Mobile Data Offloading – Challenges and Solution

Aradhana[1], Dr. Samarendra Mohan Ghosh[2], Sudha Tiwari[3], Smita Suresh Daniel [4]

[1]Research Scholar in Dr. C.V. Raman University Bilaspur,
[2]Professor in Dr. C.V. Raman University Bilaspur,
[3]Assistant Prof. in Rungta College of Engineering and Technology Bhilai,
[4] Assistant Professor in Sat. Thomas College Bhilai.

Abstract

Mobile cloud computing is emerging at the rapid rate with evolutions in IT industries but various challenges are also coming up during data and task migration from mobile devices to cloud. Major issue confronted by mobile cloud computing is security of data during offloading It requires awareness of growing security threats associated with data offloading and strategic planning to resolve the issue. In this paper, we bring out various security issues subjected to mobile data offloading and challenges during computational data offloading on clouds. By virtue of our study on mobile cloud computing and its related threats and the avenues to tackle these issues we developed an agent based framework for data offloading in a secure and energy efficient manner. Using this proposed framework we can enhance the level of security and use this as a tool to address many security issues arising during computational data offloading from mobile to cloud.

Keywords: Code Obfuscation, Encryption, Computation Offloading, IaaS, PaaS, SaaS.

1. Introduction

Mobile Cloud Computing is a phenomena of migrating the computational process to server that executes some events or application on behalf of the user mobile, but it may suffer many security challenges like authentication, code integrity, access control, availability, anti-tempering and trust management. So, to design and develop a security mechanism for mobile cloud computing, the data protection risk may vary according environment and platform. This risk is about **69%** for mobile devices, **45%** for cloud computing infrastructure and **33%** for mobile applications [1].

Although Mobile Cloud Computing is a new phenomenon but it can be set to revolutionize the world by its features. As a matter of fact we are already using cloud services via our mobile phones without even been knowing that we are doing it. As we have discussed in this work that there are many challenges and security threats while using mobile cloud computation that need to be resolved to gain trust and acceptability of the user. There are many solutions available to address these circumstances but none of them have proved to be fully efficient. Thus a method or prototype is required to be developed to meet all such needs. Various challenges related to the mobile cloud computing are also unfolding as we start using these services more and more

Data privacy, data ownership and location, data access and integrity are the main factor of concern on which cloud computing can be the target of various attacks. Moreover, various components of an application may communicate with cloud or with other web services so these communication channels can be the target of network attacks such as man in middle attack. When the attacker connects with the victims and takes controls over their communication system that may result in data breach, privacy loss, tempering on data etc.

Many researches and experts to collect the facts about mobile computation offloading and its security risks as addressed in Table 1.

Table 1: Various factors that affects the offloading

#	List of Factors
1	On demand of mobile user enlist the security and vulnerable risk requirements for mobile cloud computing technologies andservices?
2	How do mobile cloud computing technologies and services increase, decrease, or perhaps don't affect security and compliance risks?
3	What mobile cloud computing characteristics are generating themost positive and negative impacts on security and compliance risks?
4	What is the best way to detect and protect a mobile user's computational data against vulnerabilities and malicious attacks coming from Cloud? Do you have risk mitigation recommendations?
5	Can mobile cloud computing frameworks evaluate and mitigate security and compliance risks?
6	What applications and security solutions are appropriate to adopt and run on clouds?
7	How to share the workload managements of mobile client after offloading the computation on Cloud?
8	How do you save the energy consumption from client side to move toward the green computing technologies?

Following sub sections have given light on the challenges faced while using cloud computing and solutions available for addressing these challenges are discussed below.

1.1 Mobile Application's Challenges

Mobile end user demands accurate and express functionality, crisp responsiveness and rich user interface from their computational resources. The hardware and software configuration of mobile devices are also changing frequently so user may suffer from many computational related problems or they may require to upgrade or replace their phones in quick succession which is neither economical nor eco-friendly. By moving towards mobile cloud computing these issues can be resolved in much economical and ecology friendly manner. We extensively survey the literature of mobile application and find out major challenges that restrict the success and deployment of resource intensive mobile application. The different types of challenges faced by users in employing resource intensive mobile application are shown in Figure 1.

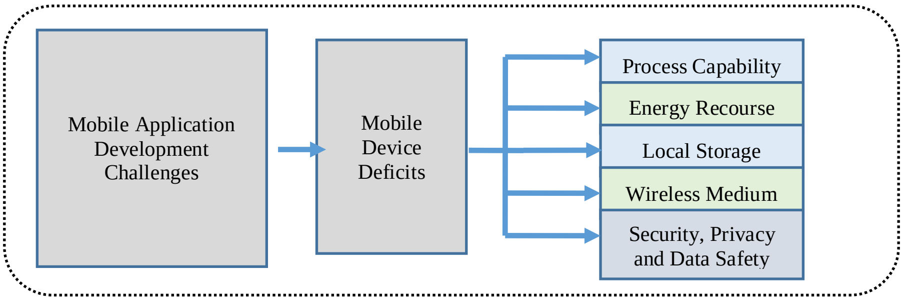


Figure 1: Mobile Application Development Challenges

The discussions of the various challenges of Mobile Application can be classified as follows:

- **Limited Processing Capability**: With new developments in smart phone and their functionality, user expects computing capability of a computer system from their mobile devices. This vision requires more processing power and huge amount of memory unit, which is still a field of debate and exploration. These expectations of user are still far beyond the processing capabilities of mobile phones.
- **Limited Power Source**: Energy is the only non-replenish able resource in mobile phones that requires external resource to renew it after certain time or usage. Recently, storage transactions and wireless communication are recognized as the most energy-hungry tasks in mobile phones. Smartphone manufacturers also aim to craft device with handiness, so bulk energy options cannot be deployed. Moreover, energy capacity growth is about 5% annually since energy cells are excessively dense sundry energy harvesting sought to replenish energy from renewable resources like human movement, solar energy, and wireless radiation, but these resources are mostly intermittent and not available on-demand. Considering all these points, restraint energy resources of mobiles phones remain a challenge to develop and deploy rich applications.
- **Limited Local Storage**: The mobile devices have limited storage facility which is already occupied by installed application, user’s personal data and files and some utility library files. While computer systems have large amount of storing capability which mobile devices lacks and also any extension into this has limited scope.
- **Wireless Medium**: Mobile devices use wireless communication for communicating with remote locations. These networks are unreliable as compare to wired networking and vulnerable to different types of attacks in terms of malwares and security breaches to the computation and data.
- **Security, Privacy, and Data Safety Risks**: The security risk of mobile data is major concern among users while using mobile applications. Some mobile application requires more safety and privacy on data e.g. mobile banking applications etc. This information stored in mobile application is generally subjected to security breaches due to physical damage, device failure or in case of robbery. Some features like GPS and accelerometer in mobile phones can potentially violate user security and privacy.

1.2 Mobile Cloud Running System Challenges

In an ideal mobile cloud application running system mobile devices are given the advantage to easily discover and compose cloud resources for its applications. As an outcome, development of mobile cloud computing can significantly curtail the mobile application development overhead and greatly improve the agility and durability of a mobile device by building a personalized mobile cloud computing environment that can be customized for every mobile user. Various challenges to mobile cloud running system are presented in Figure 2.

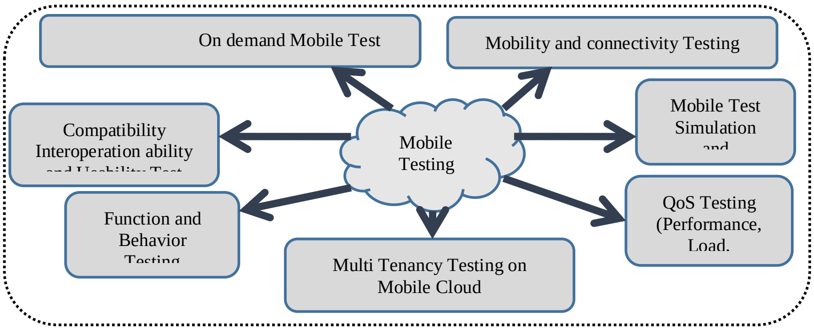

On demand Mobile Test
Mobility and connectivity Testing
Compatibility Interoperation ability and Usability Test
Mobile Testing
Mobile Test Simulation and
Function and Behavior Testing
QoS Testing (Performance, Load,
Multi Tenancy Testing on Mobile Cloud

Figure 2: Mobile Cloud Running System Challenges

1.3 Offloading Strategy Challenges

The computation power and device energy are limited due to the device dimension. The computation offloading is the most critical topic in mobile cloud computing because offloading may not only save mobile device energy but also improve the application performance. However, offloading is not the final solution. Offloading introduces cost on bandwidth and energy as well as security risk on the application availability as shown in Figure 3. We should consider the offloading strategies carefully to get the best benefit.

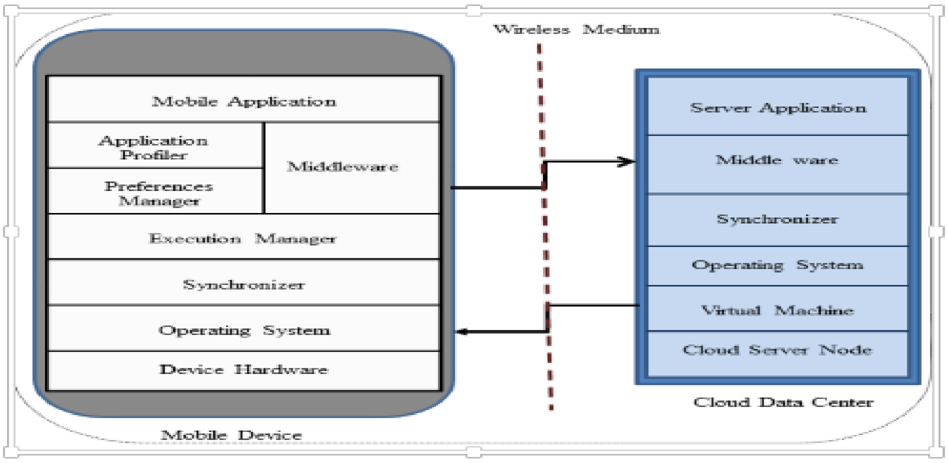


Figure 3. Offloading Strategy Challenges

1.4 Network Unavailability Challenges

Network condition has great impact during offloading. The network connection may be lost when mobile device moves into some area that is not covered by wireless network. When the connection to cloud is lost, the original execution routine is interrupted and the application has to wait until the connection resumes. The aim of mobile code offloading is to improve performance and reduce energy consumption rate. The expected benefit of mobile cloud collaboration may not be obtained due to interruption of execution plan. The collaboration may even lead to negative impact to execution time or energy consumption in such scenario.

1.5 Device Capability Challenges:

Mobile **data offloading during execution time** is the most challenging area for us because trust is a critical factor for the success of the growing MCC paradigm which could limit the use of cloud computing. It is because the data along with Application /code /component /complete VM are offloaded to the cloud location for execution. In case of security and privacy issue in software, computation and mobile application development models are also affected and exploited. The difficulty mainly lies in the following aspects:

- **Architectural Issues**: Architecture of MCC works on heterogeneous environment. It is critical towards unrestricted computing. It penetrates the security mechanism.
- **Low Bandwidth**: Lack of signals and low bandwidth are the main challenges in the way of adopting mobile cloud computing for users. Some alternate solutions like compression and optimization are required to be developed to overcome bandwidth limitations.
- **Limited Energy Life**: As the device in consideration may continuously move from one place to another even when in use so it is impossible to find an eternal power source which can keep the device working continuously for long hours. Mobile devices have to rely on their internal energy, which has a charge life of only a few hours. If computation is continuous or various applications are running simultaneously, energy drains rapidly.
- **Low Processing Power:** Smart phones are capable of running only small and a limited number of applications as they have ARM processors. Mobile devices like laptops have fast processor units like i3, i5, and i7 often they are not affordable due to their high cost and they are not frequently as handy devices. Processors of Mobile devices are not replaceable part, so if someone wants to upgrade every time with changing scenario, it may not be possible.
- **Heterogeneous Networks:** Mobile devices supports a variety of networks technology developed for them like CDMA, GSM, WI-FI and WiMAX and managing such heterogeneous network is somewhat a difficult task [7].
- **Interoperability between Platforms:** There are different operating system for different mobile devices e.g. phones based out of Android technology like HTC use Android Operating system, Symbian is used by Nokia, Apple Phones use IPhone, IOS hence developing a mobile application which may work in all systems is appealingly a tricky task.
- **Trust, Security and Privacy**: Trust is an essential factor during migration of task whether it is data or computation. Several security factors and threats may leak the privacy of MCC
- **Computational Offloading:** It is a complex process that can offload the computation during runtime. This will eliminate the expensive software and hardware requirements but computational offloading is vulnerable to risks [8].

2. Threats on Cloud

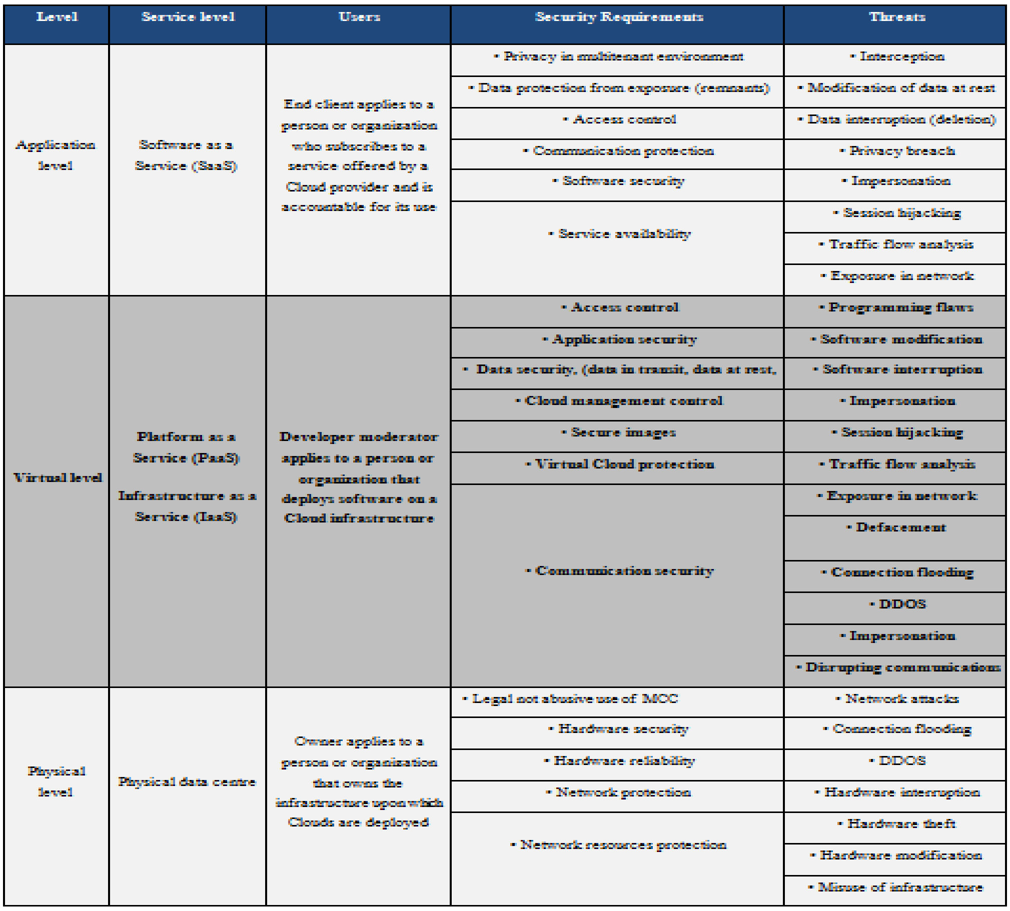
Security concern of cloud is fall on two broad categories first is security issue faced by cloud providers called cloud threads and second is their end users called as mobile threads. We have analysed that the responsibility is shared and implements the security on both ends. Threats can arise during offloading the computation (SaaS) services. Here we describe some security threats facing cloud users. Cloud Security Alliance (CSA) did survey on related issue and find the following threats [16]:

- Tracing and hacking our sensitive information by attackers.
- Data leakage in cloud environment.
- Lacking of skilled hands and experts.
- Data loss on cloud environment.
- Data Segregation from other recourses.
- Security culture among different providers.
- Evolving threats may target clouds.

- Hardware and software modification.
- Interruptions on software.
- Software theft.
- Misuse of infrastructure.
- Privacy Concerns.

We have listed the security requirements and threats to identify possible source and target of an attack that can affect the cloud and mobile computation as shown in Table 2.

Table 2: Security Requirements and Threats



Level	Service level	Users	Security Requirements	Threats
Application level	Software as a Service (SaaS)	End client applies to a person or organization who subscribes to a service offered by a Cloud provider and is accountable for its use	▪ Privacy in multitenant environment	▪ Interception
			▪ Data protection from exposure (remnants)	▪ Modification of data at rest
			▪ Access control	▪ Data interruption (deletion)
			▪ Communication protection	▪ Privacy breach
			▪ Software security	▪ Impersonation
			▪ Service availability	▪ Session hijacking
				▪ Traffic flow analysis
				▪ Exposure in network
Virtual level	**Platform as a Service (PaaS)** **Infrastructure as a Service (IaaS)**	**Developer moderator applies to a person or organization that deploys software on a Cloud infrastructure**	**▪ Access control**	**▪ Programming flaws**
			▪ Application security	**▪ Software modification**
			▪ Data security, (data in transit, data at rest,	**▪ Software interruption**
			▪ Cloud management control	**▪ Impersonation**
			▪ Secure images	**▪ Session hijacking**
			▪ Virtual Cloud protection	**▪ Traffic flow analysis**
			▪ Communication security	**▪ Exposure in network**
				▪ Defacement
				▪ Connection flooding
				▪ DDOS
				▪ Impersonation
				▪ Disrupting communications
Physical level	Physical data centre	Owner applies to a person or organization that owns the infrastructure upon which Clouds are deployed	▪ Legal not abusive use of MOC	▪ Network attacks
			▪ Hardware security	▪ Connection flooding
			▪ Hardware reliability	▪ DDOS
			▪ Network protection	▪ Hardware interruption
			▪ Network resources protection	▪ Hardware theft
				▪ Hardware modification
				▪ Misuse of infrastructure

A lot of work is already going on to address these threats. We also attempt to develop a prototype to resolves these threats but my research work is mainly focused on the area highlighted in the table which is security risk while using *cloud as a PaaS and IaaS.*

3. Solutions and Direction for Secure Mobile Data offloading

In this paper we have discussed various security issues and to create a better understanding about business and compliance risk associated with mobile data offloading. There are so many risks which have been identified during our study about computational data offloading. To protect mobile and cloud environments from security attacks, we prescribe three categories of security solutions i.e. solutions for data security, solutions for privacy and solution for platform authenticity. These solutions are presented in the following sub-sections. We also envisage a method to combine these solutions to augment their effectiveness and usability.

i) Data Security Solutions: Several solutions has been already proposed by many researches to ensure the data security in terms of confidentiality and integrity but we found that these solutions has some limitation e.g. to takes more time and consume more energy than normal execution time. Some algorithm like AES has required key to unsecure the data for execution and also identified that these solution are not fit to mobile data offloading during run time. This work proposed a solution and also seeks to be an energy efficient secure framework for mobile data offloading. The concepts designed by Incremental approach of obfuscation method for trust computing. The major components of this framework are: 1) Mobile phones, 2) AWS Cloud and 3) Agent. The mobile phones proves user interface environment, cloud provides execution environment of application and Agent provides a security combination by incremental hybrid approach of security algorithm using obfuscation and de-obfuscation method rather than encryption and decryption and Secure Hash Algorithm.

ii) Privacy Solutions: Every user is concerned about their personal data. To maintain data privacy it is necessary to build third party super vision mechanism on which the user can have better level of trust. For this we provide an intermediate node agent manager, it maintain the privacy using giving the permission to access only to authorised user.

iii) Platform Authenticity: To implement platform authentication we configure the framework with providing the dedicated lines between mobile phones and cloud .So no one can interact directly with this framework. The framework is available for authorized mobile phones they already register using same Wi-Fi addressing. After registration, mobile phones user can offload data either as a single user or a group simultaneously.

4. Proposed methods for Securing Mobile Data

In experimentation we have observed that the existing framework that offload the data with various security risk on different unsecured resources of clouds. We proposed a model that overcomes the limitations of existing frameworks and enhance the various security parameters, energy consumption rate and taken time to offload. We have implemented an incremental approach using Data Obfuscation and Dead Value Injection techniques to maintain confidentially to protect the mobile data from malwares and for integrity it combines the protected code with hybrid approach of cryptographic hash function (SHA- 256) to detect the tempering on data during offloading.

5. Contribution

The current mobile environments uses internet based application it comes with dangerous threats. To manage these issues we require an innovative solution. Inspired by the behaviour of human societies and federalism, this developed framework enhances the integrity and security of off-loadable mobile data and provides secure platform. This work is based on data integrity and confidentially which is developed for mobile cloud computational offloading with virtualization technique, malware detection and informal behavioural of monitoring.

6. Conclusion

In this paper we have discussed the scope of mobile data offloading approach, concerned security issues, the complexity of these challenges and there possible remedies so that the benefits of data offloading can be availed by any end user without any security concern regarding its data or device. We also proposed one approach that combines security solutions with time and energy efficient characteristics into one framework. First this framework enhances the security issue for mobile data. Second, it is reducing the amount of computation on the Mobile device within a secure channel of communication. Third, it reduces the energy consumption rate, increase reliability and enhance the security and performance of mobile device by utilizing the resources in the Cloud. The Survey of different mobile data offloading framework techniques exhibit that researched has not found any best technique that improves all the parameters .i.e. *execution time, energy consumption and security solutions with effective cost together*. Before offloading, various parameters such as cost such as network cost, time taken to offload and energy consumption are taken into account and if all these parameters results into lower consumption of power then offloading can be done so that it may result out beneficial.

7. References:

1. Kumar G, Jain E., Goel S,,Panchal V.K. (2014), "Mobile Cloud Computing Architecture, Application Model and Challenging Issues", IEEE Xplore, DOI**:** 10.1109/CICN.2014.137**,** INSPEC Accession Number: 15021280.
2. Agrawal S. and Choubey D. (2015), Enhanced Agent Based Scheduling and Monitoring System in Cloud Computing, International Journal of Computer Science And Technology, Vol. 6, Issue 1,188-196.
3. Akherfi K., Gerndt M. and Harroud H. (2018), Mobile Cloud Computing for Computation Offloading Issues and Challenges, Applied Computing and Informatics, dx.doi.org/10.1016/j.aci.2016.11.002 ,1–16.
4. Arjun G. (2015), Efficient Task Scheduling for Mobile Cloud Computing Environment to Increase the Performance of Mobile Devices", International Journal of Innovative Works in Engineering and Technology, Vol. 1, No. 2,61-71.
5. Bahar A., Habib A. and Islam A. (2012), Security Architecture for Mobile Cloud Computing, International Journal of Scientific Knowledge Computing and Information Technology, Vol. 3, No.3, 11-17.
6. Chen X., Chen S., Zeng X., Zheng X, Zhang Y. and Rong C. (2017), Framework for context-aware computation offloading in mobile cloud computing, Journal of Cloud Computing Advances, Systems and Applications, DOI 10.1186/s13677-016-0071-y.
7. Dudeja M. and Soni k.(2014) International Journal of Computer Applications (0975 – 8887) Volume 96– No.8,
8. Date A. and Datar D. (2014), A Multi-Level Security Framework for Cloud Computing, International Journal of Computer Science and Mobile Computing, Vol. 3 Issue.4, 528-534.
9. POPA D. (2013), Security of Mobile Cloud Applications, Ph.D Thesis, Technical University of Cluj-Napoca
10. Patel C., Chauhan S. and Patel B. (2015), A Data Security Framework for Mobile Cloud Computing, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 2, 254-257.
11. Ramya V. and Kumar A. (2018), Secured Framework for Data Outsourcing using ABE in Cloud Computing, International Journal of Science Engineering and Advance Technology, Vol. 6, Issue 5, 269-275.
12. Saouli H.1, Kazar O. and Benharkat A. (2012), A Cloud Computing Framework Based Mobile Agents for Web Services Discovery and Selection, International Journal of Emerging Trends and Technology in Computer Science, Vol. 1, and Issue 2,171-189.
13. Venkateshwaran K, Malviya A., Dikshit U. and Venkatesan S. (2018), Security Framework for Agent-Based Cloud Computing, International Journal of Artificial Intelligence and Interactive Multimedia, Vol. 3, No. 3, 35-42.
14. Vijay P. and Verma V. (2013), Opportunistic Job Sharing for Mobile Cloud Computing , International journal of application or innovation and engineering and management, Vol. 2, Issue 4, 426-430.
15. Secure Hash Algorithms, https://en.wikipedia.org/wiki/SHA-2.
16. SecurityPrinciple,https://dwheeler.com/secure-programs/Secure-Programshowto/security-principles.html.
17. Cloud Security Alliance The Treacherous 12 **-** Top Threats to Cloud Computing + Industry Insights.