UNIFIED HANDHELD WITH SPECIAL SECURITY FOR PERVASIVE COMPUTING

I Gusti Agung Gede Arya Kadyanan,

Ida Bagus Made Mahendra

Faculty of Computer Science

University of Indonesia

Abstract-Inspired by a *swiss knife army* with several other equipment that accompany such as pliers, screwdrivers, a corkscrew and many others. So as these devices are able to do everything. From this vision of the function of a handheld / smart-device which is growing rapidly and most people have today. How could a handheld perform all these functions? In this article will discuss about how to maximize handheld functions but still watched from the side of security. In short it's how to ensure that all devices can be connected but still within our control.

Keyword-pervasive computing, handheld, security, encryption, Rijndael, AES

I INTRODUCTION

Nowadays many people become familiar with handheld / smart-device. In addition to basic skills as a communication device, it also able to perform other functions such as electronic music player / video, cameras, radios, recording media, wireless, Bluetooth, Infra-Red, office, and many more other functions. But generally someone who has a handheld does not use its full potential. From many functions that only a few have been used such as for call, sms, and cameras. Some other functions will be very rarely used or even not used at all. Though these functions can support the daily productivity can be maximized.

II MORE PERVASIVE with HANDHELD

We choose handheld because not only most people already have this device, but also these devices meet the criteria for pervasive and ubiquitous computing. People will never feel that this device accompanied in all of our daily activities. Maybe this nature can be owned also by other devices such as a wrist watch, but a wrist watch is not realistic for the implementation of a highly varied functions. Besides visually limitations, wrist watch is too small, this also a consideration to choose another alternative. For example, when we type a short message / sms, maybe the size of a wrist watch that is too small will cause difficulties for users.

III UNIFIED USER IDENTIFICATION

With this unified User Identification can be used in a variety of access needs. Starting from the campus environment, insurance, bank, and many others function. Here we define a User Identification is a unique number and can represent a user at the same time as the identifier for identification purposes when accessing various resources such as files in a system of information. In this case, we can use this device as same as identity card like KTP (Kartu Tanda Penduduk), KTM (Kartu Tanda Mahasiswa) and the others kind of identity card. In this case we exploit the Device ID number and identity code as well then make a single identity device.

IV UNIFIED DATA TRANSFER WITH XML

As we know the data format is still a problem in the data transfer mechanism. Therefore, the mechanism in this article will use the XML format for various data to be transmitted. Here is the line serialization of documents into an XML form as shown in the picture bellow:

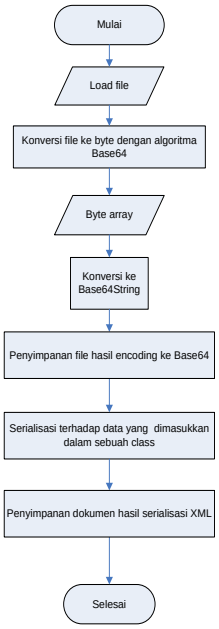

Fig.1 Flowchart of data serialization

V UNIFIED E-BAY

Certainly related to the Unified User Identification, Unified E-Bay can be used when online shopping. Here we can assume that the handheld using a Bluetooth connection can be used as identification when shopping online. When blue-tooth enable, it will be detected automatically by a reader which was at the computer and the transaction can be done immediately.

Fig. 2. Online shopping identification.

VI. UNIFIED SECURITY & PRIVACY

For an important data security, one solution is to use a particular program or data encryption protection. We have had many outstanding special programs for better data protection which freeware, shareware, and commercial on the market that are specifically intended for handheld devices. In general, these programs not only provide a single method, but some kind so that we can choose what we think is the most secure. However, to guarantee the security level higher then we should create their own encryption programs by combining the techniques and methods that already exist to be applied only on the handheld device. One of them is a combination of XML serialization and the device ID key using the Rijndael algorithm. So the main idea of the security system to strengthen the key here is to be used at the time of last encryption. The following is process flow of Rijndael encryption algorithm:

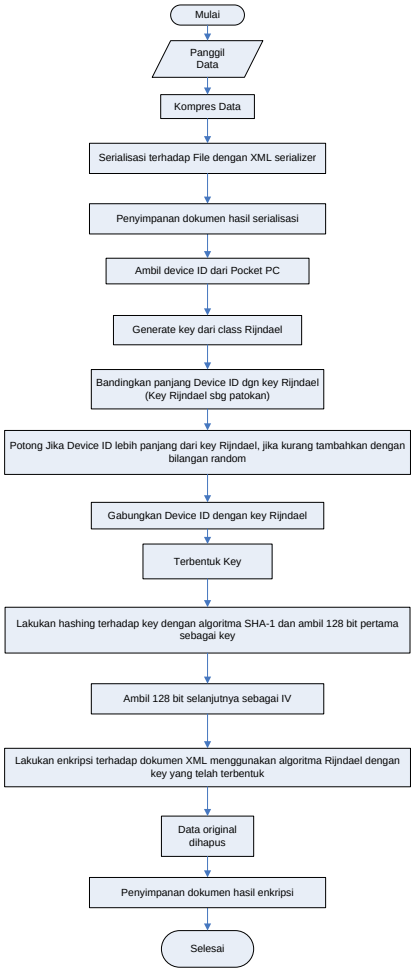

Fig. 3 Encryption flowchart with Rijndael algorithm

The following pseudo-code to retrieve ID Pocket PC devices:

1. Add the device ID with the class library "CoreDll.dll"
2. System.Security.Cryptography Namespace
3. Do take the Device ID

In this encryption will be done directly using the Rijndael class that has been provided by Visual Basic.NET. Rijndael class that is derived from the Cryptography namespace with the following structure:

System.Object

System.Security.Cryptography.SymmetricAlgorithm

System.Security.Cryptography.Rijndael

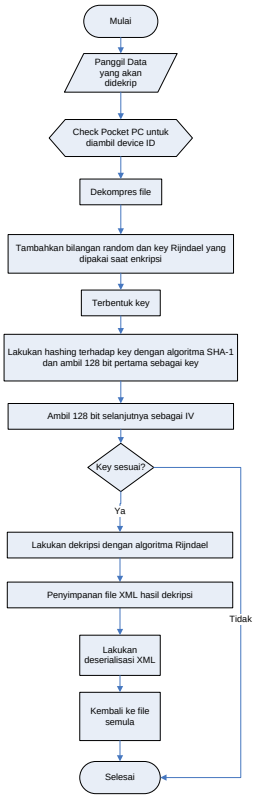

Fig. 5. Decryption flowchart with Rijndael algorithm

Fig. 6. Data encryption User Interface

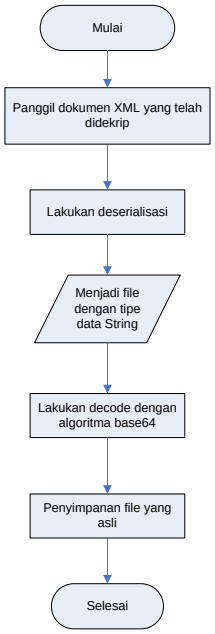

Fig. 4 Deserialization flowchart of XML document

VII APPLICATION ARCHITECTURE

In the following schema is a representation of whole architecture :

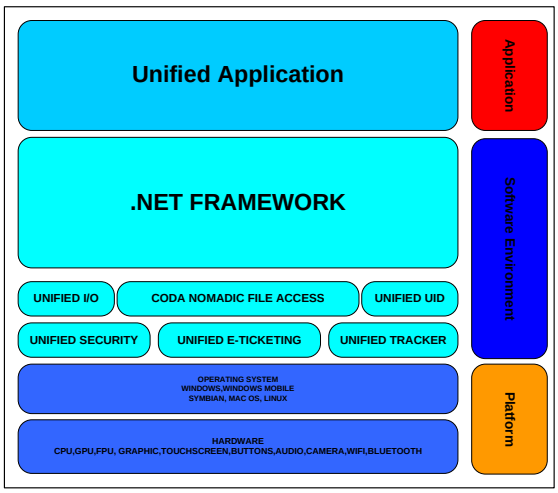

Fig. 7. Application architecture schema

In these architectures utilize. NET Framework for the various functions contained in this application. Including the security functions of Rijndael encryption algorithm. Here we do not necessarily use these functions, we also modified in advance to strengthen the existing mechanisms. For example in the security process, the key that is used has been strengthened to include device ID which is owned by the handheld, so the encryption becomes relatively stronger.

VIII. UNIFIED E-TICKETING

Electronic ticket (e-ticket) is a method of ticket purchase without requiring the printing of paper tickets as proof of payment. All ticket purchases data already entered in an online server system, facilitating the sale / purchase of tickets.

E-ticket system has many benefits or advantages include: transaction processing ticket reservations or payments faster and easier because it can be done via telephone or online websites. Minimize the possibility of missing tickets also stolen, and no longer need to bother with tickets for shows sufficient identity card and the ticket code.

IX. UNIFIED TRACKING

Unified Tracking is used as tools by adopting GPS navigation. Today many people have used GPS for navigation aids, by adding a map, it can be used to guide us, so we can know which path should be selected to achieve the desired objectives. For the user interface when done tracking process can be seen in the picture below:

Fig. 8 GUI of Unified Tracking

X. WIRELESS TECHNOLOGY 802.11AC

With this technology, wireless data transfer can be done through the air at speeds up to 1 Gbps (gigabits per second). This is an improvement 802.11ac the 802.11a standard which works at 5.0 GHz frequency band. The part is a wide channel added. If the standard is now used to use 20 MHz channels, the new standard uses 40 Mhz, 80 Mhz, 160 Mhz even. With a wider channel, even greater throughput so that users can enjoy faster data access. This technology will increase the device's ability in carrying out all functions of the existing connections.

XI. TRACK YOUR LOSE HANDHELD

To anticipate the worst case when the handheld is stolen, the system has been equipped with tracking systems to track the existence of such handheld. When the handheld is lost or stolen, they will likely replace sim card. Thus the system will notify this information to the owner via email and even short message services. In addition the system also can provide information about the approximate location of the handheld. At the same time owner can also perform remote formatting, which is a mechanism to perform remote data formats, so the security of data and system functions can be guaranteed. The image schema as follow:

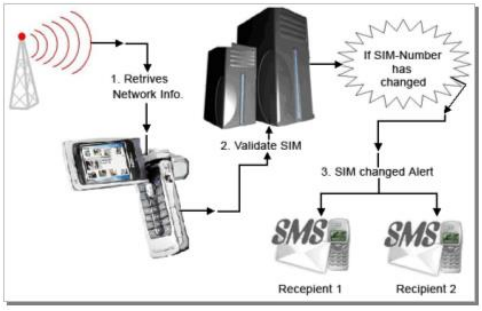

Fig. 9 Schema Lose Handheld

XII. REAL SCENARIOS

Agung is MIK student, as usual, he usually going to his campus in early morning, then he went straight to the lab GRID COMPUTING. To get into the lab he had to show KTM. But he realized that his wallet was left behind his house, where all identity cards, including KTM contained. Luckily he did not forget to bring his handheld which the already installed Unified Application. In addition to Unified Application has been installed, in the handheld has also been equipped with data complete personal identity. Staying close to your handheld is available in front of the tag lab door, it automatically opens the lab door.

Not only were many great things to do today but also need of cash as spending money in the cafeteria for lunch and bought some other purposes, of course, this has yet to be done online. Thus he was immediately rushed to the nearest ATM, when he got there with

the handheld he bring to the tags that are automatically detected by the ATM machine and be done withdrawals through ATM successfully.

Promptly at 3 that afternoon lecture was over but there is activity to do is attend a friend's birthday which is in Central Jakarta. He immediately looked toward the nearest station to buy a ticket and waited for the train, ticket payment must be use the Unified E-Ticketing.

XIII. FUTURE WORK

There a lot of development still needed to support the realization of this as a Unified Handheld infrastructure uniform standards, management software that can save power consumption become a challenges because many of the functions provided in this device.

XIV. CONCLUSION

Pervasive computing technology will be a future challenge. With so many experiment results in the last few years, would encourage us to be able to produce something more comprehensive in terms of implementation. For that if the exposure of the Unified Handheld in this article may represent a small part of what is aspired to the fore of a pervasive computing technology. Simplicity is the final destination of the proceeds even though the technology that we tend towards grappling with a very complicated thing. Last but hopefully the exposure in this paper may be less useful to readers in the hope that one day will emerge the idea and implementation better.

ACKNOWLEDGMENT

My particular thanks goes to Mr. Bob Hardian for guidance and information has been provided so far. What really has changed our paradigm about the computer network so far. It turns out many things that we did not know so far, and with the TD classes Jarkom makes us more aware of this science.

REFERENCES

[1] M. Weiser, "Some Computer Science Issues in Ubiquitous Computing," *Commun. ACM*, vol. 36, no. 7, July 1993.

[2] H. Balakrishnan, S. Seshan, and R. H. Katz, "Improving Reliable Transport and Handoff Performance in Cellular Wireless Networks," *ACM Wireless Networks*, vol. 1, no. 4, Dec. 1995.

[3] D. Brown, "Techniques for Privacy and Authentication in Personal Communication Systems," *IEEE Pers. Commun.*, pp. 6-10, Aug. 1995.

[4] E. Brewer *et al.*, "The Design of Wireless Portable Systems [InfoPad],"

Proc. Spring COMPCON '95, Mar. 1995.

[5] Joan Daemen, Vincent Rijmen, The Rijndael Block Cipher AES, AES Proposal, National Institute of Standard and technology, September 1999.