A SURVEY ON CLOUDIOT PARADIGM TOWARDS MODERN TECHNOLOGY

1) Nirmit Singhal 2)Aniket Navghare
B. Tech Computer Science and Engineering, Vishwakarma Institute Of Information Technology Pune, Maharashtra, India

ABSTARCT

Cloud computing is currently the most hyped evolution in the computing dimension, delivering computing services via the internet on demand and pay-per-use access to shared resources such as storage, network, and services without having to physically receive them and on a leased-basis, as well as elaborates various dimensions such as parallel, distributed, grid, and soft-computing. the beginning of a developed era. Cloud computing is becoming a prominent aspect of business computing as it holds the probable abilities to eliminate the requirements for setting up excessively- costly computing infrastructure for Information technology services. In this paper, we present an overview of the concept of cloud architecture and computing models. The dawn of a more evolved era Cloud computing is becoming a popular feature of business computing because it has the potential to eliminate the need for expensive computing resources in order to provide information technology services. We provide an overview of the philosophy of cloud architecture and computing models in this paper.Furthermore, since security is one of the primary impediments to the growth of cloud computing, we will be shedding light on the major security threats that cloud computing systems face, and we will be effectively monitoring cloud computing security on a very technical level, focusing on attacks and hacking attempts related to cloud computing providers, resulting in more stable cloud computing scenarios.

KEYWORDS

Models for deployment and service, the IoT healthcare paradigm, security issues and remedial measures, cloud computing, and the IoT migration paradigm are all covered.

INTRODUCTION

With the availability of high-scope and capacity networks, low-budget computers, and storage devices with small size and high storage capacity, our technology has reached a whole new stage of remarkable development. The widespread use of hardware virtualization, service-oriented architecture, and autonomous and utility computing have contributed to the emergence of a modern computing ageCloud computing is a term used to describe a form of computing that Cloud computing is a form of cyberspace-based computing that delivers shared computer resources and data to other computers and devices on demand from a shared pool of configurable computing resources that can be quickly released with little management effort or service provider involvement.

It allows companies to concentrate on their core operations rather than wasting time and resources on computer infrastructure. Virtualization is the technology that makes cloud computing possible. It enables IT applications to run faster and costs to be reduced by increasing infrastructure application. The principles of Service-Oriented Architecture are used in cloud computing (SOA).Cloud computing delivers all of its properties as services, and it uses a well-established model and the best practises learned in the domain of SOA to provide consistent global and fast access to cloud services. Cloud computing has influenced the development of health-care paradigms significantly. It helped the elderly, who tend to be alone and need continuous medical care. guidance, as well as for people who live in rural or isolated areas and need regular medical care. We advanced to electronic facilities in order to enter those places and be accessible to elderly people at all timesand computers that are made accessible to anybody, anywhere, at any time, via a cyberspace network. Wireless devices enable data about a patient's condition to be transmitted to caregivers. This portable system detects medical conditions such as a patient's heart rate, blood pressure, and breath alcohol level simply by touching it, and provides an antidote for the patients or users.As a result, in order for wireless devices to connect and communicate with the Internet, a new level of communication known as machine-to-machine communication (M2M) was needed, which was aided by Cloud Computing systems. The Internet Of Things (IoT) is the term for this form of device-to-device communication over the internet (IOT). It's a system that connects physical objects with electronics and allows them to communicate with one anothersystems, sensing units, actuators, and network connectivity that enable devices to capture, process, and exchange data It provides advanced computer, system, and service connectivity that extends beyond machine-to-machine (M2M) communications and covers a wide range of responsibilities, territories, and applications. We addressed some deployment models in the first section of this research paper, and then we moved on to the second section.Some terms related to IoT and Cloud Computing were addressed in later parts. Potential risks related to cloud computing and IoT, as well as their protection and remediation measures, are discussed in the following pages. In the final section, we'll go over IoT and Cloud Computing in detail, including how we manage their operations and applications in tandem, as well as how they're used in a real-time environment.

1)DEPLOYMENT MODELS

A cloud deployment model, as the name suggests, depicts a specific sort of cloud environment that is defined by scalability, access, and ownership.Firms benefit from it because it lowers capital spending and keeps operating costs under control. Each company will have its own deployment model that is tailored to that particular website. The most important task is to choose the appropriate model, which necessitates one. You can accomplish your business goals more quickly and easily if you gain enough information about the business and evaluate the demands in order to select the most suitable model. The deployment models are divided into four categories, each of which has been thoroughly described in this paper.

a) <u>PRIVATE CLOUD:-</u>

As the name implies, private cloud refers to cloud storage services provided in private networks that are not open to networks outside the private domain because it gives only registered users or private organisations control over their data. Because of its ability to set up inside an organization's own business data, it's also known as the internal cloud.In a private cloud, the cloud provider will provide cloud users with scalable tools and virtual applications that he or she will pool together and make available to them for use or sharing. The public cloud has a more stable environment than the public cloud since it has unique internal exposure and is generally secured by firewalls. It is a little more expensive, but it provides a safer environment for consumers. The private cloud varies from the public cloud in that the firm controls the cloud services.Organizations that have diverse requirements that can't be predicted in advance, such as mission-critical tasks, security alerts, and management demands, use private cloudcompanies Despite being the most stable deployment model, private cloud is vulnerable to internal data theft. A private cloud can be owned or rented by a third party or by someone who is not the owner of the company. What makes private computing more functional and comfortable is that it is not subject to the same security restrictions, legal requirements, or bandwidth constraints as public cloud computing.

b) <u>PUBLIC CLOUD :-</u>

The term "public cloud" refers to cloud computing in its most common form, in which resources are dynamically provisioned on a self-service basis over the Internet, through applications and cloud services, and where the services are provided on a public domain and are not limited to a specific set of users.Furthermore, this is more akin to an off-site third-party contractor who shares services and bills on the basis of utility computing. The basic model on which it is based is the "pay-as-you-use" model, which simply means that the consumer only pays for what they use, preventing underutilization.Public clouds are less secure than other cloud models not only because the cloud services are accessible on a public network and can be used by all, but also because it puts an additional responsibility on the user to ensure that all applications and data accessed on the public cloud are not subjected to malicious or vengeful attacks.The fact that the infrastructure is shared with a large number of clients and is managed by a third party outside of the company's firewall adds to the security issues.The security problems will be discussed in depth later in the research paper.The cloud services and infrastructure can be used by many users at the same time, avoiding problems such as server failures due to overloading. The cloud provider is in charge of all aspects of cloud management, including implementation, management, and maintenance. The public cloud is more cost effective because it has lower capital and maintenance costs.The public cloud has its own set of restrictions, most of which are related to security concerns. Organizations that require complete and overall control of the cloud by their users should not turn to the public model, as this can compromise their security. Since it is a public domain model, there are no restrictions on the authentication methods that can be used or implemented.Customers of public cloud providers like Google and Amazon have access control, which is unusual because complete control of the cloud by users is impossible to acquire.Microsoft Azure and Google App Engine are two examples of public clouds.

c) HYBRID CLOUD :-

The word "hybrid" refers to a system that combines a private model with two or more external cloud implementation models and is managed by a single entity that handles data transmission across the models without interfering with the models and guarantees that the clouds remain separate entities.By aggregation and assimilation, the customer may increase his or her capacity or capability while also overcoming the provider's limitations. The business creates the cloud, and both the business and the cloud provider manage it.Even though cloud services are accessible without any user restrictions on the internet, hybrid cloud is a more protected model than public cloud. Interfacing with other systems is also possible, thanks to the cloud's open architecture, which also allows it to provide virtual IT solutions. The biggest challenge in successfully developing and implementing such solutions is. It may also refer to setups that combine virtual and physical properties, such as a fully virtualized environment that necessitates physical servers, routers, and other hardware, as well as a firewall for spam filtering.Hybrid cloud hosting improves and integrates features including scalability, flexibility, and security. One of the organisations that has moved to a hybrid cloud model is Amazon Web Services (AWS).

d) COMMUNITY CLOUD :-

The phrase "community cloud" refers to cloud infrastructure that is shared by a number of organisations rather than being restricted to a single entity for the common good.Management is handled by the company or a third party, and it can be done internally or outside. The clouds are a type of hosting in which the setup is shared by numerous organisations belonging to the same group, and they are based on an agreement between different corporate organisations.The various communities have similar concerns about performance and protection. These communities' primary goal is to accomplish their business-related goals.The fact that the group will be sharing the burden makes cloud computing even more competitive and economical. Community cloud hosting is exemplified by Facebook. Community cloud hosting is ideal for companies and organisations working on joint ventures, tenders, or initiatives that include centralised cloud storage.

2)SERVICE MODELS

Many services that are routinely used by online applications all around the world have been made possible by cloud computing.The services provided vary depending on the model. Infrastructure as a Service (IaaS) is one of three standard service models (IaaS). Platform as a Service (PaaS) and Software as a Service (SaaS) are two types of cloud computing services (SaaS). The aim of these service models is to increase abstraction. As a result, in a cloud system architecture, they are depicted as layers: infrastructure-layer, platform-layer, and software-layer. Without any underlying PaaS or IaaS layers, SaaS can be implemented on physical devices, and vice versa, one can run a programme on IaaS and approach it specifically without binding it as SaaS.

a. SOFTWARE AS A SERVICE MODEL(SaaS):-

This programme gives customers the ability to use the provider's cloud-based software. This software can be accessed from a variety of user devices through a client interface, such as a web application, or a programme interface. The consumer has no control on the underlying cloud infrastructure, which includes grillwork, servers, operating systems, storage, and even individual operation capabilities, but user-specific application configuration choices are possible.It usually gives the customer what they want when they want it when they want it. SaaS services include Amazon EC2, GoGrid, and Flexiscale, to name a few.

b. PLATFORM AS A SERVICE MODEL(PaaS):-

This service provides users with the opportunity to branch out onto cloud infrastructure built specifically for them or to gain access to applications created with programming languages and software provided by the provider. The client does not have control or management of the underlying cloud infrastructure, such as grillwork, servers, operating systems, or storage, in this service model either, but they do have control over the distributed applications and configuration settings for the application-hosting context. It mainly focuses on operating system maintenance and software development. PaaS services include Google App Engine and Microsoft Windows Azure, to name a few.

c. INFRASTRUCTURE AS A MODEL(IaaS):-

This service allows users to define processing, storage, networks, and other significant computing resources, as well as instal and run arbitrary software, such as operating systems and applications. The user does not manage or operate the underlying cloud architecture in this service model, but they do have control over the operating systems, storage, and distributed applications. This service usually refers to the provision of infrastructure services in response to a customer's request. Some IaaS examples include GoGrid and Flexiscale.

3)SECURITY

Cloud computing has a bright future for IT applications; however, security and privacy concerns are the key roadblocks to its expansion. There are two basic types of functions: data storage and data computation. Cloud service users only need an internet connection to get access to the data and perform computing tasks. Clients are unaware of where the data is stored and which computers are responsible for performing the calculation task at this time. The threats are classified according to different perspectives, resulting in a comprehensive list of known and unknown threats.Following that, a list of successful countermeasures is presented and explained. We'll go over security threats and safeguards in cloud computing, as well as strategies that a company may use to remove or mitigate security risks, as well as improve resource protection and reliability while a third party is processing sensitive data. The primary factors in gaining user confidence and making cloud technology effective are data storage, data security, and data safety.

4)DATA INTEGRITY

Data integrity is an important aspect of cloud storage because it protects data from unauthorised access, which can result in unintended deletion, alteration, or fabrication. Since there are so many entities in a cloud environment, authorization is critical in ensuring that only approved entities can communicate with data. It's the foundation for cloud services like SaaS, PaaS, and IaaS, as well as applications. Controlling access to relevant enterprise resources ensures that sensitive information and services are not exploited, misused, or stolen.A single database is required in a standalone technique to achieve data integrity, which is maintained by database limitations and transactions.Authorization is a method of restricting data access. Monitoring is a process that aids in determining what or who could have altered the system, resulting in a violation of integrity. This improves data security while also increasing consumer trust.

5)DATA CONFIDENTIALITY

This is a critical feature that allows data to be stored in the cloud while also ensuring that the data or information is only accessible by the user. By monitoring and restricting user access, authentication techniques are used to ensure data confidentiality. As these problems are properly addressed, cloud reliability and trustworthiness among users can improve. Encryption is a standard method for ensuring data security. Homomorphic encryption is a form of encryption that ensures that the results of the cypher text algebraic operation match those of the clear operation after encryption.For database encryption, Manivannan and Sujarani [Authors] suggested a lightweight mechanism (TSFS)algorithm known as transposition, swapping, folding, and deviating algorithm. There will be a synchronizer between the client and the owner when a client requests data. The client will be given a key by the synchronizer in order to decrypt the encrypted data it receives from the owner. The synchronizer is often used to keep track of data and keys. The fact that the delays occur as a result of unnecessary contact is a flaw in this algorithm. Other methods for maintaining data confidentiality and thereby improving client relationships include cryptography and data isolation.

6)DATA AVAILABILITY

When the machine suffers from disc damage, hard disc failure, network problems, or failures, data availability comes to the rescue. Data availability refers to the degree to which a customer can use or retrieve missing data, as well as how users validate their data using techniques rather than relying solely on the cloud service provider's credit guarantee. The key aim of data availability, as the name implies, is that data should be accessible to users at all times and at all locations.Users of a cloud computing system can access their resources and applications from any place. The two most critical strategies used to improve the availability of the Cloud infrastructure or services hosted on it are hardening and redundancy. Cloud computing providers also have virtual machine-based cloud infrastructures. This gives cloud vendors an incentive to rent Amazon services on demand. As a result, the virtual machine serves as the foundation for hosting these services. Virtual computers have the potential to meet the user's needs and expectations while still increasing the cloud system's data availability.

7)DATA PRIVACY

Privacy is characterised as an individual's or a group's right to keep themselves or their data private and only disclose it selectively. The following are the components of privacy.
If a person is comfortable with their information being shared publicly or with requests for his information. To prevent data manipulation and unauthorised access, which compromises privacy.
In terms of legal enforcement and user confidence, privacy is critical. The biggest challenge for software engineers is to design cloud services and applications in such a way that privacy risks are minimised and legal enforcement is ensured. To protect your privacy, take the following steps:

- Don't submit or store personal information in the cloud.

- Use a privacy setting to keep the details secure.

- User access and option should be made available.

- Data use should be restricted and precise.

- It is important to receive feedback.

8) CONTROL

Control refers to the ability to regulate the usage of cloud services and applications. It involves large-scale distributed computing with data spread over a large number of computer nodes. When a user accesses the cloud, he or she has the option of contributing data to the cloud system, which can then be used. A user's click stream through a collection of websites (e.g., the Flipkart store, the Yahoo search web pages, and so on) can be used to provide targeted ads.

9)USER THREATS

Migration from an IT system to a cloud platform is an important part of the business because it gives cloud service providers some leverage over the cloud. This lack of governance is dependent on the service model; for example, IaaS only delegated hardware and network management to the provider, while SaaS degraded OS applications.

USER CONFIDENCEPROBLEMS:- Due to the cloud service's black-box functionality, it can be difficult for a cloud service customer to determine the cloud provider's level of confidence. There is no way to formally quantify or describe a security level.

LOCK FOR SERVICE PROVIDER: The inability to move from one cloud service to another results in a lack of governance. If a cloud provider uses non-standard hypervisors and does not have tools to migrate virtual machines to a structured format, this is a possibility.

ACCESS BY AN UNAUTHORIZED USER: Since the cloud environment is made up of various models, each has its own set of privacy and security controls. Manipulation, deletion, and abuse of data result from unauthorised access. For example, your account may be used as a base for a hacker. As a result, he or she will now use the strength of your prestige to launch additional attacks.

AN INADEQUATE LEVEL OF INFORMATION: Cloud service providers have serious concerns about asset management, including service details, inadequacy of physical control for data storage, security, countermeasures for data loss or theft, and disaster recovery. Furthermore, cloud service users are concerned about data being exposed to foreign governments, which would be a violation of privacy laws.

10)PROVIDER THREATS

INCONSISTENCY IN PRIVACY: Since the cloud is built on a decentralised framework, the security mechanisms are more likely to be inconsistent across distributed security models. Attackers take advantage of this reality to compromise the cloud's protection and privacy.

EVOLUTIONAL DANGERS: Deferring decisions from the design to the execution process is a type of cloud conceptual improvement that essentially means that certain software-dependent entities of a system can be chosen and implemented while the system is being executed. Traditional risk management strategies can't keep up with such rapid change. Because of new software components, a well-secured system in the design phase could achieve vulnerabilities during execution.

HIJACKING OF ACCOUNTS AND TRAFFIC: Theft of traffic is a serious problem that cloud users should be mindful of. These attacks include phishing and spam campaigns, account theft, and denial of service.

MULTI-LOCATION: Storing private data in multiple locations is risky.

If the company's confidential information is stored on a third-party computer. In this case, the private data of the companies is stored on someone else's computer and in someone else's facility, and the cloud service provider may go out of business.

DATA COMBINATION: The cloud must ensure that a client's private data is stored separately from other data. If they are mixed with the information of other customers, this can be harmful. This could result in the spread of viruses, because if one client were hacked, the attack could compromise the data integrity of other clients in the same environment.

SQL INJECTION ATTACK: The attacker inserts malicious code into a SQL query in this form of attack. This gives the attackers full access to the database, invading users' privacy.

XSS (CROSS-SITE SCRIPTING) ATTACKS: This attack works by injecting malicious scripts into the web. These attacks indiscriminately infiltrate data and can be carried out in two ways: -

- Malicious codes are permanently stored in the resources handled by web applications using Stored XS. As a result, critical data information is shared between users.

- The attack scripts are not permanently stored with Reflected XSS. In this type of attack, an entity attempts to intrude into an active conversation between a sender and a recipient in order to inject false information and gain access to the sensitive data being exchanged.

DENIAL OF SERVICE ATTACKS (DOS): A DOS attack floods the destination server with a large number of packets that the target server can't manage, effectively shutting down the computer's essential services.

CAPTCHA BREAKING: Spammers can now easily break CAPTCHA, which is supported by Hotmail and Gmail. For visually impaired people, they use an audio device that can read the CAPTCHA characters. To stop CAPTCHA breaking, techniques such as letter overlap, different fonts of the alphabets and numbers used for captcha design, and increasing the string length can be used.

11)SECURITY MEASURES

AUDIT OR VERIFICATION: Monitoring what is happening in the cloud system is what auditing the cloud system entails. This could be applied on top of the virtualized application environment as an extra layer. This is more safe because it can monitor the length of access. Monitoring should be restricted to what is fairly required by the Cloud provider in order to operate their services.

OBEDIENCE :-

A systematic approach to oversight and enforcement aids cloud service providers and their customers in planning for the evolution of cloud computing models. To drive enforcement and productivity while also improving risk management, cloud service providers must incorporate a robust internal control monitoring system.

INTRUSION DETECTION SYSTEM: These systems track and document the activities of the system in order to detect any intrusion, unauthorised activities, or policy destruction over vast networks. These systems are effective in detecting and documenting possible threats in the vast majority of cases.

DATA SEGREGATION: The user should be aware of the measures taken to segregate their data and should be able to request proofs that encryption schemes are in operation.

DISASTER RECOVERY VERIFICATION: Obtain appropriate information from the cloud provider about the effects and countermeasures of a disaster, including whether the provider will be able to restore data and services, as well as the time it will take to do so.

LONG-TERM VIABILITY :-Ask the cloud providers if and when they will be able to restore data in the event of a data failure. If data recovery is not feasible, one must determine whether the data's format is appropriate for import into a replacement programme.

SYSTEM FOR SECURITY INFORMATION AND EVENT MANAGEMENT: Alert, report generation, trend analysis, and security enforcement are some of the basic measures that these systems take to identify threats. These measures are repeated on a regular basis in order to collect data and provide reports in the event of a threat.

12)BRINGING CLOUD COMPUTING AND IOT TOWARDS A REAL TIME ENVIRONMENT

Cloud computing has been expanded to the network's edge in today's technology, allowing for the creation of a new breed of applications and devices. IoT and Cloud Computing have recently been widely studied and applied in a variety of fields, resulting in new approaches for intelligent perception and establishing M2M links. Furthermore, it allows for more and more flexible resource sharing on request.

The Internet of Things has grown to the point that it needs to be combined with cloud computing.The large amount of data produced by IoTs and the need for constant authorization for virtual resource use and storage, but with the help of cloud computing, it is possible to build more efficient storage and retrieval of data from the data generated by IoTs and develop more crafty applications for users without much need for authorization.

Cloud computing also offers a cost-effective way to handle and compose IoT services, as well as the operations that use the stuff or data they generate.Apart from that, cloud computing benefits from IoT by broadening its horizons to deal with real-world issues in a more relevant and efficient manner, as well as provide new services in a wide range of real-world scenarios.

While integrating IoT operations and data with cloud storage provides significant benefits in terms of cost reduction and the elimination of complications associated with direct hardware management, it also raises a slew of issues that threaten to derail both of their operations. Confidence in the service provider, knowledge of service quality, and knowledge of the physical location of data storage are all issues that must be addressed. The distributed design also raises questions about its remedial solutions, such as SQL injection, session hijacking, and virtual-machine escape.

13)ISSUES INVOLVED AND THIER SOLUTIONS

QUALITY OF SERVICE: As the amount of data and its forms grows, quality of service has become a serious concern. Any form and quantity of data, including emergency data, can be activated at any time. On the cloud side, dynamic request pollution will be implemented. QOS must be supported depending on the form of data and the need for it to be sent to the sync node.

DATA STORAGE DESTINATION: The most important factor in captious and latency or keen data is location. Users expect immediate results after conducting a search, which can only be obtained by storing data in the nearest physical location.Important data, such as video or audio, should be stored as close to the user as possible in order to reduce the amount of time it takes to access big data. A nearby accessible virtual storage server must be reserved for multimedia data.

IDENTITY MANAGEMENT: Different types of nodes that communicate over the internet are uniquely defined. Devices or artefacts that become part of the Internet (IoT) need a specific identification as well. However, as IoT and Cloud Computing evolve, there will be a large number of devices connecting to the IoT that will require a unique identity.IPv6 addressing is considered an effective method of supporting this form of ubiquitous networking since it can accommodate such a large number of devices. The most logical method for managing the identities of different devices is to assign IPv6 addresses to each of them.

CONCLUSION

Our daily lives, activities, and lots of IT operations have all changed dramatically as aresults of theadoption of the IoT and Cloud Computing paradigms. This model encourages the event of innovative services, market opportunities, and healthcare applications. It's paved the way for brand new research projects.
In this article, we glance at how IoT and cloud computing have greatly enhanced our daily lives and web applications. Despite the actual fact that they enabled many new crafty devices and new services to web apps, they also faced some new security challenges. We looked into these problems and came up with some solutions. We also checked out how IoT and cloud computing have shifted the passive world toward a healthcare model that's more accessible and convenient for patients in rural areas. We've got conducted a survey to work out how IT operations and web applications are managed within the most straightforward manner possible, allowing new services to be implemented quickly.

ACKNOWLEDGEMENTS

Under the guidance and supervision of Prof. Kirti Wanjale, Nirmit Singhal (Computer Science and Engineering, VIIT) , Aniket Navghare (Computer Science and Engineering, VIIT)
surveyed this research paper (Assistant Professor-CSE, VIIT).

REFERENCES

[1] Nicola Bui, Michele Zorzi, "On the combination of Cloud Computing and Internet of Things ", proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, Barcelona, Spain — October 26 - 29, 2011.

[2] Nicola Bui and Michele Zorzi "Health Care Applications: an answer supported the webof Things", proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, Barcelona, Spain — October 26 - 29, 2011.

[3] JiongJina, JayavardhanaGubbib, Slaven Marusicb, MarimuthuPalaniswamib, "An Information Framwork of making a wise City through Internet of Things", IEEE Internet of Things Journal, 09 January 2014.

[4] Soumya Kanti Datta, Christian Bonnet, Amelie Gyrard, Rui Pedro Ferreira da Costa, Karima Boudaoud "Applying Internet of Things for Personalized Healthcare in Smart Homes" , Wireless and Optical Communication Conference (WOCC), 07 December 2015.

[5] Dharmendra Singh Rajput, Rakesh Gour" An IoT Framework for Healthcare Monitoring Systems", International Journal of applied science and knowledge Security (IJCSIS), Vol. 14, No. 5, May 2016.

[6] J. Sathish Kumar, Dhiren R. Patel," A Survey on Internet of Things: Security and Privacy Issues", International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2014.

[7] Evdokimos I. KONSTANTINIDIS, Giorgos BAMPAROPOULOS, Antonis BILLIS and Panagiotis D.BAMIDIS, " Internet of Things For an Age-Friendly Healthcare", published online with Open Access by IOS Press and distributed under the terms of the Creative Commons Attribution Non-Commercial License. doi:10.3233/978-1-61499-512-8-587.

[8] SomayyaMadakam, R. Ramaswamy, Siddharth Tripathi, "Internet of Things (IoT): A Literature Review" Journal of Computer and Communications, 2015, 3, 164-173 Published

Online May 2015 in SciRes..

[9] Feng Xia1, Laurence T. Yang, Lizhe Wang and Alexey Vinel, " Internet of Things, International Journal of Communication Systems", Int. J. Commun. Syst. 2012; 25:1101–1102 Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/dac.2417.

[10] Mohammad Aazam , Pham Phuoc Hung , Eui-Nam Huh, "Cloud of Things: Integrating Internet of Things with Cloud Computing **and therefore the** Issues Involved," Applied Sciences and Technology (IBCAST), 2014 11th International Bhurban Conference, 14-18 Jan. 2014.

[11] R.M. Dijkmana, B. Sprenkels , T. Peeters , A. Janssenb,"Business models for **the web** of Things", volume 35, Issue 6, December 2015, Pages 672–678

[12] AshviniBalte , AsmitaKashid, Balaji Patil, "Security Issues in Internet of Things (IoT): A Survey", Volume 5, Issue 4, 2015 ISSN: 2277 128X International Journal of Advanced Research in engineering science and Software Engineering.

[13] Yazid Benazzouz, Christophe Munilla, Ozan Günalp, Mathieu Gallissot, LeventGürgen, "Sharing User IoT Devices with in Cloud", published in: Internet of Things (WF-IoT), 2014 IEEE World Forum on 6-8 March 2014.

[14] Khan, S. U. Zaheer, & Khan S, "Future Internet: **the web** of Things Architecture, Possible Applications and Key Challenges" , published in: 2012 10th International Conference on Frontiers of knowledge Technology (FIT): Proceedings.

[15] Wentao Liu, "Research on Cloud Computing Security Problem and Strategy", Published in: Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on 21-23 April 2012.

[16] Ling Qian, Zhiguo Luo, Yujian Du, and Leitao Guo, "Cloud Computing: An Overview", conference paper,doi: 10.1007/978-3-642-10665-1_63.

[17] Lizhe Wang, Gregor von Laszewski, Marcel Kunz, Jie Tao, " Cloud computing: A Perspective study", doi: 10.1007/s00354-008-0081-5, cite **this text** as:Wang, L., von Laszewski, G., Younge, A. et al. New Gener. Comput. (2010) 28: 137. doi:10.1007/s00354-008-0081-5.

[18] Deyan Chen, Hong Zhao, " Data Security and Privacy Protection Issues in Cloud Computing", published in: computing and Electronics Engineering (ICCSEE), 2012 International Conference on 23-25 March 2012.

[19] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya, "Service-Oriented Cloud Computing Architecture", published in: Information Technology: New Generations (ITNG), 2010 Seventh International Conference on 12-14 April 2010.

[20] Ramgovind S, Eloff MM, Smith E," The Management of Security in Cloud Computing", published in: Information Security for African country (ISSA), 2-4 Aug. 2010.

[21] Rachna Arora, AnshuParashar ," Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.

[22] Victor Chang, David Bacigalupo, Gary Wills,

David De Roure," A Categorisation of Cloud Computing Business Models", published in: CCGRID '10 Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing.