GPCET

Pioneering Innovative Education

Tech Spark

G PULLAIAH COLLEGE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

TECHSpark
2018-2019

VISION

To deliver the qualitative, innovative and ethical computer science technocrats who strive for the benefit of society

MISSION

Nurturing the future leaders in academia, information technology, industry and entrepreneurial pursuit, through a contemporary curriculum of theory and application that develops the ability to solve problems individually and in teams.

Program Educational Objectives (PEO's):
A graduate of the Computer Science and Engineering Program should:

PEO 1 :Apply principles of Computer science and engineering with analytical thinking and problem solving skills for developing software systems.

PEO 2 :Adapt to rapidly changing industry needs by acquiring required technical skills .

PEO 3:Assess real time problems and develop suitable technological solutions to full fill the needs of society.

PEO 4: Develop leadership skills and engage in life-long learning to meet the changing global needs.

Program Specific Outcomes (PSO's):
Upon completion of the program, student will be able to

PSO 1 : Design, Develop, Test and maintain software systems for business applications.
PSO 2 : Evaluate and tune software systems for better performance.

TECHSpark

2018-2019

Patrons
Mr. GVM Mohan Kumar
Chairman

Advisory Committee
Dr C Srinivasa Rao
Principal

Editors
Dr S Prem Kumar
Dean / HOD CSE

Coordinators
Mr P Suman Prakash
Associate Professor / CSE

Mr N Parasuram
Assistant Professor / CSE

Tech Vedha is an annual magazine, brought out by G Pullaiah college Of Engineering & Technology Department of CSE, Kurnool. If you have any queries or feedback, address them to info@gpcet.ac.in

EDITORS' NOTE

Dear readers

It gives us great pleasure to bring you the first issue of Tech Vedha, the college magazine of GPCET. The name and fame of an institute depends on the caliber and achievements of the students and teachers. The role of a teacher is to be a facilitator in nurturing the skills and talents of students.

This magazine is a platform to exhibit the literary skills and innovative ideas of teachers and students. Tech Vedha presents the achievements of students and contributions of teachers.

We would like to place on record our gratitude and heartfelt thanks to all those who have contributed to make this effort a success. We profusely thank the management for giving support and encouragement and a free hand in this endeavor. Last but not the least we are thankful to all the authors who have sent their articles. We truly hope that the pages that follow will make an interesting read.

Dr S Prem Kumar
Professor / HOD / CSE

ABOUT COLLEGE

College

G Pullaiah College Of Engineering & Technology, Kurnool has come a long way since its modest beginning in 2007. The 13 acre lush campus with a state of the art built up area of over 5 lakh sq.ft., welcomes about 1000 students every year, in various branches including ECE, CSE, EEE, Civil, Mech and PG courses M.Tech (CSE), M.Tech (ECE), M.Tech(EEE), MBA.

Situated in a picturesque location at Nandikotkur, Kurnool, GPCET offers a great ambience for wholesome development of students. The college is emerging as one of the top notch engineering colleges, affiliated to JNTU. The ISO 9001:2008 Certification and Accreditation by AICTE further substantiate the high standards of excellence that the institution has set for itself. With an ever growing enthusiasm for education and research, GPCET is committed to excellence in education. It has stringent recruitment policies, high standards for academic performance, outstanding infrastructure and proactive placement initiatives.

The students are well trained in their academic curriculum and also in skills that are required for the industry. They are given customized and employability training both in technical as well as in communication skills. A unique feature of GPCET is the Business English Certification (BEC) Club. Considering the importance of communication skills for the career growth of students, GPCET has initiated BEC course for all students. Students undergo BEC (preliminary) examination and get BEC certification of Cambridge University.

Our students do industry oriented mini-projects in their pre-final semester and gain experience and exposure on industry practices and challenges. For more details visit: www.gpcet.ac.in

ABOUT FOUNDER

Founder

I appreciate your evincing zeal in our college. I feel elated to inform that GPCET is one of the emerging giants in Technical Colleges in the region. The college has all ingredients a Technocrat should possess GPCET is committed to serve the needs of industry and corporate sectors. We offer undergraduate programmes in B.Tech (ECE/CSE/EEE/CIVIL/ME), and post graduate programmes in MBA, MCA and M.Tech all recognized by JNTUA. Besides the technical skills, a student is imparted soft skills.

The four storied campuses are enabled with Wi-Fi and e-classrooms which are the platform for learning. Interactive lecture sessions, weekend seminars, Technical forums mould an ordinary student into on extraordinary personality. The invincible strength of GPCET is its erudite and dedicated faculty. I believe, as a leader, that such a blend of academicians is just a differentiating factor of our college. The student centric and conceptual base of teaching will no doubt be a fortifying factor. This alone enables them to face any challenge in life. The GPCET assiduously keep faith in promoting humanistic approach to our students.

Ambient intelligence

Ayesha Shariff, Asst Prof, GPCET, Kurnool

Ambient Intelligence (AmI) is a new paradigm in Information Technology that has potential for great impact in the future. The vision of AmI is that the people will be surrounded by intelligent objects that can sense the context and respond according to the desire of the people. AmI is a multidisciplinary topic, since it combines the features of many of the areas in Computer Science. Ambient Intelligence (AmI) is growing fast as a multi-disciplinary topic of interest which can allow many areas of research to have a significant beneficial influence into our society. The basic idea behind AmI is that by enriching an environment with technology (mainly sensors and devices interconnected through a network), a system can be built to take decisions to benefit the users of that environment based on real-time information gathered and historical data accumulated.

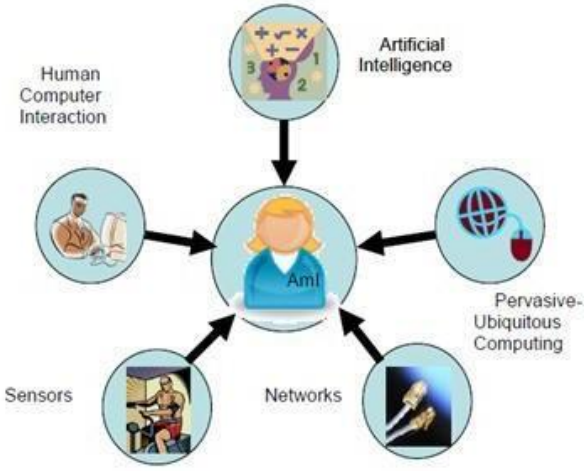


Fig: Relation in between AmI and other areas in Computing Science

Networks, Sensors, Human Computer Interfaces (HCI), Pervasive Ubiquitous Computing and Artificial Intelligence (AI) are all relevant and interrelated but none of them conceptually covers the full scope of AmI. Ambient Intelligence puts together all these resources to provide flexible and intelligent services to users acting in their environments.

Ambient Intelligence builds on three recent key technologies:

1. Ubiquitous Computing: Computing means integration of microprocessors into everyday objects like furniture, clothing, white goods, toys, even paint.
2. Ubiquitous Communication: enables these objects to communicate with each other and the user by means of ad-hoc and wireless networking.
3. Intelligent User Interfaces: enables the inhabitants of the AmI environment to control and interact with the environment in a natural (voice, gestures) and personalised way (preferences, context).

Smart Home: A Prominent example of an environment enriched with AmI. For E.g. a room can have a sensor to decide when its occupant is in or out and on that basis keep lights on or off. It sense it with the movements of person(s) in the room.

Other Applications of AmI

- Health-related applications.
- Public transportation sector
- Education services.
- Emergency services.
- Production-oriented places.
- Public Surveillance

Blockchain

M Janardhan, Assoc Prof, GPCET, Kurnool

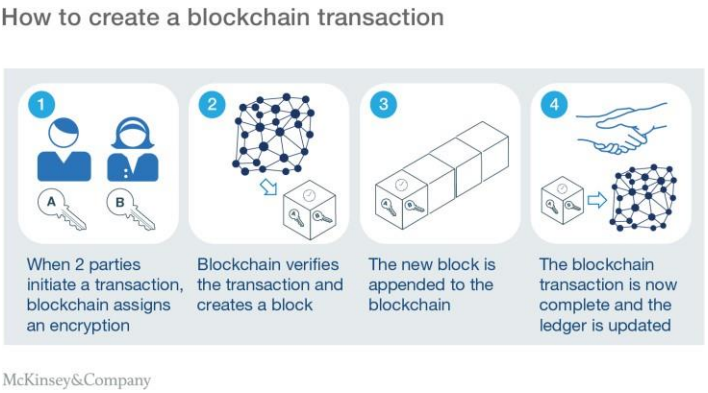
A blockchain originally block chain, is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a merkle tree root hash).

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications, and blockchains which are readable by the public are widely used by cryptocurrencies. Blockchain is considered a type of payment rail. Private blockchains have been proposed for business use. Sources such as the Computerworld called the marketing of such blockchains without a proper security model "snake oil".

Structure

- Blocks
- Decentralization
- Openness



Uses

- Cryptocurrencies
- Smart contracts
- Banks
- Blockchain with video games

Types of blockchains

- Public blockchains
- Private blockchains

Capability of Multi Keyword investigation in Cloud Computing

M.Sri Lakshmi
Assistant professor, Dept. of CSE, GPCET, Kurnool

1. Introduction :

An ever increasing number of individuals and endeavours are inspired to re-appropriate their nearby archive the executives frameworks to the cloud which is a promising data system (IT) to process the unstable extending of information In spite of the benefits of cloud administrations, releasing the delicate data, for example, individual data, organization money related information and government archives, to people in general is a major danger to the information proprietors. Moreover, to make full utilization of the information on the cloud, the information clients need to get to them adaptable and effectively. An instinctive methodology is scrambling the records first and after that re-appropriating the encoded archives to the cloud.

Ranked search can also elegantly eliminate unnecessary network traffic by sending back only the most relevant data, which is highly desirable in the “pay-as-you use” cloud paradigm. For privacy rotation, such ranking operation, however, should not leak any keyword related information. On the other hand, to improve search result accuracy as well as to enhance the user searching experience, it is also crucial for such ranking system to support multiple keywords search, as single keyword search often yields far too coarse result. As a common practice indicated by today’s web search engines (e.g., Google search), users may tend to provide a set of keywords instead of only one as the indicator of their search interest to retrieve the most relevant data. Searchable encryption schemes usually build up an index for each keyword of interest and associate the index with the files that contain the keyword. By integrating the trapdoors of keywords within the index information, effective keyword search can be realized while both file content and keyword privacy are well-preserved. Although allowing for performing searches securely and effectively, the existing searchable encryption. Techniques do not suit for cloud computing scenario since they support only exact keyword search. The aim of this paper is to achieve an efficient system where any authorized user can perform a search on a remote database with multiple keywords, without revealing neither the keywords he searches for nor the contents of the documents he retrieves.

2. Related Work :

Traditional searchable encryption has been widely studied as a cryptographic primitive, with a focus on security definition formalizations and efficiency improvements. So they first introduced the notion of searchable encryption. They proposed a scheme in the symmetric key setting, where each word in the file is encrypted independently under a special two-layered encryption construction. To further enhance search efficiency, a per-keyword-based approach was proposed, where a single encrypted hash table index is built for the entire file collection, with each entry consisting of the trapdoor of a keyword and an encrypted set of related file identifiers. Searchable encryption has also been considered in the public-key setting. Then the first public-key-based searchable encryption scheme construction, with the public key can write to the data stored on the server but only authorized users with the private key can search. As an attempt to enrich query predicates, conjunctive keyword search over encrypted data.

These include the following (a) Secure searchable encryption scheme does not perform any functions when new updates in files or when any modifications are performed. (b) The relevance score algorithm is not updated frequently when there are some modifications in the owner files.

Contributions: In Cloud Computing, an outsourced file collection might not only be accessed but also updated frequently for various application purposes. Hence, supporting the score dynamics in the searchable index for a secure storage engine which is reflected from the corresponding file collection updates, is thus of practical importance. In our system, we consider score dynamics as adding newly encrypted scores for newly created files, or modifying old encrypted scores for modification of existing files in the file collection. Symmetric key encryption doesn't have major scope in security perspective that's why we are opting MD5 encryption algorithm which is bit more complex, when compared to the traditional algorithms in storing the data. B-Tree indexing and storing of data provides a peak level performance in searching times.

3. Existing System:

Figure1: Architecture for search over encrypted cloud data

Design Goals :

To enable ranked searchable symmetric encryption for effective utilization of outsourced and encrypted cloud data under the aforementioned model, our system design should achieve the following security and performance guarantee. Specifically, we have the following goals:

1) Ranked keyword search: to explore different mechanisms for designing effective ranked search schemes based on the existing searchable encryption framework;

2) Security guarantees: to prevent the clouding server from learning the plaintext of either the data files or the searched keywords, and achieve the "as-strong-as possible" security strength compared to existing searchable encryption schemes;

3) Efficiency: above goals should be achieved with minimum communication and computation overhead.

Disadvantages:

The secure searchable encryption scheme does not perform any function when new updates in files or when any modifications are performed. The relevance score algorithm is not updated frequently when there are some modifications in the owner files.

4. Proposed System:

In this paper, we solve the problem of supporting efficient ranked keyword search for achieving effective utilization of remotely stored encrypted data in Cloud Computing. This is done by developing an efficient clustering algorithm to group the 'related' keywords together. One-to-many order preserving technique protects the score information.

Overall description:

The scenario of the score dynamics mechanism is based on the one-to-one order preserving mapping. An efficient clustering algorithm is used to retrieve encrypted cloud data for multiple related keywords. The multiple related keywords are clustered together and ranked, the information is stored in the index which results in accurate search result when the user searches database with multiple related keywords in the same transaction. The proposed system also ranks cloud data based on end user feedback on top of existing ranking algorithms (which relies on keyword occurrence increases the accuracy of data retrieved).

Authentication function : Authentication function describes the interface between the user and system and the admin provided the type of authentication. The user is allowed to create his testimonial to login into the system. An admin needs to approve the users created and login approval the user will be allowed to access the application. Authentication is provided by encrypting the user name and password; this protects sensitive information from unauthorized users.

Clustering algorithm: Clustering is an important application area for many fields including data mining, statistical data analysis, compression, vector quantization, and other business applications. Clustering has been formulated in various ways in the machine learning, pattern recognition, optimization and statistics literature. The fundamental clustering problem is grouping together (clustering) similar data items. During the search process, the user has always desired to input multiple related keywords of his interest rather than a single keyword. Basically any document deal with single concept in brief and the interrelated sub-topics. Grouping the related topics together and forming cluster helps customers to get the desired document of their interest.

Ranked Keyword Search : Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., Keyword frequency), so achieve the privacy preserving data hosting service in context of cloud computing. Ranked keyword search method protect the relevance score of keyword to leaking the information about keyword for that integrate the new crypto primitive order preserving symmetric encryption and properly modify it for purpose of protect the sensitive weight information

This technique is providing some functionality. 1. It provides effective protocol, which fulfils the secure ranked search functionality with little relevance score information leakage against keyword privacy. 2. Ranked searchable symmetric encryption scheme is provide as-strong-as-possible security guarantee compared to previous Searchable symmetric encryption schemes.

The steps of ranked search are shown below.

1. Data owner collects the file and generate the index by extracting the keyword from data files and published index and data files on cloud server.

2. After outsourced the data files user is enable to search and download the data files from cloud server.

3. User can search through only single keyword that is encrypted and using this keyword one trapdoor is generated.

4. Using trapdoor the relevant keyword data files is searched using query and searched data is shown to the user.

Multi Keyword Ranked Search : In this method searching of cloud data using Privacy Preserving Multi keyword Ranked Search (MRSE). Here basic concept is used is co-ordinate matching. Coordinate matching obtains the similarity between search query and documents. Inner product similarity is also used to describe the multi keyword ranked search over encrypted cloud data (MRSE). The features of this method are, multi-keyword ranked search, privacy preserving, high efficiency is eliminating unnecessary traffic and improve search accuracy.

The steps of ranked search are shown below.

1. Data owner collects the file and generate the index by extracting the keyword from data files and published index and data files on cloud.

2. After outsourced the data files user is enable to search and download the data files from cloud server.

3. User can search through single or multiple keywords that is encrypted and using this keyword one trapdoor is generated.

4. Using trapdoor the relevant keyword data files is searched using query and searched data is shown to the user

5. Conclusion:

After the study above two methods are ranked search and multiple keyword ranked search conclude that multi keyword ranked search is better. Multi keyword rank search is enabling semantic keyword search with more accuracy and efficiently because here multiple keywords is used for searching the data files so the frequency of keyword and rank is increased compare to ranked search.

Intrusion detection systems for IoT-based smart environments

P.Suman Prakash
Associate professor, Dept. of CSE, GPCET, Kurnool

1. Introduction :

Incredible developments in the routine use of electronic services and applications have led to massive advances in telecommunications networks and the emergence of the concept of the Internet of Things (IoT). The IoT is an emerging communications paradigm in which devices serve as objects or “things” that have the ability to sense their environment, connect with each other, and exchange data over the Internet. By 2022, one trillion IP addresses or objects will be connected to the Internet through IoT networks [1].

The IoT paradigm has recently been used in creating smart environments, such as smart cities and smart homes, with various application domains and related services. The goal of developing such smart environments is to make human life more productive and comfortable by solving challenges related to the living environment, energy consumption, and industrial needs .This goal is directly reflected in the substantial growth in the available IoT-based services and applications across different networks. For example, the Padova Smart City in Italy is a successful example of a smart city based on an IoT system.

Smart environments consist of sensors that work together to execute operations. Wireless sensors, wireless communication techniques, and IPv6 assist in the expansion of smart environments. Such environments are wide ranging, from smart cities and smart homes to smart healthcare and smart services. The integration of IoT systems and smart environments makes smart objects more effective. However, IoT systems are

susceptible to various security attacks, such as denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks. Such attacks can cause considerable damage to the IoT services and smart environment applications in an IoT network. Consequently, securing IoT systems has become a major concern . For example, on Friday, October 21, 2016, a series of DDoS attacks were launched across the US that exploited the security

vulnerabilities in IoT systems. These attacks affected IoT devices, websites and online services such as Twitter, Netflix, and PayPal [2].

An intrusion detection system (IDS) is a security mechanism that works mainly in the network layer of an IoT system. An IDS deployed for an IoT system should be able to analyze packets of data and generate responses in real time, analyze data packets in different layers of the IoT network with different protocol stacks, and adapt to different technologies in the IoT environment. An IDS that is designed for IoT-based smart environments should operate under stringent conditions of low processing capability, fast response, and high-volume data processing. Therefore, conventional IDSs may not be fully suitable for IoT environments. IoT security is a continuous and serious issue; thus, an up-to-date understanding of the security vulnerabilities of IoT systems and the development of corresponding mitigation approaches are required.

This article offers a comprehensive review of IDSs as a security solution for IoT-based smart environments. The primary goal of this study is to present the most recent designs and approaches for IDSs operating in IoT-based environments. Although related surveys have been published in the literature this article focuses on the important factors that affect IDS performance in smart environments, such as the detection accuracy, false positive rate, energy consumption, processing time, and performance overhead. In addition, this article introduces a solid foundation for the development of IDSs for IoT-based smart environments [3].

2. The IOT paradigm:

The IoT concept has been established since the founding of the Auto-ID Center at the Massachusetts Institute of Technology (MIT) in 1999. The Auto-ID Center created the electronic product code (EPC) number, which depends on radio frequency identification (RFID), in 2003. This idea is the crucial technology of the IoT .

However, the IoT is a well-established paradigm, and it is defined in several ways from various perspectives. Thiesse et al. defined the IoT as consisting of hardware items and digital information flows based on RFID tags. The IoT definitions and architectures provided by various standards and industrial organizations will be described in the following.

The Institute of Electrical and Electronics Engineers (IEEE) defines the IoT as a collection of items with sensors that form a network connected to the Internet .The International Telecommunication Union (ITU) defines the IoT through three dimensions, as a network that is available anywhere, anytime, and by anything and anyone . The European Telecommunications Standards Institute (ETSI), rather than using the expression “Internet of Things (IoT)”, defines machine-to-machine (M2M) communications as an automated communications system that makes decisions and processes data operations without direct human intervention .

The Coordination and Support Action for Global RFID-related Activities and Standardisation (CASAGRAS) project has created a new concept of the IoT that encompasses two viewpoints: the connection of physical objects with virtual objects over a global network without any human intervention to the greatest extent possible and the incredible increase in IoT applications within traditional networks due to the extent of IoT marketing . Moreover, Cisco, an industrial organization, works on IoT technology under the title of the Internet of Everything (IoE). Cisco has summarized the IoE concept as a network that consists of people, data, things, and processes. Thus, information and actions are created in and moved through this network[4].

IOT and Smart environments:

The objective of smart environments is to make human life more comfortable and more efficient by using sensors. IoT-based smart environments enable the effective realization of smart objects. By means of an IoT network, sensors can be monitored and controlled remotely. According to Navigant Research, the global smart city services market is expected to increase from 93.5 billion US dollars in 2017 to 225.5 billion US dollars by 2026 .

Ahmed et al. state that “The term smart refers to the ability to autonomously obtain and apply knowledge, and the term environment refers to the surroundings”. A smart city is one type of smart environment. The core element of a smart city is an integrated information center operated by the IoT service provider, which provides information on services such as electricity, water, and gas.

Smart health, smart industry, smart buildings and smart homes are other types of smart environments. The objective of such smart environments is to provide services via smart methods based on the information collected by IoT-enabled sensors. The architecture of such IoT-based smart environments is shown in Fig 1.

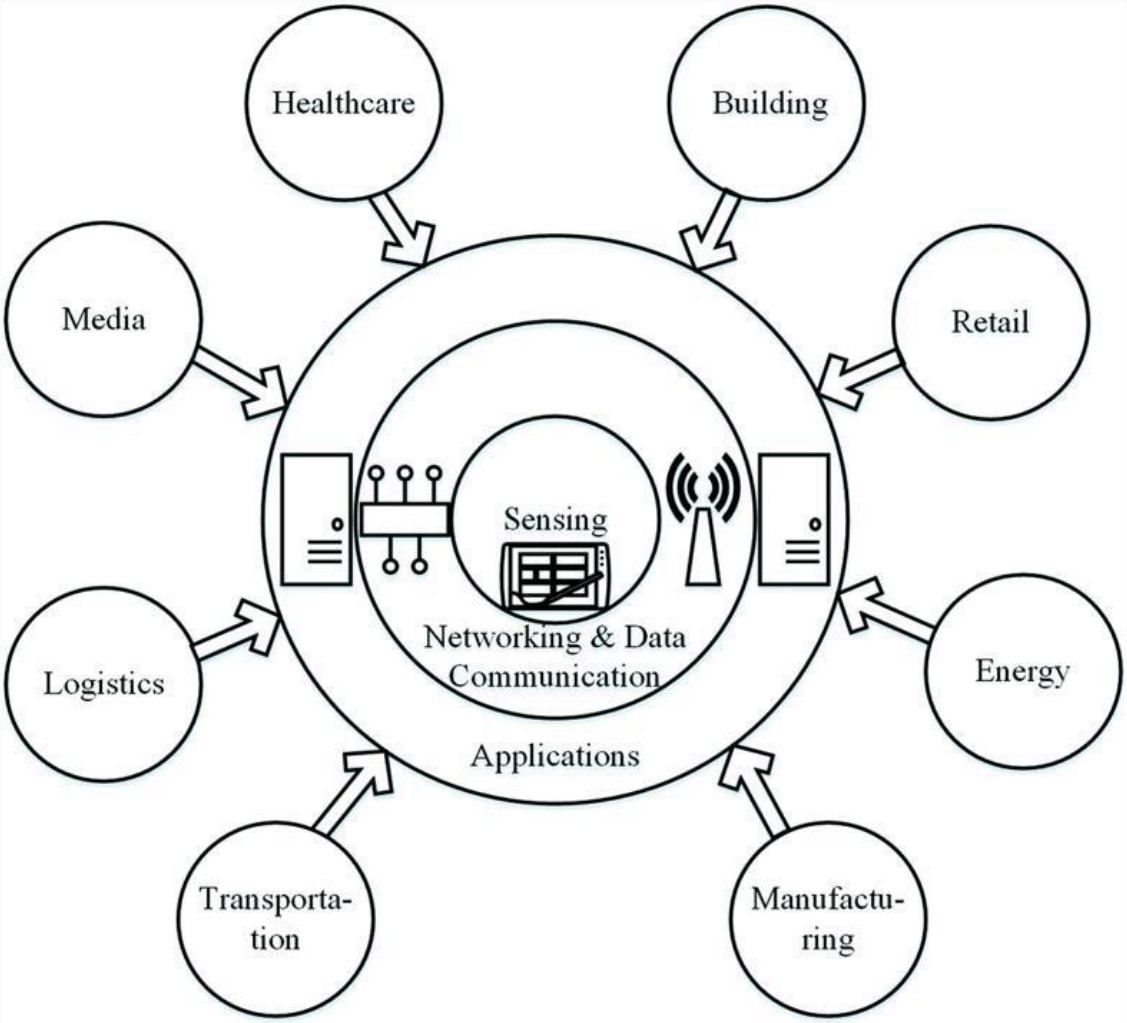


Fig1: IoT-based smart environments. The architecture of the IoT and the extent of the IoT market

Smart environments based on the IoT paradigm have certain special characteristics, and hence, special needs arise in the deployment of such environments. For instance, remote monitoring and remote control capabilities are required to allow smart objects to

collect and process data and to execute operations remotely. Moreover, the ability to make decisions is an important characteristic in such a system. A smart object should be able to make intelligent decisions without human intervention by using data mining and other techniques for extracting useful data[5].

By virtue of these characteristics, smart environments offer certain features that can be used to enhance the quality of service (QoS) of user applications. Real-time information is one of these features. Smart objects can collect and analyze data and make intelligent decisions in real time. Moreover, the cost-effectiveness of cloud applications can be used to increase the QoS of smart environment applications. The integration of smart and IoT environments offers new opportunities with respect to the QoS of services and applications.

References:

1. Mohamed Faisal Elrawy,Ali Ismail Awad and Hesham F. A. Hamed," Intrusion detection systems for IoT-based smart environments: a survey", Journal of Cloud ComputingAdvances, Systems and Applications2018
2. Tariqahmad Sherasiya1 , Hardik Upadhyay2," Intrusion Detection System for Internet of Things", IJARIIE-ISSN(O)-2395-4396, Vol-2 Issue-3 2016.
3. Arbia Riahi,Yacine Challal,Enrico Natalizio,Zied Chtourou,Abdelmadjid Bouabdallah," A systemic approach for IoT security",
4. Yacine Challal, Internet of Things Security: towards a cognitive and systemic approach, HDR Thesis, Université de Technologie de Compiègne, 2012.
5. V. Gligor and J. M. Wing, Towards a Theory of Trust in Networks of Humans and Computers, 19th International Workshop on Security Protocols, Cambridge, UK, March 28-30, 2011 V. Gligor and J. M. Wing, Towards a Theory of Trust in Networks of Humans and Computers, 19th International Workshop.

Blockchain Technology – Everything you need to know in layman's language

Dr. K.Seshadri Ramana
Professor of CSE

The Blockchain technology has become a regular news item with the emergence of cryptocurrencies like Bitcoin. Now, this technology is disrupting almost all markets, changing the way we do our day to day business.

The blockchain is an incorruptible digital ledger of transactions that can be programmed to record virtually everything of value. Each list of record in a blockchain is called block.So a blockchain is a continuously growing list of records called blocks, which are linked and secured.

Blockchain Technology was invented by Satoshi Nakamoto in 2008 for use in the cryptocurrency bitcoin, as its public transaction ledger. Satoshi Nakamoto's aim in creating the decentralized Bitcoin ledger—the blockchain—was to allow users to control their own money so that no third party, not even the government, would be able to access or monitor it.The creator of Bitcoin, Satoshi, disappeared back in 2011, leaving behind open source software that the users of Bitcoin could update and improve.The invention of the blockchain for bitcoin made it the first digital currency to solve the double spending problem without the need of a trusted central authority or central server.

Technologies behind blockchain technology

Private Key Cryptography

P2P Network (Peer-2-Peer)

Program (the blockchain's protocol)

Need of blockchain technology

The blockchain is a mechanism to bring everyone to the highest degree of accountability. No more missed transactions, human or machine errors, or an exchange that was not done with the consent of the parties involved.

The most critical area where Blockchain helps is to guarantee the validity of a transaction by recording it not only on the main register but a connected distributed system of registers, all of which are connected through a secure validation mechanism.

Applications of blockchain in future:

Smart contracts – Any industry heavily reliant on contracts, such as insurance, financial institutions, real estate, construction, entertainment, and law, would benefit from blockchain's indisputable way to update, manage, track and secure contracts. Smart contracts, those that are embedded with if/then statements and be executed without the involvement of an intermediary, also use blockchain technology.

Supply chain management – Whenever value changes hands or the status of asset changes, blockchain is ideally suited for managing the process.

Asset protection – Whether you're a musician who wants to ensure you get royalties when your music gets played or a property owner, blockchain technology can help you protect your assets by creating an indisputable record of real-time ownership.

Personal Identification – Governments manage vast amounts of personal data from birth and death records to marriage certificates, passports and census data. Blockchain technology offers a streamlined solution for managing all of it securely.

Payment processing – Blockchain has the potential to be highly transformative to any company that processes payments. It can eliminate the need for intermediaries that are common in payment processing today.

Crowdfunding – As with traditional crowdfunding, a blockchain powered crowdfunding campaign seeks to secure investment for a new project from an interested community. But in this instance, funding is most likely to come in the form of bitcoin or other cryptocurrencies.

Advantages:

1. The blockchain allows our smart devices to speak to each other better and faster.

2. Blockchain solves the problem of manipulation. It brings everyone to the highest degree of accountability.

3. Online identity and reputation will be decentralized. We will own the data that belongs to us.

4. Cryptocurrencies take the power away from governments to control the value of currencies and hand it to people.

5. The potential is great for people in the informal economy to exploit the blockchain's middleman-free way to exchange asset.

6. Blockchain-based systems allow for the removal of intermediaries involved in the record keeping and transfer of assets.

7. The removal of intermediaries and settlement on distributed ledgers allows for dramatically increased transaction speeds compared to a wide range of existing systems.

8. Data entered on the blockchain is immutable, preventing against fraud through manipulating transactions and the history of data. Transactions entered on the blockchain provide a clear trail to the very start of the blockchain allowing any transaction to be easily investigated and audited.

Criticisms and Challenges

Huge power required: Remember all that computing power required to verify transactions? Those computers need electricity. Bitcoin is a poster child of the problematic escalation in power demanded from a large blockchain network. That's not appealing given today's concerns about climate change, the availability of power in developing countries, and reliability of power in developed nations.

Security about the private key: The private key must remain secret at all times because revealing it to third parties is equivalent to giving them control over the bitcoins secured by that key. The private key must also be backed up and protected from accidental loss, because if it's lost it cannot be recovered and the funds secured by it are forever lost, too.

Transaction speed: Transaction speed is also an issue. As we noted above, blocks in a chain must be verified by the distributed network, and that can take time.