ISSN Application ID: 13010

Global Journal of Computer and Internet Security

Volume No. 13

Issue No. 3

September - December 2025

ENRICHED PUBLICATIONS

ENRICHEDPUBLICATIONSPVT.LTD

S-9,IIndFLOOR,MLUPOCKET,
MANISHABHINAVPLAZA-II,ABOVEFEDERALBANK,
PLOTNO-5,SECTOR-5,DWARKA,NEWDELHI,INDIA-110075,
PHONE:-+(91)-(11)-47026006

ISSN Application ID: 13010

Global Journal of Computer and Internet Security

Aims and Scope

The Journal of Computer and Internet Security presents research and development results of lasting significance in the theory, design, implementation, analysis, and application of secure computer systems. It also provides a forum for ideas about the meaning and implications of security and privacy, particularly those with important consequences for the technical community.

ISSN Application ID: 13010

Global Journal of Computer and Internet Security

(Volume No. 13, Issue No. 3, September - December 2025)

Contents

ISSN Application ID: 13010

Virtualization Security Management

Ashima Narang
Computer Science Department, Amity University, India.

ABSTRACT

Cloud computing is turning out to be the key component in the future of internet. And, Virtualization is the term that refers to the abstraction of the resources mainly the computer resources. The resource utilization can be improved with the help of virtualization. This provides integration to the platform of the user and aggregation to the heterogeneous resources and the autonomous behaviour of the resources. Here in this paper, the review of virtualization, its security and the performance is discussed.

KEYWORDS - *Virtualization, Cloud Computing, Security, Network Virtualization*

1. INTRODUCTION

Cloud Computing can be classified as a new paradigm for dynamic provisioning computer services supported by data centres that usually employ virtual machine (VM) technology for consolidation[1]. Cloud computing provides infrastructure, platform and software as services that is available to the consumer under the pay as you use model. The technology named virtualization is being used by the clouds to provide the resources to the customer whenever required. Clouds are provided to the customers for giving them three models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a- Service (IaaS). As commercial activities used over the internet we can already see the cloud such as Amazon EC2 [1] , Google Apps [2] and Force.com [3].

Generally, Cloud is said to be a service provider and so Cloud is discussed in terms of services. Cloud is an area which has gained attention both from the industry and from the academia. From the research areas of Service oriented architecture and the virtualization which can be combined to get a computing paradigm where the resources in the architecture of computing are provided as a service over the internet. There are various different problems faced by Cloud computing may it be the emerging topic of research these days. Security of the data is the biggest problem being faced in cloud.

The storage of the data or the sensitive information on the servers of the cloud has become a major issue. The commercial providers which are mostly outside the trusted domains of the users and the clients. The confidential data desired frequently when the outsourced data is desired by the user to store in the cloud. It also turns out to be a juristic concern along with confidentiality and it cannot be solves easily. This raises a big issue. With the help of virtualization technology, multi tenancy is possible, but this further raises to different problems such as the storage of the data physically or the protection of the data in the same virtual environment as the other parties are also using the same environment. May be this is the reason that majority of the users think that cloud is not a secure network to store the data in. [4]

Cloud Computing has widely been adopted by the industry or organization though there are many existing issues like Load Balancing, Virtual Machine Consolidation, Energy Management, etc. which have not been fully implemented. Central to these issues is the issue of load balancing, that is required to distribute the excess dynamic local workload equally to all the nodes in the whole Cloud to achieve a high user satisfaction [2]. Data mining is another concept which uses Cloud Computing with virtualization. [9][10]

The virtual machines are exposed to many kinds of filtering assuring the security at a high degree. So, the virtualization is being used for the security component. Security in Cloud has many different instances. In this paper, we may discuss only about the virtualization security management. The ways how we can manage the security vulnerabilities in virtualization and various virtual system security issues. There are different options how we can manage the security of the data while the virtualization of the resources is being done.

2. SECURITY MANAGEMENT IN VIRTUALIZATION

A. Migration management

VM migration is easy to attack and is a vulnerable process. Special security mechanisms should be applied when a VM is migrated from a place to somewhere else. It sounds an easy process but it is not. When any of the organization or an enterprise tries to use any of the automated tool such as live migration there are many other factors which creep in. While we run two different VMs on a single machine may cause violation to Payment Card Industry (PCI). This problem occurs when The VM can be located with the customer's credit card data on the same physical machine with the public accessibility web server. So, to analyze the physical servers for security and compliance postures should be done to provide the security to the sensitive data of the users. The governed live migration can also violate the policies of the corporate if the migration does not go through A strict IT infrastructure

Library process for the approval by a change approval board or configuration management system. The Migration management system is necessary for the virtualization security and it should be planned. If the migration is not planned then It may even cause the issues with resources outside the environment which may further introduce database contention or overload of network device or the delays in I/O storage which may not be expected.[4]

B. VM Image Management

VM Image (VMI) is a type of file or the format of the data which is used to create the virtual machine in the environment of virtualization. Hence, the confidential data and the integrity of VMIs is very important when the VMs are migrating or its starting.

C. Patch Management

Patch management is acquiring, installing or testing of system management or inserting a code changes to the computer system administration. It also includes on the available patches of the maintaining current knowledge ensuring the patches are installed properly and after installing test them and lastly documenting all the procedures associated and all the configurations required.

To identify and test the various types of code changes, the patch management is built. Patch management also extends the monitoring of the functions of the code to identify any of the circumstances that may emerge in the phase of testing. It helps the programming of the function code much more efficient. Efficient patch management also decreases the possibility of attacking at the VM level. In the virtual environment the distribution of patches to the VMs is a key issue.

D. Audit

In the lifecycle of the Virtual machines, the sensitive data and the behavior of the virtual machines should be monitored throughout the virtual system. This may be done with auditing which provides the mechanism to check the traces of the activities left by the virtual system.

To monitor the virtual machine behavior and the sensitive data whether it operates the virtual system well in a safe manner, we audit. We can get the destruction reasons of the system and data easily from the records, if we regularly log all the activities left by the virtual system. This helps when the destruction of any type of data happens. The required strategies can be developed against the harmful results on the basis of these records.[4]

3. CONCLUSION

Cloud computing as of now we know that it refers to the sustained storage and the advanced sharing of data over the internet. But, the threats from the security is embedded in cloud computing approach is proportional to the offered advantages directly. In this framework, the security can be achieved using the various methods given for the security management. It helps in virtual environment to achieve the security of the sensitive data. Also, it allows the users to store the data privately as per the requirement. Various methods for computation and strategies in cloud computing for different functioning are elaborated. Every person who accesses the internet does not use the applications of cloud properly so that the use of cloud can be efficient. This is because of the threats to the entire concept of Cloud computing and its security which creates the doubt in user's mind to use and rely upon the services being provided. Security issues may be of any kind. There are new security techniques being added to the list of different techniques already being used to reduce the risks in cloud. But still there are many more hindrances and computational problems that are and might occur today or in the coming future. The work has to be done in order to support cloud computing and virtualization and also understanding the challenges regarding security issues in cloud.

REFERENCES

1. Amazon:AmazonWebServices,http://aws.amazon.com/
2. Google,GoogleApps,http://www.google.com/apps/intl/en/business/index
3. Salesforce.com,Force.com,http://www.salesforce.com/platform/
4. Shengmei Luo, "Virtualization security for cloud computing service", IEEE- International conference on Cloud and service computing, 2011, Pg 174- 179.
5. Ashima Narang, "A review-Cloud and cloud security" , International journal of Computer Science and mobile Computing, Vol 6 Issue 1, January, 2017, Pg 178-181
6. Karanpreet Kaur, Ashima Narang and Kuldeep Kaur, " Load Balancing Techniques in Cloud Computing", IJMCR,2013.
7. R. Yamini, "Power Management In Cloud Computing Using Green Algorithm", IEEE- International Conference On Advances In Engineering, Science And Management (ICAESM- 2012), March 30, 31,2012,Pg. 128-133.
8. Ashima Narang, Vijay Laxmi "Various Load balancing techniques in Cloud Computing", International journal of Computer Science and Mobile Computing , December 2014, pg 502-509
9. Sonamdeep , Sarika Chaudhary, " A survey- Clustering Algorithms in Data Mining", International Journal of Computer Applications, 2015
10. S Malik, S Chaudhary, " comparative study of decision tree algorithm in food data Analysis", International Journal of research in Computer Engineering and Electronics, 2013.

Challenges On Security Attacks In Wireless Sensor Network: An Assessment

Meena Chaudhary[1]**& Dr. Rajeev Kumar** [2]

Department of Computer Science and Engineering

[1,2]Sri Venkateshwara University, Gajaraula (Amroha), U.P. India

ABSTRACT

A remote sensor organize (WSN) has imperative applications, for example, remote natural checking and target following. This has been empowered by the accessibility, especially inrecent years, of sensors that are littler, less expensive, and shrewd. These sensors are furnished with remote interfaces with which they can speak with each other to shape a system. In this paper we manage the security of the remote sensor systems. Gazing with a short review of the sensor arranges, and talks about the present condition of the security assaults in WSNs. Different sorts of assaults are examined and their countermeasures exhibited. A concise talk on the future heading of research in WSN security is additionally included

Keywords: *Wireless Sensor Networks (WSNs), Attacks, Security, Threats.*

1. INTRODUCTION

Remote sensor systems (WSNs) are inventive extensive scale remote systems that comprise of dispersed, self-governing, low-control, minimal effort, little size gadgets utilizing sensors to agreeably gather data through infrastructure less specially appointed remote system. The improvement of remote sensor systems was initially propelled by military applications, for example, war zone observation. Notwithstanding, remote sensor systems are currently utilized as a part of numerous regular citizen application ranges, including condition and natural surroundings checking, medicinal services applications, home computerization, and activity control. Security assumes a major part in numerous remote sensor arrange applications.

Since sensor systems posture interesting difficulties, security procedures utilized as a part of routine systems can't be straightforwardly connected to WSNs due to its extraordinary attributes. To start with, sensor hubs are extremely delicate of creation cost since sensor systems comprise of an extensive number of sensor hubs. [1] Contended that the cost of a sensor hub ought to be considerably less than one dollar all together for sensor systems to be doable. In this way, most sensor hubs are asset controlled as far as vitality, memory, calculation, and correspondence capacities. Typically sensor hubs are fueled by batteries, and reviving batteries are infeasible much of the time. Vitality utilization turns into a key thought for most sensor system conventions [2].

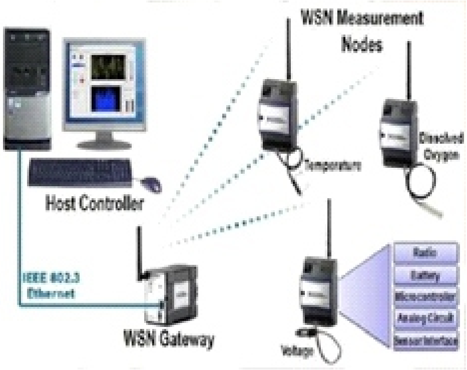

Figure 1: Common Wireless Sensor Network Architecture

2. CONSTRAINTS IN WIRELESS SENSOR NETWORKS

A remote sensor arrange comprises of a substantial number of sensor hubs which are intrinsically asset obliged. These hubs have restricted handling ability, low stockpiling limit, and compelled correspondence transfer speed. These constraints are because of restricted vitality and physical size of the sensor hubs. Because of these requirements [3],a portion of the real imperatives of a WSN are recorded underneath.

Energy constraints: Vitality is the greatest limitation for a WSN. When all is said in done, vitality utilization in sensor hubs can be ordered in three sections:

(I) energy for the sensor transducer,
(ii) energy for correspondence among sensor hubs, and
(iii) Energy for chip calculation.

3. SECURITY REQUIREMENTS

The objective of security administrations in WSNs is to shield the data and assets from assaults and rowdiness [4]. The security requirements in WSNs include:

- Availability, which guarantees that the fancied system administrations are accessible even within the sight of denialof- administration assaults
- Authorization, which guarantees that exclusive approved sensors can be included in giving data to network administrations

- Authentication, which ensures that the correspondence beginning with one center point then onto the following center point is true blue, that is, a malevolent center can't go up against the presence of a put stock in framework center point
- Confidentiality, which ensures that a given message can't be fathomed by anyone other than the needed recipients
- Integrity, which ensures that a message sent beginning with one center then onto the following is not changed by pernicious transitional centers

4. SECURITY GOALS

Wireless sensor systems are helpless against many assaults in view of communicate nature of transmission medium, asset constraint on sensor hubs and uncontrolled conditions where they are left unattended. Like other correspondence frameworks [5], WSNs have the following general security goals:

- Confidentiality: shielding mystery data from unapproved elements
- Integrity: guaranteeing message has not been changed by malevolent hubs - Data Origin Authentication: confirming the wellspring of message;
- -Entity Authentication: verifying the client/hub/base - station is for sure the substance whom it cases to be
- Efficiency: stockpiling, taking care of and correspondence requirements on sensor center points must be considered

5. CHALLENGES

Providing efficient data aggregation while preserving data privacy and integrity is a challenging problem in wireless sensor networks due to the following factors:

1. Trust administration in WSN is extremely testing. Clients in the remote sensor systems can be exceptionally inquisitive to take in others' private data, and the correspondence is over open available remote connections, subsequently the information gathering is helpless against assaults which undermine the security [6]. Without legitimate assurance of security, the correspondence of privacy sensitive information over nonmilitary personnel remote sensor systems is viewed as unrealistic.

2. During in-system collection, enemies can without much of a stretch adjust the halfway conglomeration result and make the last total outcome veer off from the genuine esteem extraordinarily. Without assurance of information trustworthiness [7], the information accumulation result is not dependable.

3. Data accumulation over remote sensor systems does not depend on committed foundation. Much of the time, the quantity of hubs noting an inquiry is obscure before the information accumulation is directed.

6. CONCLUSION

Security is turning into a noteworthy sympathy toward vitality obliged remote sensor arrange due to the expansive security-basic uses of WSNs. Therefore, security in WSNs has pulled in a great deal of consideration in the current years. The remarkable components of WSNs make it exceptionally difficult to plan solid security conventions while as yet keeping up low overheads. In this paper, we present sensor arranges, its related security issues, dangers, dangers and attributes. Arrange security for WSNs is still an exceptionally productive research bearing to be further investigated.

REFERENCES

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A review on sensor frameworks. IEEE Communications Magazine, 40(8):102– 114, 2002.
2. Wireless sensor masterminds: an outline I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci*
3. J. Slant, R. Szewczyk, A. Beguile, S. Hollar, D.E. Culler, and K. Pister, " Structure plan headings for masterminded sensors", In Proceedings of the ninth International Conference on Architectural Support for Programming Languages and Operating Systems, New York, ACM Press, 2000, pp. 93-104.
4. S. Slijepcevic, M. Potkonjak, V. Tsiatsis,
S. Zimbeck, and M.B. Srivastava, "On correspondence security in remote off the cuff sensor frameworks" , In Proceedings of eleventh IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), 2002, pp. 139-144.
5. L. Yuan and G. Qu, "Arrange space examination for essentialness beneficial secure sensor frameworks", In Proceedings of IEEE International Conference on ApplicationSpecific Systems, Architectures, and Processors, July 2002, pp. 88-100.
6. http://ww .xbow.com/wireless_home. aspx, 2006.
7. A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, and J.D. Tygar,"SPINS: Security traditionsfor sensor frameworks", WirelessNetworks, Vol.8 , No. 5, pp. 521-534, September 2002.

ISSN Application ID: 13010

STUDY OF SECURE DATA TRANSMISSION IN WSN: A PRACTICAL APPROACH

Anu Chaudhary[1], Dr. Rajeev Kumar [2]

Department of Computer Science and Engineering

[1,2]Sri Venkateshwara University, Gajaraula (Amroha), U.P. India

ABSTRACT

In light of the remote method for Sensor framework, secure data transmission beginning with one center point then onto the following center point is transforms into a noteworthy issue for remote correspondence. The remote framework progressions are powerfully grabbing thought.For various circumstances there are diverse applications are grow, for example, watching, control and following application. For these systems, camera sensor can repossess graphical insights from a controlled field, expected that vital data for various applications. Such systems have assets constraints to taking care of, capacity, and vitality and transmission data transfer capacity, eminent many plan tests. Due this the remote sensor arranges needs exceptionally secure correspondence channel to utilize them being in open field and broadcasting innovation. In this paper to guarantee the security to the different applications we will utilize cryptographic framework. We will propose a framework to safely transmit provenance for sensor information. We will present successful strategy for provenance information confirmation. We will layout the new structure system intentionally and tentatively, and the results exhibit its support and gainful for secure provenance encoding and unraveling.

Keywords-Wireless sensor network, cryptography

1. INTRODUCTION

The innovation of remote sensor hub is outstanding innovation in light of its notoriety. An extensive number of self-deal with sensor centers are spatially circled autonomous sensor to screen physical or biological conditions, for example, temperature, sound, weight, and so on the remote sensor system is worked of "hub" – from a couple to a few hundred or more, where every hub is associated with another sensor. There are a few parts for every sensor organize hub: an inside receiving wire of radio handset or outside reception apparatus association, a microcontroller, in electronic Way with sensors and vitality source interfacing, require a battery. The mind boggling calculation can't be played over it, since hubs have not all that well off as far as assets. Henceforth security turns into a major issue in remote sensor arrange.

To safely transmit the different sort of data over system a few unique calculations cryptographic, steganography and different methods are utilized. In this paper we examine the system security basics and how cryptography procedure is implied for remote sensor systems [1].

A sensor system is a framework included detecting (measuring), processing, and correspondence components that gives an executive the capacity to instrument, watch, and respond to occasions and wonders in a predetermined domain . The executive ordinarily is a common, administrative, business, or a mechanical element. The calculation and correspondence foundation are related with the sensor frameworks which is as often as possible specific to the earth and set up in the contraption and application-based nature of these frameworks. For example, not in any manner like the most unique settings, in- framework dealing with is appealing in the sensor frameworks; also, center point control (and moreover battery life) is a key blueprint thought [2].

Sensors in a WSN have an assortment of the reasons, capacities, and abilities. The field is currently progressing under the push of the current innovative advances and the draw of a bunch of potential applications. The radar systems utilized as a part of the aviation authority, the national electrical power lattice, and the across the nation climate stations sent over a normal topographic work are all cases of early-sending sensor arranges; these frameworks, be that as it may, utilize specific PCs and correspondence conventions and thusly, are extremely costly [3].

2. SECURITY OF DATA TRANSMISSION IN SYSTEM

Security of system transactions is seemingly the most vital issue on the planet today given the limitless measure of important data that is passed around in different systems. As we presumably am mindful the information identifying with the banks, charge cards, individual unpretentious components, and the organization courses of action are traded from place to put with the help of frameworks administration foundation.

The openness on WWW has brought about the different systems being subjected to diverse assaults from incomprehensibly divergent sources. Sensor hubs regularly sense theinformation bundles and exchange it to the base station by means of some transitional sensor hubs. There are two Types of the information transmission in the remote sensor orchestrate, these are – facilitate transmission and multi-hop data transmission. A typical method for the security which is used to shield the data from falling into the wrong hands is encryption.

3. REMOTE SENSOR SYSTEM FOR DATA TRANSMISSION SYSTEM

Remote sensor systems comprise of numerous little minimal gadgets, furnished with sensors (for instance acoustic, seismic or picture sensors), that frame a remote system. Every sensor hub in the system gathers thedata from its environment, and sends it to the base station, either from sensor hub to sensor hub i.e. multi bounce, or specifically to a base station i.e. single jump [5]. A remote sensor system may comprise of the hundreds or up to a huge number of the sensor hubs and can be spread out as a mass or put out one by one.

The sensor hubs team up with each other over a remote media for setting up a detecting system. In perspective of the conceivably considerable size of the remote sensor composes, each individual sensor center point must be nearly nothing and of the insignificant exertion. The openness of the straightforwardness sensor center points has realized the change of various other potential application regions, e.g. to screen the significant or adversarial fields, forests, houses, lakes, oceans, and procedures in ventures. The sensor system can give access to data by gathering, handling, breaking down and circulating information from the earth [6]. In numerous application territories the remote sensor arrange must have the capacity to work for the drawn out stretches of time, and the unwavering quality and additionally security of transmitting information is vital. The mystery sharing-based multipath directing issue as an Owing to the few issues for the most part relating to the key administration, the hypothetical onetime cushion has been difficult to actualize for all intents and purposes. Various endeavors have been made yet under the changing suppositions and conditions. A standout amongst the latest has been clarified in [7] where one-time cushions are utilized to secure the Visa utilization on the Internet. It has been battled that the unlimited security can be obtained before long using the non-information-theoretically secure procedures. This approach keeps up that in the even minded world, nobody can gain complete information about a system owing to certifiable parameters like disturbance.

The disjoint multipath directing plan with the mystery sharing is broadly perceived as one of the viable steering systems to guarantee the wellbeing of the data. This sort of plan changes every information bundle into the few shares to improve the security of transmission. A three- stage disjoint directing plan which is called Security and Energy-proficient Disjoint Route (SEDR) is proposed. In light of the secret sharing figuring, the SEDR plot dispersive and self- assertively passes on the shares wherever all through the framework in the underlying two phases and after that transmits these shares to the sink center point.

Think about on security of remote sensor arrange, in this day and age remote innovation quick created and generally utilized as a part of numerous segments. Thus, the need for security turns out to be exceptionally essential element. However, the remote system innovation has some confinement, for example, restricted battery control, preparing capacity, and limit of memory stockpiling, and so forth. For this obliges, numerous new security system and innovations have been create to beat this difficulties. There are numerous innovations are accessible to give security against the assailants, one of the best innovation is cryptography.

They concentrate on various issue in remote sensor arrange. Likewise ponder on various conceivable assaults on WSN. In paper "Condition Based Secure Transfer of Data in Wireless Sensor Networks", chat on the security in change. In recent years absence of data is spread starting with one place then onto the next consequently it is imperative that the information ought to exchange safely without information misfortune.

4. CONCLUSION

Confide in WSNs is as yet difficult field because of its dynamic nature. Be that as it may it is an extremely remunerating range as the greater part of the WSN applications are conveyed in antagonistic situations, for example, military fields. The TDES calculation can give high security to change of information. The TDES calculation gives fast execution extremely reduced equipment usage. TDES has preferable execution over DES. The electronic business utilizes Triple DES to secure client substance and framework information. Also mysteries key, for example, passwords is should have been secured in PC frameworks for a long time. Their utilization in encryption leaves assets helpless against disconnected assault. Nectar encryption can offer profitable extra security in such situations. Nectar encryption gives security against Brute-Force assault.

REFERENCES

[1] *SalminSultana,GabrielGhinita, Member, IEEE, Elisa Bertino, Fellow, IEEE, and Mohamed Shehab, Member, IEEE " Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks,"IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTIN VOL. 6, NO. 1, JANUARY 2015*

[2] Mahfuzulhoq Chowdhury1, MdFazlul Kader2 and Asaduzzaman1 " Security Issues in Wireless Sensor Networks: A Survey,"International Journal of Future Generation Communication and Networking Vol.6, No.5 (2013), pp.97-116

[3] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani " New Comparative Study Between DES, 3DES and AESwithin Nine Factors,"JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617

[4] Mrs. B. Vidhya1, Mrs. Mary Joseph2, Mr. D. Rajini Girinath3, Ms. A. Malathi4 " Condition BASED SECURE TRANSFER OF DATA IN WIRELESS SENSOR NETWORKS" , International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1,February 2015

[5] [Mandeep Singh, NarulaSimarpreet Singh " Execution of Triple Data Encryption Standard utilizing Verilog" , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014 ISSN: 2277 128X

[6] Ari Juels, Thomas Ristenpart "Nectar Encryption: Security Beyond the Brute-Force Bound," University of Wisconsin, January 29, 2014Version 1.1

[7] AmitDhir "Information Encryption utilizing DES/Triple-DES Functionality in Spartan-II FPGAs," White Paper.

ISSN Application ID: 13010

Need and Challenges for Software Engineering in Pervasive Computing

Gurmeet Kaur,
Assistant Professor, Dyal Singh College, Karnal

ABSTRACT

Moving away from decades of machine- centric computing and designing pervasive human- centric computing, the new wave of computing, a reality revolutionizes the relationship between humans and computing systems. The growing interest in the use of context-awareness as a technique for developing pervasive computing applications that are flexible, adaptable, and capable of acting autonomously on behalf of users. In order to implement the vision of pervasive human-centric computing, it is necessary to reform software engineering education to well prepare graduates of software engineering programmes for the new opportunities and challenges of software engineering in the pervasive computing era. The software challenges to turn such pervasive or ubiquitous computing environments into reality are enormous, to say nothing of software , hardware and social challenges. In this paper, we review some of the work of software components and analyze where our solutions are lacking and must be adapted for pervasive computing..

1. INTRODUCTION

It is widely acknowledged that pervasive computing introduces a radically new set of design challenges as compared with traditional desktop computing. In particular, pervasive computing demands applications that are capable of operating in highly dynamic environments and of placing minimal demands on user attention. late Michael Dertouzos, Director of the MIT Laboratory (1974-2001) for Computer Science, who pioneered MIT Project Oxygen to make pervasive human-centric computing a reality, pointed out the need for pervasive computing. He stated the following:

If computers are to live up to the promise of serving us, they will have to change drastically and never again subject us to the infuriate experiences we all have shared [1].

It is envisioned that pervasive computing systems will help people to achieve more while doing less. These systems will:

- Understand user when he speak to them;
- Do much of our routine brainwork for user;
- Get us the information for user when and where we want it;
- Help us work with other people across space and time;
- Adapt on their own to our individual needs and desires [1].

In the pervasive computing era, there will not need to carry our own physical devices with us any more. Instead, configurable generic devices, either embedded or handheld in the environment, will bring computation to user, whenever he need it and wherever he might be. As user interact with these *anonymous* devices, they will adopt our information personalities. They will respect our desires for security and privacy. The user need not have to type click, or learn new computer jargon. Instead, he will communicate naturally, using gestures and speech that describe user intent (*send this to Soni* or *print that picture on the nearest colour printer*), and leave it to the computer to carry out our will [2].

Pervasive human-centric computing systems will change how businesses, organizations and governments work with each other, as well as how individuals interact. It represents the dawn of a new era in Information Technology (IT) [1].

To shift the focus of computing from machines to humans, major changes are required not only in technologies and systems, but also in the approach to deploying , developing and managing technologies and systems. Weiser presented his vision for pervasive human centric computing in 1991. He further articulated his vision as follows:

There is more information available at our finger tips during a walk in the woods than in any computer system, yet people find a walk among trees relaxing and computers frustrating. Machines that fit the human domain instead of forcing humans to enter theirs will make using a computer asrefreshing as taking a walk in the woods
[4][3].

2. Motivation

Challenges which are based on natural characteristics of pervasive computing systems (i.e. dynamism , mobility, and heterogeneity) can be evaluated from a more domain specific perspective, that is, e-learning in our case. E learning refers learning which uses muliple technologies such as internet, television etc. in a manner pointed out by [5]:e-enhancements of models of learning. That is to say that; using technology to achieve better learning outcomes, or a more effective assessment of these outcomes, or a more cost-efficient way of bringing learning environment to the learners [5].

Hence, we particularly list following basic interrelated requirements for such pervasive learning environments:

(1) Device Independence: Applications and data should be always accessible without any dependence on device

(2) Application Independence: Data should be always accessible without any application dependence,

(3) Adaptivity and Adaptability: Learning environment and elements of this environment should dynamically adapt according to context of learner(s) and users should be able to configure such environments such as composing/decomposing applications and data

(4) Collective Operation: Applications in such domain must be able to collectively operate for the benefit of users in a seamless manner. Adaptivity is long studied both in adaptive web systems and adaptive e-learning systems [6], and in such systems adaptivity is generally considered as an aspect between user and application based on user profiles and models.

Pervasive human-centric computing systems are dedicated systems that are capable of sensing, measuring, monitoring, predicting and reacting to physical world conditions. To support a wide range of human activities, pervasive human-centric computing systems must be:

Pervasive: Should be available everywhere and accessing the same information base through every portal .

Nomadic: Allowing users and computations to move around freely to meet the users' needs;

Embedded: Sensing and affecting the physical world;

Adaptable: Providing flexibility and spontaneity in response to changes in the operating conditions and user's requirements ;

Intentional: Enabling people to name services and software objects by intent;

Powerful yet efficient: Freeing itself from restriction imposed by bounded hardware resources, addressing system constraints imposed by user demands and available power or communication bandwidth;

Eternal: Never requiring shut down or reboot while components are added or removed in response to errors ,demands, or upgrades [2].

In a pervasive computing environment, user and perceptual technologies will directly address human needs and consist of the following:

Knowledge Access Technologies: Offering vastly improved access to information and customized to the needs of users (ie people, applications and software systems);

Collaboration Technologies: Enabling the formation of spontaneous collaborative regions that `accommodate the needs of mobile people and computations, and also provide support for recording and archiving video and speech fragments from a variety of sources and/or events;

Perceptual Technologies like Speech and Vision Technologies: Enabling communication with devices, networks and software to extend the range of user technologies delivered to all places.

Automation Technologies: Offering Natural, easyto-use, customisable and adaptive mechanisms for automating and tuning repetitive information and control tasks;

3.Context Aware Pervsive Computing

Context aware computing aims to enable device to provide better service for people through applying available context information [7].

Above a generic definition of context aware computing is given, which emphasizes the relation between user, context and computing, but how do one apply available context information? Although multiple categorizations for context-aware systems are already given [8], one can prefer to re-interpret these categorizations based on adaptive systems, particularly according to adaptive web systems. This is because one can defined adaptivity as a key factor of intelligence and as a key relation between context and computing for context-aware computing systems. Therefore by referring to [8] and the field of adaptive web [6] for categorization of context aware computing applications, we propose below categorization:

(1) Context Based Filtering and Recommendation of Services and Information: Examples might include accessing the history of a nearby object , finding the nearest printer etc.,

(2) Context Based Service and Information Searching: e.g. location aware query rewriting for a search for available restaurants (query rewriting is a technique used in adaptive web systems for information filtering by rewriting a user query according to the user profiles) etc.,

(3) Context Based Presentation and Access of Information and Services: e.g. selecting voice when screen displays are not available (multimodal information presentation and user interfaces), dynamic user interfaces etc.,

(4) Context Adaptive Navigation and Task Sequencing: Adaptive navigation is a technique employed in adaptive web systems. The user can extend this idea in pervasive computing since a user's interaction might consist of multiple related sub-tasks in relation with his goals and might lead to context aware task sequencing,

(5) Context Based Application and Services Modification/Configuration : This need mainly arises from varity of devices available in the environment, e.g. disabling particular features depending on the capabilities of target device,

(6) Context Based Resource Allocation: This might include allocating physical recourses (e.g. memory, even non-hardware physical resources) for the use of other entities in the setting (e.g. , users , applications etc.).

(7) Context Based Actions: [9] Proposes three levels of context dependent automatic actions: manual, semi- automatic, [10] and notes that fully automatic actions based on context are rarely useful, and incorrect actions can be frustrating.

It is worth to note that, adaptive behaviors of context aware systems are not necessarily need to depend on the present context, rather such systems should also be able to adapt dedicately by making use of present context or historical context to predict future context of the setting. An example is given in [11] where a user walks through the building and submits a printing request, the selected printer should not depend on the user's current location but rather to his final destination. According to presented categorizations and elaborations, we extend previous definition of context-aware systems as follows:

Context aware computing aims to enable better service delivery through proactively adapting access,use, structure and behavior of information, applications, services and physical resources with respect to available context information.

An up-to-date and specific example is a famous social networking website, Facebook. This web application provides users with the contextual information of their network (by means of notifications) like who watches, reads what or who becomes friend with whom. In this way users can identify people with similar likes and arrange their own environment accordingly. Such case is also of use in the domain of e-learning, a system can provide users with the contextual information of the environment and other learners like who read what, who knows what, who takes the same courses or who works on the same problem, so learners can find appropriate mentors or construct a learning path for themselves. Such approach might be called as —environment awareness" for users which is counterpart of context- awareness for machines.

4. Strategies for Software Engineering Challenge in Pervasive Computing

As we know that to achieve real life application of pervasive computing is challenging task. To implement this a lot of challenges have to resolved for software engg. discipline and software component. The suggested core strategies for software engineering education reform include the following:

1. Redesign of software engineering curricula by integrating pervasive human-centric computing and autonomic computing into the curricula;

2.Systematic integration of applied and experimental research in software engineering for pervasive human- centric computing into software engineering education;

3. Industry-academic partnerships in both research and education;

4. Engaging students in cross-disciplinary research and development;

5. Institutional support and funding for cross disciplinary collaborations in research and education;

6. Fostering life-long learning;

7. Systematic updating of the contents and structure of software engineering curricula.

It is necessary to restructure software engineering curricula by integrating pervasive human-centric computing and autonomic computing into the curricula [12][13][14].

The rapidly evolving and multidisciplinary nature of pervasive human-centric computing and autonomic computing requires the systematic integration of appliedand experimental research into software engineering education to enhance students' learning experiences. Engaging software engineering students in applied and experimental research helps them to acquire invaluable experience that they cannot gain by simply reading technical articles and attending lectures.

To further enhance students' learning experiences, it is crucial to develop and nurture industry-university partnerships in research and education. This will also help students to work with industry sponsors while enhancing their hands-on experiences, as well as their technical competences and skills [12][13][14-18].

Furthermore, the multidisciplinary nature of pervasive computing requires collaborations in educational and research activities among field experts from different areas, as explained in earlier parts of this article. Hence, it is essential for engineering educational institutions to foster cross disciplinary collaborations in research and education so that students can engage in collaborative, multidisciplinary projects with faculty and other field experts and professionals across various fields from universities, industry and research organizations. This will also help students to enhance and learn their engineering knowledge and skills, as well as their professional skills (e.g. teamwork, written and verbal communications, etc).

Collaborative multidisciplinary projects require extra efforts to ensure effective and productive cooperation among all the people involved. Thus, it is critically important to change the culture, funding structure and faculty performance evaluation system in academia to provide the necessary institutional support and funding for cross-disciplinary collaborations among faculty from different departments, colleges, and universities, and other researchers from industry and non-academic institutions.

Due to the nature of software engineering for pervasive computing and autonomic computing, software engineers need to be strongly committed to life-long learning and regularly update their technical knowledge, competences and skills. To help graduates become self- motivated and life-long learners, it is crucial to provide students with opportunities to acquire both the awareness of the necessity of life-long learning and the knowledge, skills and abilities to engage in life-long learning.In order to ensure that software engineering educational programmers provide the best learning opportunities for students, it is crucial to maintain the flexibility of software engineering curricula, and to update systematically the contents and structure of the curricula.

4.1 Software components for pervasive computing

The pervasive computing environment drive us to face the need for components and their boundaries more clearly. Pervasive services will have to be composed from individual ―components‖ residing in the large number of heterogeneous computing elements. The hardware domain itself will drive a natural boundary between components. This may be the most clear-cut definition of a component. A component will be an independently deployable piece of software that resides on one hardware component and provides a service element heterogeneity

The most striking characteristics of software components in the pervasive computing environment are the need to deal with heterogeneity and the need for dynamic (ad hoc) adaptation to, and interaction with, communicating components. Current component models are homogeneous in the kind of components for example, JavaBeans components are for desktop environments while Enterprise JavaBeans are for server and enterprise- wide components. To make application evelopment manageable, we probably need a single component model that is ―scalable‖ in the sense that it supports the development of components of various granularity, components that can reside in tiny computing elements. [Jazayeri95]. While language-specific components are still important, the pervasive environment requires us to also deal with heterogeneous components. The work of Johann Oberleitner [Oberleitner01] deals with the heterogeneity of component models. He has designed and built the Vienna Component Framework (VCF) that captures the essential characteristics of different component models such as simple X-Windows components , COM, CORBA, JavaBeans, Enterprise JavaBeans. The VCF provides foundational support for (CBSE) component-based software engineering. It is used as the lower layer of a CBSE environment called the Component Workbench [Oberleitner02]. The Component Workbench provides transparent access to each component model and allows applications to be built from components coming fromidf ferent component models. It also supports the user in maintenance activities such as replacing components with other components. For example, if an application is to be moved to an environment where a needed component is not available, that component can be replaced with an equivalent component in the new environment. Consider an application that is built in the MS Windows environment and it uses the Internet Explorer as a component. In moving the application to a UNIX environment, the browser can be replaced by a Mozilla or Opera browser. The Component Workbench supports this replacement by helping the user match interfaces, methods, and attributes from one component to another component.

The Vienna Component Framework captures the common characteristics of different component models by providing a uniform type system across component models . It supports an event-based communication mechanism for the interconnection of components. It also offers an architectural description language that describes the composition of an application in terms of components.

One of the key problems of building applications out of components—component based software engineering— is what to do if the component you need is not available in the catalogs you have. Clearly, no catalog will have every component that an application developer needs. But, often, there will be a related component, or one that is ―almost‖ the one needed. There are several possible paths to take in this case. One is for the developer to modify the related component to make it fit user needs. This approach defeats the purpose of component-based development because of the fundamental reason that it breaks the separation of concerns between component development and component usage. A more effective approach is to automatically ―adapt‖ the existing component to the need of the application. Ideally, with automatic adaptation, the component developer can provide a minimal catalog of components but the user gains the benefits of a larger catalog.

The goal in the component work reported in [Jazayeri95] was to use generic programming to build powerful yet minimal catalogs. Thomas Gschwind's dissertation [Gschwind02] concerns the topic of automatic component adaptation and introduces a particular kind of adaptation called ―type-based adaptation.‖

Modern languages such as Java, and modern component models such as Cobra Components support strongly- typed components and provide mechanisms for querying the type of the component at run-time and type-based adaptation exploits these features to automate the adaptation process. The Component Workbench uses type-based adaptation to support the replacement of components from one component by components from another model.

Type-based adaptation is also a good fit for pervasive computing environments because the communication protocols they use and the devices that need to communicate with each other are not known a –priori.

The Vienna Component Framework and type-based adaptation are clearly two important ingredients for dealing with the heterogeneity of components that will have to face. But they are only preliminary steps towards meeting the wide heterogeneity and dynamicity that is expect to face pervasive computing environments. Components will have to compose dynamically and adapt dynamically. Versioning and legacy issues associated with such dynamically evolving services and their components will pose enormous challenges for software engineers.

5. Conclusion

The vision for pervasive human centric computing, the new wave of computing, cannot be implemented without software engineering programmers. This article presents the necessity of integrating pervasive computing into software engineering curricula and presents a set of suggested core strategies for integrating pervasive into software engineering education. The suggested core strategies include redesigning software engineering curriculated to incorporate pervasive computing into the circular systematically integrating pervasive computing the search into education, engaging students in applied and experimental research ,establishing and nurturing industry-academic partnerships in research and education, providing institutional support and funding for cross-disciplinary collaborations in the search and education, systematically updating the contents and structure of software engineering curricula to better prepare students for the new challenges and opportunities of software engineering and software component to make feasibility of pervasive computing in real life application era.

6. REFERENCES

[1] Dertouzos, M.L., The Unfinished Revolution: Human-Centered Computers and What They Can Do for Us. New York: HarperCollins (2001).
[2]. MIT Project Oxygen, http://www.oxygen.lcs.mit.edu/
[3]. Weiser, M., The computer for the twenty-first century. Scientific American, 265, 3, 94-104 1991
[4]. Weiser, M., Some computer science issues in ubiquitous computing. Comm. ACM, 36, 7, 75-84 (1993).
[5] T. Mayes, S. de Freitas, ―Review of E-Learning Theories, Frameworks and Models,‖ JISC E-Learning Models Study Report, Joint Information Systems Committee, www.jisc.ac.uk/elp_outcomes.html, 2004.
[6] P. Brusilovsky, A. Kobsa, W. Nejdl (Eds.), The Adaptive Web, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Germany, 2007.
[7] L. Han, S. Jyri, J. Ma, K. Yu, ―Research on Context- aware Mobile Computing‖, Proceedings of Advanced Information Networking Applications Workshops, pp 24- 30, 2008.
[8] J. Pascoe, ―Adding generic contextual capabilities to wearable computers‖, Proceedings of 2nd International Symposium on Wearable Computers, pp. 92-99, 1998.
[9] J. Mäntyjärvi, U. Tuomela, I. Kansala, J. Hakkila,―Context-studio–tool for personalizing context-aware applications in mobile terminals‖, Proceedings of Australasian Computer Human Interaction Conference, Addison-Wesley Longman, pp. 64-73, 2003.
[10] P. Korpipää, J. Hakkila, J. Kela, S. Ronkainen, I. Kansala, ―Utilizing context ontology in mobile device application personalization‖, Proceedings of Mobile and Ubiquitous Multimedia, ACM Press, pp. 133-140, 2004.
[11] J. Coutaz, J. Crowley, S. Dobson, D. Garlan, C̈ontext is Key,"Communications of the ACM, 48(3), March 2005.
[12] Pour, G., Pervasive computing reforming software engineering education. World Trans. on Engng. and Technology Educ., 2, 3, 357-360 (2003).
[13]. Pour, G., Restructuring software engineering education towards cross-disciplinary collaborations to create pervasive information systems and
technologies. World Trans. on Engng. and Technology Educ., 3, 1, 85-88 (2004).
[14]. Pour, G., Expanding the horizons of software component Workbench,‖ Proceedings of the 3rd Intl. workshop on Software Engineering in Middleware , Jan 2002.
[Gschwind02] T. Gschwind, Adaptation and Composition Techniques for Component-Based Software Engineering, PhD dissertation, Distributed Systems Group, Technical University of Vienna, 2002.
engineering education: integrating autonomic computing into the curriculum. World Trans. on Engng. and Technology Educ., 5, 1, 179-182 (2006).
[15]. Pour, G., Griss, M. and Lutz, M., The push to make software engineering respectable. IEEE Computer, 33, 5, 35-43 (2001).
[16]. Pour, G., Engineering curriculum reform to introduce students to security and privacy in the Internet era. World Trans. on Engng. and Technology Educ., 4, 2, 285-288 (2005).
[17]. Pour, G., Agent-Oriented Software Engineering (AOSE): its emergence as a cornerstone of enterprise software engineering education. World Trans. on Engng. and Technology Educ., 2, 2, 225-228 (2003).
[18]. Pour, G., Component-based development refining the blueprint of software engineering education. World Trans. on Engng. and Technology Educ., 2, 1, 45-48 (2003).
[Jazayeri95] M. Jazayeri, ―Component programming: a fresh look at software components,‖ Proc. 5th European Software Engineering Conference (ESEC '95) (Sitges - Barcelona, Spain), LNCS 989, pp. 457-78, September 1995. [Oberleitner02] J. Oberleitner and T. Gschwind, Composing Distributed Components with the component Workbench,‖ Proceedings of the 3rd [Gschwind02] T. Gschwind, Adaptation and Composition Techniques for Component-Based Software Engineering, PhD dissertation, Distributed Systems Group, Technical University of Vienna, 2002.

.

ISSN Application ID: 13010

NECESSITY OF FOG COMPUTING FOR SECURITY OF CLOUD DATA

Gurmeet Kaur,
Assistant Professor, Dyal Singh College, Karnal

ABSTRACT

Cloud computing is using as a delivery platform which is a promising way for storing user data and provides a secure access to personal and business information. The users are provided with on-demand services through the Internet. But there is a risk of the involvement of a third party which makes it difficult to trust that user data is secure enough and will not be misused. To deal with such malicious intruders there are some technology which are used to secure user data called "Fog computing". It is gaining attention of the cloud users nowadays. This paper review the work that has been done using this technology and discussed the paradigm for preventing misuse of user data and securing information.

1. INTRODUCTION

Small and medium businesses (SMBs) are increasingly opting for outsourcing data, information and computation to the Cloud. Cloud computing is achieving popularity and gaining attention in business organizations. It provides a variety of services to the users. It is an convenient, ubiquitous, on- demand network access to a shared pool of configurable computing resources [1].

Business agencies and software companies are admiring cloud computing for its ease of access and flexible architecture. For attaining more and more operational efficiency and managing data organization with small or large businesses are using cloud environments. Cloud Computing is a combination of many computing strategies and service oriented architecture such as virtualization and networking. Although, Cloud Computing provides an easy way for managing, accessing and computation of user data, but it also has some severe security risks as data leakage, data theft. There are some traditional security mechanism such as authorization, identity, and authentication but now these are not sufficient [2].

To resolve these issues a mechanism which can detect such malicious activities is required. For this, Fog computing is introduced by CISCO which monitors the data and helps in detecting an unauthorized access. According to CISCO, due to its wide geographical distribution the Fog computing is well suited for big data and real time analytics. As Fog nodes provide localization, therefore enabling low latency and context awareness, while Cloud provides global centralization [3]

Salvatore J. Stolfo [4] et al. used fog computing for making disinformation attacks against the malicious intruder or attacker Fog Computing is an extension of Cloud Computing. As in a Cloud, Fog computing also provides data, storage, compute, and application services to end-users. The difference is Fog provides proximity to its end users through dense geographical distribution and it supports mobility too. Set-up boxes and Access points are used as end devices to host services at the network. These end devices are also termed as edge network.

Sabahi, F.[5] mentioned threats and response of cloud computing. He presented a comparison of the benefits and risks of compromised security and privacy. In his paper he has summarized availability and reliability elated issues of cloud resources provided by the trusted third party. He also discussed about the most common attacks nowadays are Distributed Denial of Service attacks. The solution to these attacks can be, cloud technology providing the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown [5].

Claycomb, W. R. (2012) [6] has characterized a hierarchy of administrators within cloud service providers and also gave examples of attacks from real insider threat cases. They discussed how cloud architecture let attackers to break the security. They have also presented two additional cloud related insider risks: the insider who exploits a cloud-related vulnerability to steal information from a cloud system, and also the insider who uses cloud systems to carry out an attack on an employer's local resource. They mentioned the key challenges faced by cloud providers and clients for securing their highly confidential data.

2. Need of Security on cloud

Kaufman L. et al. (2009) [7] has examined some security issues and the associated regulatory and legal concerns that have arisen as cloud computing. Interestingly, a major concern included in the Security Content Automation Protocol (SCAP) is the lack of interoperability between system-level tools. By combining industry best practices with the oversight National Institute of Standards and Technology US and other entities are developing, it is effectively address cloud computing future security needs for providing data confidentiality which can impact the incident reporting.

Godoy et al. [8] explained that there is a need of such profiling strategies or methods through which user profiling can be done. As there is a huge amount of data and information available on the internet therefore from last few years personal information agents are helping the users to manage their information. In his paper the authors have discussed a learning technique for data acquisition for user profiling and mentioned some methods for adaption with the changes which happen timely by changing user's interest. They said earlier only supervised learning technique used in general. But for moving the information agents to the next level authors are focusing research on assessment of semantically useful user profiles. They also said that account hijacking is a disadvantage for such user profiling.

3. Literature survey

Madsen.H and Albeanu. G [9] presented the challenges faced by cloud computing paradigms and discussed how Fog computing platforms are feasible with cloud and are reliable for real life projects. Fog computing is primarily done for the need of the geographical distribution of resources instead of having a centralized one. A multi-level architecture is followed in Fog computing platforms. In first level there is machine to machine communication and the higher level deal with visualization and reporting. The higher level is represented by the Cloud. They said that building Fog computing projects are challenging and difficult [4]. But there are methodologies and algorithms available that deal with reliability and ensure fault tolerance. With their help such real life projects are possible.

Grobauer B. Et al. (2012), [10] provided an overview of vulnerabilities in security of cloud. They explained the meaning of the term vulnerability that its the probability that an asset is unable to defend itself against an threat or attack. They said vulnerabilities should always be defined in terms of resistance to attacks or threat. Control challenges mainly highlight situations in which otherwise successful security controls are ineffective in a cloud setting. They have discussed about the core cloud computing technologies such as services and web applications which use PaaS SaaS and platforms, virtualization and said that there are many such security requirements which are solvable only with the help of cryptographic techniques.

Park, Y. Et al. (2012) [11] developed a technique that was a software decoy for securing cloud based data using software. They proposed a software-based decoy system that aims to detect the exfiltration of proprietary source code and to deceive insiders. The system designs a Java code which provides valuable information of the attacker. Further static obfuscation method is used to generate and transform original software. Bogus programs are designed by software that is automatically transformed from original source code, but designed to be dissimilar to the original[11].This deception method confuses the insider and also obfuscation helps the secure data by hiding it and transferring bogus information for insider. Beacons are also injected into the bogus software to detect the exfiltration and making an alert if the decoy software is touched, executed or compiled.

Salvatore J. Stoflio et al [4] proposed a new technology and named it as Fog computing. They implemented security by using decoy information technology. They discussed two techniques, namely User behavior profiling and Decoy technology. In User behavior profiling they checked how, when and how much amount of data and information a user is accessing. They monitored their user's activity to check for any abnormality in the data access & usages behavior of the user. The second technology is decoy in which information which is bogus or one can say fake such as honey pots, honey files etc. are used to confuse the malicious intruder or attacker by depicting the information in such a way that it seems real.

Z. Jiang et al. [12] discussed Fog computing architecture and used it for improving Web site's performance using of edge servers. They said that the emerging architecture of Fog Computing is highly virtualized. They presented their idea that the Fog servers, monitor each and every requests made by the users and keep a record of each request by using the user's MAC address or IP address. Further, when a user requests for same website increases than a given decided number (N is tunable parameter) then the user's browser can cache the common CSS and JS files and then furthers send them externally. They also mentioned that it is possible to measure page rendering speed with the help of snippets.

4. Securing clouds using fog

The proposals for cloud based services describe methods to store documents, files, and media in a remote service that may be accessed are broadly accepted concerns guarantees for securing a user's data in a manner where that guarantees only the authorized user and no one else can gain access to that data.

The problem of providing security of confidential information remains a main core security problem that, till date, has not provided the levels of assurance most people desire. Figure 1 shows role of fog computing for security of data on cloud.

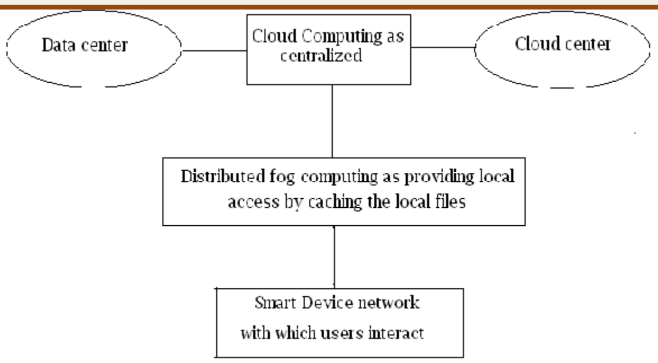
Data center
Cloud Computing as centralized
Cloud center
Distributed fog computing as providing local access by caching the local files
Smart Device network with which users interact

Figure 1 shows Role of Fog computing for security on cloud computing

Many proposals have been made to secure remote data in the Cloud using encryption and standard protocols. It is fair to say all of the standard approaches have been demonstrated to fail from time to time for a variety insider attacks, mis-configured services, faulty implementation buggy code, and the creative construction of effective and

Sophisticated attacks not envisioned by the implementers of security procedures.

A Twitter incident [13] is one example of a data theft attack from the Cloud Several Twitter corporate and personal documents were ex-filtrated to technological website Tech Crunch and subscriber's accounts, including the account of U.S. President Barack Obama, were illegally accessed. The attacker used a Twitter administrator's password to get access to Twitter's corporate documents hosted on Google's infrastructure & server as Google Docs.

A trustworthy cloud computing environment is not enough, because accidents continue to happen, and when they do, and information gets lost, there is no right way to get it back. One needs to prepare in advance for such accidents. The basic idea is that limit the damage of stolen data if we decrease the value of that stolen data and information to the attacker. This can achieve through a 'preventive' disinformation attack.

To overcome this Fog computing tries to secure the storage of data in the by using decoy information. This technology introduces disinformation against harmful persons or malicious insiders, preventing real sensitivity data to worthless data.

4.1 Case study

The services would have be implemented by giving two features:

User Behavior Profiling: It is expected that access to a user's data and information in the Cloud will exhibit a normal method of access. User profiling is a technique that can be applied to model when and how much times a user accesses their information in the Cloud. In this way 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. This technique of behavior-based security is commonly used in fraud detection applications and services. Such profiles would actually include volumetric information, how many documents are typically read and how often.

Legitimate users of a computer system are familiar with the files on that system and where they are located. Any search for specific files is likely to be targeted and limited. A masquerade or harmful person is one which gets access to the victim's system illegitimately or unofficially, is unlikely to be familiar with the structure and contents of the file system. Their search is likely to be widespread and untargeted. On the bases of this key assumption, user search behavior is profiled and then developed user models trained with a one class Modeling technique, namely one-class support vector machines. The importance of using one-class modeling originates from the ability of building a classifier without having to share data from different users. The privacy of the user and their data is remain preserved.

Decoys Technology: Decoy information, such as decoy documents, honey files, honey pots and various other bogus information can be generated on demand and serve as a means of detecting unauthorized access to information and to 'poison' the thief's exfiltraed information. Serving decoys will confound and confuse an adversary into believing they have ex-filtrated useful information, when they have not. Decoy files or documents are trap files. The traps can be placed within the file system. These traps are nothing but basically decoy files downloaded from a site of Fog computing , an automated service that offers several types of decoy documents such as medical records, tax return forms, e-bay receipts credit card statements.

The decoys, then, serve two purposes:

(1) Validating whether data access is authorized or legal when abnormal information access is detected, and

(2) Obfuscating or confusing the attacker with bogus information. The decoy documents use a keyed-HMAC, Hash Message Authentication Code which is hidden in the header section of the document. The HMAC is computed or designed over the file's contents using a key unique to each user.

The advantages of placing decoys in a file system are three ways:

(1) The detection of masquerade or harmful activity

(2) The confusion of the attacker and the additional costs incurred to distinguish real from bogus information, and

(3) The deterrence effect which, although hard to measure, plays a significant role in preventing masquerade party activity by risk-averse attackers.

Combining the Decoys Technology with User Behavior Profiling : -

The relationship of search behavior anomaly detection with trap-based decoy files system should provide stronger evidence of malfeasance, and therefore improve a detector's accuracy. It is hypothesize that detecting abnormal search operations performed prior to an unauthorized user opening a decoy file will confirm the suspicion that the user is indeed impersonating another victim user. This scenario covers the threat model of illegitimate or unauthorized access to Cloud data. Furthermore, an accidental opening of a decoy file by a authorized or legitimate user might be recognized as an accident if the search behavior is not deemed abnormal. In other words, detecting abnormal behavior search and decoy traps together may make a very effective masquerade or harmful activity detection system. Combining the two techniques improves detection accuracy.

In addition to these techniques , fog computing also suggest about user profiles that are accurate enough to detect unauthorized cloud use and access .When such illegitimate or unauthorized access is detected, one can respond by presenting the user with a decoy document or with a challenge question to validate whether the access was indeed unauthorized, similar to using decoys in a local file setting, to validate the alerts issued by the anomaly detector that monitors user file search and access behavior.

5. Conclusion

With the increase of data theft attacks or threat, the security of user data is becoming a serious issue for cloud service providers, for which Fog Computing paradigm is introduced which helps in monitoring the behaviour of the user and also providing security to the user data. The paper title “Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud “discussed about how to monitor data and provides data security from harmful person or malicious intruders and also helps in confusing the attacker about the real information by using User Behavior Profiling and Decoy Information technology[4].The paper title “Software decoys for insider threat “discussed a technique that confuses the insider and also used obfuscation which helps to secure data by hiding it and making it bogus information for insider using a technique that was a software decoy for securing cloud data using software[11] .The paper title” Reliability in the Utility Computing Era: Towards Reliable Fog Computing “Provides the concept of Fog computing and its feasibility for real life projects using three level architecture for Fog Computing [9]. In this way by continuing the work on Fog Computing platforms can lead to improved defensive techniques for masquender activity and would contribute in increasing the level of security if user data on the cloud.

6. REFERENCES

[1] Hashizume K., Rosado D. G.,Fernandez- Medina E. and Fernandez E. B. “An analysis of security issues for cloud computing”. Journal of Internet Services and Applications, 2013.
[2] Marinos A. & Briscoe G., Community Cloud Computing (pp. 472-484). Heidelberg: Springer, 2009, pp. 472484.
[3] Bonomi, Flavio, et al.Fog computing and its role in the internet of thingsProceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, 2012, pp. 13-16.
[4] Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis.Fog computing: Mitigating insider data theft attacks in the cloudSecurity and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012.
[5]. Sabahi, F. “Cloud computing security threats and responses”, In Communication Software and Networks (ICCSN), 2011 IEEE 3rd In ternational Conference on 2011,pp. 245-249.
[6] Claycomb, W. R., & Nicoll, A. “Insider Threats to Cloud (Computing: Directions for New Research Challenges”, In Computer Software and Applications Conference COMPSAC), IEEE 36th Annual, 2012, July, pp. 387-394.
[7] Kaufman, L. M. “Data security in the world of cloud computing”. Security & Privacy, IEEE, 2009, 7 (4), 61 - 64.
[8] Godoy D., “User profiling for web page filtering”, IEEE Internet Computing, Jul. 2005, vol. 9, no. 4, pp. 56–64.
[9] Madsen, Henrik, et al. Reliability in the utility computing era: Towards reliable Fog computing."Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. IEEE, 2013.
[10] Grobauer, B., Walloschek, T., & Stocker, E. “Understanding cloud computing vulnerabilities”. Security & Privacy, IEEE, 2011, pp. 50-57.
[11] Park, Y., & Stolfo, S. J. “Software decoys for insider threat”, In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, 2012, May, (pp. 93-94).
[12] Zhu, Jiang, et al. Improving Web Sites Performance Using Edge Servers in Fog Computing Architecture." Service Oriented System Engineering (SOSE), 2013 IEEE.
[13] P. Allen, “Obama’s Twitter password revealed after French hacker arrested for breaking into U.S. president’saccount,”March 2010. [Online].Available: http://www.dailymail.co.uk/news/article-1260488/Barack- Obamas-Twitter-passwordrevealed-French-arrested.html.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Notes: