and debugging, and the ability to leverage online Web services for additional storage, communication, and processing. We believe the ability to quickly prototype, test, and deploy devices will be a key element in accelerating our understanding of the challenges and benefits of networked things.

Give a summary of Text B.

UNIT 2

Text A. Privacy and the Quantum Internet

From Scientific American,
October 2009, pp. 80–84

"Courtesy of some of the weirdest laws of physics,
we may someday be able to search and surf the Web
without anyone collecting our data" (Seth Lloyd)

Privacy is hard to come by these days, particularly on the Internet, where every time you Google something your desires are recorded for posterity — or at any rate, for advertisers.

The laws of physics, however, could come to the rescue. Communication over special "quantum channels" already enables banks and other institutions to send data with virtually unbreakable encryption. Thus, the technology already exists to hide your searches from eavesdroppers who might intercept your queries. But in the future a new "quantum" version of the Internet may enable you to send queries and receive answers with the assurance that no one — not even Google — knows what questions you have asked.

Moreover, the same technologies that will guarantee private searching could also guarantee privacy during the entire online experience. Of course, search engines save and analyze users' data so that they can display targeted ads. That is how they cover their expenses and make a profit. If they decide to keep the users' data private, the search engines will need a new business model. And users may have to decide if they are willing to pay for searching or if they would rather do it free and give their searches away.

Nonclassical Listeners. The ability of quantum physics to supply complete privacy stems from a simple fact: systems in the quantum realm (which includes anything from elementary particles to molecules) can exist in multiple states. At any particular time, an atom can be in several different places; a particle of light, or photon, can be polarized both vertically and horizontally; an electron's magnetic moment can point up and down, and so on. As a consequence, whereas classical (as opposed to quantum) data bits register either the value 0 or the value 1, quantum bits can register 0 and 1 at the same time. Also, whenever a quantum bit takes on the values 0 and 1 simultaneously, you cannot make an exact copy of that quantum bit, and any attempt to do so will change the state of the bit. This rule, known as the no-cloning theorem, also applies to strings of quantum bits, which, for example, can represent words or sentences. As a consequence, someone eavesdropping on a quantum channel — typically an optical fiber carrying photons in multiple polarization states — will not be able to "listen" to the communication without disturbing it, thus revealing the intrusion.

Several different quantum encryption techniques exist to exchange data in complete privacy thanks to no cloning. Yet such techniques presume that the addressees be allowed to read the data you sent them: merely sending Google an encrypted search query would not help.

The search engine searches its database for the answers to your multiple questions and combines questions and answers into a new quantum package, which it sends back to you. If the search engine makes a copy of the questions for its records, you will be able to tell that your privacy was violated because the quantum state of your original questions will be perturbed in a way that your computer can detect. Crucially, the search engine can provide answers without physically detecting (let alone cloning) the string of bits that encodes the questions and thus without knowing what the questions were.

Although such magic is impossible with current computers, databases and networking hardware, we realized that it is not technologically out of reach. The first requirement for quantum private queries is a rudimentary quantum Internet. The technology to exchange quantum messages along a dedicated line already exists and is in use for secure communication. A full-fedged quantum Internet, however, will have to be not just a line between two points but a network whose nodes route data packets so that any user can reach any other user or any Web server. It turns out that routing data without making temporary copies of them—and thus without suffering the consequences of the no-cloning theorem—is a nontrivial task and requires a sophisticated technology now at the experimental stage, called a quantum router. A prototype of such a network may become available within five to 10 years.

The second requirement for private Web searching is that users and data servers possess rudimentary quantum computers, meaning computers that are able to store and handle quantum bits. Unfortunately, quantum bits are notoriously fickle and tend to spontaneously lose their multiple quantum states within a fraction of a second. Experimental quantum computers that store quantum bits in the magnetic states of single ions suspended in a vacuum, for example, can store only eight bits or so at a time so far. A full-fledged quantum computer would require hundreds if not thousands of quantum bits and is probably many decades away, even as a laboratory demonstration. Fortunately, though, for the purpose of quantum private searches, only 30 quantum bits or so will be sufficient: if properly coded, a 30-bit query can pull an answer out of a database with more than a billion entries. Such 30-bit "quantum microprocessors" might also become available in five to 10 years.

Not So Random. To answer a user's multipronged quantum question, a search engine's database must be able to supply the answer to each component of the question simultaneously. Doing so will require a new type of data storage called quantum random — access memory, or quantum RAM.

RAM is just a device for storing data, arranged in a treelike structure. Each piece of data is a sequence of eight bits, or a byte, and has an address that is itself a sequence of bits. Bytes are like the leaves on the tree; the address controls the route from the trunk to the particular leaf. The first bit of the address specifes which of two branches to take at the lowest level of the tree, the second bit controls the second-level branching, and so on. The branches double at each level, and in a traditional RAM with 30-bit addresses, retrieving data requires throwing 230 (more than one billion) switches.

One could design a quantum version of traditional RAM. The only difference is that the switches that route information through the binary tree must now be capable of routing information through two different

branches simultaneously, because each bit of a quantum question can specify two different routes. Such quantum switches can be built using existing technology, such as semitransparent mirrors that "split" photons making them follow two different paths at once. The problem is that quantum circuits are exquisitely sensitive to noise and errors: if just one of the switches is messed up, the privacy of the corresponding bit is lost. Because a typical address bit controls a huge number of switches, the chances of losing privacy are very high.

Give a summary of Text A.

Text B. Enforcing Security Mechanisms in the IP-Based Internet of Things

The Internet of Things (IoT) is an emerging concept that refers to billions of interconnected (non-human) information sources, also denoted as "smart objects", typically equipped with sensors or actuators, a tiny microprocessor, a communication interface, and a power source. Existing deployed smart objects typically use proprietary technologies, tailored to one specific application, which results in poor, if any, interoperability and thus limited diffusion on a large scale. Building interconnected and interoperable smart objects requires the adoption of standard communication protocols.

International organizations, such as the Internet Engineering Task Force (IETF) and the IPSO Alliance, promote the use of the Internet Protocol (IP) as the standard for interoperability for smart objects. As billions of smart objects are expected to come to life and IPv4 addresses have eventually reached depletion, IPv6 has been identified as a candidate for smart-object communication. The protocol stack that smart objects will implement will try to match classical Internet hosts in order to make it feasible to create the so-called Extended Internet, that is, the aggregation of the Internet with the IoT. Security in the IoT scenarios is a crucial aspect that applies at different levels, ranging from technological issues to more philosophical ones, such as privacy and trust, especially in scenarios like Smart Toys.

The security challenges derive from the very nature of smart objects and the use of standard protocols. The security challenges and require-