

# Online Identity in the E-development of Saudi Arabia

Moudhi M. AL-Jamea

Dept. Computer Science ,King's College London , London WC2R 2LS, England

[Mudhi.aljamea@kcl.ac.uk](mailto:Mudhi.aljamea@kcl.ac.uk)

2012

## Abstract:

Information security is one of today's most interesting and challenging topics, especially if one considers the ever-changing development of the Internet and the increasing number of cyber-crimes. Furthermore, there are worries specifically about e-society and e-services. Most people are worried about their online identities and whether the online users they are dealing with on social networks or in any other business websites are the right person. However, we are beginning to see some changes that can improve how we manage our identities online. We can create online identity protection systems that are more powerful and more trustworthy than the ones available currently. Moreover, these online identity systems could provide greater protections for security and privacy than we currently achieve when using documents to prove identity in the physical world. Developing trustworthy online systems that can positively identify each person will help decrease the number of cyber-crimes. However, these online systems can't work alone; there should be a third party or a solution that will match the physical identity with the online one.

## Keywords :

Online identity ,information security , web algorithms, security algorithms , identity theft.

# INTRODUCTION

As more and more of our social identity information is shared online, so managing it will become increasingly difficult and increasingly important. With the introduction of the e-government portal in Saudi Arabia, citizens are worried about using it and how they will adapt to it. How can they trust it? The answer to these questions plays a key role in fighting identity fraud and cyber-crimes. Answering these questions and developing a solution will be the main purpose of this proposal, and I will investigate Saudi Arabia as a case study.

The Internet in Saudi Arabia was introduced in the late 1990s; however the online services transformation wasn't implemented until recently. "The e-Government project started in 1998 but according to the UN report, in the context of e-Government readiness, Saudi Arabia has significantly transformed its electronic service delivery from 2005 to 2008" (UN 2008).

Moreover, compared to other developed countries, businesses websites are not as popular in Saudi as in other countries. There are famous and successful businesses with no websites for their customers to contact them or to offer services through it. However this is not because they care about the cost or the development, but because they don't think that a website would improve their business since the citizens don't care much about online services. This is mainly because of the lack of trust of the online services in Saudi.

## Research Questions

- How can we make sure that we're talking with the right person or system?
- Can anyone confirm his/her identity?
- What if someone stole my identity and committed frauds on people using my name?
- Can we create online identity systems that are more robust than the ones currently available in order to increase trust?

Standard username and password authentication systems are becoming outdated, and technologies like Facebook Connect, OpenID, identity in the browser or biometrics on mobile phones may be poised to take over the role of disclosing our identity online. My PhD argument is going to be about the user's online identity, concentrating specifically on the online identity in the e-development of Saudi Arabia where the e-services are considered to be new compared to other developed countries. The greatest challenge facing Saudi Arabia is transforming the offline services to e-services and how the government can get citizens to trust them. Furthermore, the government is now faced with complex decisions in how it approaches issues of identity and the increasing integration of technology into the daily lives of citizens.

Governments need ways to empower citizens to identify themselves online and to identify the services that are offered to them. What we mean by "our identity" can change depending on where we are and what we're doing, and that may be the most difficult problem of all to solve. Some people agree in having one single identity, as Mark Zuckerberg, founder of Facebook once said, "having two identities for yourself is an example of a lack of integrity" (Zimmer 2010). However, others strongly disagree with that and think its a very bad security solution; others think that they want to have more than one identity, for example, a Twitter identity is different than the Facebook personality and different than the serious work personality and so on. As Evan Williams, co-founder of Twitter, said, "Online identity is still a messy problem with lots of opportunities" (Williams 2011).

## **Literature review**

Over the years, Information Communication Technology (ICT) has been considered to be significant in modernising and transforming most organisational functions and operational practices (Beynon-Davies, 2005).

According to the Merriam-Webster dictionary, identity is "the condition of being the same with

something described or asserted”. Essentially, identity is made up of characteristics that describe “an entity, be it a person or thing”.

Scholars have been arguing for the past decade about how to prove the user’s identity online and whether it should be one single identity or multiple identities for the same person. There are many online identity management systems and their goal is to identify the users online, “The ultimate goal of any identity system is to provide identity assertions that are sufficiently reliable for the intended purpose” (Smedinghoff 2011, p. 24), but most of it failed to reach this purpose.

Former Twitter CEO Evan Williams noted in a blog post that online identity is one of the thorniest issues any web-based service has to deal with (Howard 2011). However, Jim Dempsey of the Center for Democracy and Technology (CDT) highlighted a critical problem at a forum on identity in January 2011: government needs a better online identity infrastructure to improve IT security, online privacy, and support e-commerce but that it can’t create it itself (Howard 2011).

Even Google+ is facing online identity issues. According to CNET News, “Now two weeks old and growing like a weed, Google+ is facing issues that became common once the Internet made people’s identity into information that can reach potentially anyone on the planet. With Google+ and the Google Profiles service on which it relies, the company is trying to build a service without pseudonyms, anonymous cowards, or impersonation” (Shankland 2011).

There are some identity management systems but they are either not accepted or popular, for example the OpenID solution. “If you have not heard of or noticed OpenID around the Web, it’s because it’s still not universally accepted. Even sites that accept OpenID do not always make it readily apparent. OpenID has probably yet to become ubiquitous because of security concerns. Some people consider OpenID too vulnerable to phishing attacks. If exploited, it could become a potential gateway into all of a user’s private, OpenID-linked information” (Ovadia 2010).

However, so many people support the single online identity and think it will solve almost all the security concern/issues that are related to their online identity. For example, Facebook Connect gives Facebook users the ability to login to non-Facebook websites using their Facebook login information. There is also OpenID, where the user creates an account and uses the same personal information to login to other websites that support the OpenID solution. Still the idea of single idea wasn't acceptable to most people. "The concept of a single online trusted identity...started with OpenID, but was not very popular due to its limitation around assurance and trust" (Kohli 2011).

"One username and password for everything is actually very bad 'security hygiene,' especially as you replay the same credentials across many different applications and contexts (your mobile phone, your computer, that seemingly harmless iMac at the Apple store, etc.)" said Chris Messina in a WebProNews interview (Crum 2011).

According to a RNCOS report (2009), the online identity market is growing very fast and "the Identity and Access Management (IAM) market has been witnessing exponential growth globally, as it has emerged as the most efficient way of identity management."

Some countries in Europe tried new identity management solutions like electronic ID cards, but it didn't fully succeed (Ovadia 2010). Ovadia (2010) adds that these cards have not been able to help resolve the challenges of managing web identities and some researchers find that keepers of personal information, or "infomediaries", are "a challenge to an all-encompassing electronic government-sponsored identity strategy".

Online identity systems could provide greater protections for security and privacy than we currently achieve when using documents to provide identity in the physical world. However, "if we want the Internet to reach its full potential, we need a safer, more trusted online environment" (Charney 2010).

Cyber-crime has been increasing for the past couple of years and it is costing governments a lot of money, for example in the UK, according to BBC "Cyber crime costs the UK economy £27bn a year" and those figures are "made up of £21bn of costs to businesses, £2.2bn to government and £3.1bn to citizens" (BBC News 2011).

However, in order for any new online identity management solution to succeed it should be accepted by the online society. "The success of any new identity management solution will be decided by how willing users and organizations are to invest in the new technology" (Tsui 2006, p. 15).

### **The E-development of Saudi Arabia**

Among others, "Saudi Arabia is one such developing country that has cultivated its web presence since the late 1990s" (AlSobhi et al 2009). "Saudi Arabia is a rich developing country in the Middle Eastern region that has started implementing national e-Government projects since 1998" (AlSobhi et al 2009), but these e-government services and e-commerce transactions have not been very popular until now. According to a January 2011 survey by The Arab Advisors Group, the total number of Internet users in Saudi Arabia who make online transactions is only around 12% of the total population of the country, which is around 3.1 million. Furthermore, these 12% have spent an estimated US\$3 billion on online transactions (Arab Advisors Group 2011).

# Online Identity

## 1- Identity theft statistics

The basic definition of “identity theft” is when someone impersonates the person whose identity he or she stole and commits a fraud or frauds under the victim’s name. It happens every minute around the world to different kinds of people with different backgrounds and of different ages. Moreover, the identity thief might attack your bank account, emails, social accounts etc. and use your information for other types of cybercrime.

Online identity fraud is a problem that makes many people think twice before purchasing anything online. It’s been a major problem since the start of the social networking sites in early 2000 when people started to engage more with the internet and started sharing a lot of information online.

According to the 2011 Identity Fraud Survey Report that was released by Javelin Strategy & Research ([www.javelinstrategy.com](http://www.javelinstrategy.com)) and the US Federal Trade Commission (FTC) Report, in 2010 the number of identity fraud victims decreased by 28% to 8.1 million victims in the US, three million fewer victims than the previous year. Moreover, the total annual cost of fraud decreased from \$56 billion to \$37 billion.

Moreover, according to the US Federal Trade Commission:

- “Friendly” fraud, when a customer pretends he or she was the victim of identity fraud to claim back the cost of goods received, increased by 7% over 2009
- The FTC received 250,854 identity theft complaints in 2010
- For the 11th year in a row, identity theft complaints represented the largest number of complaints received by the FTC
- The IRS reported 245,000 incidents of identity theft, compared to 169,087 in 2009

## **2- Various ways of stealing your online identity**

There are various ways to steal an online identity including taking bank account information or other personal information. However, there are very sophisticated techniques developed for the purpose of stealing online identities and every day they develop new and better ways:

1. Collecting information online such as through social networking sites, chat rooms, online CVs
2. Fake e-commerce websites, and fake pop-up ads
3. Stealing credit card information online through hacking of e-commerce sites
4. Trojan horses, spyware: after these programs have been downloaded on the computer, they will collect the user's personal data and send it to the criminals
5. Physical theft of a wallet or purse with important cards (ID cards, bank cards, license etc.) can be used to make online transactions under the victim's name
6. Signing agreements and policies without reading them might also cause some information to leak to unwanted people
7. Email phishing, spam emails with fake links that will direct the user to websites with an identical design of their bank, e-commerce site, or social site and ask them to enter their personal data as an updating process, for example

## **3- Current solutions to prevent online identity theft**

There are many ways to protect your online identity and to identify the online person you're dealing with. For example, to protect our online identity here are some of the common ways that might help:

1. Choose strong passwords, and change them frequently
2. Shred important papers that include very personal information such as bank statements, utility bills
3. Do not share too much information online with strangers
4. Check your bank statements regularly at least once a month
5. Be aware of phishing emails, spam, viruses

6. Try to use encryption software when sending sensitive information online, and also make sure to update the security software on your computer
7. Cancel any unused accounts online

On the other hand, there are some less effective solutions to verify the online user's identity such as authentications with the help of a third party. As mentioned before, some of solutions have not been implemented yet and some are not yet acceptable:

- One user name and password solution, which has its disadvantages as well as its advantages
- Identifying online users through their browsing experience, specifically through linking the search engines with the algorithmic identity and trying to match the user's browsing behaviour with a standard pattern
- Using a third party for user authentication, or an outside authentication tool like what some of the banks are using now by providing every user with a token or passcode as an extra authentication

However, these and many other solutions either didn't succeed or they are still in the testing phase, so we can still consider online identity theft as one of biggest problems that has developed since the creation of the internet.

#### **4- Proposed solution**

The solution will be to find the best web algorithm that will help identify online users and that will minimize online identity theft crimes and give the online user more trust and encourage them to engage more in online transactions.

## **Methodology**

- I will do both field study and experiments to collect quantitative and qualitative data.
- **Field study:** The research methodology will focus on examining existing techniques for online identity authentication and figure out why the current online identity management systems didn't win the users' trust
- **Data collection:** I will collect data about online user behaviors, especially in Saudi Arabia and will investigate the people's attitude towards online security: What scares them the most about entering their data or questioning someone's identity, and why didn't the existing online identity techniques help them? For this, I will be adopting interview and survey techniques
- **Data analysis:** To find out what would make them trust the other party or websites when it comes to entering sensitive information about themselves online
- Next, I will design some experiments, and algorithms according to the previous methods, and will be able to develop a new theory for online identity and will implement it into an online identity solution
- To develop the system that will adopt RAD (rapid application development) methodology
- As I am choosing Saudi Arabia as a case study, I will try to implement the findings there and observe the results

## **Expected results**

I will aim to answer the research questions and develop the online identity theory about how users can trust whom they are dealing with online, and give them the confidence to do a major transaction online or even share their sensitive information. I will also implement the findings on Saudi Arabia as a case study by developing an online identity solution and observe how it affects the users' behaviours when they think about doing a real online transaction or using any of e-services in Saudi Arabia.

## Bibliography

AlSobhi, F., Kamal, M., Weerakkody, V. (2009) Current State of E-Services In Saudi Arabia: The Case of Intermediaries in Facilitating Government Services In Madinah City. Available at: <http://dspace.brunel.ac.uk/bitstream/2438/4017/1/C84.pdf> [accessed 9/8/11].

Arab Advisors Group (2011) Saudi Arabia's Internet users spent around US\$ 3 billion in 2010 on buying products and services through e-commerce [press release]. Available at: <http://www.arabadvisors.com/Pressers/presser-170211.htm> [accessed 9/8/11].

BBC News (2011) UK Cyber Crime Costs £27bn a year. Available at: <http://www.bbc.co.uk/news/uk-politics-12492309> [accessed 9/8/11].

Beynon-Davies, P. (2005) Constructing Electronic Government: The Case of the UK Inland Revenue. *International Journal of Information Management*, 25(1), 3-20.

Charney, S. (2010) The Evolution of Online Identity and Trust. Available at: <http://www.scmagazineus.com/the-evolution-of-online-identity-and-trust/article/164753> [accessed 9/8/11].

Collings, T. (2008) Some Thoughts on the Underlying Logic and Process Underpinning Electronic Identity (e-ID). *Information Security Technical Report* 13: 61–70.

Crompton, M., McKenzie, R. (2010) Current Issues and Solutions in Identity Management. Available at: <http://www.justice.gov.il/NR/rdonlyres/E1685C34-19FF-47F0-B460-9D3DC9D89103/26388/201010CurrentIssuesinIdentityManagementNICTAJerusa.pdf> [accessed 9/8/11].

Crum, C. (2011) Google's Open Web Advocate Talks White House Web ID Plan. Available at: <http://www.webpronews.com/googles-open-web-advocate-talks-white-house-web-id-plan-2011-01> [accessed 9/8/11].

Kohli, M. (2011) Transformation from Identity Stone Age to Digital Identity. *International Journal of Network Security & Its Applications (IJNSA)*, 3(3): 121-136.

- Howard, A. (2011) A Manhattan Project for online identity. Available at:  
<http://radar.oreilly.com/2011/05/nstic-analysis-identity-privacy.html> [accessed 9/8/11].
- MacMillan, D. (2009) Why Facebook Wants Your ID. *BusinessWeek* 4161: 92–93.
- OpenID (n.d.) Surprise! You may already have an OpenID. Available at: <http://openid.net/get-an-openid> [accessed 9/8/11].
- Ovadia, S. (2010) Internet Connection. The Trouble with Logins: The Challenges of Online Identity. *Behaviour & Social Sciences Librarian*, 29: 296-300.
- RNCOS (2009) Identity and Access Management Market Forecast to 2012 (research report). Available at: <http://www.rncos.com/Report/IM181.htm> [accessed 9/8/11].
- Sahraoui, S., Gharaibeh, G., Al-Jboori, A. (2006) Government in Saudi Arabia: Can it Overcome its Challenges? *Government Workshop '06 (eGOV06)*, Brunel University.
- Shankland, S. (2011) Google+ Faces Thorny Online Identity Issues. Available at:  
[http://news.cnet.com/8301-30685\\_3-20078671-264/google-faces-thorny-online-identity-issues/#ixzz1UFet1E1i](http://news.cnet.com/8301-30685_3-20078671-264/google-faces-thorny-online-identity-issues/#ixzz1UFet1E1i) [accessed 9/8/11].
- Smedinghoff, TJ. (2011) Introduction to Online Identity Management. Available at:  
[http://www.uncitral.org/pdf/english/colloquia/EC/Smedinghoff\\_Paper\\_-\\_Introduction\\_to\\_Identity\\_Management.pdf](http://www.uncitral.org/pdf/english/colloquia/EC/Smedinghoff_Paper_-_Introduction_to_Identity_Management.pdf) [accessed 9/8/11].
- Tsui, W. (2006) Digital Identity Management on the Internet. [dissertation]. Available at:  
[http://zoo.cs.yale.edu/classes/cs457/tsui\\_digital\\_identity\\_management.doc](http://zoo.cs.yale.edu/classes/cs457/tsui_digital_identity_management.doc) [accessed 9/8/11].
- United Nations (2008) World Public Sector Report: UN E-Government Survey: From E-Government to Connected Governance. New York: UN.
- Williams, E. (2011) evhead: Five Easy Pieces of Online Identity. Available at:  
<http://evhead.com/2011/04/five-easy-pieces-of-online-identity.html> [accessed 9/8/11]

Zimmer, M. (2010) Facebook's Zuckerberg: "Having two identities for yourself is an example of a lack of integrity. Available at: <http://michaelzimmer.org/2010/05/14/facebooks-zuckerberg-having-two-identities-for-yourself-is-an-example-of-a-lack-of-integrity> [accessed 9/8/11].

Javelin Strategy & Research (2011) Identity Fraud Fell 28 Percent in 2010 According to New Javelin Strategy & Research Report. Available at: <https://www.javelinstrategy.com/news/1170/222/Identity-Fraud-Fell-28-Percent-in-2010-According-to-New-Javelin-Strategy-Research-Report/d,pressRoomDetail>. Accessed 13 February 2012.

## Contents

Online Identity in the E-development of Saudi Arabia .....	1
Abstract:.....	1
INTRODUCTION.....	2
Literature review.....	3
The E-development of Saudi Arabia .....	6
Online Identity .....	7
1- Identity theft statistics .....	7
2- Various ways of stealing your online identify .....	8
3- Current solutions to prevent online identity theft .....	8
4- Proposed solution .....	9
Methodology.....	10
Expected results.....	10
Bibliography .....	11