Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.4, No.9, 2014

Cloud Biometric - Ethical Implications, Authentication, Security and Usability

Kevin Tole
School of Engineering and Information Technology, department of computer Science and Technology.
Technical University of Mombasa, PO box 90420-80100.
*kevintolesolomon@yahoo.com

ABSTRACT.
The study examines the contribution of personal data stored in the cloud may contain account numbers, passwords, notes, and other critical information that could be used and misused by other users. These data can be cached, copied, and archived by Cloud Service Providers (CSPs), often without user's authorization and control. The specific objective of this study is to keep data secure by Self destructing data. The study aims at protecting the user data's privacy to avoid unethical implications. All the data with their copies become destructed or unreadable after a user specified time, without any user intervention. The biometric information is decrypted and the user is subscribed to access the cloud. This decides whether the user is approved or denied. Once the user is recognized as an authorized user, the user can view, upload or download the data stored in cloud. Over the next few years the amount of biometric data being at the disposal of various agencies and authentication service providers is expected to grow significantly. Such quantities of data require not only enormous amounts of storage but also security and usability.
Keywords- biometric data, cloud service providers, Authorization, biometric data

1. INTRODUCTION.

Biometrics could be the ideal tool to protect private consumer data in the cloud. In the wake of a Cloud security flaw integrating biometric authentication into its next iteration of Cloud security. Authentication is the process of validating users, ensuring that they are who they say they are. Solutions range from traditional alphanumeric username. This paper summarizes my personal views and opinions of the journal in a crucial part of the access control that makes the major building block of any system's security. User identification/authentication has been traditionally based on: Something that the user knows (typically a PIN, a password or a passphrase) or something that the user has (e.g., a key, a token, a magnetic or smart card, a badge, a passport).These traditional methods of the user authentication unfortunately do not authenticate the user as such. Traditional methods are based on properties that can be forgotten, disclosed, lost or stolen. Passwords often are easily accessible to colleagues and even occasional visitors and users tend to pass their tokens to or share their passwords with their colleagues to make their work easier. Biometrics, on the other hand, authenticates humans as such – in case the biometric system used is working properly and reliably, which is not so easy to achieve. Biometrics is an automated method of identity verification or identification based on the principle of measurable physiological or behavioral characteristics such as a fingerprint, an iris pattern or a voice sample. Biometric characteristics are unique and not duplicable or transferable.

2. BIOMETRICS IN THE CLOUD

There are certain aspects of biometric systems that are specific to cloud computing. First of all, the biometric engine is located in the cloud and not on some local processing unit, as it is the case with traditional (e.g. access control) biometric recognition systems. This characteristic makes the cloud- based biometric technology broadly

accessible and provides the necessary means for integration in other security consumer applications. Second of all, storing biometric data in the cloud makes the system highly scalable and allows quick and reliable adaptation of the technology to an increasing user base. On the other hand, storing biometric data in the cloud may raise privacy concerns and may not be in accordance with national legislation. Last but not least, a cloud implementation of biometric technology may harvest all merits of the cloud, such as real-time and parallel processing capabilities, billing by usage etc. All of the presented characteristics make cloud-based biometric recognition technology extremely appealing. When developing biometric technology for the cloud, one needs to make a number of design choices. Probably the most important choice is, which components to move to the cloud and which to implement locally. A review of some existing market solutions from the field of cloud-based biometrics reveals that most often both the biometric engine as well as the biometric database is moved to the cloud. The commercial solutions typically operate on the principle of the client-server model. The local client (e.g. on the user's computer) is responsible for capturing a biometric sample of the user and sending it to the server (hosted in the cloud), where the matching process is executed. For the safety of the network traffic between the client and the server designated security protocols are commonly used.

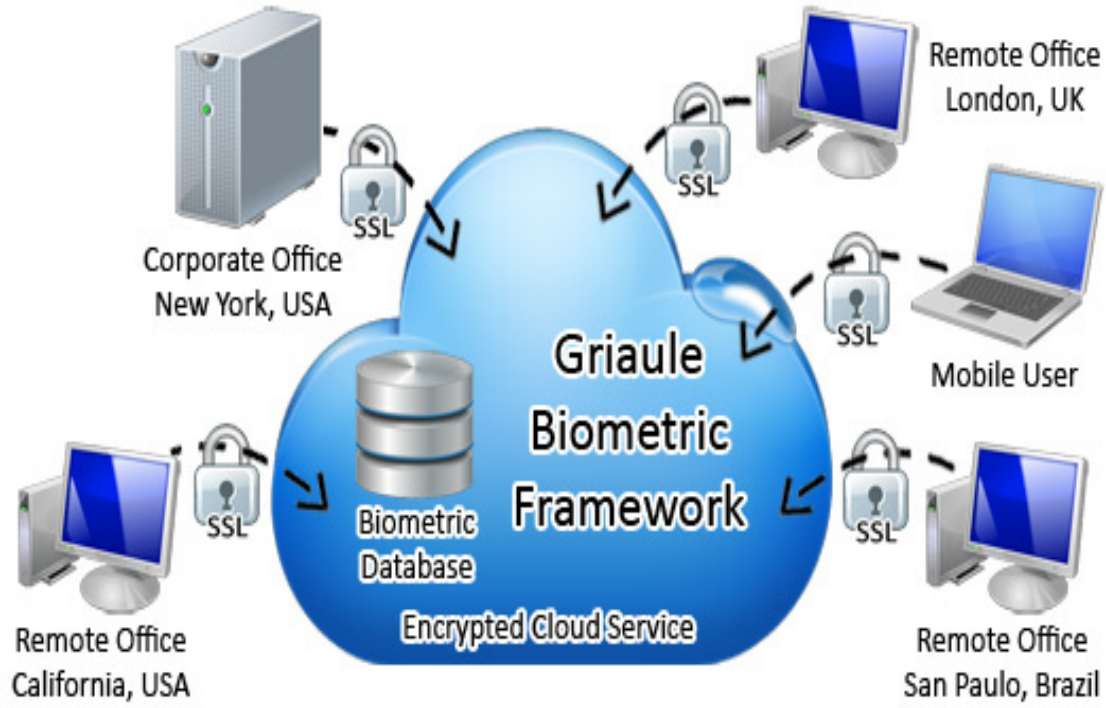
3. ETHICAL IMPLICATIONS

However, there are serious ethical issues in the use of biometric technology. The main issues concern is the personal privacy, the conflict with one's beliefs and values and the collection, protection and use of personal biometric data. The civil liberty organizations argue that the technology undermines the human rights for privacy and anonymity. It is intrusive and has the capability to make serious impact on personal freedom and democratic rights. The technology is prone to failure and is not fake proof as it can be spoofed, But due to many issues and threats around the world, e.g. threat of terrorism, identity theft and fraud, security, illegal immigration, benefit fraud and crime prevention and detection issues, it has become important to have the capability to freeze someone identity for later identification and verification. At the same time since 9/11 the biometric technology has advanced tremendously. The hardware has improved in design and accuracy, the prices have come down and, therefore, biometrics has firmed its place in the security world. The public concern regarding the issues mentioned above cannot be ignored. There is a compelling need to find "Workable and Deployable" solutions to these issues. The academics have a very important role to play through consultations, workshops and student education.

4. AUTHENTICATION, SECURITY AND USABILITY.

Current biometric measurements must be obtained for the system to be able to make comparison with the master template. These subsequent acquisitions of the user's biometric measurements are done at various places where authentication of the user is required. It is often up to the reader to check that the measurements obtained really belong to live persons. In many biometric techniques (e.g., fingerprinting) the further processing trusts the biometric hardware to check the person and provide genuine biometric measurements only. Some other systems (like the face recognition) check the user's in software (time-phased sampling). a system that meets this challenge through a novel integration of cryptographic techniques with active storage techniques based on T10 OSD standard. On the other hand a proposed system, user's biometric information are encrypted and stored in a database. Batch homomorphism encryption technique is used to encrypt the biometric information provided by user biometric information and are compared with the database where the authenticated user's encrypted information are stored. User's fingerprints are encrypted by batch homomorphism encryption technique. The biometric information is encrypted and the user is subscribed to access the cloud. This decides whether the user is approved or denied. Once the user is recognized as an authorized user, the user can view, upload or download the data stored in cloud.

Encrypted biometric cloud service



5. Conclusion

Cloud based biometric services have an enormous potential market value and as such attract research and development groups from all around the world. In this paper some directions on how to safeguard and an ethical system biometric technology to a cloud platform were presented. Issues that need to be considered regarding privacy-based biometric services have been presented. Biometrical recognition is done by using batch homomorphism encryption technique. In this, privacy of data has become increasingly important in the cloud environment. A new approach for protecting the data from attackers who retroactively obtain, through legal or other means, a user's stored data and private decryption keys is implemented. It causes sensitive information, such as account numbers, passwords and notes to irreversibly self destruct, without any action on the user's part. The second phase of the system is focused on security. The reason for providing security is that the unknown users should not access the authorized data. The server provides access rights to access the data in the cloud.

6.ACKNOWLEDGEMENT.

I would like to express my gratitude to my family especially my Loving mother, Daniel Vidzo and brother who saw through this journal and provided support, talked things over, read, wrote and encouraged me in spite of all the time it took me away from them.

I would like to thank my dearest friend Juliah Kulola Nyatta who spearheaded the breakthrough of this journal despite a lot of challenges.

In addition I am indebted to Technical university of Mombasa for allowing me to use her library as a resource in my creation of this journal.

Special thanks also go to all faculty members of Technical University who helped me with valuable suggestion of the journal for the improvement of our teaching unit.

Finally, I would like to thank all of my friends who supported me while I was working on the journal.

REFERENCES

[1]. S. Wolchok, O. S. Hofmann, N. Heninger, E. W. Felten, J. A. Halderman,C. J. Rossbach, B. Waters, and E. Witchel, "Defeating vanish with low cost sybil attacks against large DHEs," in Proc. Network

[2] A.K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition,"Transactions on Circuits and Video Technologyvol. 14, no. 1, pp. 4-20, 2004.

[3] E. Kohlwey, A. Sussman, J. Trost, and A. Maurer, "Leveraging the Cloud Meeting the performance requirements of the Next Generation Biometric Systems," in the IEEE World Congress onServices2011.
[4] V. Štruc and J. Žganec Recognition Technology for Biometrics servicein: pp. 68-75, 2012.
[5] J. Bule and P. Peer, "Fingerprint Verification as a Service in KC CLASS," in: 2012, pp. 76-82, 2012.
[6] The KC Class projecthttp://www.kc-class.eu/, Transactions on Circuits and Video Technologyvol
[7] D. Gonzales Martinez, F.J. Gonzels Castano, E. Argones Rua, J.L. Ala Castro, D.A. Rodriguez Silva, "Secure Crypto-Biometric System for Cloud Computing," in: InternationaSecuring Services on the Cloud.
[8] H. Vallabhu and R.V. Satyanarayana, "Biometric Authentication as a Service on Cloud: Novel Solution," International Journal of Soft Computing and Engineering, vol. 2, no. 4, pp. 163
[9] S. Suryadevara, S. Kapoor, S. Dhatterwal, R. Naaz and A. Sharma, "Tongue New Prospects of Cloud Computing Security," in: international Conference on Information and Network Technology, vol. 4, 2011.
[10] S.N.S. Raghava, "Iris Recognition on Handoop: a
Biometrics System Implementation on Cloud Computing," in: Proceedings of IEEE CCIS,
[11] C. Senk and F. Dotzler, "Biometric Authentication as a Service for Enterprise Identity Management Deployment: A Data Protection Pers International Conference on Availability, Reliability and Security.
[12] E. Kohlwey, A. Sussman, J. Trost Leveraging the Cloud for Big Data Biometrics: Meeting the Performance Requirements of the Next Generation Biometric Systems Congres on Services,pp. 597
[13] D.M. Dakhane and A.A. Arokar, "Data Secuity in Cloud Computing for Biometric Application," International Journal of Scientific & Engineering Research, vol. 3, no. 6, pp. 1

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar