Privacy Preserving Service Discovery for Interoperability in “Power to the Edge” Approach

Research and Development Initiative, Chuo University

Hiroshi Yamaguchi, Masahito Gotaishi, Shigeo Tsujii, Norihisa Doi
“Power to the Edge” Approach for the non-Military Activity

- Masahito Gotaishi,
  - A member of the Japanese Translation team of “Power to the Edge”
  - Long for the application of “Power to the Edge” approach to Medicine and Care

- Hiroshi Yamaguchi
  - Once presented in ICCRTS (2009)
  - Application of PTE to control the performance of Orchestra
  - Best Paper of the Section
Problem to Solve

• Information is necessary in “Self-Synchronization” and “Shared Situation Awareness”
• Information is shared in the organization
• Typically information is shared with the partners
• These information are internal ones and often Confidential
Examples in the Real World

• e-Administration: Taxing, refund of high medical charge, allowance for female-headed household, etc.
  – Information is not widely shared within the public administration office
  – because it is “Personal Information”

• Medicine & Care: Making use of the chart data, result of the treatment, etc.
  – Strictly confidential
  – But medicine needs the data
Dilemma

• “Value” of the Information is realized ONLY WHEN it is used
• Usually solved by "Trade-Off."
• Is there a "Best of the Both World" solution?
Our Proposal (medicine & care)

• Clinical data computed while they are encrypted (secret sharing) -assuming cloud computing
• Protecting the search operation information, while enabling semantic search
• Anonymous Feedback
• Access Control using Cryptosystem
Privacy Preserving Data Processing (PPDP)

- Encrypted Medical Information DB (Personal Information)

  Privacy Preserving Data Processing
  - Functional Operation ($\Sigma, \Pi$ etc.), while encrypted
  - Data Processing (Statistics, Mining etc.)
  - Semantic Computing (Natural Language, etc.)

  Patients are able to confirm that their privacy are preserved.
  ‘Relieved!’

  Medical researchers are able to obtain processed data without decrypting the encrypted data

Proof of validity Protocol
PPDP is correctly Processed (i.e. Personal Information Is not revealed)?
Access Control using the next-generation Crypto

Medical Information Systems Infrastructure

Medical History, Search Activity, Questionnaires (Personal Information)

Anonymous Survey  Private-Info Protecting Search

Patients  Careworker  Care manager  Home doctor
Semantic Computing
- Natural Language Interface
  Structured Natural Language (SNL)
  Semantic Query Description Language (SQDL) Parser
  SQDL/SCDL Synthesizer
  Semantic Objects
  SCDL Parser

Private Information Retrieval including Content-based Multimedia Inf.
Access Control / Operation without Decryption

Raw Information
Physicians (access to ALL)

Encrypted Chart
- Name, date of birth
- Symptoms, test result

Decrypted data
Nurses
- Name of the patient
- Bill

Defining the level of confidentiality and access permission

Encrypted Information
- Name, Sex, Age
- Name of Disease
- Blood Type, Past Treatment
- Medical History
- Payment

Computing the statistics while protecting each data (while encrypted)

Tallying the Number:
# of patients of Flu, etc.

Tallying the Accounting Information

Correlation between data:
Effectiveness of the Medicine, etc.
Access Control Scheme by Next Generation Cryptographic Algorithm

Manager

Personal Inf.

Encryption

Encrypted Personal Inf. `A`

Encrypted Personal Inf. `B`

Encrypted Personal Inf. `C`

Decryption `A`

Decryption `B`

Decryption `C`

Doctor

Nurse

Accountant
New Cryptosystem

- Multivariate Public Key Cryptosystem (MPKC)
- One of Post-Quantum Cryptosystems
- New feature, with an identical **Public Key**, the range of the decryption defers depending on **Secret Keys**
## Difference between other Systems

<table>
<thead>
<tr>
<th></th>
<th>Our Cryptosystem</th>
<th>Conventional system</th>
</tr>
</thead>
<tbody>
<tr>
<td>situation</td>
<td>Access control of the members of organization, depending on the responsibility</td>
<td>Usually designed for Access Control of individuals</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Control the access depending on the properties of individuals</td>
</tr>
<tr>
<td>usage</td>
<td>Dynamically Changes depending on the change of organization, new roles, etc..</td>
<td>Generally Static</td>
</tr>
<tr>
<td></td>
<td></td>
<td>,,,, whether the person is US national, over 21, bought the content,,,</td>
</tr>
<tr>
<td>crypto-system</td>
<td>Multi-variate Public Key</td>
<td>ID-base, Pairing, elliptic-curve, ,,</td>
</tr>
</tbody>
</table>
Summary

• Confidential Information and detailed information of operation be protected
• Our proposal assumes medicine and care. But the system is applicable to any situation handling confidential information
• The system is fitted for the "Power to the Edge" organization
Thank you!

• Questions?