Cloud Computing Login Authentication Redesign

Eric Opoku Osei[1], James Benjamin Hayfron-Acquah[2],
(Corresponding author: Eric Opoku Osei)

Computer Science Department, Kwame Nkrumah University of Science and Technology[1]
Private Mail Bag, KNUST Kumasi

Computer Science Department, Kwame Nkrumah University of Science and Technology[2]
Private Mail Bag, KNUST Kumasi
(Email: eoosei@gmail.com)

(Received Dec. 23, 2013; revised and accepted Feb. 13, 2014)

Abstract

Trusted-security is a concern for cloud adoption by many enterprises. The work was to improve login security process at cloud's user-end using biometric to replace secret code generation as step-2 authentication. System development life cycle-revolutionary waterfall method was adapted for the design process and verified the redesign using Delphi technique with security experts. The work alerts authorised user to block domain intrusion on phone at real time as phone is permanently interlinked to access server. On experiment, authorised user must submit cloud username and password on computer workstation as step-1 key. On submission, a text message is generated to a predefined biometric-compatible phone for user to scan bio-feature. As backdoor, if predefined biometric phone is temporarily lost; open the alternative link sent to authorised user e-mail account to capture and resend the scanned bio-feature to server as step-2 key for access privilege. Results indicated rigidity to prevent hacking via user-workstation. We recommended multi-nodal bio-scanning to reduce authentication failure rate and argued conclusively that this work improves user-end login security for cloud clients.

Keywords: Access control; Biometric-phone; Cloud Computing; Security; 2-step Authentication;

1 Introduction

Cloud computing has come to stay. Cloud Security Alliance (2013) rated nine notorious cloud computing top threats. On account of severity; data breach came first on the rank [4]**.** Wentao Liu (2012) rated data privacy as the key security problem. The work further emphasized that a single security method cannot solve the cloud computing security problem and many traditional and new technologies and strategies must be used together for protecting the total cloud computing system [10]. Adam Maguire published a survey conducted amongst Chief Information Officers (CIO's) and I.T Directors during the 2010 pricewaterhouse Coopers forum (www.irishtimes.com, 2010) [11]. The publication provided feedback that clearly shows "Security" as the biggest concern for enterprises thinking about the cloud evolution. Simply put; Cloud Computing is the new evolution to expand ICT for development and virtual application subscription. The new idea is to leverage this virtual subscription concept into everyday enterprise business. In the late 1960's, the computer scientist John McCarthy once brought the concept of utility computing into the technology world, predicting that the life cycle of technology will not only stick as tangible products. Today, whatever the term, cloud computing, happens to do could be referenced to the primary research of the utility concept by John McCarthy [6].

Débora DG & Brunzel T, (2010) discussed in their thesis, the various services in the cloud. Service providers offer to corporate clients: *Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS)*; all at pay-per-use and without initial Capital-intensive demand. Cloud offers better economic advantages over the traditional in-house-acquired IT infrastructure**.** However, the issue of security threatens small medium enterprises to leverage transactional and query traffics unto the cloud platform. Cloud computing is a flexible, cost-effective and proven delivery platform for providing business or Consumer IT services over the Internet [5]. Bill Claybrook in his contributory work in the SearchCloudComputing.com E-guide report explained that cloud resources can be rapidly deployed and easily scaled, with all processes, applications and services provisioned "on demand," regardless of user

location. Improving its security has great potential for I.T deployment and integration in business operations. The very near concept of today's cloud computing was called grid computing. The intangible difference between cloud and grid is that cloud comes with service Level Agreement (SLA) between customer and the provider. The term grid computing also originated in the early 1990s as a metaphor for making computer power as easy to access as an electric power grid. Unlike Cloud; the Grid has disadvantages of relying heavily on dispersed data management and connectivity errors. There are different types of cloud computing and summary of differences are shown in Table 1 [3]: (www.mcrinc.com)

Table 1: Cloud topologies – benefits and risks

TOPOLOGY	BENEFITS & RISK
Public Cloud	-**Benefit***:* Low investment hurdle -**Risk**: Multi-tenancy security threat
Private Cloud	-**Benefit**: Sustains in-house security policy -**Risk:** High operation and maintenance cost
Hybrid Cloud (Public-Private)	-**Benefit***:* Constant network availability -**Risk:** vulnerable to all public network risk

Specific research question to improve on cloud security and robust access control at the user-end workstation pointed to the use of Two-step authentication method to help ensure that a hacker cannot access corporate data when in full possessions of authorised username, password, PIN code and the stolen mobile phone that is used to issue the second factor secret code. The need for 2-step authentication is critical for now. Mark Burnet [2] stated in their 182-page book on access control methods that user passwords are the keys to the network kingdom, yet most users choose overly simplistic passwords (like password) that anyone could guess, while system administrators demand impossible to remember passwords littered with obscure characters and random numerals. The need for more rigid access control to improve cloud trusted security has been the focus of this new work.

The issue of Trusted-security remains peculiar, either we move enterprise data unto a private, public or hybrid cloud platforms. In the same manner, an enterprise decision to stay in-house with corporate data would not change security challenges. A company gains some amount of administrative control, whiles it remains within in-house than on cloud platform. This is so because corporate clients are compelled to work with unknown cloud system administrators managing such a multitenant data house. The most popular end-user authentication is the use of secret code generation. In an attempt to login, authorized user is required to generate a secret code and add to the password as second factor access pin to gain access. However the use of secret code generation has limitation. A hacker holder username and password can isolate the mobile phone from the login server since designers give option for mobile isolation option to users. A hacker can install password sniffer (keylogger) on the computer to track keys used by the authorised end user.

The discussion on unknown cloud administrator and the activities of hackers prompted a redesign of cloud login architecture to offer sufficient protection at user-end workstation. In this work the purpose was to redesign login architecture so that any attempted domain login or intrusion by unknown user is observed and blocked on real-time by the authorised user via permanently connected user mobile phone that is biometrically compatible. The next was to shift from the use of secret codes for authentication to biometric scanning on the mobile phone to complete the login process for authorised enterprise cloud user. This study primarily investigated existing 2-step authentication security methods and observed how to improve the method for cloud computing implementation. The main research question was to know what improvement on Two-step authentication method would ensure that a hacker in possession of authorised username, password, authentication PIN code and the stolen mobile phone cannot get access to corporate data sitting on cloud computing infrastructure using authorised end-user network route. The follow up question was to find a way an SME's subscribing to cloud computing platform could administer security control to block real time intrusion by a hacker criminally holding cloud credential to enter corporate domain. As a limitation we could only provide the descriptive results after applying Delphi technique. Some detailed challenges spelt out in material and method section in this paper.

Literature surveys revealed limitation in the existing two-step authentication methods used by giant cloud operators such as Google, Amazon, Dropbox, Barclay's internet banking, Fujitsu limited and others. Cloud operators using this method attempts to focus on improving either the secret code issuant process or avoid keylogger hacking attempts.
Within the limitations, the 2-step authentication method still provides some level of login security and confidentiality to enterprise data. The unique discovery was the fact that almost all the introductions in different cloud houses adopted similar or closely refined architecture as shown in Figure 1 and developed for use by Fujitsu limited.
S. Sotashi (2009) patented two-step authentication architecture at Fujitsu Limited to improve data security as shown in Figure 1 [12]**.** They discussed that an authentication system includes a user terminal to perform authentication based on a password corresponding to a seed number generated in accordance with a predefined rule. The system further includes a password issuance apparatus to issue the password in response to reception of a request message including the seed number as shown in Figure 1.

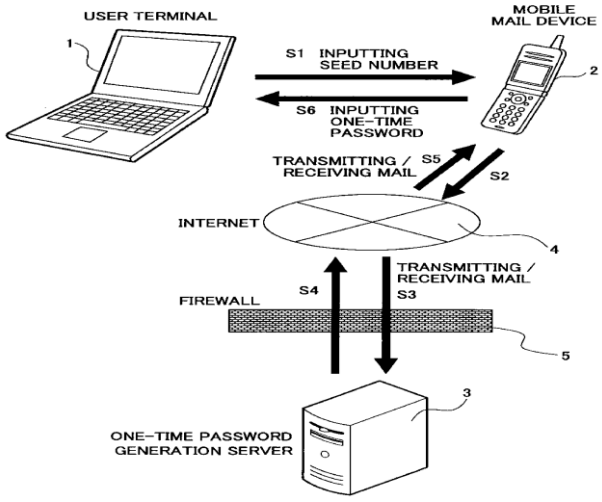

Figure 1: The implementation of Two-Step Authentication as used by Fujitsu Limited

The method of design has three main device segments: User terminal, Mobile device, Server, and transmission medium.
Figure 1: The mobile device has software uploaded to communicate with the authentication server. Each user has a code called seed number; user enters that seed number on the mobile device and the seed number transmits to the authentication server. Authentication server compares SIM number sending request and Seed number assigned to that authorise user. If SIM and SEED numbers corresponds to pre-defined numbers on the server, then server grants the request to transmit one-time- password to the phone. Authorised user can now obtain password and use it to log-in through the computer domain to access corporate data on business operations server. *[Patent Document 1] Japanese Laid-open Patent Publication No. 2007-58469]*.
The work of Google [9] and Dropbox Inc**.** [7] are highly connected to the architecture by Fujitsu. The same as Barclay's internet banking with additional soft feature [8]. Barclays introduced to the same architecture, soft screen keypad for entering the secret code sent via the user phone to avoid keylogger sniffing activities to track keys. Amazon [1] improved the method with the use of barcode scanning to compare with stored template. We will discuss the review further under results and discussion section in this paper since a common and fundamental architecture as execution process is used by aforementioned entities.

2 Materials and Methods

We investigated the design using survey with some IT security experts in Ghana and only provided descriptive results concluded with the help of the experts that were engaged. The design, which supposed to provide experimental results, has to adopt the alternate approach of using the Delphi technique with security experts, local software developers and Telecom data switching engineers due to lack of biometric laboratory in the region. The cost of international lab assistance was another challenge. One typical challenge was the need for biometric compatible mobile phone that can that has multimodal feature to accept more than one biometric templates of the human anatomy. The largest area to

acquire very related secondary materials on 2-step authentication method were online libraries of the companies using the approach as second factor security for their clients' data privacy. Most academic and journal papers reviewed on two-step authentication have to deal with network paths and address protocols using 2-step methods; not for the purpose of user-end workstation as in our work. These papers were later avoided as part of secondary data collection in this paper to reduce scope deviation. Primary data collection was captured through unstructured interviews with I.T security experts, cloud administrators and mobile switching engineers to improve on the descriptive work. The System Development Life Cycle-revolutionary waterfall approach was adopted to make decision on the software development process.

Prototyping the design has been the major choice for initiating these codes. The advantage was to give chance to both the designers and potential users suggest improvement to the project completion. It was important to determine the testing standard suitable for this design to pre-inform the implementation stage of the system development Life cycle-SDLC. There are three basic testing methods (Thomas Vian, 2002) .Top-down, Bottom-up and Ends-in and we selected the Top-down approach. Top-down is a method in which a programmer joins the overall skeletal structure of the program before performing test. Next, the programmer would 'load in' the reviewed codes in some sections and then test it again and so on until the final program is completed and tested**.** The advantage of this method is that the programmer is always looking at the whole problem in one go, as all the parts of the program are related to each stage of execution [13].

3 Results and Discussions

A new login architecture design was developed using the 2-step authentication concept as shown in Figure 2. The design has 4-minutes validation or expiration period within which an authorised user has to provide biometric authentication input to gain access to data.

Figure 2: The use of biometric for 2-step authentication process

Unique feature introduced to this concept was the use of logic "AND" gate mathematical model for interlocking user computer (workstation) to user mobile phone permanently. Cloud password "AND" biometric scan input must be provided at any log-in attempt to gain access to data. This is quite different form the existing works. The existing works make use of logic "OR" function so that users can have the option to disconnect and re-connect their mobile device the use to accept authentication sms link. User self-service privilege to connect and disconnect authentication phone from the login security server is a limitation and a threat to data privacy or protection in the cloud.

On experiment as shown in Figure 3, an authority user must login with cloud username and password on computer as step-1 key to do access request. The user has to complete login using biometric input for authentication as step-2 key. The authentication server picks the request by step-1 password key "AND" embeds login link to a pre-defined user mobile phone to allow biometric scan and resend to the server. The scan is finally sent back to the authentication server to compare with stored biometric template. There is a backdoor alternative to login when phone is lost: Figure 3 shows the backdoor routing link to user corporate e-mail account.

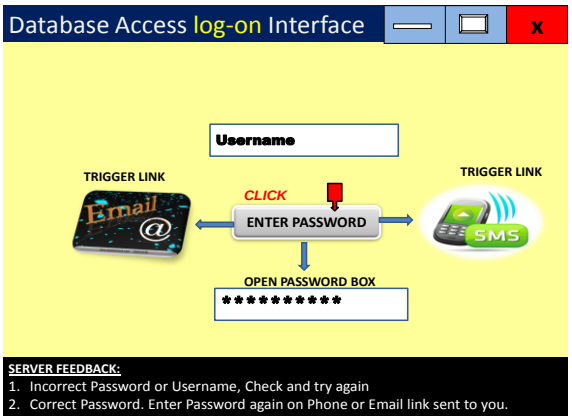

Figure 3: Backdoor Authentication routing through user E-mail account

Imagine you lose your biometric compatible phone in a car; what alternative can ensure business continuity in the cloud by such user? Backdoor entry is important in any access design and programming. There is backdoor login process as shown in Figure 3; link is sent through E-mail account so that any enterprise computer with embedded biometric scanner is used to authenticate user when the pre-defined mobile phone stolen is pending for replacement. The implementation is geared towards enterprise interest so as to provide level of trust to operate both transactional and query-based traffics on the cloud platform with hope for data confidentiality and integrity assurance.

Discussing the literature review further; it was observed that the Two-step authentication in general is a customer-felt security method that can convince and attract more clients to trust cloud adoption as well as improve domain access control to users of the cloud. If the issuance of existing secret code or OTP by some cloud operators through mobile device is powerful to some extent, then the use of biometric scan on mobile device to complete second factor authentication would be a great potential to improve loud security. Again, it was noted that a hacker who steals the configured mobile phone in addition to username and password could fully access every data on the cloud datacenter because of the use of OTP codes. We can resolve this problem with the use of biometric introductions. Therefore, for small and medium enterprises to hook unto cloud business solutions, each corporate user requires specialised multi-modal biometric compatible mobile phones, which is now coincidentally made available for different purpose by the U.S department of defense research sponsorship to AOptix development limited (2013). Using such same biometric iPhone, a hacker holding username, password and stolen iPhone cannot access data as the life body of the authorised user may still be required to complete the second factor authentication. The only source of breakthrough for a hacker is when the user biometric is decoded into the logic digit representation. As a way forward to combat any transmission interception and decoding, the biometric data requires encryption within the transmission path to ensure data privacy.

The Algorithm Format

Algorithm 1: Authentication Execution through mobile phone

1: Begin
2: Initialize u*ser terminal side: Enter correct cloud username and password.*
3: Send service request to the dedicated login server.
4: while Not end of user session do
5: Accept transaction data on login server and compare with stored user credential.
6: Belief sent credential.
7: Send authentication request to predefined user mobile phone.
8: Capture biometric feature on user phone and send back to authentication server
9: **if** biometric captured on phone matches template on authentication server
then
10: Open user domain when username, password "AND" biometric feature matches for that user domain.
11: **end if**
12: Periodically block access in ideal situation to allow fresh login
13: **end while**
14: End

Algorithm 2: Backdoor Authentication on Laptop/E-mail

1: Begin
2: Initialize u*ser terminal side: Enter correct cloud username and password.*
3: Send service request to the dedicated login server.
4: while Not end of user session do
5: Accept transaction data on login server and compare with stored user credential.
6: Belief sent credential.
7: Send authentication request to both predefined user mobile phone and Email account.
8: Capture biometric feature on biometric compatible laptop and send back to authentication server
9: **if** biometric captured on laptop matches template on authentication server
then
10: Open user domain only.
11: **end if**
12: Periodically block access in ideal situation to allow fresh login
13: **end while**
14: End

Sample Alert SMS shown in Figure 4.

From: servicedesk.mtncloud.com
To Mobile: +233 244910077018
To E-mail: jbihka@cloudknust.edu.gh
Subject: Authentication request message
Dear cloud user, based on your access request, KNUST000000446395, click on the link to scan for authentication.
http://servicedesk.mtncloud.com/knustdomain/user&pwd=GenericUser

Figure 4: Authentication SMS link to user.

There is no way to assume perpetual motion machine in the world of knowledge advancement. Although the new design predicts a robust access control to data, the programming involved alert message after third time password attempt as shown in Figure 5. This is to create real time awareness to user to change cloud password suspected to be compromised.

From: servicedesk.mtncloud.com
To Mobile: +233 244910077018 (voice alert)
To E-mail: jbihka@cloudknust.edu.gh
Subject: Incident alert voice call & SMS

Dear cloud user, someone else might be trying to access your cloud account jbihka@cloudknust.edu.gh
Tuesday, April 2, 2013 1:51:46 PM UTC
IP Address: 196.201.54.56
Location: Unknown

If you do not recognize this sign-in attempt, you should sign in to your account and reset your password immediately.

Figure 5: Alert message after three times password entry

4 Conclusions and Recommendations

Unlike the existing works, a hacker holding user-password, user-phone or any biometric computer, cannot access enterprise cloud data without authorised fingerprint or other biometric feature scans provided as second factor input by

authorised cloud user. In conclusion, the experience obtained from observing the trailing of existing software packages and discussions with experts have enhanced the development of the idea to implement two-step authentication method using multi-modal biometric to enhance cloud security trust for clients. Similarly, the use of real time biometric authentication, instead of secret codes for authentication, offers rigid security and trust on cloud data access. We recommended eye and fingerprint scans (multi-nodal scanning) to reduce authentication failure rate and argued conclusively that this re-design work can improve cloud trusted-security.

1). Recommendation for further work is to investigate encryption and decryption algorithms to secure biometric data transmission from the mobile phone to the authentication server so that when such biometric data is intercepted on the gateway it will be useless information when decoded.

2). E-government datacenters in developing countries stand a chance to benefit from this login security authentication. Many developing countries are integrating ICT or yet to use ICT in day-to-day government sector transaction. With this development, many civil and public servants are likely to depend on their family relatives to support them process government electronic data at home and office. With such biometric authentication, supporting relatives would find it difficult to login without consent of authorised user. This may enhance data privacy on the e-government platform.

Acknowledgement

I am grateful to my interviewees: Wilfred Bruku (SMS transmission engineer), Edgar Zormelo (Cloud system administrator) and Eric Afanu (I.T security consultant) for immense contribution gathered from their experiences. I also thank all the various IT users recruited to comment and criticise the design for possible limitation for security breech.

References

[1] Amazon web services library, Multifactor authentication system; (2009) Available from: <http://aws.amazon.com/mfa> Accessed on 28/02/2013.

[2] Mark Burnett and Dave Kleiman, "Perfect Password: Selection, Protection Authentication Illustrated", Syngress Publications, 2005, Chapters 1, 2, 13 pp. 182.

[3] Bill Claybrook, "Differences explained: Private vs. Public vs. hybrid cloud computing. Available from: http://www.mcrinc.com/Documents/Newsletters/201207/, Accessed on 6/03/2013.

[4] Cloud Security Alliance**,** "The notorious nine cloud computing top threats in 2013", cloud security Alliance top threat working group report, 2013.

[5] D. G. Débora & T. Brunzel, " Cloud computing Evalation-How it differs to Traditional IT outsourcing", Jönköping University academic archive online, Master student Thesis, pp. 1-29, 2010.

[6] Definitions of theories associated with cloud computing. Available from: http://en.wikipedia.org/wiki/Cloud_computing/, Accessed on 6/03/2013.

[7] Dropbox support-2-step authentication system; Available from: https://www.dropbox.com/help/363/en/, Accessed on 21/03/2013.

[8] Barclays Bank Ghana, "Internet banking library-step authentication system", Available on http://barclays.ghana@barclays.com/internetbanking/OTP, Accessed on 15/03/2013.

[9] Google support- 2-step verification system; Available from: http://support.google.com/accounts/bin/answer.py?hl, Accessed on: 04/02/2013.

[10] Wentao Liu, "Research on cloud computing security problem and strategy", 2nd International Conference on Consumer Electronics, Communicatons and Network, Three Gorges, China, April 2012.

[11] Adam Maguire, "PricewaterhouseCoopers forum on cloud", Available http://www.irishtimes.com, Accesseed on 5/03/2013.

[12] Sotashi Samba (2009) Fujitsu limited 2-step authentication system and method http://www.google.com/patents/EP2131302A2?cl, Accessed on 11/02/2013.

[13] Thomas Vian, "Design an interactive website to help teach maths, to year two, key stage one children", Academic thesis, Pages 82, Accessed on 2/04/2013.

Eric Opoku is a graduate of Kwame Nkrumah University of Science and Technology-Ghana. He holds an MPhil in Information Technology and a telecom network engineer at Mobile Telecommunication Network and Cloud computing

operator (MTN-Ghana). His research interest is in cloud computing –Security & IT applications for business solutions.

James B. Hayford-Acquah is a senior lecturer in Kwame Nkrumah University of Science and Technology-Ghana. His main research interests are image processing and securities. He was the former Head of department and currently the Exams officer of the department of computer science. He has extensive teaching experience at both postgraduate and undergraduate levels.