IGE | IPI
ip-search

Factsheet: Digital, Data Security

A technology field created by ip-search

1 Definition

Data security in cyber space refers to data access security and data retention security. Data access security includes data confidentiality, data integrity and data privacy. Data retention security includes data storage, data backup, data recovery etc.

Data security employs protection measures at three levels, i.e. user/device level, application/service level and connectivity/network level.

Data security is also named as cyber security, computer security, IT security, information security, internet security, etc.

Advances in quantum computing risk unraveling data encryption with far-reaching implications for data security. Although the technology is not yet commercially deployed, quantum-safe solution already exist and ready for large-scale deployment.

2 Classification

2.1 Cooperative Patent Classification (CPC)

CPC/IPC/FI Symbols	Description
G	PHYSICS
G06	COMPUTING; CALCULATING; COUNTING
G06F	ELECTRIC DIGITAL DATA PROCESSING (computer systems based on specific computational models G06N)
G06F21/00	Security arrangements for protecting computers, components thereof, programs or data against unauthorised activity
G06F21/10	. Protecting distributed programs or content, e.g. vending or licensing of copyrighted material
G06F21/30	. Authentication, i.e. establishing the identity or authorisation of security principals
G06F21/50	. Monitoring users, programs or devices to maintain the integrity of platforms, e.g. of processors, firmware or operating systems
G06F21/60	. Protecting data
G06F21/70	. Protecting specific internal or peripheral components, in which the protection of a component leads to protection of the entire computer
G06F2221/00	Indexing scheme relating to security arrangements for protecting computers, components thereof, programs or data against unauthorised activity
G06N	COMPUTER SYSTEMS BASED ON SPECIFIC COMPUTATIONAL MODELS
G06N10/00	Quantum computers, i.e. computer systems based on quantum-mechanical phenomena
G06Q	DATA PROCESSING SYSTEMS OR METHODS, SPECIALLY ADAPTED FOR ADMINISTRATIVE, COMMERCIAL, FINANCIAL, MANAGERIAL, SUPERVISORY OR FORECASTING PURPOSES; SYSTEMS OR METHODS SPECIALLY ADAPTED FOR ADMINISTRATIVE, COMMERCIAL, FINANCIAL, MANAGERIAL, SUPERVISORY OR FORECASTING PURPOSES, NOT OTHERWISE PROVIDED FOR
G06Q20/00	Payment architectures, schemes or protocols (apparatus for performing or posting payment transactions G07F7/08, G07F19/00; electronic cash registers G07G1/12)

CPC/IPC/FI Symbols	Description
G06Q20/30	. characterised by the use of specific devices {or networks}
G06Q20/36	.. using electronic wallets or electronic money safes
G06Q20/367	... {involving electronic purses or money safes}
G06Q20/3674	.... {involving authentication}
G06Q20/38	. Payment protocols; Details thereof
G06Q20/382	.. {insuring higher security of transaction}
G06Q20/40	.. Authorisation, e.g. identification of payer or payee, verification of customer or shop credentials; Review and approval of payers, e.g. check credit lines or negative lists
G06Q2220/00	Business processing using cryptography (postage metering system using cryptography G06Q2250/05)
H	ELECTRICITY
H04	ELECTRIC COMMUNICATION TECHNIQUE
H04L	TRANSMISSION OF DIGITAL INFORMATION, e.g. TELEGRAPHIC COMMUNICATION ({coding or ciphering apparatus for cryptographic or other purposes involving the need for secrecy G09C;} arrangements common to telegraphic and telephonic communication H04M)
H04L9/00	{Cryptographic mechanisms or cryptographic} arrangements for secret or secure communication {(network architectures or network communication protocols for network security H04L63/00 or for wireless network security H04W12/00; security arrangements for protecting computers or computer systems against unauthorized activity G06F21/00)}
H04L9/002	. {Countermeasures against attacks on cryptographic mechanisms (network architectures or network communication protocols for protection against malicious traffic H04L63/1441)}
H04L9/006	. {involving public key infrastructure [PKI] trust models (network architecture or network communication protocol for supporting authentication of entities using certificates in a packet data network H04L63/0823)}
H04L9/008	. {involving homomorphic encryption}
H04L9/06	. the encryption apparatus using shift registers or memories for block-wise {or stream} coding, e.g. DES systems {or RC4; Hash functions; Pseudorandom sequence generators}
H04L9/08	. Key distribution {or management, e.g. generation, sharing or updating, of cryptographic keys or passwords (network architectures or network communication protocols for supporting key management in a packet data network H04L63/06)}
H04L9/14	. using a plurality of keys or algorithms {(network architectures or network communication protocols wherein the sending and receiving network entities apply hybrid encryption, i.e. combination of symmetric and asymmetric encryption H04L63/045)}
H04L9/30	. Public key, i.e. encryption algorithm being computationally infeasible to invert or user's encryption keys not requiring secrecy
H04L9/32	. including means for verifying the identity or authority of a user of the system {or for message authentication, e.g. authorization, entity authentication, data integrity or data verification, non-repudiation, key authentication or verification of credentials} ({network architectures or network communication protocols for supporting entities authentication in a packet data network H04L63/08; applying verification of the received information H04L63/12;} computer systems G06F; coin-freed or like apparatus with coded identity card or credit card G07F7/08)
H04L12/00	Data switching networks (interconnection of, or transfer of information or other signals between, memories, input/output devices or central processing units G06F13/00)
H04L12/54	. Store-and-forward switching systems (packet switching systems H04L12/56)
H04L12/56	.. {Packet switching systems}
H04L12/5601	... {Transfer mode dependent, e.g. ATM}
H04L2012/5687	.... {Security aspects}
H04L12/64	. Hybrid switching systems
H04L12/6418	.. {Hybrid transport}
H04L2012/6445	... {Admission control}
H04L63/00	{Network architectures or network communication protocols for network security (cryptographic mechanisms or cryptographic arrangements for secret or secure

CPC/IPC/FI Symbols	Description
	communication H04L9/00; network architectures or network communication protocols for wireless network security H04W12/00; security arrangements for protecting computers or computer systems against unauthorised activity G06F21/00)}
H04L63/02	. {for separating internal from external traffic, e.g. firewalls}
H04L63/04	. {for providing a confidential data exchange among entities communicating through data packet networks}
H04L63/06	. {for supporting key management in a packet data network (cryptographic mechanisms or cryptographic arrangements for key management H04L9/08)}
H04L63/08	. {for supporting authentication of entities communicating through a packet data network (cryptographic mechanisms or cryptographic arrangements for entity authentication H04L9/32)}
H04L63/10	. {for controlling access to network resources (restricting network management access H04L41/28)}
H04L63/14	. {for detecting or protecting against malicious traffic}
H04L63/16	. {Implementing security features at a particular protocol layer}
H04L63/18	. {using different networks or paths for security, e.g. using out of band channels (cryptographic mechanisms or cryptographic arrangements for key distribution involving distinctive intermediate devices or communication paths H04L9/0827; cryptographic mechanisms or cryptographic arrangements for authentication using a plurality of channels H04L9/3215)}
H04L63/20	. {for managing network security; network security policies in general (filtering policies H04L63/0227)}
H04L63/30	. {for supporting lawful interception, monitoring or retaining of communications or communication related information (circuit switched telephony call monitoring H04M3/2281)}
H04L2209/00	Additional information or applications relating to cryptographic mechanisms or cryptographic arrangements for secret or secure communication H04L9/00
H04L2209/56	. Financial cryptography, e.g. electronic payment or e-cash
H04L2209/60	. Digital content management, e.g. content distribution
H04L2209/64	. Self-signed certificates
H04L2209/68	. Special signature format, e.g. XML format
H04L2209/72	. Signcrypting, i.e. digital signing and encrypting simultaneously
H04L2209/76	. Proxy, i.e. using intermediary entity to perform cryptographic operations (network architectures or network communication protocols using hop-by-hop encryption H04L63/0464)
H04L2209/80	. Wireless (network architectures or network communication protocols for wireless network security H04W12/00)
H04W	WIRELESS COMMUNICATION NETWORKS (broadcast communication H04H; communication systems using wireless links for non-selective communication, e.g. wireless extensions H04M1/72)
H04W12/00	Security arrangements; Authentication; Protecting privacy or anonymity
H04W12/009	. {specially adapted for networks, e.g. wireless sensor networks, ad-hoc networks, RFID networks or cloud networks}
H04W12/02	. Protecting privacy or anonymity, e.g. protecting personally identifiable information [PII]
H04W12/06	. Authentication
H04W12/08	. Access security
H04W12/10	. Integrity
H04W12/12	. Detection or prevention of fraud

The complete description of the CPC classes with IPC- and FI-concordances can be found in the Internet at https://www.wipo.int/classifications/ipc/ipcpub/?notion=scheme&fipcpc=yes.

2.2 International Patent Classification (IPC)

IPC Symbols	Description
G	PHYSICS
G06	COMPUTING; CALCULATING OR COUNTING
G06F	ELECTRIC DIGITAL DATA PROCESSING (computer systems based on specific computational models G06N)
G06F21/00	Security arrangements for protecting computers, components thereof, programs or data against unauthorised activity [2006.01,2013.01]
G06F21/10	.Protecting distributed programs or content, e.g. vending or licensing of copyrighted material (protection in video systems or pay television H04N7/16) [2013.01]
G06F21/30	.Authentication, i.e. establishing the identity or authorisation of security principals [2013.01]
G06F21/50	.Monitoring users, programs or devices to maintain the integrity of platforms, e.g. of processors, firmware or operating systems [2013.01]
G06F21/60	.Protecting data [2013.01]
G06F21/70	.Protecting specific internal or peripheral components, in which the protection of a component leads to protection of the entire computer [2013.01]
G06N	COMPUTER SYSTEMS BASED ON SPECIFIC COMPUTATIONAL MODELS [7]
G06N10/00	Quantum computers, i.e. computer systems based on quantum-mechanical phenomena [2019.01]
G06Q	DATA PROCESSING SYSTEMS OR METHODS, SPECIALLY ADAPTED FOR ADMINISTRATIVE, COMMERCIAL, FINANCIAL, MANAGERIAL, SUPERVISORY OR FORECASTING PURPOSES; SYSTEMS OR METHODS SPECIALLY ADAPTED FOR ADMINISTRATIVE, COMMERCIAL, FINANCIAL, MANAGERIAL, SUPERVISORY OR FORECASTING PURPOSES, NOT OTHERWISE PROVIDED FOR [2006.01]
G06Q20/00	Payment architectures, schemes or protocols (apparatus for performing or posting payment transactions G07F7/08, G07F19/00; electronic cash registers G07G1/12) [2006.01,2012.01]
G06Q20/30	.characterised by the use of specific devices [2012.01]
G06Q20/36	..using electronic wallets or electronic money safes [2012.01]
G06Q20/38	.Payment protocols; Details thereof [2012.01]
G06Q20/40	..Authorisation, e.g. identification of payer or payee, verification of customer or shop credentials; Review and approval of payers, e.g. check of credit lines or negative lists [2012.01]
H	ELECTRICITY
H04	ELECTRIC COMMUNICATION TECHNIQUE
H04L	TRANSMISSION OF DIGITAL INFORMATION, e.g. TELEGRAPHIC COMMUNICATION (arrangements common to telegraphic and telephonic communication H04M) [4]
H04L9/00	Arrangements for secret or secure communication [1,2006.01]
H04L9/06	.the encryption apparatus using shift registers or memories for blockwise coding, e.g. D.E.S. systems [5,2006.01]
H04L9/08	.Key distribution [5,2006.01]
H04L9/14	.using a plurality of keys or algorithms [5,2006.01]
H04L9/28	.using particular encryption algorithm [5,2006.01]
H04L9/30	..Public key, i.e. encryption algorithm being computationally infeasible to invert and users' encryption keys not requiring secrecy [5,2006.01]
H04L9/32	.including means for verifying the identity or authority of a user of the system [5,2006.01]
H04W	WIRELESS COMMUNICATION NETWORKS (broadcast communication H04H; communication systems using wireless links for non-selective communication, e.g. wireless extensions H04M1/72) [2009.01]
H04W12/00	Security arrangements; Authentication; Protecting privacy or anonymity [2009.01,2021.01]
H04W12/02	.Protecting privacy or anonymity, e.g. protecting personally identifiable information [PII] [2009.01]
H04W12/06	.Authentication [2009.01,2021.01]

IPC Symbols	Description
H04W12/08	.Access security [2009.01,2021.01]
H04W12/10	.Integrity [2009.01,2021.01]
H04W12/12	.Detection or prevention of fraud [2009.01,2021.01]

The complete description of the IPC classes can be found in the Internet at https://www.wipo.int/classifications/ipc/ipcpub.

2.3 Japanese F-Terms Classification

FTCLA Symbols	Description
5B017	STORAGE DEVICE SECURITY
5B025	Electrically-alterable read-only memory (EAROM)
5B025/AE00	FUNCTIONS
5B025/AE10	. Security
5B050	PROCESSING OR CREATING IMAGES
5B050/GA00	OTHER (*)
5B050/GA06	. Characteristic techniques or functions *
5B050/GA07	.. Security; Protecting data from being destroyed
5B062	Microcomputers
5B062/AA00	PURPOSE AND EFFECTS
5B062/AA07	. Protection of security
5B076	Stored program control
5B084	INFORMATION TRANSFER BETWEEN COMPUTERS
5B084/BB00	PROBLEM OR PURPOSE
5B084/BB16	. Improving security
5B084/FA00	PEER-TO-PEER COMMUNICATION SYSTEM
5B084/FA41	. Security
5B085	On-line systems
5B089	Computer and data communications
5B089/KA00	PURPOSE
5B089/KA17	. Prevention of fraudulent activities or security
5B089/KB00	OBJECTS OF PROCESSING OR MANAGEMENT
5B089/KB13	. Access authority or security
5B125	READ-ONLY MEMORY
5B125/CA00	PURPOSE OR EFFECT
5B125/CA22	. Preservation of secrecy security or copy protection
5B185	ONLINE SYSTEMS
5B276	SECURITY IN STORED PROGRAMMES
5B285	SECURITIES OF ONLINE SYSTEMS
5J104	Ciphering device, decoding device and privacy communication
5J104/AA00	PURPOSE OR EFFECT
5J104/AA01	. Secret communication or privacy communication
5J104/AA12	. Detection or prevention of unauthorised use of data
5J104/AA17	. Secret computation
5J104/KA00	ENTITY AUTHENTICATION
5J104/KA05	. Authentication by asymmetric cipher systems
5J104/KA14	. Authentication by unmodifiable unique information
5J104/KA20	.. using location information of entities
5K023	TELEPHONE SET STRUCTURE
5K023/AA00	Applications
5K023/AA12	. Security telephones
5K030	Data exchanges in wide-area networks

FTCLA Symbols	Description
5K030/GA00	PURPOSES OR EFFECTS (A FREE WORD IS ASSIGNED TO THE SUBJECT MATTER CLASSIFIED IN VIEWPOINT 00)
5K030/GA11	. Improvement in reliability or improvement in maintenance or managing
5K030/GA15	.. Security confidentiality protection encryption or authentication
5K039	Automatic arrangements for answering calls
5K039/AA00	PURPOSE AND EFFECTS
5K039/AA02	. Improved reliability
5K039/AA05	.. Security measures
5K127	TELEPHONE FUNCTION

The complete description of the F-Terms can be found in the Internet at https://www.j-platpat.inpit.go.jp/p1101.

3 Keywords

In addition to the classification, the following keyword concepts were used:

Quantum computing: quantum crypto, quantum safe algorithms, quantum key distribution, etc.

4 Confidence Interval for Precision

Precision is expressed in percent of relevant counts. The 95 % confidence interval for the precision of a technology field is assessed on a mix of 100 randomly selected patent families based on a binomial distribution.

Precision Confidence Interval: 79 – 92 %

5 Contact

For specific information regarding the technology field, please contact info@ip-search.swiss

6 History

Version	latest update	Comment
_06_19	20.06.2019	no change
_11_19	29.11.2019	no change
_03_20	09.03.2020	Added quantum computing for cybersecurity
_09_20	20.08.2020	no changes
_03_21	10.03.2021	Precision confidence interval updated
09 21	13.08.2021	Classification and precision confidence interval update