European Journal of Academic Essays 2(1): 6-9, 2015
ISSN (online): 2183-1904
ISSN (print): 2183-3818
www.euroessays.org

E-Voting security system through Biometric Cloud Computing Integration with virtual server application

Chakraborti, Bratati[1]

[1]WBUT University, NSHM College,
91(124) B.L saha Road,India ,Kolkata 53
bratatikiit@gmail.com

Abstract: Today, biometric cloud security creates a new explosion in technology. With the advent of Cloud Computing biometric security and reliability plays important role in national and international e-governments. In e-voting system, if we incorporated cloud based computing through biometrics then it will create more authentication, transparency and security in voting system. To operate e-voting management system requires vast cloud database applications and Big data application to store massive biometric data. In this method helps user to access remotely the voting system through biometric authentication device. Migrating the massive amount of biometric data is difficult. So Virtual server plays important role to reduce the hazards. Cloud computing helps to reduce workload and provide efficient streamlined of security. We will propose a system that reduces the security risk in cloud by various Biometric recognition systems. Physiological and behavioral feature of a person are required in biometrical systems. Physiological biometric includes Fingerprint scan, face recognition, geometry of hand, Iris scan and retinal scan .The main advantage of Biometrics integration with Cloud provide on demand services so organization or Government purchase or rent the infrastructure as required and install it.

Keywords: Biometric, cloud computing, e-voting, SaaS, PaaS, IaaS, fingerprint recognition.

1. Introduction

In cloud computing Biometric security plays a reliable and secure role in e-voting system and able to eradicate loss, misuse and theft of data. Biometric data previously related to cryptographic security which needs much cost. The aim of this paper, we describe cloud biometric security in e-voting system. The large amount of biometric database is stored in big data in encrypted form and send to large cloud servers. In a biometric security a credential is generated by owner of database and he submits it in cloud. With the help of credential cloud servers make comparison and identification process of encrypted database and outcome send to the database owner and privacy of biometric data preserved by cloud service. Main advantage of this service that cost is very less. The main objective of this paper is to implement secure e-Voting System through biometric cloud. Some criteria we should maintain such as Privacy, accuracy, Integrity, Reliability and security. Through biometric system authorities can able to understand whether a customer is legal voter or not. In this system voters have the opportunity to verify their vote in future. Motivation of this article is that large number of processes are required to perform voting operation .If we can able to map these operation in electronic world and stored information in cloud database it will be more efficient.

1.1 Literature Review:

In Election people have a fundamental right to choose government through voting. To secure the voting system E-Voting is applied which is actually a cryptographic protocols. Last two decade there are so many research about e-voting. E-voting can able to overcome the challenges and limitation of geographical proximity. Caltech-MIT (2001) tried to find out new solution of e-voting of real world.[1] Vein Jefferson et al. (2004) solved various challenge of e-voting and make it more trustworthy to public.[2] The e-voting protocol proposed by Baraani et al.[3]. Amir Omidi and Mohammad Abdollahi Azgomi also proposed an E-voting architecture system based on dependable web services [4]..

2. Cloud security integrated with biometric solution

Cloud computing creates a new era of network technology. User need not buy the technology provided by cloud server

Corresponding Author: Bratati Chakraborti, Assistant professor NSHM College, bratatikiit@gmail.coml,9051466981

they can rent it. It becomes so cost effective. But security is one of the most critical challenges of cloud computing. Biometric security such as Fingerprint scan, face recognition, geometry of hand, Iris scan and retinal scan are incorporated in cloud computing. Cloud user is authenticated by their fingerprint, face, retina, iris scan [5],[6].

3. Biometric security involved with cloud computing:

NIST invented new protocol for authentication using biometry in web service .Cloud service will also adopt this services. Recently biometric authentication creates a revolution in cloud service and WS-BD(Web Services Biometric Devices) created by NIST rely on standardized forms of communication .Cloud service adopts standardized forms of communication which save cost and time both. Biometrics is essential in recent day mainly for big data and wider access of user. Massive amount of biometric data stored in big data base. Large numbers of biometric data such as fingerprints, iris, and facial scan images which are needed for verification technology are too stored in large database. Data warehouse and Big data are the solution of storing large database. Cloud provide wider access in biometric data .such as voice recognition where voice channel is treated as input and voice are collected by speech application mechanism .Cloud service are used to stored these voice service without overhead. From some research report shows some challenges about biometrics as population are increased day by day and it may be inherently probabilistic. But when biometric integrated with cloud computing it effectively handle the challenges.[5][,6],[7]. Biometric security services are as follows:

- Cloud computing with Biometrics as a Service (Baas)
- Identity as a Service (IDaaS)
- Biometric authentication for the cloud.

3.1. Cloud computing with Biometrics as a Service (Baas)

Reliability, security and non-repudiated identification are the big challenges of the evolution of Cloud computing. Cloud authentication is related to user's identity and therefore gain a level of trust of user and different It industry and organizations adopt the cloud services. Cloud computing integrated with biometric assurance it will provide more reliable service. BaaS includes matcher, biometric capture, enrollment process for authentication with full biometrics capabilities [8].BaaS supports on demand process to reduce cost and enhance the elasticity feature of cloud also. BaaS providers provides the support of scalability (management of large number of biometrics), multiple modalities (management of different types of biometrics), and matching performance. BaaS responsible for easiness of security of biometric data[9],[10].

3.2. Identity as a Service (IDaaS)

IDaaS is also another service similar to BaaS but it provides more comprehensive delivery of Cloud-based identity management which includes biometric data. IDaaS supports scalability and reliability feature with on-demand facility.

3.3. Biometric authentication for the cloud

Security data access scheme related with identity-based encryption and biometric authentication for cloud. The Department of Homeland Security (DHS) IDENT Database in 2010 hosts 110 million identities and enrolls or verifies over 125,000 individuals per day. Biometric feature based on following characteristics. Design considerations, arbitrary records and metadata, Common biometric matching API, Real-time, parallel and bulk processing, Flexibility, recovery, redundancy strategies communication.[10],[11].

4. Different biometric in cloud computing

Security and identification are basic functions for reliable and secure cloud communication. Different biometrics models are fingerprints, retina, iris, voice, face, hand geometry, palm, handwritten signature dynamics .Biometric recognition can able to recognize a person identity based on physiological and or behavioral traits. Physiological characteristics of a person are related to body such as fingerprint and Behavioral are related to the behavior of a person. A biometric recognition system is categorized by two modes: verification and identification. Verification or authentication accepts or rejects the identity of a person. Identification determines the registered person's identity with help of biometric data. Different Physiological Biometrics is Fingerprint, Facial recognition, Hand geometry, Iris scan, Retinal scan and Behavioral biometrics are Speaker recognition and signature dynamics.[12],[13]. Person verification and identification by voice: Different biometric verification process about speaker verification have been performed based on “one-to-one” search method. In this method a person claimed his/her identity and device verifies whether he or she is claimed person or not .

5. Design of biometric infrastructure in cloud systems:

Designing the biometric infrastructure in the Cloud , we first configure SaaS(Software as a service ,PaaS(Platform as a Service) and IaaS(Infrastructure as a Service).The biometric cloud configuration should comprise a template biometric database and good network connectivity for conducting verification test in cloud. [14]

5.1. Configuration of IaaS:

Some hardware tools (pattern recognition tools authentication /verification device) need to be installed. Virtual server, storage ,network are needed to control on biometric cloud service. Total administrative control are handled by server in the business point of view . Biometric operating system (Linux, windows) are the key component of biometric server. Biometric template database are stored in storage. Various transactions result (verification ,identification)are stored in associated database and lo are stored in to storage. Biometric cloud infrastructure should need a good connectivity to host provider and recognize identity of a person through biometric device.

5.2. Configuration of SaaS:

SaaS component can be rented or purchased by consumer in on demand basis for customized development. With these software platform provide the opportunity to user to develop their own biometric platform that are integrated with cloud infrastructure.

5.3. Configuration of PaaS :

PaaS is the combination structure of IaaS and SaaS and work accordingly also. PaaS supports larger version biometric application in business scenario.

6. Virtualization related with biometric cloud computing:

Different virtual servers, storage and network are major part of infrastructure of cloud Biometrics. Administrator of cloud service should need a total control in biometrics application. Biometrics Operating System is main requirement of this service which supports closed and open source platform. All transaction, biometric templates and database are stored in cloud storage for authentication and verification. Biometric network in cloud should have good connectivity and the device to recognize biometric data. Each cloud data based biometrics application contains their own unique Internet Protocol (IP) address so that they can be uniquely identified[15].

6.1. E-voting system through biometric cloud

We know that election is our fundamental right to choose our government. Voting system is a major part of our democratic process. The vote we give to formation of our government should be secret, restricted. If biometric identification is included then security system will be increased and remove various flaws. Biometric data of a person is collected and stored in cloud which helps to find out the real identification of people. Biometric matcher implemented by Software-as-a-Service and anti-spoofing technologies makes the authentication of a person. In E-voting system votes are taken electronically and software System controlled the process. In cloud computing SaaS (software as a Service) will be responsible for e-voting which will control the device, define the ballot, cast, count the vote and calculate the vote to show result[14],[15].

6.2. Different process of E-voting:

Registration: Registration process is related with eligible voters.
Legitimation: This process includes identification, authentication of eligible voters
Casting of Votes: The electronic ballot is shown to vote for voting process.
Collection of Votes: After voting collection of vote are performed which are monitored and counted by a Counter server.
Data collection or gathering tools: It is required for data capture by image or video which is used for person identification.
Database template generation tools: It is used for voter registration process and recognition device stored here. Input data processed here.
Matcher: It make the comparison of input data with appropriate template and take decision to identify of a person.
Cloud database: Large amount of biometric data are stored in cloud data base in Nosql or sql data base such as table ,BLOB ,queue etc.

7. Conclusion and Future Work:

Security, integrity and authentication are three main criteria in biometric cloud computing. The limitation of this system is maintaining integrity, confidentiality and securing the democratic process by preventing coercion. Biometric system denies the unauthenticated voter to access the system and prevent the same voter to cast multiple votes. Biometrics integrated with Cloud will be highly accepted in future. Infrastructure of biometrics can be configured very quickly and it is on demand basis. We can add biometrics when needed and deleted accordingly and it is affordable and highly scalable. We have discussed in this paper biometric security such as Cloud computing with Biometrics as a Service (Baas), Identity as a Service (IDaaS), Biometric authentication for the cloud. If cloud biometric is incorporated with e-voting system it will be more reliable. Cloud computing with biometric is a reliable and secure solution of e-voting and various business systems. Biometric security brings more secure and authentication technique in e-voting system. Future work will incorporate new development of encryption algorithms like elliptic-curve cryptography which makes the system more effective, convenient, user friendly and efficient in e-voting system. In future large number of voting process can be implemented through this system. Cloud computing database will efficiently store the large database of e-voting system.

References

[1] A. Baraani, J. Pieprzyk, and R. Safavi, “A practical electronic voting protocol using threshold schemes,” Centre for Computer Security Research, University of Wollongong, Australia, 1994. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[2] Chaum David (2000) Secret Ballot Receipts and Transparent Integrity, David Chaum draft. Available at http://www.vreceipt.com/article.pdf

[3] http://searchcloudcomputing.techtarget.com/definition/SPI-model.

[4] David Jefferson, Aviel D. Rubin, Barbara Simons and David Wagner, (2004) “Analysing Internet voting security”. Communications of the ACM. 47 (10), pp. 59-64. from http://repositories.cdlib.org/postprints/1197

[5] R. Das,B.V "Biometrics in the cloud".

[6] D.Pugazhenthi, B.Sree Vidya," Multiple Biometric Security in Cloud Computing ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013

[7] J. Bule and P. Peer , “Fingerprint Verification s a Service in KC CLASS”, pp. 76-82, 2012

[8] http://www.ceelox.com/ceeloxidonline.html

[9] http://www.passwordbank.com/passwordbankprivate-cloud

[10] Slovenian Information Commissioner biometrics, https://www.ip-rs.si/varstvo-osebnihpodatkov/informacijske-tehnologije-in-osebnipodatki/biometrija/

[11] M. Ahmed, A. Sina Md. R. Chowdhury, M. Ahmed,, Md. M. Hasan," An Advanced Survey on Cloud Computing and State-of-the-art Research Issues", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 1, January 2012

[12] M. BAČA and M.ČUBRILO,"Towards a General Definition of Biometric Systems, Markus SCHATTEN" ,IJCSI International Journal of Computer Science Issues, Vol. 2, 2009

[13] Gartner report “Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014.” The report is available on Gartner’s website at http://www.gartner.com/resId=1378513.

[14] Business Week June 2010: businessweek.com.

[15] Assessing the Security Risks of Cloud Computing 2008 Gartner, Inc.

Author Profile

Bratati Chakraborti received the MCA and M.Tech degrees in Computer Science and Engineering from WBUT and KIIT university in 2008 and 2014, respectively. She is the Assistant Professor of NSHM College.She is OCA.