EMERGENT TECHNOLOGY: CLOUD COMPUTING SECURITY NETWORK

BASAKY D. FREDERICK, PhD.
Information Technology Department
Salem University, Lokoja
Kogi State

&

BAKARE KAREEM, PhD.
Information Technology Department
Ahmadu Bello University, Zaria
Kaduna State

Abstract

The exponential growth of cloud computing is changing the way organizations are functioning now a days. A cloud based system changes the services seamlessly without expending much time and resources in setting up new systems. Apart from this, there are lots of benefits like scalability, significant cost reduction, high availability and quality in a cloud based system. Although there are many advantages cloud computing, issues related with security and privacy are some of the major challenges, which needs to be addressed for the successful deployment of a cloud based system. Therefore, it is absolutely critical to have a robust security services fully implemented based on cloud-based security framework/Guidelines. At present there are a number of standard security framework/Guidelines like ISO 27001/27002, NIST 800-53, but these entire standard are in evolving stage for the cloud computing Environment. Apart from this, the security requirements of an organization also vary based on specific security risks of the organization. This paper first introduces a new set of security control Theory. These principles theory is based on People, Process and Technology Theory (P^2T^2) from the Enhance Concept Security Matrix (ECSM) basically a cloud based Security Framework CSF.

Keywords: Cloud-Based, Security Framework, Security Requirements, Cloud Computing

Introduction

The exponential growth of internet has not only changed our life, but it has also changed the functioning and service delivery models of the governments. The rise of e-Government has been one of the most important developments of the web. E. Governance is the application of information and communication technologies (ICT) to exchange information between the government and the citizens, government and businesses and between government organization {1} According to the National institute of standards and technology (NIST), “Cloud computing is a model for enabling ubiquitous, convenient, no-demand network access to a shared pool of configurable computing resources (e.g., network, servers, storage, applications and services)that can be rapidly provisioned and released with minimal management effort or service provider interaction" Muzaffar, et al (2015)**.** Cloud computing is a new way of providing services over internet. Cloud based e-Governance system provides services reduced cost and manages security, scalability and accountability [3]. The available resources such as storage, memory, processing power and bandwidth are used efficiently in a cloud based system. It also ensures high availability and quality. Although there are many advantages of cloud computing, issues related with security and privacy are some of the major challenges, which needs to be addressed for the successful deployment of a cloud based e-Government system [4]. Security of information means confidentiality, integrity, proper authentication and reliability of information. The issue of security and privacy is further enhanced in a cloud based e-Government system as the confidential data is being stored outside stored outside the physical.

International Journal of science, Technology & Management
Volume No.04, Issue No. 02, February 2015

Boundary of the organization. Therefore, it is absolutely critical to have a robust security services fully implemented based on security framework/Guidelines. At present there are a number of standard security framework/guidelines like ISO 27001,] 27002 NIST 800-53, but all these standards are in evolving stage for the cloud computing environment. Although ISO/IEC 27001 Provides generic guidance in developing the security objectives and metrics, but it still does not provide methods to guide the organizations. Apart from this, the security requirements of an organization vary based on the specific security risks of the organization. Therefore it is absolutely essential to have a comprehensive end-to-end security framework based on industry standards, but tailored to the specific requirement of an organization. During literature survey it has been found that very limited work has been done in the field of security framework of an cloud security especially for a cloud based While reviewing industry security framework and guidelines, it was found out that there are no cloud security framework, best practices and guidelines for a cloud based security This paper first introduces a new set of security control principles called e-Governance Security Matrix (EGSM) especially for the cloud based e-Governance Systems based on the security control principles described by Vic (J.R.) Winkler and after mapping the security requirement of other industry standard framework like ISO 2001, Cloud control Matrix (CCM), NIST SP 800 -144. A new e-Governance Security Framework (EGSF) has also been proposed for such cloud based e-Governance systems. The most important feature of the proposed security framework is to devise a mechanism through which an organization can have a path of improvement along with understanding of the current security maturity level & defining desired state in terms of security metric value. The paper is organized as follows: section 2 presents the existing work on cloud security and security maturity levels. Section 3 presents the new set of security control principles called e-Government security matrix (EGSM). Section 4 presents the proposed security framework for cloud based e-Governance (EGSM). Section 4 presents the proposed security framework for cloud based e-Governance (EGSF). Section 5 present conclusion and future work.

The state of insecurity in Nigeria today is no news to anyone and although, it can be attributed on some factors that have been left unchecked for a long time by both the Government and people of Nigeria but the level of insecurity in the country today is threatening to tear her apart and requires quick, adequate and a new approach to deal with the security challenges plaguing the nation. Apart from food insecurity, financial insecurity, terrorism, health insecurity and others, security failure has eaten deep into the fabrics of the country.

The situation in Nigeria since the beginning of this decade in which dozens of military groups emerged and challenged in the most violent form the authority of the Government; the growing level of urban crime including armed robbery, kidnappings, ritual killings, and cultism; the continuing erosion of the moral authority of religions in which people engage in acts in open defiance of their religious and moral teachings; the culture of impunity that characterizes public affairs; the corruption that is submerging the average Nigerian; and the collapsing social and political institutions in the country over the last few years, more than anything demand for quick and lasting solutions that will at least reduce the security threats facing Nigeria today.

There is general agreement among historians that insecurity have been the core cause of bloodshed in Nigeria and the world at large.

The deep scars that insecurity leave on people and nations are often obscured by historical accounts that, more often than not, glorify conquest and ignore aggression. One major challenge been faced by Nigerians deserving for more attention as far as security, aping and conflict management is concerned is their effect on everyday life. Muzaffar, et al (2015) The inevitable security issues leading to subsequent destruction of lives, properties and the environment calls for a holistic approaches through effective used of information technology.

Thus, ICT has consistently been proven a powerful double-edged sword with a capability for both overwhelming good and devastating evil, all depending on the skills and values of thee user (s) in harnessing its powers in either or both directions. In this paper, we trace the evolution of Nigeria security challenges possible cause of insecurity and develop a framework of solving the challenges through using information technology as regards internet of things.

Although Nigeria have taken bold steps to settle their insecurity issues through combat approach, there still exist several unresolved issues bordering the country peaceful coexistence on one hand, and accurate mapping of contiguous area using geospatial science and technology such as satellite Remote Sensing (RS), Geographic information System (GIS) and Global Navigational Satellite Systems (GNSS) on the other hand.

Hofstede, 2002 stated that "One of the most important features of the digital age is the use of new communications technologies to build digital citizenship

Existing Work on Cloud Security Blueprint Muzaffar, et al (2015)

There are several organization/consortia actively involved in the development of security standards/guidelines. Some of the cloud security framework/Guidelines being developed by several consortia/organizations are as following:

National Institute of Standards and Technology

(NIST) has released special drafts and reports on security issues as well as recommendations for the cloud computing. It has released a special publication "Guidelines" on security and privacy in public cloud computing (NIST SP 800-144)" Muzaffar, et al (2015). The guidelines provide, in NIST'S description "an overview of the security and privacy challenges facing public cloud computing and presents recommendations that organizations should consider when outsourcing data, application and infrastructure to a public cloud environment. The document provides insights on threats, technology risks and safeguards related to public cloud environment to help organizations make informed decision about this use of this technology." The recommendations have been given in following Areas:

1. Availability
2. Identity and Access Management
3. Architecture
4. Software Isolation
5. Data Protection
6. Incident Response
7. Compliance
8. Trust

ISO/IEC 27000 Family Code of Practice for Information Security, Muzaffar, et al (2015)

Management

The ISO/IEC 27000 Family of information security standards is developed and published by the international organization for standardization (ISO) and the international Electro technical Commission (IEC). It is one of the most widely used security framework for the information security and management. The security standards related with the cloud computing are as following:

ISO/IEC 27002:2013 is the security framework which describes the security control objectives and controls. The twelve guiding security control principles of the ISO/IEC 27002 are:

i. Access control
ii. Physical and environmental security
iii. Risk assessment and treatment
iv. Security policy
v. Organization of information security
vi. Assets management
vii. Communications and operations
viii. Information systems acquisitions, development and maintenance
ix. Information security incident management
x. Business continuity management
xi. Human resource security
xii. Compliance

ISO/IEC 27017

The ISO/IEC 27017 is in draft stage and well provide a framework for some additional security controls beyond provided in ISO/IEC 27002. The standard will provide guidance on the information security elements of cloud computing, recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO2K standards including ISO/IEC 27018 on the privacy aspects of cloud computing, ISO/IEC 27031 on business continuity, and ISO/IEC 27036-4 on relationship management, as well as all the other ISO27k standards

ISO/IEC 27018

The ISO/IEC 27018 is a security framework which covers PII (Personally identifiable information in public clouds.

ISO/IEC 27036:2013+

The ISO/IEC 27036:2013+ is a multi – part security framework for providing guidelines for supplier relationships including the relationship management aspects of cloud computing (parts 1,2 and 3 have been published so far)

ISO/IEC 21827: System Security Engineering Capability Maturity Model

The systems security engineering capability maturity model (SSE-CMM) is also known as the ISO/IEC 21827 standard. It defines five levels of maturity models as shown in fig. 1 below:

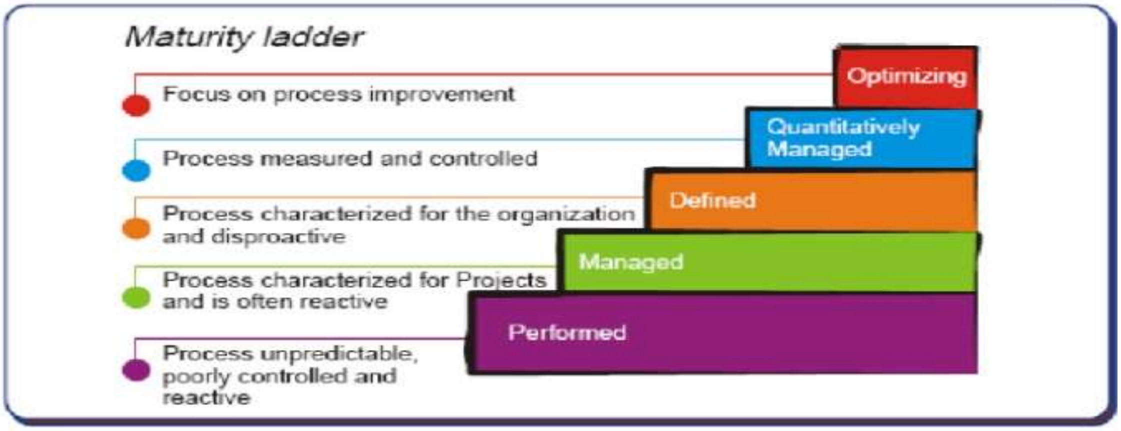

Maturity ladder
Focus on process improvement
Process measured and controlled
Process characterized for the organization and disproactive
Process characterized for Projects and is often reactive
Process unpredictable, poorly controlled and reactive
Optimizing
Quantitatively Managed
Defined
Managed
Performed

Figure 1: System Maturity Model

Cloud Security Alliance (CSA) Muzaffar et al (2015)

The CSA alliance provides advice for both cloud computing customers as well as for cloud service providers. The Cloud Security Alliance Cloud Controls Matrix (CCM) is the security framework for guiding cloud vendors and prospective cloud customers assessing the overall security risk of a cloud provider. The framework is based on other industry-accepted security standards, regulations and controls frameworks such as the ISO 27001/27002, NIST, ISACA COBIT, PCI and Jericho Forum. The CSA CCM Framework provides information regarding information security control requirements. It identifies security threats and vulnerabilities in the cloud as well as provides information regarding standardized security and necessary security measures to be taken. Various strategic domains as covered in CCA CCM (CSA guide version 3.0) are as following:

1. Application & Interface Security
2. Audit Assurance & compliance
3. Business Continuity Management & Operational Resilience
4. Change control & Configuration Management
5. Data security & Information Lifecycle Management
6. Data Centre security
7. Encryption & Key Management
8. Governance and Risk Management
9. Human Resources
10. Identity & Access Management
11. Infrastructure and virtualization security
12. Interoperability and portability
13. Mobile Security
14. Security Incident Management, E-Discovery & Cloud Forensics
15. Threat and vulnerability Management
16. Supply Chain Management, Transparency and Accountability

Distributed Management Task Force (DMTF)

The distributed Management Task Force (DMTF) is an organization which is actively involved in the development, adoption and interoperability of management standards and initiatives for the enterprise and internet environment. It has established a Framework to promote standards for cloud security and interoperability between clouds.

Storage Networking Industry Association (SNIA)

The storage Networking Industry Association (SNIA) has developed an framework, cloud Data Management Interface (CDMI), which is a open standard for data as a service as part of cloud computing.

Open Grid Forum (OGF)

The open cloud computing interface (OCCI) [18] is a framework developed by open Grid Forum. OCCI is a protocol and API for all kinds for management tasks, which was originally developed for creating remote management API for IaaS model based service. The current release of the framework is now suitable to all models (IaaS, PaaS and Saas) and addresses all technical and operational security issues in the grid and cloud environments.

Association for Retail Technology Standards (ARTS)

The Association for Retail Technology Standards (ARTS) Version 2.0 is a framework for the cloud computing in Retail. The framework provides guidelines for the reliability, availability and security for cloud – based solutions.

Cloud standards Customer Council (CSCC)

Cloud standards customer council (CSCC) is an end user advisory group working for the acceleration of cloud adoption and addressing security and interoperability issues surrounding the transition to the cloud. The council provides cloud users with the opportunity to drive client requirements into standards development organization and deliver materials such as best practices and use cases to assist other enterprises.

Organization for the Advancement of Structured Information Standards (OASIS)

OASIS (Organization for the Advancement of Structure Information Standards) is an international consortium for promoting the adoption of product-independent standards for information formats such as Extensible Markup Language (XML), Standard Generalized markup Language (SGML), and Hypertext Markup Language (HTML). The OASIS Cloud Application Management for Platforms (CAMP) Technical committee has developed an interoperable protocol that cloud implementers can use to package and deploy their applications. It defines interfaces for self – service provisioning, monitoring, and control.

This history and words of Biafra civil war is yet healed n us in May 1999 Nigeria’s return to civil rule was accompanied with fresh hopes and latent optimism. This optimist is predicated on the fact that democracy would guarantee freedom, liberty, and equity and enhances security of lives and property, which would indeed repositions development trajectories to sustainability. Regrettably this optimism seems to be a mirage. Nigeria is presently related as one of the poorest nations in the world with debilitating youths' unemployment. For instance, Aganga (2009) observed that over ten million Nigerians were unemployed by March 2009 and unemployment is running at around 19.7 present on average (National Bureau of Statistics Report 2009). This figure geometrically increases yearly with less realistic efforts by the managers of the state to abate the rampaging unemployment problem.

In Nigeria, like many other developing countries, about 70% of the population lives in poverty (Otto and Ukpere, 2012). Majority of the population seem to lack access to pipe borne water, health care facilities, electricity and affordable quality education. Amidst these development challenges, the security situation in the country deteriorated drastically. Nigeria's return to democratic rule is threatened by security disaster. Arguably, series of resource based conflict (Niger Delta), ethno-religions crisis (Jos crisis), and communal conflicts persisted. The climax of these security threats is the insurgence of a group called Boko Haram in the Northern Nigeria. Thus, a considerable effort to end the violence and build a sustainable peace to steer the economy to sustainability seems far from realization. The basic questions are: why development has continued the elude Nigeria in spite of numerous amounts of human and material resources? To what extent has security crisis impacted or contributed to development crisis in Nigeria? Is Boko Haram really a threat to development in Nigeria the latest in Fulani Herdsmen needed urgent attention especially now Nigeria is struggling to be among twentieth world developed countries in 2020?

Dimensions of security Crisis in Nigeria: Implications for National Development in the discourse of security in Nigeria, Okorie (2011), Salawu (2010), Onyishi (2011), Ezeoha (2011), Lewis (2002), have identified several causes of security crisis in Nigeria that pose grave consequences to national development. Chief among them is ethno-religious conflicts that tend to have claim many live in Nigeria. By "ethnic - religious", it means a situation in which the relationship between members of one ethnic or religious and another of such group in a multiethnic and multi-religious society is characterized by lack of cordiality, mutual suspicion and fear, and a tendency towards violent confrontation (Salawu, 2011).

Since independence, Nigeria appears to have been bedeviled with ethno-religious conflicts. Over the past decades of her Nationhood, Nigeria has experience a palpable intensification of religious polarization, manifest in political mobilization, sectarian social movements, and increasing violence (Lewis2002). Ethnic and religious affiliations determine who gets what in Nigeria; it is so central and seems to perpetuate discrimination. The return to civil rule in 1999 tends to have provided ample leverage for multiplicity of ethno-religious conflicts.

Uhunmawuangho and Epelle (2011) contended that democracy has increased the culture of impunity in some people while political differences are believed to have fuelled some of the violence that have erupted.

What this means theoretically is that poverty and unemployment increase the number of people who are prepared to kill or be killed for a given course at token benefit, (Salawu, 2010). It could predispose one to engaging in illicit activities that would undermine security of the environment.

A cursory look at electoral politics in Nigeria since 1999 depicts a catalogue of election related assassinations. For instance, on 23rd of December, 2001, the former Attorney General of the Federation Chief Bola Ige was assassinated and on March 5, 2003 Harry Marshall – the national Vice Chairman for the South – South Zone of all Nigeria peoples party was also assassinated (Iduh 2011).

The former Nigeria Bar Association Chairman, Onitsha Branch in Anambra State Barnabas Igwe and his wife were gruesomely murdered on September 1,2002 and Engr. Funsho Willians, Dr.Ayodeji Daramola former gubernatorial candidates of PDP in Lagos and Ekite State suffer the same fate (Iduh 2011). Recently, a serving senator from Plateau State, Sentor Dantong Gyang Daylop, the majority leader of Plateau State House of Assebly Honorabless Gyang Fulani were gruesomely murdered while many where left injured by unidentified gunmen (Sun newspaper July 9, 2012). Indeed, incessant political violence in Nigeria could be attributed to over-zealousness and desperation by political gladiators to win elections or remain in office at all cost.

Also systemic and political corruption in Nigeria seems to have added another dimension of violent conflicts which has eroded National values. Corruption is bad not because money and benefits change hands, and not because of the motives of participants, but because it privatizes valuable aspects of public life, bypassing processes of representation, debate, and choice (Thompson in Graflambsdorff 2001).

More succinctly, Jega, 2002 captures the symptoms that cause insecurity in Nigeria when he observed that Nigeria is one of the nations in the world whose political landscape has been inundated, suffused with and deeply enmeshed in spectrum of recurring complex conflicts ranging from resource, communal, to political and ethno-religious conflicts. The implication of all these setbacks is poor implementation of policies, rising unemployment, hardship, economic and political stagnation that gives rise to the present threatening insecurity which seems to be developing beyond the capacity of state.

Boko Haram as a Threat to National Security in Nigeria

Boko Haram is a religious Islamic sect that came into the limelight in 2002 when the presence of the radical Islamic sect was first reported in Kanama (Yobe State) and also in Gwoza (Borno State). “Boko Haram,” which in the local Hausa languge means “Western education is forbidden,” officially calls itself “Jama “atul Alhul Sunnah Lidda “wati wal Jihad,” which means “people committed to the propagation of the prophets “teachings and Jihad” (Meehan and Speier 2011). Beyond religious explanations, Boko Haram could be arguably described as a “home - growth” terrorist group that romances with some desperate politicians in the North. It appears that the sect enjoys effective support from some well-to – do individuals, religious leaders, allies, admires of their ideology and highly placed politicians in the North who claim to be Nigerians but are clandestinely working against the State.

For instance, Lister, (2012), observed that it is no longer a sect of Islamic fanatics but has the support of disgruntled politicians and their paid thugs (Adagba, Ugwu and Eme, 2012). Recently, revelations and security investigations into the activities of the sect tend to affirm that the group is also sponsored from within the country. This simultaneously transpires within the period when a serving senator from the North is on trial for aiding the activities of Boko Haram. Thus, a senior official of Boko Haram allegedly granted an interview detailing how the sect had been on the payroll of a few governors of the North (Adagba etal, 2012). Thus, Boko Haram seems to be destructive political tool with a cosmetic pretension of being religious.

This indiscriminate and sporadic bombing seem to make Northern Nigeria increasingly unsafe and has compelled most non – indigenes of the region to relocate especially the Igbos. This phobia of being attacked especially in cities like Kano, Kaduna, Maiduguri, Jalingo and Yola was responsible for the exodus of people from the North to other parts of the country as witnessed in the last few months. According to Idika, in a press statement; Today’s cities are on the frontline of crime and terrorism. While some of them are clearly more at risk than others, all of them are vulnerable. Not surprisingly, cities are experimenting with innovative approaches to preventing crime and countering extremism.

The most successful are improving intelligence gathering, strengthening policing and community outreach, and investing in new technologies to improve urban safety. Such cities are said to deploy ‘agile security’: data – driven and problem – oriented approaches that speed up decision – making and design in environmental changes to limit insecurity.

Agile security measures start with the premise that many types of crime, radicalization and terrorism are non-random and even predictable. With some exceptions, they tend to cluster in time, space and among specific population groups. The massive increase in computing power and advances in machine learning have made it possible to sift through huge quantities of data related to crime and terrorism, to identify underlying correlations causes. The harnessing and processing of these data flows crucial to enabling agile security in cities.

Methodology

Proposed cloud based Security Matrix (ECSM)

Several cloud security framework and Guidelines have been described in last section. While reviewing those security framework, best practices, and guidelines defined as per the specific security requirement of a cloud based security The new set of security control principles called e-Government security matrix (EGSM) is based on the security control principles described by vic (J.R) Winkler [9] as well as other industry standard framework like ISO 2001, Cloud control Matrix (CCM), NIST SP 800 – 144.

It consists of four security control domains as following:

1. Foundational Security Doman
2. Deep Defense Domain
3. Operational Security Domain
4. Business requirement Domain

Each domain is further divided into different Security control areas as shown in the fig. 2 below:

Discussion

Fig. 2: Security Matrix (EGSM)

Code No	Security Control Area	Security Control Principle	Principle code No
FS1	Security Policy	Security Policy	FS 1.1
		Security Principles & Standards	FS 1.2
		Security Guidelines & Procedures	FS 1.3
FS2	Cloud Service Providers (CSP)	Cloud Service Providers (CSPs) Management	FS 2.1
		Security Requirements of CSPs	FS 2.2
		Security in SCPs Operations & Support System	FS 2.3
		CSP Audit & Compliance	FS 3.1
FS3	Third Party Providers (TPA)	Third Party Providers (TPA) Management	FS 2.4
		Security Requirement of TPAs	FS 3.1

		Security in TPAs Operations & Support System	FS 3.2
		TPA Audit & Compliance	FS 3.3
FS4	Personnel Security	Security prior to employment	FS 4.1
		Security during Employment	FS 4.2
		Security after change of Employment s	FS 4.3
		Security Awareness & Training	FS 4.4

Table 1: Security Control Domain (Foundational Security)

Code No	**Security Control Area**	**Security Control Principle**	**Principle Code No**
DD1	Identity & Access Management	Federated Identity Management	DD1.1
		Privileged Identity Management	DD1.2
		Business Access Requirements	DD1.3
		User Access Management	DD1.4
		Application & information Access Management	DD1.5
		Hypervisor & O/S Access Control	DD1.6
DD2	Security of Service Delivery Model	Service Delivery Models (Saas Paas, Iaas) Management	DD2.1
		Security in Service Delivery Model Operations	DD2.2
DD3	Host & VM Security	Security Requirement of Host & VM	DD3.1
		Virtualization	DD3.2
DD4	Appln. SW Quality Assurance	Application & Software Maintenance	DD3.3
DD5	Network Security	Network Security Management	DD4.1
DD6	Wireless Security	Wireless Security	DD5.1

		Management	
DD7	Cryptography & Key Management	Cryptographic Control & Key Management	DD6.1
		User Access Management	DD7.1
		Application & information Access management	DD7.2
		Hypervisor & O/S Access Control	DD7.3

Table 2: Security Domain 2 (Deep Defense)

Code No	Security Control Area	Security Control Principle	Principle
OSI	Physical & Environment Security	Physical Access Management	OS1.1
		Environmental Control	OS1.2
OS2	Assets Management	Assets control Management	OS2.1
OS3	Governance and Risk management	Risk Management	OS3.1
		threat and vulnerability Management	OS3.2
		Data Governance	OS3.3
OS4	Security Incident Management	Security Incident Management	OS4.1
OS5	Operation practices	Operation control	OS5.1
		Configuration Management	OS5.2
		Media & memory protection	OS5.3
		Fail –safe protection	OS5.4
		Denial of service protection	OS5.5
		Application partitioning	OS5.6
		Security function isolation	OS5.7
		Honeypots	OS5.8

		Boundary & session protection	OS5.9

Table 3: Security Domain 3 (Operational Security)-

Code No	Security Control Area	Security Control Principle	Principle code no
BR1	Business continuity management	Business continuity management	BR1.1
		Disaster recovery planning	BR1.2
		Backups & contingency planning	BR1.3
BR2	Legal Compliance	SLA Planning	
		Legal Audit & Compliance	BR2.1
BR3	Audit Assurance & compliance	Audit Planning	BR2.2
		Audit Assurance	BR3.1
		Third Party Audits	BR3.2
BR4	Resource Planning	Assets Control Management	BR3.3

Step- 1 Selection of Control Areas: The selection of security control areas (group of security control principles) is /the first step for the development of a comprehensive security framework. The paper has presented a new set of security control areas/principles called e-Government security matrix (EGSM) applicable for a cloud based e-Government system in last section. However the security requirements of an organization change continuously in view of emerging new threats and vulnerabilities, therefore it is absolutely necessary to map the security control areas of the EGSM with other security framework / guidelines like ISO 27001/27002, NIST 800-53 and fill the gap, if any.

Step-2 Identify & define control principles: once different security control area (group of security control principles) has been identified as discussed in last step, it needs to be broken down into different security control principles. The security control principles should be practical and should be customized based on business requirements of the organization.

Step – 3 Build Requirement Cross matrix: Most industry security standards, while different, are based on the same security principles/requirements, therefore, similarities among the standards should be group together and combined.

Step – 4 Develop & Prioritize Requirements: once security requirement have been based mapping of different security standards and guideline, it is very important to prioritize the requirement based on constraints of available resource as well as after identifying both the impact and risk exposure. A cost analysis of the resources required for carrying out requirement is very useful in prioritizing the requirements.

Step- 5 Security Policy formalization: The next step of the security framework is to create and define a clear policy based on the security requirement finalized in last step. Policies set organizational direction and carry the weight of management. Policies should be updated as per need. Security policy states the reasons and identifies the rules, standards. It says what must be done whereas the guidelines say how it should be done.

Step – 6 Develop Security Measurement & Metrics: An effective security Measurement system is very critical to assess the effectiveness of the implemented technical security controls and ensure safeguard against current and future attacks. The mandatory requirement in ISO/IEC 27001 standard clause 4.2.2 (d) says that "Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results". The development of technical security metrics should be more focused on the critical security controls that provide high impact to the organizations. Metrics should be SMART: Specific, Measurable, Attainable, and Relevant & Timely. There are internationally accepted Framework available for the metrics Development like common Assurance Maturity model (CAMM), IT infrastructure Library (ITIL), Control Objectives for information and related Technology (CobiT), ISO /IEC 27002/ISO 27002/ISO 27004 / NIST 800-55 Metrics can be composed of sub – metrics as well as group metrics could also be formed combining different metrics.

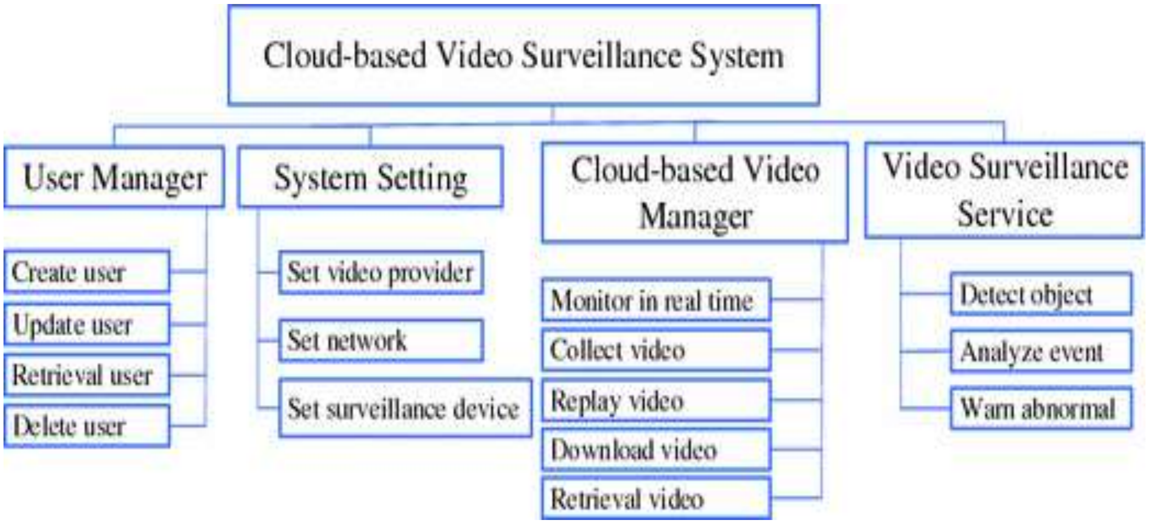
Step – 7 Establish Security & Metric benchmarks and targets: The next step of the security Framework is to establish security & Metrics benchmarks and targets, which are very important step of the framework, appropriate benchmarks would be set up for all the five maturity levels of security framework for each metric & Group Metric. Benchmarking will be done comparing the performance & practices of the organization against the peers within the industry. It will ensure that targets set are achievable as for ensuring improvements in the existing practices, which is critical for the success of the framework. The national and global metrics provided by various professional associations and published research are also very helpful. Apart from this the each Metric/sub Metric could be assigned a corresponding weight based on the common vulnerability scoring system (CVSS) Score. The CVSS based score is calculated using the information provided by the U.S National Vulnerability Database (NVD) Common Vulnerability Scoring system support v2 [20]. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

Step – 8 Security & Metric EVALUATION: The security and metric evolution is a very important step in security framework. It is a measurement for all the users, virtual machine and security services implemented. Automatic metric collection is the ideal situation, however wherever automatic metric collection is not possible, it will be done manually through system logs, questionnaires, interviews of the understanding, perceptions and implementation of Experts. Security metrics can be calculated in the form of a weighted sum. It will be calculated at Metric level & group metric level Mi = wm 1.1

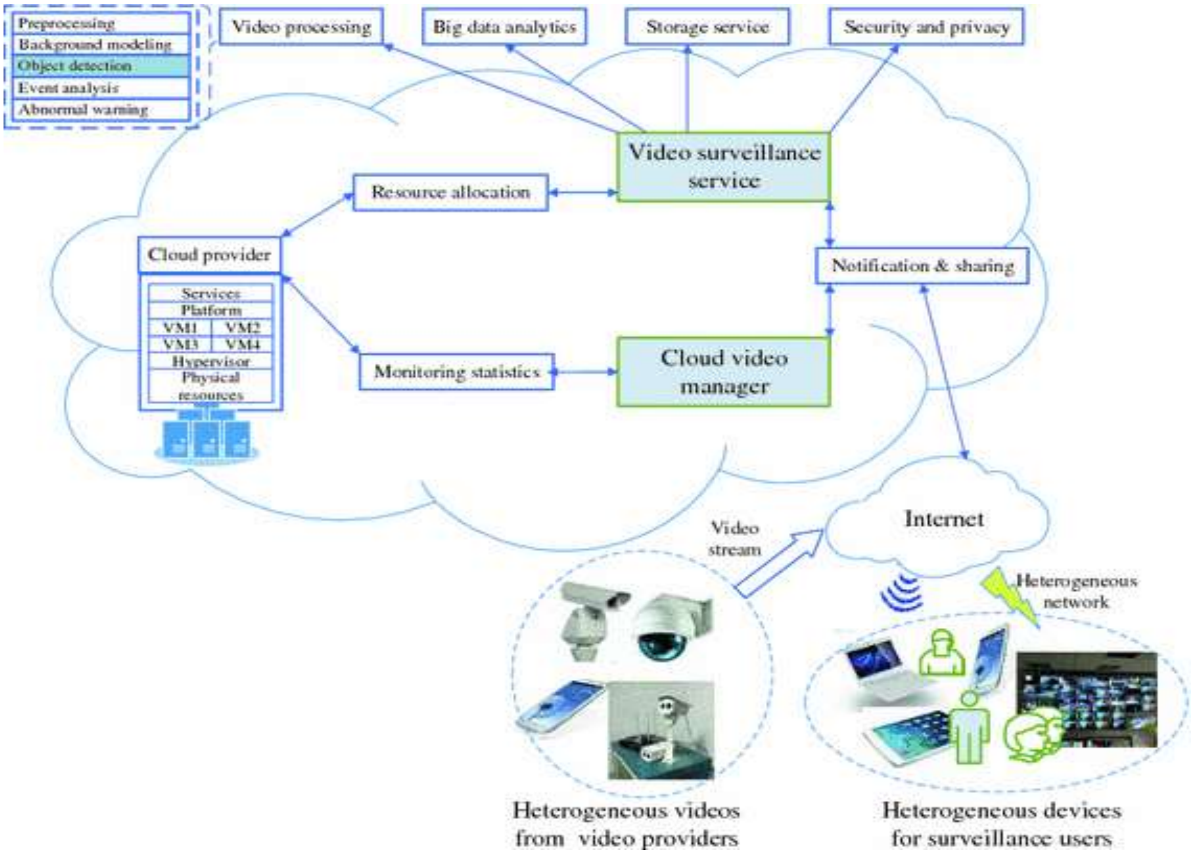
Denotes normalized and uniform scaling of the components metrics and group metric. These values will be analyzed and necessary steps will be taken to further improve the security of the system. Thus the most important feature of the proposed security framework is to devise a mechanism through which an organization can have a path of improvement along with understanding the current security maturity level & defining desired state in terms of security metric value/maturity level.

Conclusion & Future Work

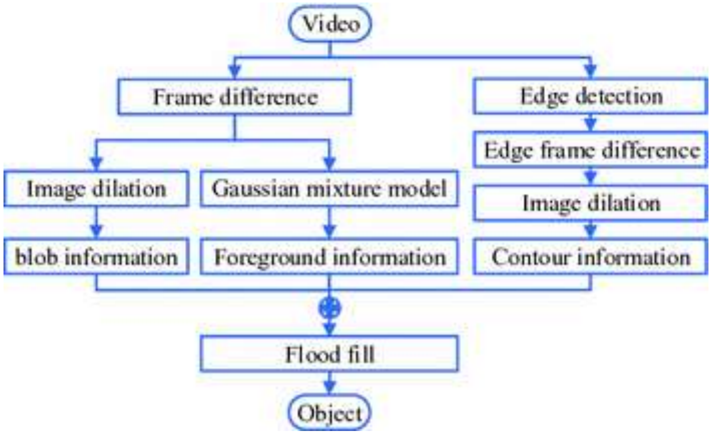
The rapid emergence of cloud computing is transforming the way organizations are functioning now a days. Although there are many advantages of cloud computing, issues related with security & privacy are some of the major challenges and obstacles, which need to be addressed for the successful deployment and operation of e-government. While reviewing industry security framework and guidelines, it was found out that there is no cloud security framework, best practices, and guidelines that meet the complete needs of an cloud based System. This paper first introduces a new set of security control principles called Security Matric (EGSM) especially for the cloud based security frame work. The validation of this proposed security control matrix by industry experts through questionnaires can be taken as a future work. The mapping of different security control principles described in this paper with other important industry standards like ISO 2002 /20017, Cloud security Alliance cloud controls Matrix (CCM) can also be taken as future work. The proposed security control matrix has defined the security control areas for cloud based system, identifying/defining some useful matrices can be taken as important future work.



The Chart of System requirements analysis, Muzaffar, et al (2015); Li, et al (2016),



The Designed architecture for a cloud-based video surveillance system, Muzaffar, et al (2015)



Flow chat of proposed method, Muzaffar, et all (2015)

References

Li, C, Su, J, Zhang, B (2016). Cloud-Based Vedio Surveillance System Using EFD-GMM for Object Detection.

Grossma, R. L (2009). The case of Cloud computing prog of IEEE, Education Activities Department, Piscataway, NJ, USA vol. 11, Issue 2.

Muzaffar, A, Naqvi, S. K (2015). A Security Framework for Cloud Based e-Governance System. International Journal of Science, Technology and Management. Vol. No 04, Issue No.02.

Raty, T.D (2010). Survey on contemporary remote surveillanace systems for public safety. IEEE Trans..Syst. Man Cybem. C Appl. Rev. 40.5.

Vic, W (2011). Securing the Cloud. Cloud Computer Security Techniques and Tactics.