CLOUD BASED SINGLE BIOMETRIC SMARTCARD SOLUTION FOR ORGANIZATIONAL INFRASTRUCTURES

K Madhura Ganesh, Sri Krishna College of Engineering and Technology

ABSTRACT:

Smart cards are increasingly used in different applications such as access controls, payment solutions, Payphones, Banking and retail, Healthcare, etc. We present a cloud based approach for various organizational infrastructure needs by using smartcards with biometrics in an interoperable cloud environment.

Though smartcards currently exist for a wide spectrum of applications, it is still difficult to find a global business model or one stop solution to cater various organizational needs. We analyze, research and present one such solution where smartcards can be used with biometric systems for various needs backed by cloud services that are practically usable in real life scenarios.

In this paper as a part we will look in detail about the smart cards & biometrics in a cloud environment. In the remaining half we present our solution using the above to create an interoperable environment which serves as a global solution. We also propose using NFC technology with smart phones or tablets to perform micro or medium payments in a pre-installed payment terminal.

.***Keywords***— Smartcards, Cloud environment, Biometric embedded systems, Organizational Needs, NFC**.**

INTRODUCTION:

Generally smartcards are widely considered as a very reliable form of electronic identification. But to provide a higher degree of identity verification, biometrics plays an important role and is essential. Authenticating a smartcard alone is just like validating the smartcard but not ensuring that the card holder is the rightful owner of the ID.

Combining the smartcard with biometrics provides a positive binding of the smartcard to the card- holder.

Let us consider a scenario involving a University. (The proposed model is not only applicable to just one sector of organizations but is common to all). Under this category, any actual organizational need can be confined into (but not restricted within) these areas: ID Verification, Restaurant / Cafeteria, access to secure servers (or databases), Access–controls etc.. Traditionally these needs were answered by a separate application each with its own philosophy without coordination. We answer these needs by presenting one single offer for all the requirements. By using a cloud environment backed by increased security provided by the combined biometric systems, a drastically different and efficient solution can be provided in different fields which in turn can be internally coupled and made to cater all the required organizational needs.

This way some of the organizational benefits would be added security, one stop solution, reliability, nearly hundred per cent uptime and more importantly a practical approach. Some of the benefits that a student of the university can enjoy include cloud based net printing anywhere within university, library check in or check out, payment at cafeteria or at vending machines, parking access, access control, logical access to secured systems, etc.. Similarly, the benefits for the tutors or the college management are multi-fold. Some of them to list are student tracking, attendance management, efficient and unbiased allocation of resources, real time monitoring, optimized report generation etc.

BIOMETRICS AND SMARTCARDS:

Today Smartcards can hold enough information which can uniquely identify or authorize a person. The information that is stored inside the smartcards is cryptographically secured thus protected against any data tampering.

We in addition to storing of the unique Id's store the biometric information of the concerned person. The biometric details can be anything but we store finger-print information. This in turn requires no complex or sophisticated equipments but a simple biometric system combined with a smartcard reader to uniquely identify and authorize a user. This way, even if the smartcard gets stolen or lost, the system is still leak proof. Since all the biometric matching can take place using biometric templates stored on the smartcard it is un-necessary to store the complete biometric image data on the smartcard.

WHY CLOUD ?

Cloud computing is the intelligent use of hardware and software resources and delivering them as a service over an internet network.

Some of the Cloud characteristics:

1. Multi-tenancy which enables sharing of resources and cost across a large pool of users therby enabling centralization of infrastructures to a large extent.
2. Reduced operational expenditures.
3. Scalability and elasticity.

4. Web services and API's allow easy interaction with the cloud machines.

In our single biometric-smart-ID based Cloud system the following elements are the key players:

a) An authentication ID (smartcard or a NFC enabled smartphone) acts as a security token.

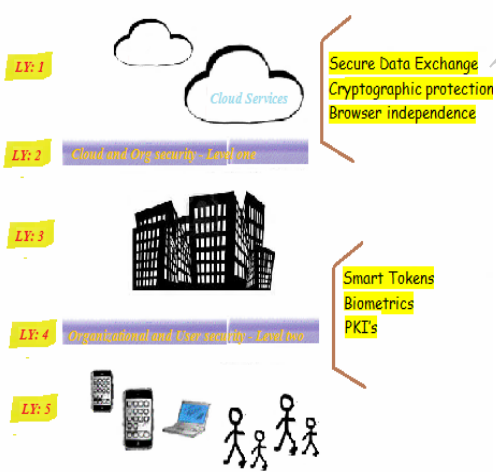
b) A desktop or a terminal application with an attached biometric system validates the presented security token, interacts with the cloud through web services and performs all the to-do's.

c) All the heavy management (database updation, report generation, data processing, live-reporting etc..) is taken care by the Cloud systems.

The cloud service delivery platform that we propose allow organizations to cater their clients' by letting them harness real-time intelligence and transform it into actionable insights. This system provides them better solutions along with increased portability and almost any-time any-where accessibility.

PROPOSED SINGLE BIOMETRIC- SMART-ID BASED CLOUD SYSTEM

We propose a five level architecture design which is described by the following diagram.



Layer 5 [End User Service Layer]

In this layer a organization shall assign an unique ID [we used a 32 bit GUID] for the person or the individual. This is followed by storing this ID information along with the individuals' biometric characteristics (respecting the biometric templates) in a smart ID. The smart ID can either be a smartcard or a emulated smartcard in case of NFC being used.

Layer 4 [Organizational and Client Secure Interaction Layer]

This layer addresses how the interaction should take place between the organisation and its stakeholders. All authentications and transactions should be biometric compared and validated with one of the smart ID's. A simple biometric validator and a smartcard reader connected to a validator application suffices this. In case of NFC a separate biometric validator is not needed as many smart phone manufacturers are now planning to incorporate it during the device production.

Layer 3 [Organizational Layer]

The roles of the organization in our model are many fold. It is responsible to talk to the cloud, build applications in it and make possible the interaction of its stakeholder with the cloud. We define two models: Intranet and internet model and describe how the organisation should connect its stakeholder and the cloud. The intranet model mainly applies for organization that has security as its main concern and all the transactions take place through its gateway. The organization is the only entity can interact with the cloud and the stakeholder but latter two cannot interact. But the internet model allows stakeholders to interact with the organization as well as the cloud facilitating scalability as well as portability.

Layer 2 [Organizational and Cloud Secure Interaction Layer]

This layer takes care to securely pass the encrypted private organizational data through a protected tunnel to the cloud. This layer is particularly vulnerable because of the nature of the data that it handles. Proper care should be taken in this regard.

Layer 1 [Cloud Layer]

The most important layer which allows organizations to store, process and manipulate its stakeholders data. All the heavy processing is taken care in this layer and organization builds rich cloud based scalable GUI applications to cater its own and its stakeholders needs. We shall also discuss about "URL-Appender" and "Cloud-Sync" - android applications developed by us to be operational in this layer.

¥ = T□ * N_{ds}

¥c = T□ * N_{ds} = T□

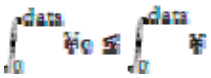
(N_{ds} equals (or nearly equals) one in cloud because of a centralized server)

¥c = Adaption time in cloud environment.

¥ = Adaptation time in traditional environment.

N_{ds} = Number of decentralized servers distributed throughout the organization.

T□ = The average time required to store or update a single record



This clearly shows that the adaptation time in cloud environment is less than those in non cloud environment.

NEAR FIELD COMMUNICATION (NFC)

NFC technology is a simple extension of ISO/IEC 14443 proximity card standard that combines the interface of a smartcard and a reader in to a single device. In simple words what interests us is that with the advent of NFC, one holds a complete identity suite in his/her control with smartcard, display and contactless reader terminal.

The NFC enabled smartcard thus can act as a contactless smartcard reader as well as a contactless smart card (the latter is achieved by means of emulation).

FUTURE OF NFC

According to a report from Juniper research almost one in five smartphones may have NFC functionality by 2014. NFC tags (passive cheap smart tags) are beginning to gain momentum and as of now the number of passive tags used in UK is more than 130,000.

Manufacturers of smart phones also plan to bring in embedded biometric systems for providing two factor authentication. Some advantages of NFC include low power consumption, does not require pairing , quick establishment of connection, compatibility with existing RFID systems, simplicity, etc..

CURRENT STATUS OF OUR RESEARCH AND FUTURE PROSPECTS:

We were able to model and develop a working model. Currently we have built applications that interacts with the smartcard and biometric devices and able to do a successful authentication. An GUI application (iCloud) is built for communicating with cloud through webservices (which were already defined by us).

With regard to NFC, an Android application "URL-Appender" has been built. The application reads from the passive NFC tag, appends the unique GUID, communicates with the Cloud services and presents the required data. Another application "iCloudSync" is being built.

As a next step we plan to concentrate more on building scalable applications on the cloud, emulating smartcards by using NFC enabled smartphones and using NFC at payment terminals.

CONCLUSION

In this paper we have proposed and built a cloud based internet platform to cater the organizational needs and describe how we can use a single biometric supported smart ID for almost all organizational purposes.

We also research using NFC in our model thus proposing a solution which is reliable and is practically feasible.

REFERENCES

[1] Security and Identity in the cloud (http://cloudidentityblog.com/tag/smart-card)/

[2] Near Field Communication and its usage. (http://identivenfc.com)

[3] Cloud Security Alliance

(https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf)

[4] Toward the trend of cloud computing, IEEE

(http://www.mendeley.com/research/toward-trend-cloud-computing/)

[5] Smartcards and biometrics

(http://www.smartcardalliance.org/pages/publications-smart-cards-and-biometrics)

[6] Smart Card Alliance Physical Access Council White Paper

(http://irisid.com/download/news/Smart_Cards_and_Biometrics_030111.pdf)

[7] Evolving smartcard and biometrics.

(http://net.educause.edu/ir/library/pdf/DEC0004.pdf)

[8] PC Magazine: Digital Persona U.are.U Delexe

(http://www.zdnet.com/pcmag/features/biometrics/387166.html)

[9] NFC and the future of the mobile industry

(http://android.appstorm.net/general/opinion/near-field-communication-and-the-future-of-mobile/)

[10] Ways to use NFC

(http://www.nearfieldcommunication.org/using-nfc.html)