public could access [24] [25].

REFERENCES

1. Danny Thakkar is the co-founder of Biometric, one of the leading biometric solution providers in the world July 2016.
2. Anil K. Jain, Arun Ross, and Salil Prabhakar, “An Introduction to Biometric Recognition,” IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004.
3. Veo Zhang (Mobile Threats Analyst) Posted on:December 3, 2015 at 8:59 am Posted in:Mobile, Vulnerabilities https://blog.trendmicro.com/trendlabs-security- intelligence/high-profile-mobile-apps-at-risk-due-to- three- year-old-vulnerability/
4. Liang H-W, Hwang Y-H (2016) Mobile Phone Use Behaviors and Postures on Public Transportation Systems. PLoS ONE 11(2): e0148419.https://doi.org/10.1371/journal.pone.0148419
5. Bernd Zwattendorfer, E-Government Innovation Center, Graz University of Technology, Graz, Austria Arne Tauber, E-Government Innovation Center, Graz University of Technology, Graz, Austria-2013
6. Khan, F., Zhang, B., Khan, S., & Chen, S. (2011). Technological leap frogging e- government through cloud computing. In Proceedings of the 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology (pp. 201-206). IEEE
7. V. Spoorthy1, M. Mamatha2, B. Santhosh Kumar A Survey on Data Storage and Security in Cloud Computing: IJCSMC, Vol. 3, Issue. 6, June 2014, pg.306 – 313
8. Sapna Malik- GGSIPU University, MM Chaturvedi – Ansal University, Privacy and Security in Mobile Cloud Computing: Review - International Journal of Computer Applications (0975 – 8887) Volume 80 – No 11, October 2013
9. Burda, D. and Teuteberg, F. (2014) ‘The role of trust and risk perceptions in cloud archiving-Results from an empirical study’, The Journal of High Technology Management Research, 25(2), pp. 172-187
10. Lian, J. W. (2015) ‘Critical factors for cloud based einvoice service adoption in Taiwan:An empirical study’, International Journal of Information Management, 35(1), pp. 98- 109.
11. E.Gorelik, “Cloud Computing Models”, Massachusetts Institute of Technology Cambridge, MA, 2013. Available: http://web.mit.edu/smadnick/www/wp/2013- 01.pdf
12. Grispos, George; Tim Storer; and William Bradley
13. Glisson. (2012). Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics. International Journal of Digital Crime and Forensics (IJDCF) 4(2), pp. 28-48.
14. Bitdefender, “IoT: Risks in the connected home”, research paper, published February 2016.
15. Angus Wong, Alan YeungG, “Network infrastructure security’’, eBook, ISBN 978- 1-4419-0166-8
16. Muthanna, Ammar, et al. "Comparison of protocols for Ubiquitous wireless sensor network." Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014 6th International Congress on. IEEE, 2014.
17. Buric, J., and D. Delija. "Challenges in Network forensics." Information and Communication Technology,Electronics and Microelectronics (MIPRO), 2015 38th International Convention on. IEEE, 2015.
18. H. Haddad Pajouh, R. Javidan, R. Khayami, D. Ali, K.-K.R. Choo, A two-layer dimension reduction and two-tier classification model for anomaly-basedintrusion detection in IoT backbone networks, IEEE Trans. Emerg. Top. Comput. (2016) 1. http://dx.doi.org/10.1109/TETC.2016.2633228.
19. J. Lopez, R. Rios, F. Bao, G. Wang, Evolving privacy: from sensors to the Internet of Things, Future Gener. Comput. Syst. 75 (2017) 46–57. http://dx.doi.org/10.1016/j.future.2017.04.045.
20. F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security:A survey, J. Netw. Comput. Appl. 88 (2017) 10–28. http://dx.doi.org/10.1016/j.jnca.2017.04.002.Strategy& (September 2016), ‘Industry 4.0: How digitization makes the supply chain more efficient, agile, and customer-focused’. Available at http:// www.strategyand.pwc.com/reports/industry-4-0(accessed 15th May, 2017).
21. Ryder, S., Le-Khac, N-A. (2016), The End of effective Law Enforcement in the Cloud? To encrypt, or not to encrypt, 9th IEEE International Conference on Cloud Computing, San Francisco, CA, USA, June 2016
22. Popken, B. (2017), Hacked Home Devices Can Spy OnYou - NBC News, OCT 26 2017, 2017. [Online]. https://www.nbcnews.com/tech/security/hacked- home devicescan-spy-you-n814671.
23. FDA (2017), Safety Communications - Cybersecurity Vulnerabilities Identified in St. Jude Medicals Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication, 2017
24. J. Yang, and B. Fang, “Security model and key technologies for the Internet of things,” in: The Journal of China Universities of Posts and Telecommunications. 2011, pp. 109-112. DOI: 10.1016/S1005-8885(10)60159-8. ISSN 10058885.
25. S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, “Proposed embedded security framework for Internet of Things (IoT),” in: 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011, pp. 1-5. DOI: 10.1109/WIRELESSVITAE.2011.5940923.