A REVIEW ON PRIVACY AND SECURITY CHALLENGES IN INTERNET BASED COMPUTING: CLOUD COMPUTING, INTERNET OF THINGS AND COT

K.Swathi, Dr A.V.Krishna Prasad
Assistant Professor, Associate Professor
Computer Science and Engineering
G.PullaReddy Engineering College, Kurnool, India

***Abstract:** This paper gives insights into the most important existing problems of security and privacy of the Cloud Computing (CC), Internet of Things (IoT) and Cloud of Things (CoT) concepts especially confidentiality issue. With the evolution of ubiquitous computing, everything is connected everywhere, therefore these concepts have been widely studied in the literature. It can be noticed that the way we use technologies is changing, a dramatic transformation is shaping the world from isolated systems to ubiquitous Internet-based-enabled 'things'. These things are capable of communicating with each other by sending data which contain valuable information. However, this new world built on the basis of Internet, contains numerous challenges as regard to the security and the privacy perspective. To tackle this issue, researchers have been focused on various approaches enforcing security and privacy. In the present paper, risk factors and solutions regarding these technologies are reviewed then current and future trends are discussed.*

***Keywords:** Cloud Computing, Internet of Things, Cloud of things, security, privacy, confidentiality.*

I. INTRODUCTION

In recent years, due to the fast development of new and more efficient computing methods, the interest of academics and practitioners has been shifting toward Internet-based Computing. Commonly known applications are Internet of Things (IoT), Cloud Computing (CC) and Cloud of Things (CoT). After a number of technology variants have appeared over the years, we found a need to classify those that can help secure computing. As a matter of fact, there is no review on which solutions are described as regard to these three points of views (i.e. IoT, CC and CoT). Besides, thousands of users of IoT, CC and CoT are communicating with each other, sharing resources and exchanging high amount of sensitive data and information impose a great need of additional level of security especially to guaranty confidence in service providers as much as controlling the dissemination of personal data and to detect and eliminate vulnerabilities .Thus, in this article, the main challenges for privacy and security purposes are described along with an analyze of various constraints and the main techniques used to face one of them such as how to enable the users control over the dissemination of their attributes and data.

II. MOTIVATION

2.1 Internet of Things: The material objects that are set in with electronics, software, sensors, actuators and network connectivity that permit these objects to gather and exchange data is nothing but IOT. This allows objects to be controlled remotely via the connected network infrastructure and facilitates direct integration between the physical world and computer communication networks. Therefore, it significantly contributes to improve robustness, accuracy, efficiency, and economic profits. This is why IoT has been widely applied in different applications such as environment monitoring, energy management, building automation, transportation, etc.

Cloud Computing: CC is a new computational paradigm which provides a novel business model for companies/organizations to adopt IT without large investment. CC also provides a new vision of internet-based; highly performance distributed computing systems in which computational resources are given as a service. It is common to define the cloud computing model just as the United States National Institute of Standards and Technologies (NSIT) did it -"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services, that can be quickly provisioned and released with minimal management effort or service provider interaction." Two important aspects of the cloud model are Multi-tenancy and elasticity. The former allows the sharing of the same service instance with others tenants. Whereas the latter allows to scale up and down resources allocated to a service based on the current service demands. However, the improvement resource utilization, cost and service availability remains the target for both of them.

Cloud of Things: Over the last years, IoT and CC have evolved gradually and continuously. They represent two of the most regarded Information and Communications Technology (ICT) concepts. As mentioned in many recent works, those different concepts can be integrated in order to create a new one called Cloud of Things (CoT).Hence; CoT is a novel concept which has emerged from the consolidation of the IoT and CC concepts. Scientific estimations say that the IoT will grow to 35 billion items by 2020.Such growth will make IoT one of the principal sources of Big Data of which the specificities could be the volume, heterogeneity, velocity, complexity, and value. Cloud computing is a more mature technology compared to IoT. It can offer virtually unlimited capabilities (e.g., storage and computation) to support IoT services and application that can exploit the data produced from IoT devices. It is not surprising that in recent years, a number of new CoT concepts arose from IoT such as Sensing-as-a-Service, Video-Surveillance-as-a-Service, Big Data Analytics-as-a-Service, Data-as-a-Service, Sensor-as-a-Service, etc.

III. CHALLENGES

The IoT is thus a kind of an intelligent system using a variety of connected devices, sensors and monitoring applications that operate over the internet. It is defined as a pervasive and ubiquitous network that enables control of the physical environment by gathering, processing and analyzing a mass of data captured and generated by sensors or smart devices and transmitted to the internet through wireless communication systems (e.g. RFID, WiFi, 4G, and IEEE 802.15.x).

IoT is a many-folded paradigm which embraces many different technologies, services and standards. It adopts different processing and communication architectures, technologies and design methodologies organized on their target. The work reported mentions that the IoT concept has three basic characteristics: comprehensive awareness, reliable transmission and intelligent processing. Firstly in IoT system, the comprehensive awareness using RFID, sensors and M2M terminal is to get information of intelligent objects in the neighborhood over time. Secondly, reliable transmission is to guarantee in real-time the security, communication, routing and encryption with high accuracy and with different networks protocols. Thirdly, intelligent processing which depends on intelligent computing technologies such as CC, fuzzy recognition, aims to analyze and pick up meaningful data collected from lots of users.

The architecture of IOT system consists of three layer they are : perceptual layer, network layer and application layer. The perceptual layer, located in the lowest level of IoT model layout, includes wireless sensors, RFID and M2M terminal achieving a reliable sensing. The network layer involves different access methods (GSM, 3G, LTE, etc) and core exchange (IPv6, VPN, etc) of which the main task is to provide ubiquitous access, information transmission, processing and storage of the core business. The application layer analyzes and processes the received information to make good decisions. Due to the model layout, the mass of data, the different technologies, devices, the process management, the traffic, the distributed control, the constraints, the power, the energy and lifetime, a wide consensus is that the most challenging requirement is the security. Day after day the risk of malicious attacks grows. Hence, it is of critical importance to deal with security issues on IoT.

Cloud Computing provides four main categories of services such as Software as a Service SaaS, Platform as a Service PaaS, Network as a Service Naas and Infrastructure as a Service IaaS. Firstly, SaaS refers to the provider's applications used by the consumer and running on a cloud infrastructure (network, servers, operating systems, storage, etc.) and accessible from various clients devices at different locations. Secondly, Paas is providing a platform to build applications and services using programming languages, libraries, services and tools supported by the cloud provider. Thirdly, Naas, which can be heterogeneous, provides the virtual networks required by users. Finally, IaaS provides processing, computation, networks, and storage services on rental basis.

In CC two key issues have to be dealt with - computing and storage. It is common that the big amount of data is managed and stored in a data center. Therefore, it is impossible for the end user to find out where its data are geographically located. This means that people have no insights as to where their data are exactly stored. Besides, they don't know by who and how they are manipulated. Moreover, in CC there are several models, the private one, the public one and the hybrid cloud one. The privacy requirement touches black at different levels of each models. The public and hybrid cloud ones are accessible by all categories of users while the private clouds are controlled by an organization. Black Nowadays, trying to tackle the difficulties above automatically raises important problems such as the security and privacy.

The complexity of the IoT requires more efficient paradigms and solutions. Hence, the design of the new concept CoT is silently and gradually evolving with web computing since 2011. Therefore, it will be more data to store which will require more advanced technologies than conventional local or temporary storage. Black New concepts have to be offered on a fair and equal basis to end users; therefore, just like the rental of storage space, processing and computation must follow the same scheme - a rental basis. This has to be applied not only to the IoT platform but also to the CC and their integration black (CoT) while considering security and privacy.

IV. SECURITY AND PRIVACY ISSUES

The security is defined as a set of mechanisms to protect sensitive data from vulnerable attacks and to guarantee confidentiality, integrity and authenticity of data. The privacy is defined as the guaranty that users maintain control over their sensitive data. This section deals with the most issues of security and privacy in the different internet-based computing domains.

4.1. Internet of Things

Some of the main challenges for the application of the IoT encompass security issues. Those challenges will be mostly based on information security management systems as well as on legal foundations. When considering the legal framework of security and privacy of the IoT, it has to be determined which model of regulation should be applied.

Discussions of security for each level and for the movement of data between levels and also for each device or system connected constitute the object of many papers for few years ago. And is said that security must pervade the entire model in order to face different types of bullying. We find insecurity in Web as it is through internet access, inadequate verification, authorization, lacking confidence network services, lack of transport encryption, privacy concerns, insufficient security configurability, insecure software/firmware and poor physical security. In IoT and In terms of user privacy, the issues include the following: (a) control of personal data, (b) improvement of privacy technologies and the relevant regulations, (c) standards techniques and software's to manage the users and objects identity. In terms of confidentiality, some of the issues include the following: (a) the need for an easy to use exchange of critical, protected and confidential information and (b) confidentiality must be an integrated into the IoT design process. Lots of meta-data or temporary data required for the execution of services might be generated due to the management and processing of large quantities of data to guarantee useful information/service, confidentiality and integrity of data. These meta-data or temporary data could have the following characteristics: size, heterogeneity, etc. Application systems for IoT must provide efficient real time processing of data on demand (user requests).

4.2. Cloud Computing

Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. Some of the security concerns which arise in a cloud computing environment.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability

Sniffer attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there will be very important information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network. A malicious sniffing detection platform based on ARP (address resolution protocol) and RTT (round trip time) can be used to detect a sniffing system running on a network.

Reused IP address issue has been a big network security concern. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. Risks arises as the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not insignificant as the address still exists in the DNS cache and the data belonging to a particular user may become open to some other user violating the privacy of the original user.

In the cloud, the privacy means when users visit the sensitive data, the cloud services can prevent potential adversary from inferring the user’s behavior by the user’s visit model (not direct data leakage). Researchers have focused on insensible RAM (ORAM) technology. ORAM technology visits several copies of data to hide the real visiting aims of users. ORAM has been widely used in software protection and has been used in protecting the privacy in the cloud as a promising technology. Stefanov et al. proposed that a path ORAM algorithm is state-of-the-art implementation. The privacy issues differ according to different cloud scenarios and can be divided into four subcategories as follows: (i) how to enable users to have control over their data when the data is stored and processed in cloud and avoid stealing, wicked use, and unauthorized resale, (ii) how to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is an usual choice, and avoid data loss, leakage, and unauthorized modification or fabrication, (iii) which party is responsible for ensuring legal requirements for personal information, (iv) to what extent cloud subcontractors are involved in processing which can be properly identified, checked, and ascertained.

4.3. Cloud of Things

Security issues and challenges are said to be linked with these areas:

- Heterogeneity: caused by a variety of devices, operating systems, platforms, services available
- Performance of communications, computations and storage aspects
- Reliability is needed for mission critical application
- Big data can cause problems of transportation, storage, access and processing
- Monitoring

4.3.1. Privacy solutions

Confidentiality: To tackle some of different issues described above such as confidentiality, many techniques are developed. Various classifications exist in the literature. Basically, these classifications can be divided into two categories - techniques and methodologies. For the techniques:

Encryption: To ensure data confidentiality, the process consists on using a cryptographic solution to encrypt data stored in a cloud by either the data owner, by the cloud service provider or by both of them. This technique is seen as a good solution but it presents some limitations such as the twitter and Google incident in 2010.

Processing Encrypted Data: It’s a technique used to overcome the limitations of the previous one. It ensures privacy and confidentiality but cannot be applicable in practice because its specific processing behavior. The cloud service provider doesn’t need to decrypt data for query execution and can execute queries directly on encrypted data.

Obfuscation: it’ s a process of disseminating sensitive data before sending it to the cloud service provider using a secret key or method unknown by the latter. Comparing to encryption process the obfuscation is the weakest and it’s currently done by hand or semi-automated.

Anonymization: Consists on eliminating personally identifiable information PII from data record before sending it to the cloud provider. Then, it can process with real data and preserving privacy of data owners. This process can be failed when using a linking attack.

Sticky Policy: it allows “attaching privacy policies to data owners and driving access control decisions and policy en-forcement”. In, Trabelsi et al propose a privacy preserving solution as a service named SPACE and based on sticky policies. Trusted Platform Module. It is a hardware based solution that provides the ability to secure actions to protect user’s data secrets but it is not intended to perform secure data processing.

Data Segmentation: It consists on storing different segment of data in separate non-linkable fragments. It considers that private data is sensitive data and the association between data is also sensitive.

Trusted Third Party Mediator: It is a mediator between customer and cloud provider to guarantee and check policy enforcement and carry out an auditing. Finally, these techniques cope with the privacy problem.

4.3.2. Security Solutions:

The Cloud Computing systems uses the asymmetric or public key and private or traditional identity based cryptography that provides secure communication as the data flows through the internet. This work aims at improving cloud computing within Cloud Organizations with encryption awareness based on Elliptic Curve Cryptography.

To secure data, most systems use a combination of techniques, including:

- Encryption, which means they use a complex algorithm to encrypt the data. To decrypt the encrypted files, a user needs an encryption key. While it's possible to break encrypted information, most hackers don't have access to the amount of computer processing power they would need to decrypt information.
- Authentication processes, which require creating a user name and password.
- Authorization practices -- the client lists the people who are authorized to access information stored on the cloud system.

Elliptical curve cryptography (ECC) is an asymmetric key encryption technique used to create faster, smaller, and more proficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. ECC helps to create equivalent protection to the data with lower power consumption and battery usage, it is becoming widely used for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products.

A. Computation Point on the Curve: The security of ECC algorithm depends on its capability to calculate a new point on the curve given the product points and encrypt this point as in turn to be exchanged between the end users.

B. Choice of Field: As RSA public key cryptography is a secure asymmetric key cryptosystem, but its safety comes with a price of larger key sizes and computational power. Many researchers have looked for an alternative to this system with a smaller key size while maintaining the same level of security. The ECC technique is based on the perception of Elliptic Curves. To evaluate the time taken by an algorithm researches have introduced polynomial time algorithms and exponential time algorithms. Algorithms with smaller computation can be evaluated with polynomial time algorithms and complex computations can be evaluated with exponential time algorithms. The equation of an elliptic curve is given as,

$y2 = x3 + ax + b$

C. Key Generation: Key generation is an important part where an algorithm should generate both public key and private key. The sender will encode the message with receiver's public key and the receiver will decode its private key. Now, select a number, d within the range of n. Generate the public key using the following equation,

$Q = d * P$

Where d = the random number selected within the range of (1to n-1). P is the point on the curve, Q is the public key and d is the private key.

D. Encryption: Let 'm' be the message that has to be sent. Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 -(n-1)]. Two cipher texts will be generated let it be C1 and C2.

$C1 = k * P$

$C2 = M + (k * P)$

E. Decryption: Use the following equation to get back the original message 'm' that was sent.

$M = C2 - d * C1$

M is the original message that was sent.

Advantages of ECC over RSA

- In RSA Shorter keys are stronger than longer key size.
- Low on CPU consumption.
- Low on memory usage.
- Size of encrypted data is smaller.

In today's world ECC algorithm is used in case of key exchanges by certificate authority (CA) to share the public key certificates with end users. Elliptic Curve Cryptography is a safe and sound also more competent encryption algorithm than RSA as it uses smaller key sizes for same level of security as compared to RSA.

For e. g. a 256-bit ECC public key provides comparable security to a 3072-bit RSA public key. The endeavor of this work is providing an imminent use of ECC algorithm for data encryption before uploading the documents on to the cloud.

Public-key algorithms create a mechanism for distribution of keys among large numbers of participants or entities in a intricate information system. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms that are much more difficult to challenge at equivalent key lengths. Every participant in the public key cryptography will have a pair of keys, a public key and private key, used for encryption and decryption operations. Public key is distributed to all the participants where as private key is known to a particular participant only.

CONCLUSION

The Cloud Computing technology offers many possibilities, but also places several limitations as well. Cloud Computing refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. In this paper, we present a survey of Internet of Things, with an explanation of its operation and use. Moreover, we present the main features of the Cloud Computing and its trade offs. Cloud Computing refers to an infrastructure where both data storage and data processing happen outside of the mobile device. Also, the Internet of Things is a new technology which is growing rapidly in the field of telecommunications, and especially in the modern field of wireless telecommunications.

As the integration of Internet of Things and cloud could be observed that Cloud Computing can fill some gaps of IoT such the limited storage and applications over internet. Also, IoT can fill some gaps of Cloud Computing, Based in motivations such those referred previously and the important issue of security in both technologies we can consider some drivers for the integration. The security issue of this integration has a serious problem. When critical IoT applications move towards the Cloud Computing technology, concerns arise due to the lack of trust, privacy and confidentiality. Multi-tenancy could also compromise security and lead to sensitive information leakage. At the end, the security challenges of the integration of IoT and Cloud Computing were surveyed through the proposed algorithm model, and also there is a presentation of how the two encryption algorithms which were used contributes in the integration of IoT and Cloud Computing. This can be the field of future research on the integration of those two technologies. Regarding the rapid development of both technologies the security issue must be solved or reduced to a minimum in order to have a better integration model.

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques like RSA now in use. As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security.

REFERENCES

[1] Luigi Atzori, et al., The Internet of things: A survey, Comput. Netw. (54) (2010)2787–2805. 28/10/.
[2] Mohammad A. Alsmirat, Yaser Jararweh, Islam Obidat, Brij B. Gupta, and Internet of surveillance: a cloud supported large scale wireless surveillance system, J.Supercomput. (2016) Springer.
[3] Jiehan Zhou, et al. CloudThings: a common architecture for integrating the Internet of things with cloud computing, in: Huazhong University of Science and Technology, Wuhan, 2013.
[4] Moataz Soliman, et al. Smart Home: Integrating Internet of things with web services and cloud computing, in: 2013 IEEE International Conference on Cloud Computing Technology and Science, Oulu, 2013.
[5] Jayavardhana Gubbi, et al., Internet of things (IoT): A vision, architectural elements, and future directions, Future Gener. Comput. Syst. (2013) 1645–1660.24/02/.
[6] Mohammad Aazam, et al. Cloud of things: Integrating Internet of things and cloud computing and the issues involved, in: Proceedings of 2014 11thInternational Bhurban Conference on Applied Sciences & Technology, IBCAST, Islamabad, 2014.
[7] Mohammad Aazam, et al., Cloud of Things: Integration of IoT with Cloud Computing, Springer International Publishing, 2016, pp. 77–94. 01/01/.
[8] Elliptic curve cryptography, https://en.wikipedia.org/wiki/ Elliptic_curve_cryptograp hy
[9] RSA (algorithm), http://en.wikipedia.org/wiki/RSA_ (algorithm)
[10] Chakraborty, T.K.; Dhami, A.; Bansal, P.; Singh, T. "Enhanced public auditability & secure data storage in cloud computing". 3rd IEEE International Advance Computing Conference (IACC), 2013.
[11] W.Diffie and M. Hellman." New Directions in Cryptography". IEEE transactions on Information Theory. IT-22(1978).472- 492.
[12] William Stallings, "Cryptography and Network Security Principles and Practices", 4th edition, Pearson Education Inc, 2006.