



How Safe is Your Data?

Kasun De Zoysa
Senior Lecturer

*Department of Communication and Media Technologies
University of Colombo School of Computing
University of Colombo
Sri Lanka*

Popular Myth?

Most computer and network users believe that their data and communications to remain private i.e. only visible and available to the author/sender and intended recipient.



Threats

Legal

- Company/employer access to data and 'personal' communications
- Local (and remote) logging of communication
- Info sent to online service providers, merchants or other users
- Web intelligence gathering

Illegal

- Eavesdropping/Interception
- Man-in-the-middle
- Keylogging



Image courtesy of: Tech Tips.com

Data Recovery

Your confidential data can be recovered after you delete it.

Be careful when you handover the devices for maintenances.

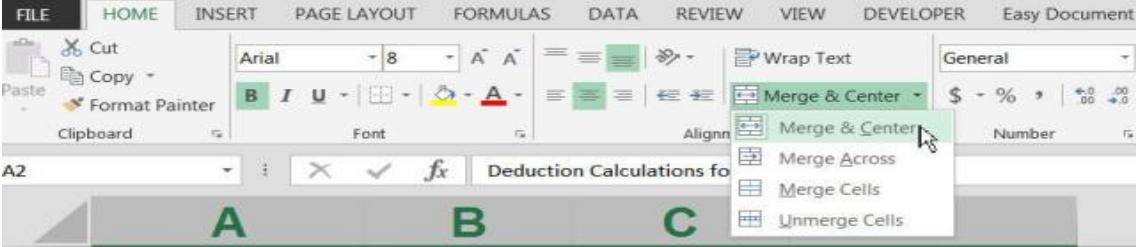
Lost your data?

**Data Recovery Tools
(foremost)**

**Memory
Extractor (LiME)**



Spreadsheets and Databases

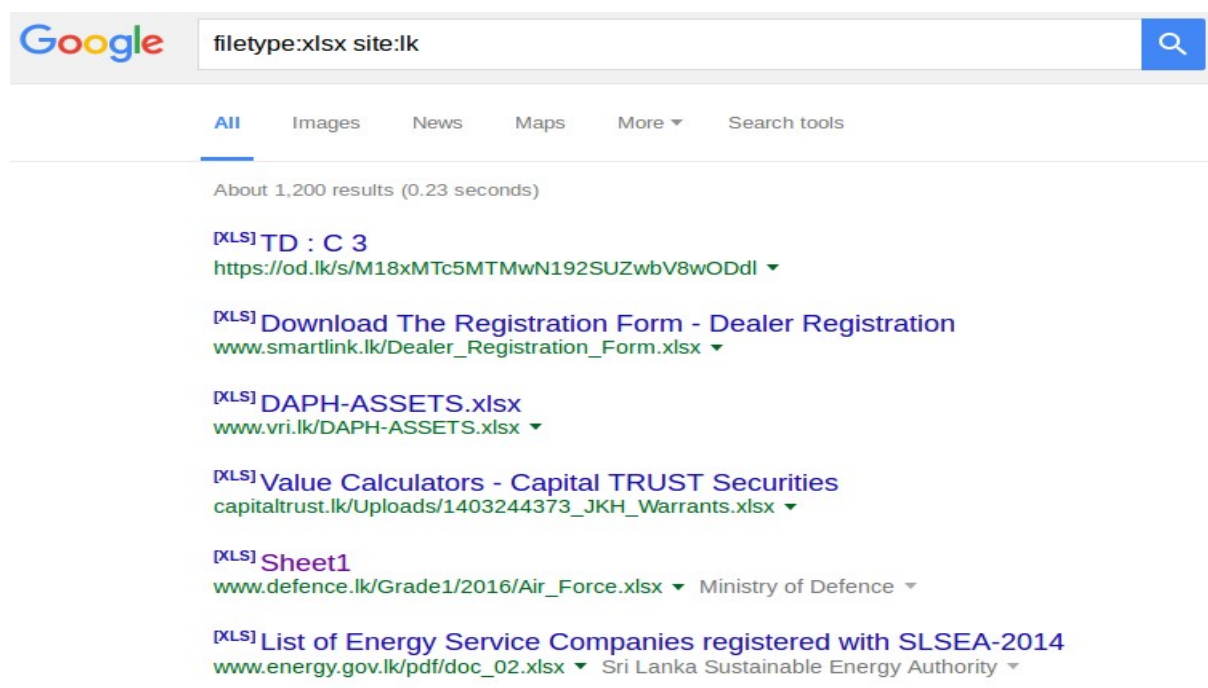


The screenshot shows the Microsoft Excel interface. The ribbon is set to 'HOME'. The 'Merge & Center' button is highlighted, and its dropdown menu is open, showing options: 'Merge & Center', 'Merge Across', 'Merge Cells', and 'Unmerge Cells'. The spreadsheet below has the following data:

	A	B	C	
1				
2	Deduction Calculations for Employees			
3		Date:	5/21/2016	
4		Deduction Rate:	12%	
5	Last Name	Salary	Deduction	Net Salary
6	Graham S.	\$85,789	\$10,295	\$1,235
7	Holt R.	\$83,211	\$9,985	\$1,198
8	Thompson A.	\$84,876	\$10,185	\$1,222
9	Wilson P.	\$81,245	\$9,749	\$1,170

- Data integrity
- Formulas can be changed
- Data can be changed
- How do you verify the integrity of your spreadsheet?

Search Engine



- Advanced search queries may reveal confidential data
- Google, Bing, Yahoo – all the major search engines track your search history

www.google.com/history

The screenshot displays the Google Web History page for a user named 'Kasun de zoysa'. The page features a navigation bar with various Google services and a search bar for 'Search Web History'. The main content area is divided into three sections: 'Hourly search activity', 'Daily search activity', and 'Web Activity'.

Hourly search activity: A bar chart showing search volume over a 24-hour period. The x-axis is labeled 'AM' and 'PM' with time intervals from 12 to 10. The y-axis represents search volume. The highest activity is observed between 8 PM and 10 PM.

Time	Search Activity
12 AM	Low
2 AM	Very Low
4 AM	Low
6 AM	Low
8 AM	Low
10 AM	Medium
12 PM	Medium
2 PM	Medium
4 PM	Low
6 PM	Low
8 PM	High
10 PM	High

Daily search activity: A bar chart showing search volume by day of the week. The x-axis is labeled 'Sun' through 'Sat'. The y-axis represents search volume. Sunday shows the highest activity, followed by Wednesday and Saturday.

Day	Search Activity
Sun	High
Mon	Medium
Tue	Medium
Wed	Medium
Thu	Medium
Fri	Low
Sat	Medium

Web Activity: A calendar for September 2012 showing search activity by date. The x-axis is labeled 'S' (Sun) through 'F' (Fri). The y-axis represents search volume. The highest activity is on September 18th and 19th.

Day	Search Activity
26	Low
27	Low
28	Low
29	Low
30	Low
1	Low
2	Low
3	Low
4	Low
5	Low
6	Low
7	Low
8	Low
9	Low
10	Low
11	Low
12	Low
13	Low
14	Low
15	Low
16	Low
17	Low
18	High
19	High
20	Low
21	Low
22	Low
23	Low
24	Low
25	Low
26	Low
27	Low
28	Low
29	Low
30	Low
1	Low
2	Low
3	Low
4	Low
5	Low

Web Activity Summary: Total Google searches: 60. The calendar also shows search activity for the first five days of the month (1-5, 6-10, 11-20, 21).

Navigation and Settings: The page includes a 'Web History' title, a lock icon indicating 'Only you can see your history', and a settings gear icon. A sidebar on the left lists various search categories: All History, Web, Images, News, Shopping, Ads, Videos, Maps, Blogs, Books, and Visual Search. A 'Remove items' button is visible at the bottom of the page.

Device Search

- Typical search engines crawl for data on web pages and then index it for searching
- Rather than to locate specific content on a particular search term, SHODAN is designed to help the user find specific nodes (desktops, servers, routers, switches, etc.) with specific content in their banners

Featured Categories



Top Voted

7,848

Webcam
best ip cam search I have found yet.

webcam surveillance cams

2010-03-15

2,842

Cams
admin admin

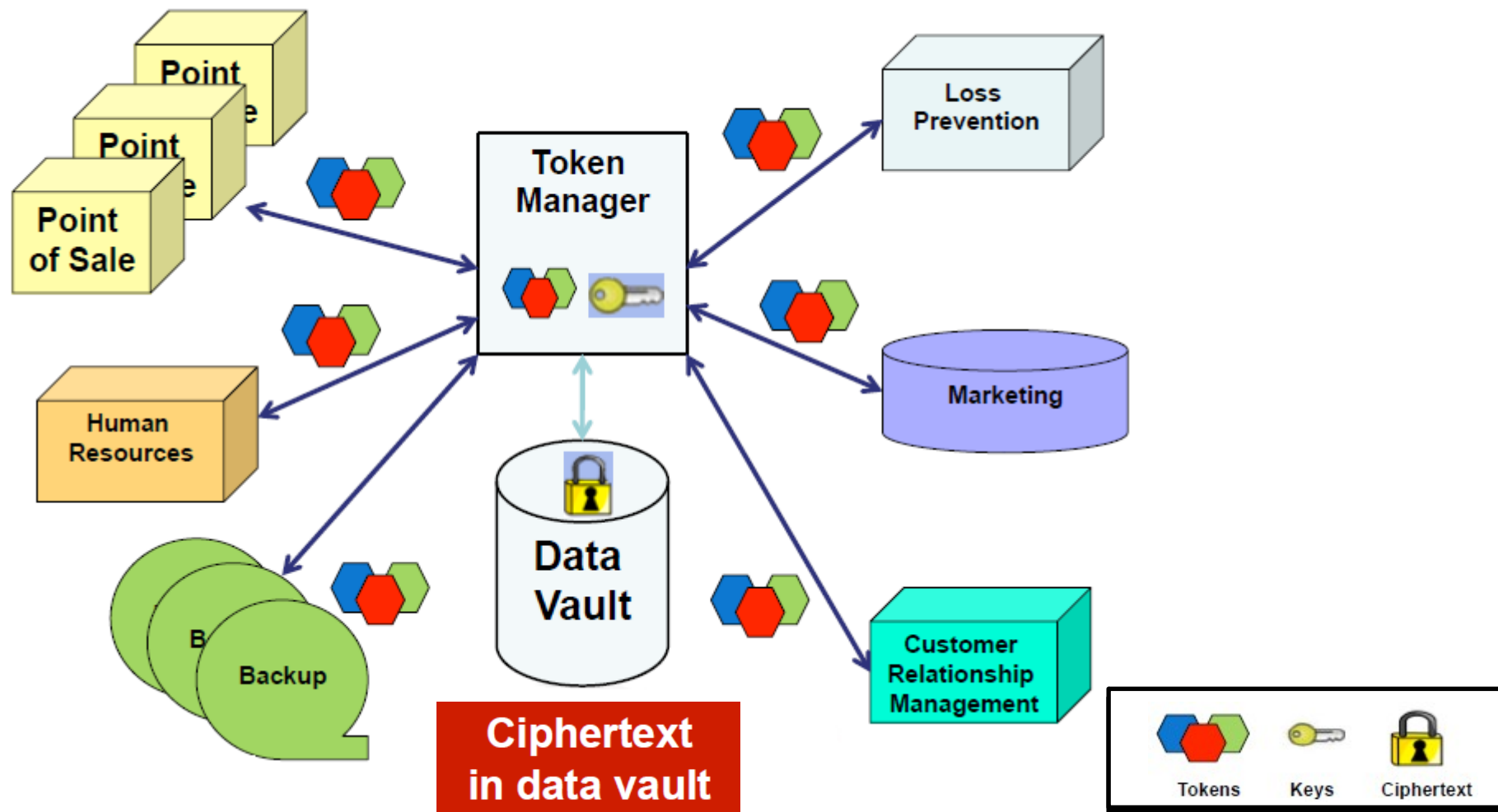
cam webcam

2012-02-06

Encryption Tools: Truecrypt, VeraCrypt

- Free open-source disk encryption software
- Creates a virtual encrypted disk within a file and mounts it as a real disk.
- Encrypts an entire partition or storage device such as USB flash drive or hard drive.
- Encryption is automatic, real-time (on-the-fly) and transparent.
- Parallelization and pipelining allow data to be read and written as fast as if the drive was not encrypted.
- Encryption can be hardware-accelerated on modern processors.
- Provides plausible deniability, in case an adversary forces you to reveal the password

Tokenization



Social Networks

- Current services (FB, GMail, GCal, Flickr, Pinterest) are “free” – users pay with their data, advertisement-based business model (“If you’re not paying, you’re the product”)
- Centralized data collection, privacy leaks
 - accidental
 - deliberate
- Information flow to third parties (companies, governments, the web-browsing public, hackers)
- Tracking
- Data Mining



Social Networks

- Once leaked, the data cannot be revoked
- Potential audience exceeds expectations, copying easy
- Not known who has what information
- Pieces of information that are harmless, taken together can be identifying or damaging



Cloud

- The ability of a user to control what information they reveal about themselves over the Cloud or to a cloud service provider (CSP)
- Also, the ability to control who can access that information
 - A CSP is a third party that maintains information about another entity
- Privacy and confidentiality concerns arise when individuals, businesses or organizations , a business, a government agency share information in the cloud, privacy or confidentiality issues will rise

Cloud

- Loss of control in the Cloud
 - Data, applications, and resources are located within CSP premises
 - The Cloud handles: IdM, user access control rules, security policies and enforcement
 - The user relies on the CSP to ensure
 - Data security and privacy
 - Resource availability,
 - Monitoring of services and resources

Cloud

- Lack of trust
 - Trusting a third party requires taking risks
 - Trust and risk are opposite sides of the same coin
 - Some monitoring or auditing capabilities would be required to increase the level of trust



Bitcasa for cloud storage

Bitcasa is a cloud storage system that encrypts your files before storing them on its servers. If its security should ever be compromised, you won't have to worry about someone finding sensitive files.



Homomorphic Encryption

Can we compute statistics on secrets?

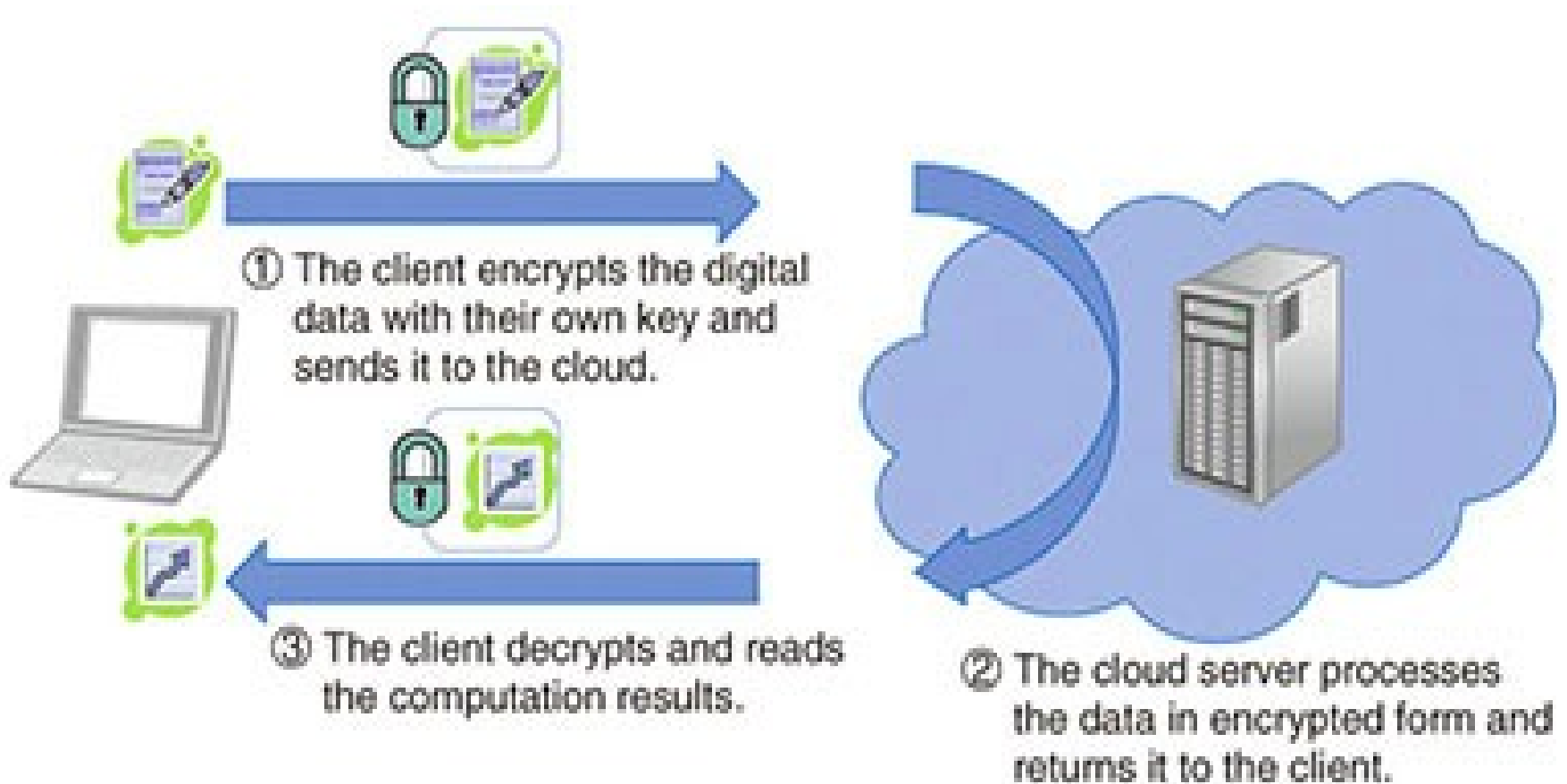
- You're in the 85th percentile for saving water today!
- Your house consumed 120% of its average energy today

Can we securely compute complex analytics?

Need new cryptographic computation models

- Support computations that IoT applications need

Homomorphic Encryption



Homomorphic Encryption

(Gentry, 2009)

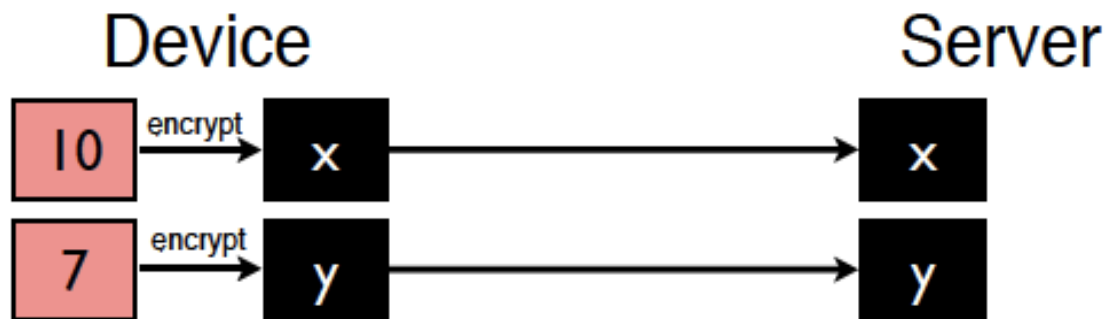
- Take a sensor value S , encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

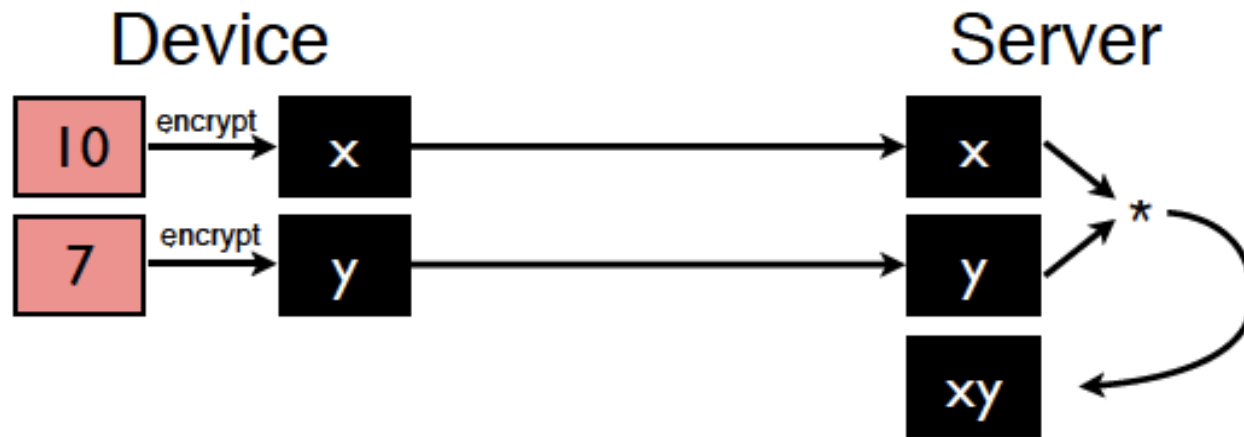
- Take a sensor value S , encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

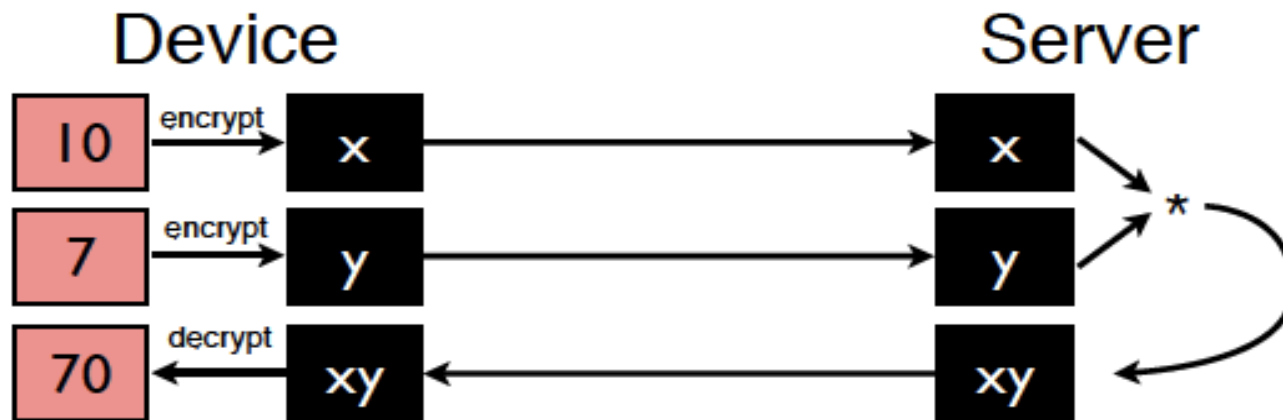
- Take a sensor value S , encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

- Take a sensor value S , encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



Homomorphic Encryption

(Gentry, 2009)

- Take a sensor value S , encrypt it to be S_e
- It is possible to perform arbitrary computations on S_e



- So confidential analytics possible, but not yet practical
 - Computations on S_e are 1,000,000 slower than computations on S
- But can be fast for *specific* computations (e.g., *)

Policies Required for:

- Backup files of databases
- Disposal of media previously used to hold confidential information
- Management of equipment sent for offsite maintenance
- Public agencies and organizations concerned with sensitive, critical or confidential information
- E-token electronic keys- Tokenization
- Storage records



Thank You

e-mail: kasun@ucsc.lk