An Investigation towards Paradigm Shift of Cloud Computing Approach and Need of New Security Protocol

Veena R.S.
Department of CSE,
K.S. School of Engineering & Management,
Bengaluru, India

Ramachandra V. Pujeri
MIT College of Engineering
Pune, India

Indiramma M.
Department of CSE,
BMS College of Engineering
Bengaluru, India

ABSTRACT
Today cloud computing platform is de-facto and strategic component of corporate and end user applications usage in pervasive and ubiquitous manner. The level based services makes the higher possibilities of availability, scalability, collaborative in most cost effective way. However integration of various service layers into cloud stack also invites intrinsic threats, risk and vulnerabilities, thus security become prime concern for the adaptabilities. This paper mainly focus on understanding the changing trends of usage of cloud computing platform for various services, fundamental research approaches towards cloud security and finally need of requirements for strengthening the security protocol. The facts, concept and statistics illustrated in this paper is of extensive use to the researchers, industries and academicians towards developing new mechanisms and protocol for future secured cloud framework.

Keywords
Cloud computing, Cloud Stack, Security Secured Cloud Framework, Vulnerability

1. INTRODUCTION
In contrast to the beginning of cloud computing era just after high performance age, today cloud computing has become a major collaborators for Internet of Things (IoT), BigData Analytics and Intelligence business solutions along with its traditional fundamental services such as platform as a services(PaaS), Storage as a Service(SaaS) and Infrastructure as a Service(IaaS). A combined report of many market research and advisory organizations such as IDC, Forrester and Gartner etc, reveals that enormous amount of enterprises are adopting cloud and making it strategic for collaborating and fulfilling their operations of entire enterprise process to meet the global challenges of competitiveness in the most cost effective way[1]. However, it is important to understand that how cloud services poses abundant data. With the proliferations of the mobile applications and Smart Phone, the user finds it convenient to access their resources from their trusted handheld devices. The present era has witnessed various forms of mobile applications that allow the user to access their data right from their Smart Phone. The mobile devices also allows parallel running of multiple applications. Hence, a massive range of data is being generated just from the usage of mobile application as well as mobile networks in cloud. A huge adoption of smart phones by both individuals and corporate forces along with many applicable Apps (Mobile Applications) will be the game changer into future. The future of mobile applications as well as enterprise applications are synchronized and collaborated with cloud. The classification of such traffic could be mobile cloud traffic (MCT) and mobile non-cloud traffic (MNCT). The MCT may includes online storage, web browsing, social networking, video streaming, audio streaming and online gaming etc. on other hand the MNCT may include File or App downloading , file sharing and voice communication. One of the leading network organizations Cisco in their white paper has illustrated a statistics of mobile data traffic from 2014 till 2019[2]. The Figure 1 shows the tread of mobile data traffic. Figure 1 highlights the generation of the mobile data traffic from 2014 till 2019. The statistics show that MCT-based traffic has generated around 85.5% of data traffic while MNCT-based traffic has generated average of only 17%. It is also essential to understand the level of effectiveness in safeguarding such sensitive and massive data over mobile networks that uses cloud services. One of the best method to provide the data security is by using the cryptographic techniques [3][4]. Owing to extensive limitations of the computational complexities, the proliferation of existing cryptographic techniques is few to find in the cloud-based environments. From the research area viewpoint, there are many research work that has focused on implementing various security standards as well as cryptographic-based security approaches in cloud environment, but it is still yet to be seen about the robustness as well as sustainance. A competitive security technique over cloud environment must ensure confidentiality, authenticity, integrity of data. The prime purpose of this paper is to understand the recent trends of security aspects in cloud computing in order to have better visualization of research trends. The prime intention is to understand the extent of research work being carried out in this regards. Section II discusses about the existing applications over cloud environment followed by discussion of futuristic cloud application in Section III. Different classification of cloud computing security requirement is discussed in Section IV. Section V discusses about the research gap while Section VI discusses about a novel technique that could possibly meet the research gap existing in security implementation over cloud environment. Finally, Section VII summarizes the paper.

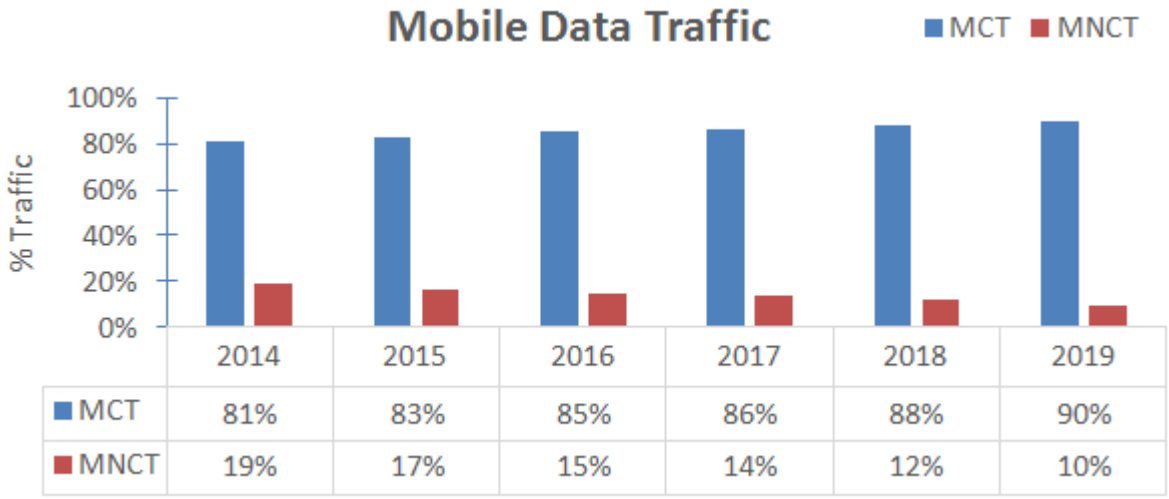

Fig 1: Mobile Data Traffic from year 2014 till 2019(Projection)

Source: Cisco VNIO mobile, 2015

2. ISSUES IN TRADITIONAL CLOUD APPLICATIONS

The traditional cloud services are provided at three different levels such as: application level, infrastructure level and platform level. Table 1 illustrates these services along with examples [5].

Table 1. Frequent Applications of Cloud

Service	Description	Examples
Software-as-a-Service (SaaS)	Applications which are delivered to the end users via a web client	CloudNumbers DropBox OfficeLive
Platform-as-a-Service (PaaS)	Customizable operating system, software and libraries specific to the specific task	VMforce Google AppEngine SalesForce
Infrastructure-as-a-Service (IaaS)	Controls where computing infrastructure can be accumulate above the operating system	IBM Cloudburst Amazon EC2 Eucalyptus

The functioning of public as well as private cloud is almost similar. All the necessary applications are server-hosted and accessed from World Wide Web. One of the common facts in the usage of traditional cloud applications is the dependency on third party organization who are presently entrusted with the sensitive and confidential information about the business. This is the start of security problems in conventional cloud applications. The critical need of security standards for the applications are secure data transfer, secure software interface, secure stored data, user access control, and data separation. The existing services e.g. SaaS, PaaS, and IaaS are not resilient against various issues that finally lead to security breach e.g. Denial-of-Service threats [6], highly capable of generating hacking points [7], lack of customized security features [8], issues of locations of data [9], and usage of shared memory [10]. The existing cloud application also doesn't define if there is a need of encrypting the data in its various state of motion or in rest. The present cloud applications and the services don't guarantee any consistency in its security profiles between the tenants [11].

Various sources of study have also claimed that SaaS is encountered with security issues of managing password [12]. As the delivery of the services are given by cloud from SaaS, the prime issues in management of multiple password for authentication single user on multiple applications. Data Encryption is one of the serious issues in PaaS. The prime reason behind this is slower performance of system leading to less supportability of potential security algorithms. PaaS supports encryption of data at the cost of multiple cycles of CPU resources. In IaaS, the prime security issue is rogue client as there is various virtual machine management done in IaaS therefore security threats are more on virtualization of services in IaaS. It is also associated with data leakage issues as well as ethical usage surveillance system, fragile infrastructure design, weak encryption policy, and usage of conventional authentication mechanism to enable authorization [13]. Although encryption of data proves better solution in securing cloud-based services, but still they are not resilient against various critical malwares and phishing attacks over internet [14]. If the sensitive root password to access running server is possessed by tenants than it leads to series of bigger security breaches. Slight mistakes in configuration of PaaS services are sure to offer the security breaches to user's confidential resources. Hence, the existing security systems offered by the service providers are not resilient enough to provide standard and fool proof data security and data privacy. There is a significant need to evolve up with more robust technique to secure the three service frameworks of cloud computing.

3. FUTURISTIC CLOUD APPLICATIONS

The continuous advancement into internet technology, wireless standards, Internet of Things (IoT), collaborative framework, pervasive computing, ubiquitous computing, Bigdata Analytics, mobile computing and inventions into smartphones along with cloud computing platform has helped the developers to conceptualized various smart applications in the field of social interaction, Enterprise data sharing, personal well being monitoring, surveillance, transportation as

few to name and many more. These applications generate various different kinds of data and it collaborated as services at different layers. The future of cloud-based application for next 15 years is going to be for Internet-of-Things and BigData Analytics. This section will discuss significant security issues in both the applications with brief of research work being carried out in this.

3.1 Internet of Things (IoT)

3.1.1 About IoT

It is basically a large network that connects multiple heterogeneous devices to capture data. The primary objective of IoT is to ensure more possibilities of integration between the hardware and the computing systems using internet (Figure 2). Various literatures predict that about billions of devices will be connected by internet to each other in next 5 years. Various applications of IoT are smart cities, home automation, healthcare, wearable, smart manufacturing, etc. IoT will also bring various forms of networking protocols as well as standards common to one platform in order to either access the service or to control it. However, it is just a starting.

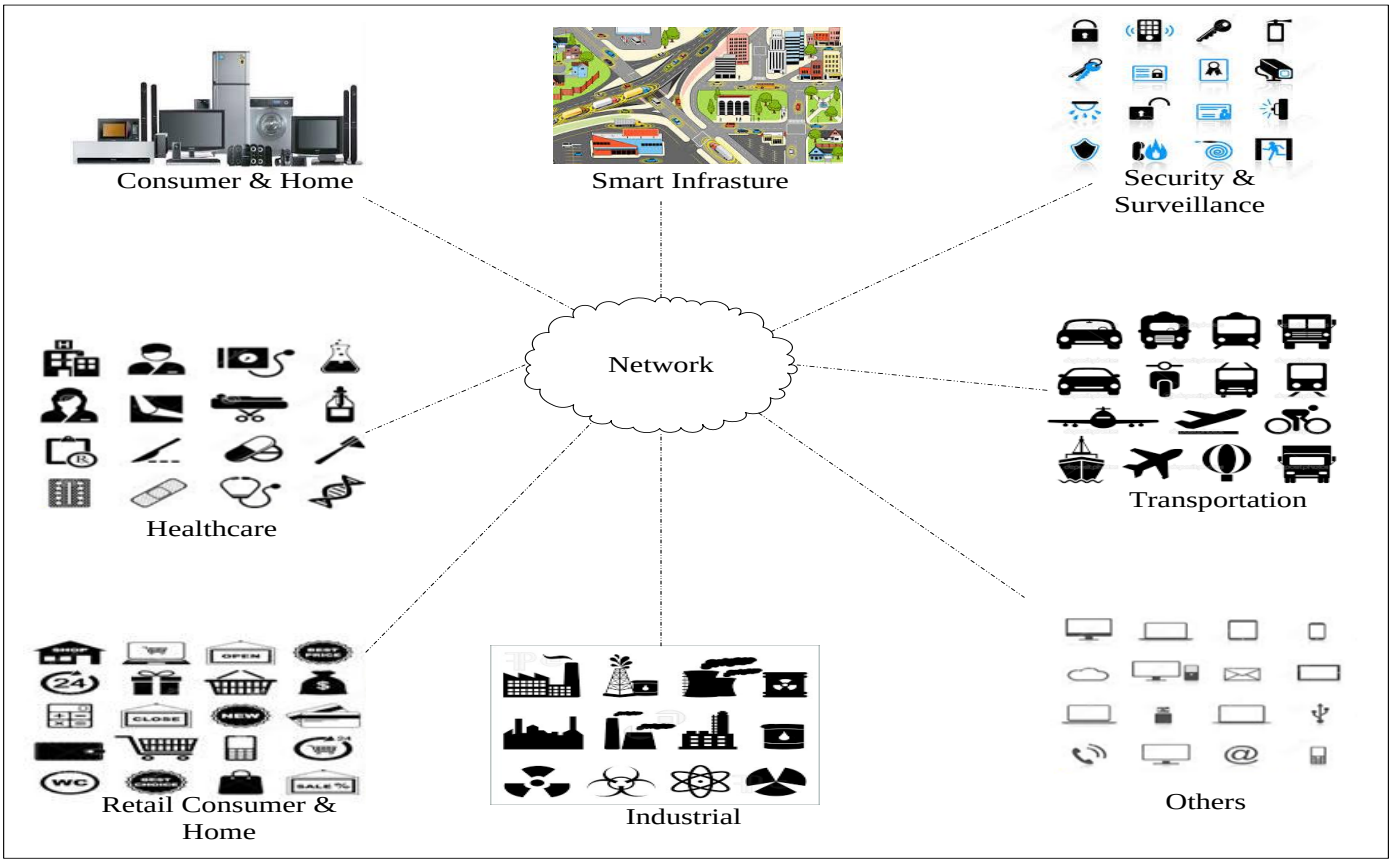

Fig 2: Internet-of-Things Integration Schema

3.1.2 Issues in IoT

As IoT integrates multiple heterogeneous devices with different technological cores, it is also associated with complexities. The initial issue in IoT is problem of sensing in complex environment, issue of selection of multiple options for connectivity, restricted energy availability in the devices, making connection with the cloud, and obviously security protocols. The security problems in IoT can be only solved if there is an availability of built-in security features over the hardware; however, such system is not only expensive in process but also requires exhausting testing to ensure its resiliency against security breaches.

3.1.3 5-Recent Research work in IoT

At present, there are 742 Journals being published in IEEE Explore during the period of 2010-2015 based on Internet-of-Things. Out of this, there are 147 Journals based on security issues of Internet-of-Things. It has been found that majority of the paper in this topic is just a discussion manuscript, so this paper discusses about 5 most relevant implementation work that has been carried out in last 5 years. He and Zeadally [15] have proposed a secure authentication scheme for RFID system using elliptical curve cryptography. The approach (Figure 3) has used finite field cryptography using 63 bytes to store key. The outcome of the study has been theoretically compared with approximately 26 prior researchers to find its effectiveness with respect to communication cost.

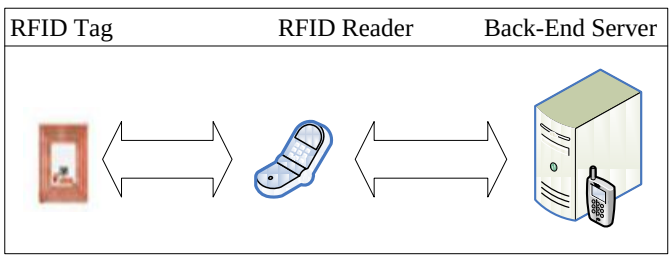

Fig 3: Scheme discussed by He and Zeadally [15]

Ning et al. [16] have presented a sophisticated authentication scheme using chaotic map and homomorphism-based approaches. This recent study has claimed to incorporate data confidentiality, access control, forward secrecy, mutual authentication, and privacy preservation. However, the study didn't discuss about the validation of its outcomes. Li and Xiong [17] applied the technique of Signcryption for securing the transmission in IoT taking the case study of wireless sensor network. The scheme is implemented through design of key set up process, developing identity-based cryptography, and public key infrastructure-based cryptography to ensure security. The study outcome was evaluated for consistency, security, computational cost with respect to three prior schemes using Signcryption. The steps are highlighted in Figure 4.

Premnath and Haas [18] had investigated on unique attacker module in IoT called as Dollar-limited Adversary and Time-limited Adversary in order to minimize the computational requirement of IoT nodes. The outcome of the study was evaluated using size of public key, processing load in comparison to Moore's law. Ramos et al. [19] have introduced an authentication scheme for smart objects in IoT using hardware-based approach using microcontrollers.

3.2 BigData Analytics (BA)

3.2.1 About BA

Big Data Analytics is a technique to process the massive flow of heterogeneous data. The inheriting characteristic of big data is data heterogeneity, data veracity, data volume. One of the serious issues of big data is in its storage and processing it as they are usually semi-structured or unstructured data, which cannot be stored in conventional SQL, based storage. Developing Big Data Analytics will mean designing an application that can process a large semi unstructured data to structured data, which can be subjected to data analysis using sophisticated mining approaches. Owing to streaming nature of data, Big Data Analytical services are closely related with cloud-based services.

3.2.2 Issues in BA

The first significant challenge in big data is the storage issues and management problems. Owing to unstructured form and increasing size of data stream, it cannot be stored in conventional database system. Even if it is stored in cloud, it is still unpredictable about the frequency of accessing it [20]. Generations of outliers or false positive owing to data veracity (or uncertainty) in existing analytics are also one of the serious problems. Apart from all these, security is a large problem in BigData Analytics. It is not possible to identify the challenges of the potential threats as well as malicious codes present in big data. Another bigger challenge in big data is data privacy.

3.2.3 Research work in BA

At present, there are 147 Journals being published in IEEE Explore during the period of 2010-2015 based on Big Data Analytics. Out of this, there are only 16 Journals based on security issues of Big Data Analytics. It has been found that majority of the paper in this topic is just a discussion manuscript, so this paper discusses about 5 most relevant implementation work that has been carried out in last 5 years. Gadepally et al. [21] have presented a cryptography based approach to encipher a big data while performing analysis of it. The system uses D4M (Dynamic Distributed Dimensional Data Model) for processing the unstructured data and have used Galois Field Cryptography with AES encryption approach. The outcome of the study was evaluated with respect to processing time essentially. Islam and Islam [22] have developed a suite that can ensure security for the big data using multiple cryptographic algorithms (Figure 6). However, the focus of the study was restricted to ciphering text data, XML data, and multimedia data. The outcome of the study was assessed using sensitivity and confidentiality mainly. However, benchmarking is missing from the analysis.

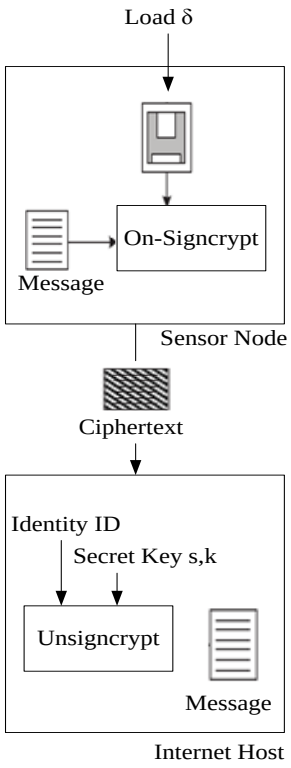

Fig 4: Scheme discussed by Li and Xiong [17]

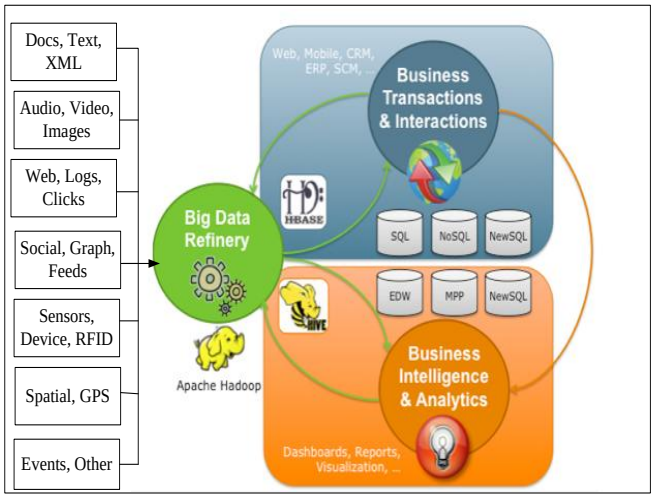

Fig 5: Big Data Analytics Architecture

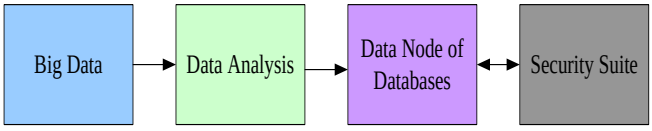

Fig 6: Scheme discussed by Islam and Islam [22]

The emphasis on privacy issues in BigData Analytics are found in the work of Lu et al. [23]. Vaquero et al. [24] have implemented a technique of data distribution of 100 tera-bytes over thousand of virtual machines. Although, the work is not related to security technique, but it presents a tightly coupled topology for deployment of BigData, where any security algorithm are easier and involves lesser computational resources. Marchal et al. [25] have emphasized their investigations towards securing phishing URLs during analyzing big data [25].

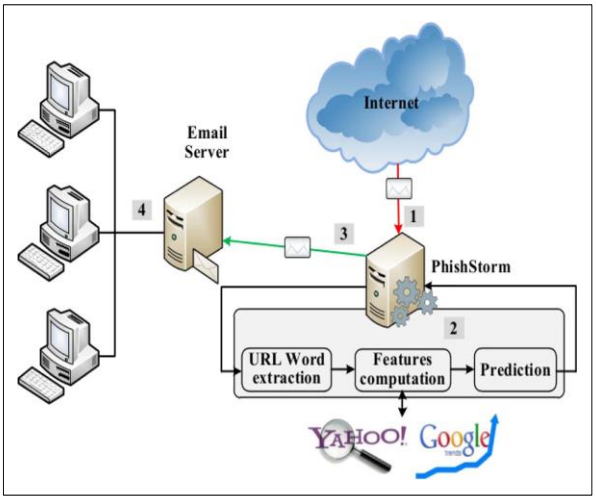

Fig 7: Scheme discussed by Marchal et al. [25]

Figure 7 shows scheme of Marchal et al. [25], which performs extraction of embedded links from the email (incoming) over internet. A computation of feature is performed using spidering mechanism and performs forecasting of vulnerability based using machine learning. A threshold-based technique is applied for every prediction for exploring the malicious emails in the servers.

Hence, it can be seen that there are some good amount of research work being carried out for security issues towards futuristic cloud applications. However this collaborative platform is susceptible to malicious attacks as these applications continuously evolves [26]. The broader classification of research directions towards a new protocol development into cloud security aspect is discussed in section 2.0.

4. CLASSIFICATION OF CLOUD COMPUTING SECURITY REQUIREMENTS

The Cloud Security Alliance acknowledges various perspectives of security in cloud computing paradigm. The broad security requirements are mainly discussed as following:

4.1 Policy Management

There are many critical challenges exist towards the policy management as well as into enterprise securities irrespective of the best efforts of technologist. A brief overview of network policy management throughout the evolution of virtualization is discussed. Right from the creation of virtual machine (VM) to dynamic partitioning of the physical resources is called virtualization and the place where the virtualization of resources is realized is called hypervisor or virtual machine monitoring [27]. The complexity, associated expenditures, eases of administration is easily handled by open VM specification. However there are associated challenges too and these challenges are associated with policy management requirements along with the evolution of virtualization. The specification provided by Distributed Management Task Force (DMTF) pave the foundation.

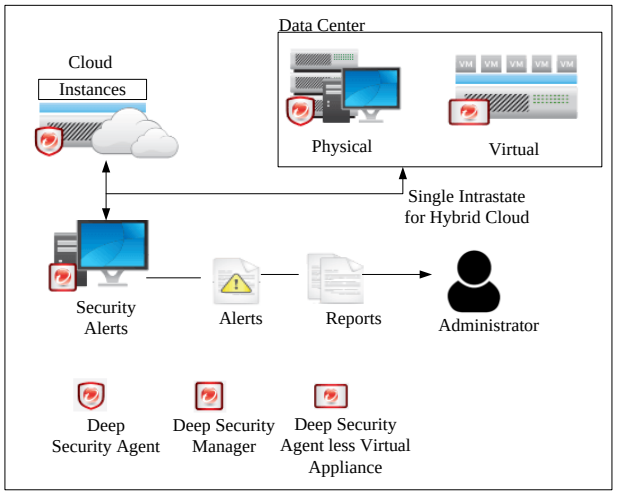

Fig 8: Development of security policy

Figure 8 shows the development of a set of security policy that is discretely defined for the user as well as administrator to access the services. The security policies are maintained by the Hypervisor that acts as bridge between virtual machine and physical server in conventional virtual switches. The global security policies are also maintained by physical switches that connects both network switches and hardware switches over data centers. Study on policy management was carried out by Hamlen et al. [28] by adopting context-based access control mechanism. Takabi and Joshi [29] have applied semantic concept to design policy management. The concept discussed in [27] was also cited by Sandhu and Chana [30] who have presented a security policy using hashing for safeguarding intrusion towards virtual machines over cloud environment.

4.2 Authentication

The core theme of authentication is revolved towards a mobile users and in coming future the smart phone or smart portable wireless devices are seems to be used as user client access machine. There are many different cloud service providers for different applications and it is a tedious task to have multiple registration and management of private keys/ passwords for each authentication need. The generic authentication scheme is pictorially shown in Figure 9.

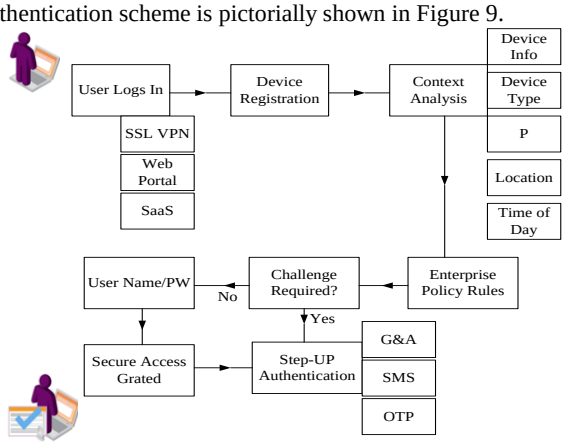

Fig 9: Development of Authentication Scheme

The existing authentication schemes are Single Sign-on-Scheme [Open ID, Passport] [31], [32]. The existing authentication scheme has used efficient cryptography with more supportability of mutual authentication and less on using Secured Socket Layer. Although TTP (Trusted Third Party) is required for carrying out user profiling but they are not continued for next user login. At present, usage of single private key allows the user to have an access from mobile devices. Various studies have also used ECC (Elliptical Curve Cryptography) [33], RSA [34], bilinear pairing [35], identity based cryptography [36] are some of protocols used for secure authentication of users over cloud. Tsai and Lo [37] have recently presented an authentication scheme that makes use of bilinear pairing for secret exchanging of private keys, mutual authentication, and rendering untraceability. The outcome of the study has been compared with 5 existing studies to find that presented scheme is highly resilient against various forms of authentication threats. The author has performed the authentication over mobile devices showing the importance of authentication over it. Studies towards authentication in cloud have been witnessed in the work of Ahn et al. [38], Kim and Moon [39], and Ghazizadeh et al. [40]. All these implementations are quite unique in their methods and the paper has presented strong background to prove its efficiency towards authentication mechanism.

4.3 Access Control

An access control mechanism can be defined as a policy that permits, rejects, or limits accessibility for user to a particular set of system over cloud environment. Another unique charecteristics of access control mechanism is to restore all the attempts being made the user to access the cloud resources for screen trust and building reputation. At present various access control schemes are- Discretionary Access Control (DAC) [41], Mandatory Access Control (MAC) [42]., and Role Based Access Control (RBAC) [43]. The generic architecture of existing access control over cloud is as shown below.

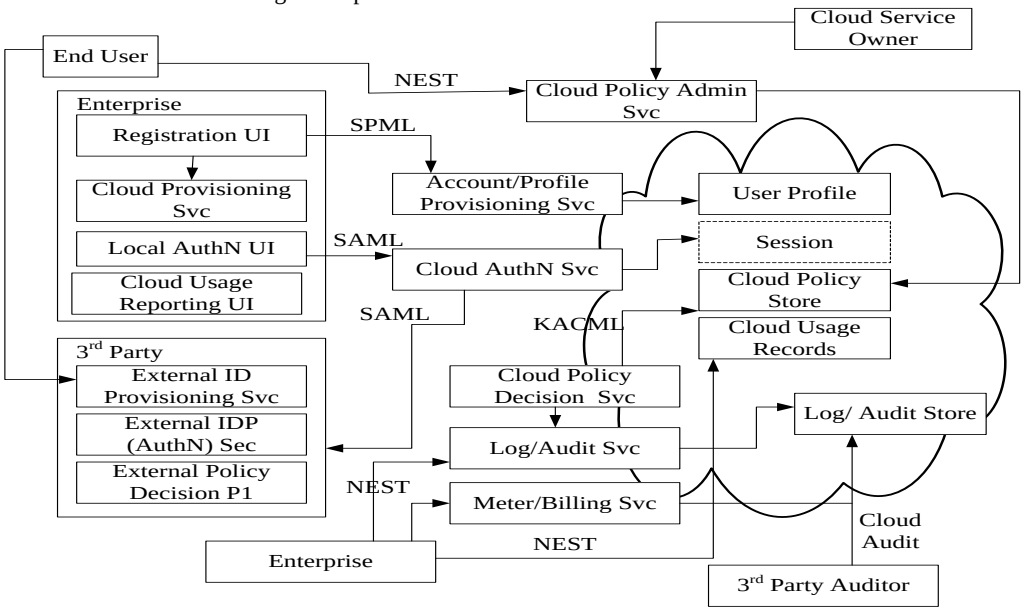

Fig 10: Development of Access Control Scheme

Study on Access control system has been carried out by Guoyan et al. [44], where the author have presented a framework for access control based on mutual trust relationship over cloud environment. Yeo et al. [45] have developed a framework for access control by incorporating dynamicity in it for securing smart grid environment. Wang et al. [46] have introduced a unique access control system using digital rights management over cloud environment.

4.4 Virtual Machine Security

Virtual machine can be defined as a container where various forms of operating system of guest user as well as numerous applications run. The design principle of VM makes them separate from each other for enhance performance as well as for security viewpoint too. Because of VM isolation (Figure 11), it is possible for cloud to securely run multiple VMs with sharing hardware as well as guaranteeing secured access to hardware without affecting the processing performance of VM. It is due to VM isolation scheme that doesn't permit even the administrator to access this secured isolation layer in order to access other VM without authorization that could be only explicitly granted by the root administrator only. From the performance viewpoint also, the application residing on VM is not effected even if that VM is not functional as there is always a backed up VM to continue the services of application in case of any failures. Therefore, reservation / provisioning of the resources ensures the optimal performance of the VM even in presence of abnormal traffic load.

There are various literatures that introduced unique techniques to secure VM. Study carried out by Liu et al. [47] has presented one such technique. The author have developed a module that is responsible for tracking the trust factor of the VM, store it in memory, and updates other VMs too.

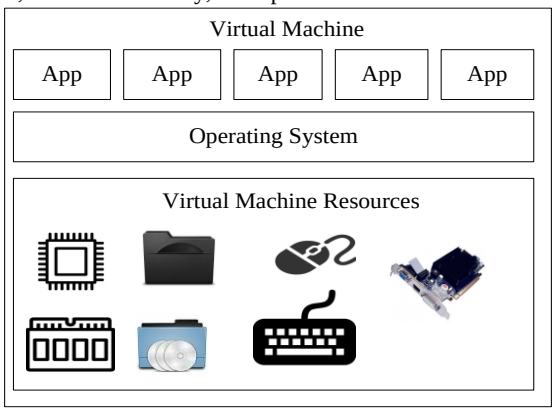

Fig 11: Virtual Machine Isolation Scheme

The module also monitors various executable that runs on VM for probability of malwares. Zhu et al. [48] have presented a secured architecture for virtualization to leverage privacy preservation and data sharing. The architecture runs in between software and hardware layer. Benninger and Neville [49] have presented a prototype that performs detection of malwares. The faster outcome of the intrusion detection proved quite effective system. Study towards securing hardware virtualization was carried out by Sharif et al. [50] in order to resist kernel-level intrusions. Bratus et al. [51] have also emphasized about need of security towards VMs by investigating the process of root-kit detections. Sammy et al. [52] have presented virtualization schemes that ensure energy conservations as well as higher level of security during VM migration.

4.5 Data Security Encryption/ Decryption

There is a greater deal of arguments among the users and service provider about the safety of their data. It is very common that every online data storage system declare in their service agreement that the data is encrypted; however, there is no evidence about it for the user. It is also scary to know that key to access such confidential data holds in the hand of such technical members in datacenter itself. After the data is being moved on to cloud, there is no clear visualization as well as transparency if the data is 100% safe in data center. According to the American Civil Liberties Union (ACLU), the governments of United States have the right to access the data which are extremely personal and online without even knowledge of the real owner of that data [53]. The conventional data security scheme is shown in Figure12 which normally uses encryption and decryption-based technique using a specific key management technique to store and access the confidential data over the cluster nodes.

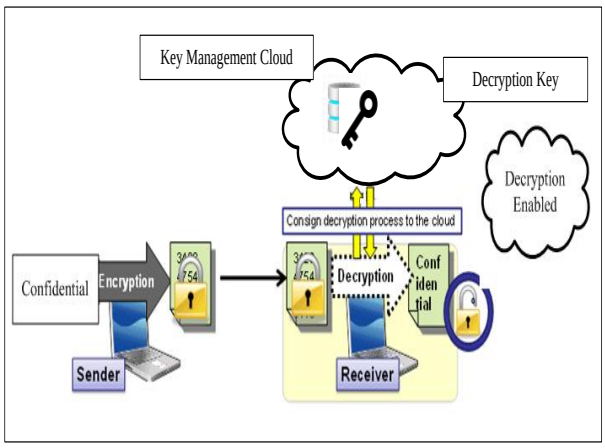

Fig12: Existing Data Security using encryption/decryption

Kaufman [9], in his work, has emphasized on the data security and has discussed about the growing cyber threats in 21st century. Pastoriza and Gonzalez [54] have used cryptography using concept of virtual signal processing. The study conducted by Tyowski and Hasan [55] have applied recursive encryption scheme for data security from mobile applications. The author has also used a unique key-management scheme. Mohanta and Gountia [56] have used homomorphic encryption mechanism while Damgard et al. [57] have harnessed the potential features of cryptographic key management for securing both online and offline sessions in cloud environment.

5. IDNETIFICATION OF RESEARCH GAP

Cloud computing provides a virtual platform of storage and processing a data to reduce the maintenance cost from the user's end. However, security is one of the biggest question mark in cloud computing. There has been constantly an attack report of various cloud based application almost every year, which essentially proves that existing security systems over cloud is definitely not capable of retaining 100% data security in cloud. The most frequently reported an attack over cloud environment is Distributed Denial-of-Services that can potentially disrupt all the three forms of cloud services. Such forms of adversaries can also disrupt the storage system as well as networks. Although cloud computing is not a new name among the research community in 2015, but still research attempts towards providing standard security protocols is still less. This section discusses about the potential research gap that is extracted after reviewing the existing studies.

5.1 Problems in Existing Approaches of IoT

In the existing system, key distribution system is one of the frequently used techniques to secure sensor application if integrated with IoT applications. However, it is quite challenging to use it over IoT. It is because there are various distinct operators controlling such devices in large numbers integrated with diverse radio access techniques in IoT. The existing studies are found to implement physical-layer based security that doesn't go well with multiple radio access technology. Such machine type communications are characterized by unique features in contrast to existing trusted hand-held devices that can feature 3G/4G network services. Unfortunately, such solution is highly limited by restricted capabilities of hardware/software, memory, and energy. Hence, existing techniques (physical layer security) are not suitable for securing IoT applications.

5.2 Problems in Existing Approaches of BA

In the area of BigData Analytics, it has been noticed that Hadoop is frequently used in storing and processing the data. But there is not encryption that is supported by Hadoop as an in-built. Owing to the open-source type of Hadoop, it is quite possible for hacker to have an illegitimate access to the machines and gain an access to valuable analyzed data. If a node posses an administrative priviledge than compromization of that node will lead other nodes vulnerable too especially in case of Hadoop as it is made of design pattern of graphical database system. In existing BigData analytics, it is possible for a node to join the cluster for enhancing the search for knowledge (datamining). However, in order to do so, there is no authentication provided in the existing system of datamining over the clusters. At present such system can allow a third party to join the cluster for intruding the storage of mined data. The most open issues for security in BigData analytics are lack of authentication followed by no record of prior or existing data accessing events. Owing to absence of such data access logs, BigData system cannot be protected from any forms of intrusion at any cost. This problem is still at a large.

5.3 Problems in Existing Policy Management

A robust policy management system should enable the user with self-manage their data over cloud, but it is hard to find in existing system. All the existing authorization system for policy management is controlled by service providers, where

different service providers follow different policy management strategies. Because of this problem, there is a usage of diverse and various forms of policy languages that are incompatible for access control policies. Apart from security, usage of multiple security policies may also result in declination of user positive experience in usage of cloud application offered from multiple service providers. The next problem that arises is interoperation among the service provider which is impossible to design. The final problem when an user takes the same services from two different service providers, maintaining anonymity and ensuring privacy protection using existing system is not addressed in existing studies.

5.4 Problems in Existing Authentication Schemes

Authentication is the next problem pertaining to security in using cloud-based applications. It is already discussed that majority of the cloud-based applications are executed over trusted handheld device. At present, the trusted handheld devices are actually called as mobile apps which run on the top of Mobile Operating system. It is quite common that huge dumps of memory piles up even if the Smartphone is kept idle for 6-7 hours. Hence, using any mobile apps for clearing the overhead memory actually makes the mobile apps automatically logs out. A user has to authenticate them again and again to use the applications. This is one of the simple examples of reality that doesn't match with the theory discussed in existing research papers. The existing single sign on technique is highly dependent on third party, which is again another risk factor.

5.5 Problems in Existing VM Security

The biggest problem with the existing solution of VM security is that it doesn't emphasize the altered association between the hardware components and operating system. Unfortunately, because of this problem the conventional security protocols are challenging to implement. The existing research has also not considered the problem of assigning and de-assigning of resources over VM during virtualization. Moreover, majority of techniques speaks about writing the data to the physical memory of VM, which involved potential security loops if they are not disposed in regular interval. Till date none of the research work has addressed the problem of invisibility of network intrusion between two VM when they are residing on same physical servers. Possibly, it is considered by the researchers are difficult job as entire network traffic from every VM should required to be closely surveilled for intrusion. Finally, none of the research work till date has attempted to discuss that infrastructure management is quite rendered sophisticated using existing virtualization scheme.

5.6 Problems in Existing Data Security

There are massive set of research work carried out in providing security of data in cloud as well as in highly distributed data storage system. Extensive use of cryptography is found in existing data security over cloud. However, there is little research that has addressed the issues of data localization, efficient access controls, instant notification of security breach, performing encryption of key, security of data in motion, etc.

6. POSSIBLE SOLUTION TO ADDRESS RESEARCH GAP

The previous paragraph has discussed about the research gap as well as open end problems that is required to be addressed for ensuring better security standard in using cloud-based applications. A novel system is required to be designed with following security operation:-

6.1 Need of Novel Authentication Scheme

There is a need of designing a unique authentication system that will consider that authentication is always carried out from the mobile devices. A novel enrollment policy can be designed that will specifically consider device information along with few private information about the user. A novel cryptosystem can be formulated which performs non-recursive operation for generating a signature from the password of the user. Hence, even if the password is stolen, the signature couldn't be possibly generated. There should be also investigation towards evolving up with novel authentication scheme for independence features from size limitation.

6.2 Need of Novel Access Control Scheme

The authorization mechanism also needs to be quite unique. There is a need of a system where the mutual authentication takes places without any human intervention. The possible solution for robust novel authorization scheme can be used for generating secure code using multi-authentication system for generating better access control mechanism. A hybrid mechanism of cryptographic algorithm can be used for securing data and the secret key. This approach will be mainly meant for addressing the research gap pertaining to data security and overcoming the existing issues of authentication and access control schemes.

6.3 Need for Development of Cloud Bucket

For an efficient data segmentation and ownership, it is essential for the data to be stored over cloud buckets created by user itself. This development has two advantages viz. i) enhancement and transparency to policy management system, and ii) enhancing the access control of data over cloud.

6.4 Development of Virtual Security

A novel cryptographic security protocol is required to be developed for enhancing the access control over virtual machines. A light weight cryptographic algorithm is required to be written for further enhancing the virtual isolation process over cloud.

7. CONCLUSION

This paper discusses about changing era of technologies in the area of cloud computing especially focusing on its loopholes that creates security breaches. Till date, there are many reputed service provider who claims standard security, but it is hard to find it in reality owing to the continuous reports of attacks. Although the existing services offer are economical, but there is no assurity of resiliency against potential security threats in the existing security policies. Right from data ownership to the present practices of cryptographic techniques are highly questionable. The paper has discussed some of the essential charecteristics of cloud computing in terms of upcoming application i.e. Internet-of-Things and BigData Analytics. The existing literatures are found to be more theoretical and less practical. Hence, availability of an efficient and standard research work towards futuristic applications of cloud-based services are just in the beginning stage. The paper has also discussed about the security issues related with them, which is still unsolved. Finally, the paper has raised the existing security techniques applied to safeguard the services rendered by the service providers. It has been explored that there is still an open problems in

access control, authentication and authorization, security of virtual machine, and finally the data security, which are definitely not sufficient enough. The final part of the paper has discussed some of the possible hints as a probable solution to outperform the existing approaches. The future work will be in the direction to implement the possible solution using experimental approach.

8. REFERENCES

[1] Forbes Technology. 2015. "Roundup of Cloud Computing Forecasts and Market Estimates Q3 Update, ,"http://www.forbes.com/sites/louiscolumbus/2015/09/27 /roundup-of-cloud-computing- forecasts-and-market-estimates-q3-update-2015/, [online, visited on 27th September]

[2] Cisco. 2019. "Cisco Visual Networking Index: Forecast and Methodology, 2014-2019 White Paper)," http://www.cisco.com/c/en/us/solutions/collateral/service -provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html, [online, visited on 27th September]

[3] Evdokimov, S., and Günther, O.2007. Encryption techniques for secure database outsourcing. In Computer Security, ESORICS, pp. 327-342

[4] Oprea, A.M.2007. Efficient cryptographic techniques for securing storage systems. PhD diss., IBM Zurich

[5] "Examples of Current Cloud Applications", .Retrieved, 22nd Sep, 2015. Link:-http://www.evo-uk.org/at-the-outset/cloud-computing/examples-of-current-cloud-applications/, Retrieved, 29th September, 2015

[6] Ko, R., Choo, R. 2015. The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues. Syngress, Computers, pp. 570

[7] Lim, I., Coolidge, E. C., Hourani, P.2013. Securing Cloud and Mobility: A Practitioner's Guide. CRC Press Business & Economics, pp. 228,

[8] Yang, X. 2013. Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing. IGI Global Computers, pp. 452

[9] Salam, A., Gilani, Z., Haq, S. U.2015. "eploying and Managing a Cloud Infrastructure: Real-World Skills for the CompTIA Cloud+ Certification and Beyond: Exam CV0-001. John Wiley & Sons Computers, pp. 456

[10] Marinescu, D. C.2013. Cloud Computing: Theory and Practice. Newnes Computers, pp. 416

[11] Sen, J.2013. Security and Security and Privacy Issues in Cloud Computing. Architectures and Protocols for Secure Information Technology Infrastructures, pp. 1-45

[12] Hwang, K., Dongarra, J., Fox, G.C.2013. Distributed and Cloud Computing: From Parallel Processing to the Internet of Things. Morgan Kaufmann Computers, pp. 672

[13] Shinder, D.2011. Security Considerations for Infrastructure as a Service Cloud Computing Model. WindowSecurity.com

[14] Potter, D.2015. SaaS, PaaS and IaaS: What you need to know about the risks. Arrow ECS E-Magazine

[15] He, D., and Zeadally, S.2015. An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment using Elliptic Curve Cryptography. IEEE Internet of things Journal, Vol. 2, No. 1

[16] Ning, H., Liu, H., and Yang, L. T.2015. Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things. IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 3

[17] Li, F., and Xiong, P.2013. Practical Secure Communication for Integrating Wireless Sensor Networks into the Internet of Things. IEEE Sensors Journal, Vol. 13, No. 10

[18] Premnath, S.N., and Haas, Z. J.2015. Security and Privacy in the Internet-of-Things under Time-and-Budget-Limited Adversary Model., IEEE Wireless Communications Letters, Vol. 4, No. 3

[19] H-Ramos, J. L., Pawlowski, M. P., Jara, A. J., Skarmeta, A. F., and Ladid, L.2015. Toward a Lightweight Authentication and Authorization Framework for Smart Objects, IEEE Journal on Selected Areas in Communications, Vol. 33, No. 4

[20] Hu, W-C.2013.Big Data Management, Technologies, and Applications. IGI Global Computers, pp. 342

[21] Gadepally, V., Hancock, B., Kaiser, B., Michaleas, J. K. P., Varia, M., Yerukhimovich, A. 2015. Computing on Masked Data to Improve the Security of Big Data", Institute of Electrical and Electronics Engineers

[22] Islam, M.R., and Islam, M. E.2014. An approach to provide security to unstructured Big Data. In Software, Knowledge, Information Management and Applications (SKIMA), 8th International Conference, pp. 1-5

[23] Lu, R., Zhu, H., Liu, X., Liu, J. K., and Shao, J.2014. Toward efficient and privacy-preserving computing in big data era. Network, IEEE, Vol. 28, No. 4, pp.46-50

[24] Vaquero, L., Celorio, A., Cuadrado, F., and Cuevas, R.2015. Deploying Large-Scale Data Sets on Demand in the Cloud: Treats and Tricks on Data Distribution

[25] Marchal, S., François, J., State, R., and Engel, T.2014. PhishStorm: Detecting Phishing with Streaming Analytics. Network and Service Management, IEEE Transactions, Vol. 11, No. 4, pp.458-471

[26] Tari, Z., Yi, X., Premarathne, U.S., Bertok, P., and Khalil, I.2015. Security and Privacy in Cloud Computing: Vision, Trends, and Challenges. Cloud Computing, IEEE, Vol. 2, No. 2, pp. 30-38

[27] Jeyakanthan, M., and Nayak, A.2012. Policy management: leveraging the open virtualization format with contract and solution models. Network, IEE, Vol. 26, No. 5, pp. 22-27

[28] Hamlen, K.W., Kagal, L., and Kantarcioglu, M.2012. Policy Enforcement Framework for Cloud Data Management. IEEE Data Eng. Bull, Vol. 35, No. 4, pp. 39-45

[29] Hassan, T., and Joshi, J.B.D.2012. Semantic-based policy management for cloud computing environments. International Journal of Cloud Computing, Vol. 1, No. 2-3, pp.119-144

[30] Sandhu, R., and Chana, I. Retrived, 12th Oct, 2015. Securing Virtual Machine in Cloud Enviroment using OVF and Hashing Function

[31] Open ID Connect Connects your Businesses: A Simple Identity Layer on top of OAuth 2.0", OPen ID, Link: - http://openid.net/, Retrieved, 22nd Sep, 2015

[32] "passport-ibm-connections-cloud", Link:- https://www.npmjs.com/package/passport-ibm-connections-cloud, Retrieved, 23rd Sept, 2015

[33] Kapoor, V., Abraham, V. S., and Singh, R.2008. Elliptic curve cryptography. ACM Ubiquity, Vol. 9, No. 20, pp.20-26

[34] Abdullah, K.2010. Comparison between the RSA cryptosystem and elliptic curve cryptography. PhD diss., The University of Waikato

[35] Meffert, D.2009. Bilinear pairings in cryptography. PhD diss., Master's thesis, Radboud Universiteit Nijmegen

[36] Kate, A., and Goldberg, I.2010. Distributed private-key generators for identity-based cryptography. In Security and Cryptography for Networks, Springer Berlin Heidelberg, pp. 436-453

[37] Tsai, J-L., and Lo, N-W.2015. Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services.IEEE Systems Journal, Vol. 9, No. 3

[38] Ahn, H., Chang, H., Jang, C., and Choi, E.2011. User Authentication Platform using Provisioning in Cloud Computing Environment. In Advanced Communication and Networking,Springer Berlin Heidelberg, pp. 132-138

[39] Kim, J-M., and Moon, J-K.2014. Research Article Secure Authentication System for Hybrid Cloud Service in Mobile Communication Environments. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, pp. 7,

[40] Ghazizadeh, E., Shams, Z. S., Dolatabadi, R. Khaleghparast, M. Zamani, A. A.Manaf, and Abdullah, M. S.2014. Research Article Secure OpenID Authentication Model by Using Trusted Computing", Hindawi Publishing Corporation, pp. 15

[41] Dranger, S., Sloan, R. H., and Solworth, J. A.2006. The complexity of discretionary access control. Springer Berlin Heidelberg

[42] Ferraiolo, D.F., and Kuhn, R.D. 2009. Role-based access controls", arXiv preprint arXiv:0903.2171

[43] Sandhu, R.S., Coyne, E. J., Feinstein, H.L., and Youman, C.E. 1996. Role-based access control models", Computer, Vol. 2, pp. 38-47

[44] Lin, G., Wang, D., Bie, Y., and Lei, M.2014. MTBAC: A mutual trust based access control model in cloud computing. Communications, China, Vol. 11, No. 4, pp.154-162

[45] Yeo, S-S., Kim, S-J., and Cho, D-E.2014. Research Article Dynamic Access Control Model for Security Client Services in Smart Grid. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, pp. 7

[46] Wang, C., Zou, P., Liu, Z., and Wang, J. 2011. Research Article CS-DRM: A Cloud-Based SIM DRM Scheme forMobile Internet. Hindawi Publishing Corporation EURASIP Journal onWireless Communications and Networking, pp. 19

[47] Liu, Q., Weng, C., Li, M., and Luo, Y.2010. An In-VM measuring framework for increasing virtual machine security in clouds. Security & Privacy,Vol. 8, No. 6, pp. 56-62

[48] Zhu, H., Xue, Y., Chen, X., Li, Q., and Li, H.2015. Research Article V-MGSM: A Multilevel and Grouping Security Virtualization Model for Mobile Internet Service. Hindawi Publishing Corporation Mobile Information Systems, pp. 9

[49] Benninger, C., Neville, S. W., Yazır, Y. O., Matthews, C., and Coady, Y.2012. Maitland: Lighter-weight vm introspection to support cyber-security in the cloud. In Cloud Computing (CLOUD), 2012 IEEE 5th International Conference, pp. 471-478

[50] Sharif, M., Lee, W., Cui, W., and Lanzi, A.2009. Secure in-vm monitoring using hardware virtualization. In Proceedings of the 16th ACM conference on Computer and communications security, pp. 477-487

[51] Bratus, S., Locasto, M.E., Ramaswamy, A., and Smith, S.W. 2010. VM-based security overkill: a lament for applied systems security research. In Proceedings of the workshop on New security paradigms, pp. 51-60

[52] Sammy, K., Shengbing, R., and Wilson, C.2012. Energy efficient security preserving vm live migration in data centers for cloud computing. International Journal of Computer Science Issues. 9, No. 2, pp.2-3

[53] Mearian, L.2015. News Analysis: - No, your data isn't secure in the cloud. Computer World,Reteived

[54] T-Pastoriza, J.R., and González, F.P.2011. CryptoDSPs for cloud privacy. In Web Information Systems Engineering–WISE 2010 Workshops, Springer Berlin Heidelberg, pp. 428-439

[55] Tysowski, P.K., and Hasan, M. A.2011. Re-Encryption-Based Key Management towards Secure and Scalable Mobile Applications in Clouds. IACR Cryptology ePrint Archive, pp. 668

[56] Mohanta, B.K., and Gountia, D.2013. Fully homomorphism encryption equating to cloud security: An approach. IOSR Journal of Computer Engineering (IOSR-JCE)

[57] Damgård, I., Jakobsen, T.P., Nielsen, J.B., and Pagter, J.I. 2013. Secure key management in the cloud. In Cryptography and Coding, Springer Berlin Heidelberg, pp. 270-289